Cisco Intrusion Policy Report

IPS Policy

**Table of Contents**

[**Policy Information**](#bookmark0) **1**

[**Firepower Recommendations**](#bookmark1) **1**

[Firepower changed 18183 rule states for 38 hosts](#bookmark2) 1

[**Advanced Settings**](#bookmark3) **1**

[Global Rule Thresholding](#bookmark4) 1

[Sensitive Data Detection](#bookmark5) 1

[**Rules**](#bookmark6) **2**

# i

**Policy Information**

Name GhnEdge\_IPS\_Policy

Drop when Inline Enabled

Current Rule Update Version 2018-11-21-001-vrt

Base Policy Balanced Security and Connectivity

Lock Base Policy to current Rule Update Version Disabled

Modified By admin

Last Modified 2018-11-24 05:02:28 (UTC)

**Firepower Recommendations**

Rule State Policy is using the recommendations

Networks

Recommendation Threshold Medium

Accept Recommendations to Disable Rules Enabled

**Firepower changed 18183 rule states for 38 hosts**

|  |  |
| --- | --- |
| Drop and generate events | 5978 |
| Generate events | 155 |
| Disable | 12050 |

**Advanced Settings**

**Global Rule Thresholding**

Type Limit

Track By Destination

Count 1

Seconds 60

**Sensitive Data Detection**

Global Settings

Mask 1

Networks

Global Threshold 25

Data Types

Credit Card Numbers

Data Type Credit Card Numbers

Pattern credit\_card

Threshold 20

Destination Ports 21,25,80,110,143

Application Protocols SMTP, IMAP, HTTP, POP3, FTP Data Email Addresses

Data Type Email Addresses

Pattern email

Threshold 20

Destination Ports 21,25,80,110,143

Application Protocols SMTP, IMAP, HTTP, POP3, FTP Data Social Security Numbers

Data Type Social Security Numbers

Pattern us\_social

Threshold 2

Destination Ports 21,25,80,110,143

Application Protocols SMTP, IMAP, HTTP, POP3, FTP Data Social Security Numbers (no dashes)

Data Type Social Security Numbers (no dashes)

Pattern us\_social\_nodashes

Threshold 20

Destination Ports 21,25,80,110,143

Application Protocols SMTP, IMAP, HTTP, POP3, FTP Data

U.S. Phone Numbers

Data Type U.S. Phone Numbers

Pattern (\d{3})\d{3}-\d{4}

Threshold 20

Destination Ports 21,25,80,110,143

Application Protocols SMTP, IMAP, HTTP, POP3, FTP Data

**Rules**

BROWSER-FIREFOX Mozilla Firefox 17 onreadystatechange memory corruption attempt 1:33088 Drop and generate

BROWSER-FIREFOX Mozilla Firefox 17 onreadystatechange memory corruption attempt 1:27568 Drop and generate

events

events

BROWSER-FIREFOX Mozilla Firefox DOMSVGLength initialize use after free attempt 1:35072 Drop and generate BROWSER-FIREFOX Mozilla Firefox DOMSVGLength insertItemBefore use after free attempt 1:35070 Drop and generate BROWSER-FIREFOX Mozilla Firefox DOMSVGLength replaceItem use afte r free attempt 1:35071 Drop and generate

events

events

events

BROWSER-FIREFOX Mozilla Firefox ESR NotifyTimeChange use after free attempt 1:40896 Drop and generate

events

BROWSER-FIREFOX Mozilla Firefox ESR NotifyTimeChange use after free attempt 1:40888 Drop and generate

events

BROWSER-FIREFOX Mozilla Firefox IDL fragment privilege escalation attempt 1:35051 Drop and generate

events

BROWSER-FIREFOX Mozilla Firefox IDL fragment privilege escalation attempt 1:35052 Drop and generate

events

BROWSER-FIREFOX Mozilla Firefox IDL fragment privilege escalation attempt 1:37626 Drop and generate

events

BROWSER-IE Microsoft Edge HTML normalize caption memory corruption attempt 1:40134 Drop and generate

events

BROWSER-IE Microsoft Edge HTML normalize caption memory corruption attempt 1:40135 Drop and generate

events

BROWSER-IE Microsoft Edge HTML normalize caption memory corruption attempt 1:40136 Drop and generate

events

BROWSER-IE Microsoft Edge HTML normalize caption memory corruption attempt 1:40137 Drop and generate

events

BROWSER-IE Internet Explorer DataSource recordset remote code execution attempt 1:35865

BROWSER-IE Internet Explorer URL file remote code execution attempt detected 1:46384 Drop and generate

events

BROWSER-IE Internet Explorer URL file remote code execution attempt detected 1:46385 Drop and generate

events

BROWSER-IE Internet Explorer WeakMap Freeze memory corruption att empt 1:44342 Drop and generate

events

BROWSER-IE Microsoft Edge anonymous function type confusion attempt 1:45387 Drop and generate

events

BROWSER-IE Microsoft Edge App-v vbs command attempt 1:48053 Drop and generate

events

BROWSER-IE Microsoft Edge App-v vbs command attempt 1:48054 Drop and generate

events

BROWSER-IE Microsoft Edge Array out of bounds memory corruption attempt 1:41557 Drop and generate

events

BROWSER-IE Microsoft Edge Array out of bounds memory corruption attempt 1:41558 Drop and generate

events

BROWSER-IE Microsoft Edge array type confusion attempt 1:45169 Drop and generate

events

BROWSER-IE Microsoft Edge array use after free attempt 1:44819 Drop and generate

events

BROWSER-IE Microsoft Edge Array.concat type confusion attempt 1:4 0661 Drop and generate

events

BROWSER-IE Microsoft Edge array.join information disclosure attempt 1:40383 Drop and generate

events

BROWSER-IE Microsoft Edge Array.prototype.fill out of bounds writ e attempt 1:38805 Drop and generate

events

BROWSER-IE Microsoft Edge ArrayBuffer.transfer information disclosure attempt 1:39506 Drop and generate

events

BROWSER-IE Microsoft Edge browser memory corruption attempt 1:471 17 Drop and generate

events

BROWSER-IE Microsoft Edge browser memory corruption attempt 1:471 18 Drop and generate

events

BROWSER-IE Microsoft Edge browser redirection vulnerability attempt 1:47474 Drop and generate

events

BROWSER-IE Microsoft Edge browser redirection vulnerability attempt 1:47475 Drop and generate BROWSER-IE Microsoft Edge CAsyncTpWorker Windows.Data.Pdf.dll object use after free attempt 1:38073 Drop and generate BROWSER-IE Microsoft Edge CAsyncTpWorker Windows.Data.Pdf.dll object use after free attempt 1:38074 Drop and generate BROWSER-IE Microsoft Edge CAsyncTpWorker Windows.Data.Pdf.dll object use after free attempt 1:38075 Drop and generate BROWSER-IE Microsoft Edge CAsyncTpWorker Windows.Data.Pdf.dll object use after free attempt 1:38076 Drop and generate BROWSER-IE Microsoft Edge CAttrArray out of bounds read attempt 1 :36984 Drop and generate

events

events

events

events

events

events

BROWSER-IE Microsoft Edge Chakra Closure use after free attempt 1 :44813 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra Core type confusion attempt 1:42 753 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra Core type confusion attempt 1:45 889 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra Core type confusion attempt 1:45 890 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra engine use after free exploit at tempt 1:47735 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra Engine use-after-free attempt 1: 42812 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra floating point type confusion at tempt 1:47638 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra floating point type confusion at tempt 1:47635 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra floating point type confusion at tempt 1:47636 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra floating point type confusion at tempt 1:47637 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra JIT memory corruption attempt 1: 42775 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra RegExp engine memory corruption attempt 1:45140 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra use after free attempt 1:46176 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra use after free attempt 1:46177 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra use after free attempt 1:46194 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra use after free attempt 1:46195 Drop and generate

events

BROWSER-IE Microsoft Edge Chakra.dll Array.splice heap overflow attempt 1:40659 Drop and generate

events

BROWSER-IE Microsoft Edge chakra.dll invalid pointer access attempt 1:39486 Drop and generate

events

BROWSER-IE Microsoft Edge class object confusion attempt 1:39199 Drop and generate BROWSER-IE Microsoft Edge clientInformation.geolocation.getCurren tPosition use-after-free attempt 1:39530 Drop and generate BROWSER-IE Microsoft Edge ClipPath out of bounds write attempt 1: 46927 Drop and generate

events

events

events

BROWSER-IE Microsoft Edge ClipPath out of bounds write attempt 1: 46928 Drop and generate

events

BROWSER-IE Microsoft Edge Content Security Policy bypass attempt 1:39233 Drop and generate

events

BROWSER-IE Microsoft Edge CSS animation style information disclos ure attempt 1:41573 Drop and generate

events

BROWSER-IE Microsoft Edge CSS writing mode type confusion attempt 1:42779 Drop and generate

events

BROWSER-IE Microsoft Edge cssText use after free attempt 1:43165 Drop and generate

events

BROWSER-IE Microsoft Edge CStr object use after free attempt 1:35 955 Drop and generate

events

BROWSER-IE Microsoft Edge CStr object use after free attempt 1:35 956 Drop and generate

events

BROWSER-IE Microsoft Edge CStyleSheet keyframes out of bounds rea d attempt 1:38483 Drop and generate

events

BROWSER-IE Microsoft Edge CTextBlock out of bounds read attempt 1 :37575 Drop and generate

BROWSER-IE Microsoft Edge denial of service attempt 1:44338 Drop and generate

events

BROWSER-IE Microsoft Edge DOMNode manipulation use after free att empt 1:35959 Drop and generate BROWSER-IE Microsoft Edge edgehtml negative length out of bound m emory copy attempt 1:39493 Drop and generate BROWSER-IE Microsoft Edge edgehtml.dll invalid history state use after free attempt 1:39822 Drop and generate BROWSER-IE Microsoft Edge edgehtml.dll normalize missing div chil d use after free attempt 1:40123 Drop and generate BROWSER-IE Microsoft Edge edgehtml.dll uninitialized pointer vuln erability attempt 1:39219 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Edge edgehtml.dll uninitialized pointer vuln erability attempt 1:39220 Drop and generate

events

BROWSER-IE Microsoft Edge edgehtml.dll uninitialized pointer vuln erability attempt 1:47057 Drop and generate

events

BROWSER-IE Microsoft Edge edgehtml.dll uninitialized pointer vuln erability attempt 1:47058 Drop and generate

events

BROWSER-IE Microsoft Edge EntrySimpleSlotGetter use after free at tempt 1:41942 Drop and generate

events

BROWSER-IE Microsoft Edge event handling use-after-free attempt 1 :47107 Drop and generate

events

BROWSER-IE Microsoft Edge event handling use-after-free attempt 1 :47108 Drop and generate

events

BROWSER-IE Microsoft Edge Form buffer overflow attempt 1:47111 Drop and generate

events

BROWSER-IE Microsoft Edge Form buffer overflow attempt 1:47112 Drop and generate

events

BROWSER-IE Microsoft Edge format rendering type confusion attempt 1:42183 Drop and generate

events

BROWSER-IE Microsoft Edge getOwnPropertyDescriptor memory corrupt ion attempt 1:44532 Drop and generate

events

BROWSER-IE Microsoft Edge graphics subcomponent use after free at tempt 1:38797 Drop and generate

events

BROWSER-IE Microsoft Edge graphics subcomponent use after free at tempt 1:38798 Drop and generate BROWSER-IE Microsoft Edge HandleColumnBreakOnColumnSpanningElemen t type confusion attempt 1:41763 Drop and generate BROWSER-IE Microsoft Edge HandleColumnBreakOnColumnSpanningElemen t type confusion attempt 1:41625 Drop and generate BROWSER-IE Microsoft Edge heap overflow attempt 1:44845 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Edge heap overflow attempt 1:47113 Drop and generate

events

BROWSER-IE Microsoft Edge heap overflow attempt 1:47114 Drop and generate

events

BROWSER-IE Microsoft Edge history.state use after free attempt 1: 35705 Drop and generate

events

BROWSER-IE Microsoft Edge iframe climbing cross site scripting at tempt 1:36932 Drop and generate

events

BROWSER-IE Microsoft Edge iframe cross-site scripting attempt 1:3 8473 Drop and generate

BROWSER-IE Microsoft Edge information disclosure attempt 1:48388 Drop and generate

events

BROWSER-IE Microsoft Edge Intl.js memory corruption attempt 1:471 02 Drop and generate

events

BROWSER-IE Microsoft Edge Intl.js memory corruption attempt 1:471 03 Drop and generate

events

BROWSER-IE Microsoft Edge JavaScript string object type confusion attempt 1:42152 Drop and generate

events

BROWSER-IE Microsoft Edge JIT floating point value type confusion attempt 1:48360 Drop and generate

events

BROWSER-IE Microsoft Edge JIT floating point value type confusion attempt 1:48361 Drop and generate

events

BROWSER-IE Microsoft Edge JsSetCurrentContext out of bounds read attempt 1:45150 Drop and generate

events

BROWSER-IE Microsoft Edge local file read information leak attemp t 1:41952 Drop and generate BROWSER-IE Microsoft Edge malformed PDF JPEG2000 object out of bo unds memory access attempt 1:39238 Drop and generate BROWSER-IE Microsoft Edge malformed UTF-8 decode arbitrary read attempt 1:41958 Drop and generate

events

events

events

BROWSER-IE Microsoft Edge memory corruption attempt 1:45162 Drop and generate

events

BROWSER-IE Microsoft Edge memory corruption attempt 1:45167 Drop and generate

events

BROWSER-IE Microsoft Edge memory corruption attempt 1:47109 Drop and generate

events

BROWSER-IE Microsoft Edge memory corruption attempt 1:47110 Drop and generate

events

BROWSER-IE Microsoft Edge memory corruption exploitation attempt 1:44831 Drop and generate

events

BROWSER-IE Microsoft Edge object mutation memory corruption attempt 1:41839 Drop and generate

events

BROWSER-IE Microsoft Edge object property type confusion attempt 1:43163 Drop and generate

events

BROWSER-IE Microsoft Edge out of bounds write attempt 1:47486 Drop and generate

events

BROWSER-IE Microsoft Edge out of bounds write attempt 1:47487 Drop and generate

events

BROWSER-IE Microsoft Edge out of bounds write attempt 1:46218 Drop and generate

events

BROWSER-IE Microsoft Edge out of bounds write attempt 1:46219 Drop and generate

events

BROWSER-IE Microsoft Edge out of bounds write attempt 1:45374 Drop and generate

events

BROWSER-IE Microsoft Edge out-of-bounds memory access attempt 1:4 6606 Drop and generate

events

BROWSER-IE Microsoft Edge out-of-bounds memory access attempt 1:4 6607 Drop and generate

events

BROWSER-IE Microsoft Edge parseFloat type confusion attempt 1:470 98 Drop and generate

events

BROWSER-IE Microsoft Edge parseFloat type confusion attempt 1:470 99 Drop and generate

BROWSER-IE Microsoft Edge postMessage use after free attempt 1:44 809 Drop and generate

events

BROWSER-IE Microsoft Edge proxy object type confusion attempt 1:4 0098 Drop and generate

events

BROWSER-IE Microsoft Edge remove range out of bounds read attempt 1:38479 Drop and generate

events

BROWSER-IE Microsoft Edge reverse helper heap buffer overflow att empt 1:41938 Drop and generate

events

BROWSER-IE Microsoft Edge Scripting Engine array memory corruptio n attempt 1:45516 Drop and generate

events

BROWSER-IE Microsoft Edge Scripting Engine array memory corruptio n attempt 1:45517 Drop and generate

events

BROWSER-IE Microsoft Edge Scripting Engine array memory corruptio n attempt 1:45508 Drop and generate

events

BROWSER-IE Microsoft Edge Scripting Engine array memory corruptio n attempt 1:45509 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine ArrayBuffer memory cor ruption attempt 1:45445 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine integer overflow attempt 1:45383 Drop and generate

events

BROWSER-IE Microsoft Edge Scripting Engine memory corruption atte mpt 1:45626 Drop and generate

events

BROWSER-IE Microsoft Edge Scripting Engine memory corruption atte mpt 1:45627 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:45659 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:45660 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:47121 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:47122 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:43465 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:45628 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:45629 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:46212 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:46213 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine memory corruption atte mpt 1:44827 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine postMessage use after free attempt 1:42749 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine security bypass css at tempt 1:42777 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine security bypass css at tempt 1:41944 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine type confusion attempt 1:45391 Drop and generate

BROWSER-IE Microsoft Edge scripting engine type confusion attempt 1:47141 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine type confusion attempt 1:47142 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine type confusion attempt 1:44811 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine use after free attempt 1:46544 Drop and generate

events

BROWSER-IE Microsoft Edge scripting engine use after free attempt 1:46545 Drop and generate

events

BROWSER-IE Microsoft Edge setSelectionRange memory corruption att empt 1:44340 Drop and generate

events

BROWSER-IE Microsoft Edge SIMD memory corruption attempt 1:40949 Drop and generate

events

BROWSER-IE Microsoft Edge spread operator memory corruption attempt 1:40971 Drop and generate

events

BROWSER-IE Microsoft Edge spread operator memory corruption attempt 1:40973 Drop and generate

events

BROWSER-IE Microsoft Edge spread operator memory corruption attempt 1:40370 Drop and generate

events

BROWSER-IE Microsoft Edge stack variable memory access attempt 1: 40683 Drop and generate

events

BROWSER-IE Microsoft Edge SysFreeString double free attempt 1:375 81 Drop and generate

events

BROWSER-IE Microsoft Edge textContent use after free attempt 1:43 169 Drop and generate

events

BROWSER-IE Microsoft Edge TextDataSlice type confusion attempt 1: 38485 Drop and generate

events

BROWSER-IE Microsoft Edge transform type confusion attempt 1:4748 8 Drop and generate

events

BROWSER-IE Microsoft Edge transform type confusion attempt 1:4748 9 Drop and generate

events

BROWSER-IE Microsoft Edge TryArraySplice memory corruption attemp t 1:47100 Drop and generate

events

BROWSER-IE Microsoft Edge TryArraySplice memory corruption attemp t 1:47101 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion attempt 1:45142 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion attempt 1:45378 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion code execution attempt 1 :47742 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion code execution attempt 1 :47743 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion memory corruption attemp t 1:46929 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion memory corruption attemp t 1:46930 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion memory corruption attemp t 1:47736 Drop and generate

events

BROWSER-IE Microsoft Edge type confusion memory corruption attemp t 1:47737 Drop and generate

BROWSER-IE Microsoft Edge TypedArray setter arbitrary write attempt 1:41936 Drop and generate

events

BROWSER-IE Microsoft Edge uninitialized memory attempt 1:43469 Drop and generate

events

BROWSER-IE Microsoft Edge uninitialized memory use attempt 1:4587 5 Drop and generate

events

BROWSER-IE Microsoft Edge uninitialized memory use attempt 1:4587 6 Drop and generate

events

BROWSER-IE Microsoft Edge url forgery attempt 1:41553 Drop and generate

events

BROWSER-IE Microsoft Edge VBScript VarType out of bounds read att empt 1:43471 Drop and generate

events

BROWSER-IE Microsoft Edge video html tag buffer overflow attempt 1:40675 Drop and generate

events

BROWSER-IE Microsoft Edge video html tag buffer overflow attempt 1:40676 Drop and generate

events

BROWSER-IE Microsoft Edge WebAssembly memory corruption attempt 1 :41950 Drop and generate

events

BROWSER-IE Microsoft Edge xlink type confusion memory corruption attempt 1:42210 Drop and generate

events

BROWSER-IE Microsoft IE array type confusion attempt 1:45389 Drop and generate BROWSER-IE Microsoft Internet Explorer 10 CTableSection remote co de execution attempt 1:32714 Drop and generate BROWSER-IE Microsoft Internet Explorer 10 CTreePos use after free attempt 1:27135 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer 10 CTreePos use-after-free attempt 1:27127 Drop and generate BROWSER-IE Microsoft Internet Explorer 10 insertImage with design Mode on deleted object access attempt 1:26845 Drop and generate BROWSER-IE Microsoft Internet Explorer 10 use after free attempt 1:30106 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer 10 use after free attempt 1:29819 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 10 use after free attempt 1:33085 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 10 use after free attempt 1:26847 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 10 VBScript array element use after free attempt 1:35213 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 11 CStyleSheet object use after free attempt 1:32495 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 CTreePos child element use-after-free attempt 1:31206 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 InsertInputSubmit use a fter free attempt 1:31801 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 onpropertychange remote code execution attempt 1:31380 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 type confusion vulnerab ility attempt 1:43521 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:32629 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:32471 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:32472 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:32473 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:32564 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:32565 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:33115 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:33116 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:33979 Drop and generate BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt 1:33980 Drop and generate BROWSER-IE Microsoft Internet Explorer 6 usp10.dll Bengali font s tack overrun attempt 1:27618 Drop and generate BROWSER-IE Microsoft Internet Explorer 7 CTreeNode object remote code execution attempt 1:41474 Drop and generate BROWSER-IE Microsoft Internet Explorer 7 CTreeNode object remote code execution attempt 1:32716 Drop and generate BROWSER-IE Microsoft Internet Explorer 8 CElement Use After Free exploit attempt 1:28880 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer 8 CElement Use After Free exploit attempt 1:29036 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 8 CTreePos use after free attempt 1:27131 Drop and generate BROWSER-IE Microsoft Internet Explorer 8 deleted object access me mory corruption attempt 1:26134 Drop and generate BROWSER-IE Microsoft Internet Explorer 8 deleted object access vi a timer memory corruption attempt 1:27061 Drop and generate BROWSER-IE Microsoft Internet Explorer 8 deleted object access vi a timer memory corruption attempt 1:26634 Drop and generate BROWSER-IE Microsoft Internet Explorer 8 mode menu tag out-of-bou nds access attempt 1:34763 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer 8 select element deleted o bject access attempt 1:26867 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 8 tree element use after f ree attempt 1:26878 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 8 use after free attempt 1 :29655 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 array element property u se after free attempt 1:26843 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 cached display node use- after-free attempt 1:26876 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 CHTMLEditorProxy use aft er free attempt 1:32438 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 CSS rules cache use-afte r-free attempt 1:26873 Drop and generate

BROWSER-IE Microsoft Internet Explorer 9 CTreeNodeobject use-afte r-free attempt 1:26875 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 deleted object access me mory corruption attempt 1:25786 Drop and generate BROWSER-IE Microsoft Internet Explorer 9 deleted object access me mory corruption attempt 1:27716 Drop and generate BROWSER-IE Microsoft Internet Explorer 9 frameset use after free attempt 1:38467 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer 9 IE5 compatibility mode u se after free attempt 1:27147 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 layout engine memory cor ruption attempt 1:26844 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 MutationEvent use after free attempt 1:27841 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 onBeforeCopy use after f ree attempt 1:26137 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 onbeforeprint use after free attempt 1:26157 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 onbeforeprint use after free attempt 1:26158 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 onbeforeprint use after free attempt 1:26159 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 onbeforeprint use after free attempt 1:26419 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer 9 use after free attempt 1 :27129 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer access violation attempt 1 :36681 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer access violation attempt 1 :31794 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer ActiveX type confusion att empt 1:33335 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer AddOption use after free attempt 1:27835 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer addRow out-of-bounds read attempt 1:38112 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer ANIMATECOLOR SMIL access attempt 1:26666 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer append and swap use after free attempt 1:34076 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer arguments type confusion attempt 1:41956 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer array memory corruption at tempt 1:44829 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Array out of bounds memory corruption 1:41587 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Array out of bounds write attempt 1:45148 Drop and generate BROWSER-IE Microsoft Internet Explorer array proto chain manipula tion memory corruption attempt 1:41561 Drop and generate BROWSER-IE Microsoft Internet Explorer array use after free attempt 1:46204 Drop and generate

events

events

BROWSER-IE Microsoft Internet Explorer beforeeditfocus use after free exploit attempt 1:27148 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer BooleanProtoObj objects JS ONStringifyArray use-after-free attempt 1:38828 Drop and generate BROWSER-IE Microsoft Internet Explorer button element onreadystat echange use after free attempt 1:30116 Drop and generate BROWSER-IE Microsoft Internet Explorer cache management code over flow attempt 1:36679 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer CACPWrap object use-after- free attempt 1:37612 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer callback function use-afte r-free attempt 1:34721 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CallInvoke type confusion attempt 1:37608 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CallInvoke type confusion attempt 1:37610 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CAnchorElement use after f ree attempt 1:33605 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CAnchorElement use after f ree attempt 1:30102 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CAnchorElement use after f ree attempt 1:30103 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CAnchorElement use after f ree attempt 1:28489 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CAttrArray object used aft er free attempt 1:33353 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CAttrArray use after free attempt 1:36986 Drop and generate BROWSER-IE Microsoft Internet Explorer CAttribute to CStyleAttrAr ray type confusion attempt 1:36962 Drop and generate BROWSER-IE Microsoft Internet Explorer CBatchParentUndoUnit objec t use after free attempt 1:33345 Drop and generate BROWSER-IE Microsoft Internet Explorer CBodyElement use after fre e attempt 1:34059 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CButton object use after f ree attempt 1:32722 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CCharFormat use-after-free attempt 1:33361 Drop and generate BROWSER-IE Microsoft Internet Explorer CChildIterator media objec t use-after-free attempt 1:38503 Drop and generate BROWSER-IE Microsoft Internet Explorer CChildIterator media objec t use-after-free attempt 1:38505 Drop and generate BROWSER-IE Microsoft Internet Explorer CDATA use-after-free attempt 1:37553 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CDeskBand use-after-free attempt 1:40731 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CDeskBand use-after-free attempt 1:40732 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CDeskBand use-after-free attempt 1:36423 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CDeskBand use-after-free attempt 1:36424 Drop and generate

BROWSER-IE Microsoft Internet Explorer CDisplayPointer use after free attempt 1:27837 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CDisplayPointer use after free attempt 1:29034 Drop and generate BROWSER-IE Microsoft Internet Explorer CDispNode float css elemen t use after free attempt 1:26753 Drop and generate BROWSER-IE Microsoft Internet Explorer CDispNode float css elemen t use after free attempt 1:26630 Drop and generate BROWSER-IE Microsoft Internet Explorer CDispScroller object use-a fter-free attempt 1:34420 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CDocument use after free attempt 1:34084 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CDomPrototype type confusi on attempt 1:37571 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CDomPrototype type confusi on attempt 1:37572 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer cdomuievent use after free attempt 1:31627 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CEditAdorner use after fre e attempt 1:28491 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CEditEventSink navigate us e after free attempt 1:38102 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CEditEventSink navigate us e after free attempt 1:36701 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement event handler use after free attempt 1:30847 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement event handler use after free attempt 1:29727 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement event handler use after free attempt 1:29728 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement input type memory corruption attempt 1:35965 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement object use after free attempt 1:36918 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement object use-after- free attempt 1:35975 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use after free at tempt 1:30961 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use after free at tempt 1:30962 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use after free at tempt 1:36742 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use after free at tempt 1:33315 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use after free at tempt 1:28160 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use after free at tempt 1:36687 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer celement use after free 1: 31403 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CElement use-after-free at tempt 1:27613 Drop and generate

BROWSER-IE Microsoft Internet Explorer CFGBitmap heap code execut ion attempt 1:37614 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CFieldSetElement object us e after free attempt 1:35196 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CFormElement use after fre e attempt 1:33324 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CFunctionPointer use after free exploit attempt 1:32184 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGeneratedSvgTreeNode use- after-free attempt 1:33314 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGeneratedTreeNode use aft er free attempt 1:33736 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGeneratedTreeNode use aft er free attempt 1:35154 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGeneratedTreeNode use-aft er-free attempt 1:31792 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGeneratedTreeNode use-aft er-free 1:38108 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGenericElement use after free attempt 1:33417 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGenericElement use after free attempt 1:36235 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CGenericElement use after free attempt 1:36237 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Chakra.dll Array.filter ty pe confusion attempt 1:40655 Drop and generate BROWSER-IE Microsoft Internet Explorer Chakra.dll proxy object pr ototype return type confusion attempt 1:41911 Drop and generate BROWSER-IE Microsoft Internet Explorer CHeaderElement object use- after-free remote code execution attempt 1:32430 Drop and generate BROWSER-IE Microsoft Internet Explorer CHTMLEditor instance use a fter free attempt 1:31782 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:25769 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26216 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26217 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26218 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26219 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26220 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26221 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26222 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26223 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CHTMLEditor object use aft er free attempt 1:26224 Drop and generate

BROWSER-IE Microsoft Internet Explorer CHtmlTab use after free at tempt 1:41589 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CImgElement object double free attempt 1:36004 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CImgElement object use aft er free attempt 1:35203 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CImgElement object use aft er free attempt 1:35205 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CImgTaskSvgDoc object doub le free attempt 1:35992 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CInput element user after free attempt 1:33093 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CInput element user after free attempt 1:29743 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CInput use after free atte mpt 1:35125 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CLabelElement object use a fter free attempt 1:35477 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CLabelElement object use a fter free attempt 1:35836 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CLayoutBlock use after fre e attempt 1:28158 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CLegendElement object use after free attempt 1:34753 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CLineCore use after free attempt 1:33415 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMapElement use-after-free attempt 1:33365 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMapStringToPtr use after free attempt 1:34064 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup insertMarquee use after free attempt 1:31629 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer cmarkup methods use after free attempt 1:29737 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup Object use after f ree attempt 1:32159 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup object use after f ree attempt 1:33425 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup object use after f ree attempt 1:33726 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup object use after f ree attempt 1:30110 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup object use after f ree attempt 1:30111 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup object use after f ree attempt 1:35209 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup object use after f ree attempt 1:35210 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CMarkup use-after-free att empt 1:36675 Drop and generate BROWSER-IE Microsoft Internet Explorer CMarkupPointer UnEmbed out of bounds read attempt 1:37003 Drop and generate BROWSER-IE Microsoft Internet Explorer CMarkupPointer with SVG us e-after-free attempt 1:27612 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer CMetaElement use after fre e attempt 1:34072 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CObjectElement type confus ion attempt 1:36926 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CoInternetParseUrl use-aft er-free attempt 1:34747 Drop and generate BROWSER-IE Microsoft Internet Explorer col onpropertychange memor y corruption attempt 1:36685 Drop and generate BROWSER-IE Microsoft Internet Explorer compatibility mode invalid memory access attempt 1:25790 Drop and generate BROWSER-IE Microsoft Internet Explorer compatibility mode invalid memory access attempt 1:25791 Drop and generate BROWSER-IE Microsoft Internet Explorer compatibility mode use aft er free attempt 1:34424 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer content generation use aft er free attempt 1:27607 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer contentEditable use after free attempt 1:32426 Drop and generate BROWSER-IE Microsoft Internet Explorer ConvertStringFromUnicodeEx out of bounds write attempt 1:38507 Drop and generate BROWSER-IE Microsoft Internet Explorer COptionElement object use after free attempt 1:34735 Drop and generate BROWSER-IE Microsoft Internet Explorer COrphanedStylesheetArray u se after free attempt 1:35475 Drop and generate BROWSER-IE Microsoft Internet Explorer COrphanedStylesheetArray u se-after-free attempt 1:35473 Drop and generate BROWSER-IE Microsoft Internet Explorer covered object memory corruption attempt 1:19809 Drop and generate

events

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CParaElement use after fre e attempt 1:33340 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CParaElement use-after-fre e attempt 1:35481 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CPeerHolder use after free attempt 1:41599 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CPhraseElement use after f ree attempt 1:27908 Drop and generate BROWSER-IE Microsoft Internet Explorer CPtsTextParaclient out of bounds error remote code execution attempt 1:32460 Drop and generate BROWSER-IE Microsoft Internet Explorer CQuickLinks object use-aft er-free attempt 1:36401 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer CQuickLinks object use-aft er-free attempt 1:36402 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CQuotes use-after-free att empt 1:32497 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CQuotes use-after-free att empt 1:33191 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CQuotes use-after-free att empt 1:33192 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CQuotes use-after-free att empt 1:33195 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CRangeSaver use after free attempt 1:31202 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer createRange user after fre e attempt 1:28496 Generate events

BROWSER-IE Microsoft Internet Explorer CSecurityContext type conf usion use after free attempt 1:34411 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSecurityContext use after free attempt 1:32478 Generate events

BROWSER-IE Microsoft Internet Explorer CSegment object use after free attempt 1:27842 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSelectElement SetCurSel r emote code execution attempt 1:30122 Drop and generate BROWSER-IE Microsoft Internet Explorer CSelectionManager use afte r free attempt 1:27606 Drop and generate BROWSER-IE Microsoft Internet Explorer CSharedStyleSheet RemoveRu le out of bounds read attempt 1:36946 Drop and generate BROWSER-IE Microsoft Internet Explorer CSpliceTreeEngine RemoveSp lice null pointer dereference attempt 1:36940 Drop and generate BROWSER-IE Microsoft Internet Explorer CSS .ipsum layout use-afte r-free attempt 1:31584 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CSS link element use-after -free attempt 1:39230 Drop and generate BROWSER-IE Microsoft Internet Explorer CSS padding property memor y corruption attempt 1:44356 Drop and generate BROWSER-IE Microsoft Internet Explorer CSS uninitialized object a ccess attempt detected 1:29708 Drop and generate BROWSER-IE Microsoft Internet Explorer CStr internal string use-a fter-free attempt 1:39826 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CStyleAttrArray use after free attempt 1:34765 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGHelpers use-after-free attempt 1:38090 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34195 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34196 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34197 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34198 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34199 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34200 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34201 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34202 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34203 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CSVGMarkerElement use afte r free attempt 1:34070 Drop and generate BROWSER-IE Microsoft Internet Explorer CTableCell invalid index m emory corruption attempt 1:36948 Drop and generate BROWSER-IE Microsoft Internet Explorer CTableCell object use afte r free attempt 1:36683 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer CTableCell Use After Free exploit attempt 1:31799 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTableLayout AddRow out of bounds array access heap corruption attempt 1:32182 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTableLayout use after fre e attempt 1:36928 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTableRow use after free attempt 1:35123 Drop and generate BROWSER-IE Microsoft Internet Explorer CTableSection object out o f bounds memory access attempt 1:35156 Drop and generate BROWSER-IE Microsoft Internet Explorer CTableSection use after free attempt 1:35145 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer CTableSelection use-after- free attempt 1:36439 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTextArea use after free attempt 1:35121 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTextBlock use-after-free attempt 1:37596 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTextElement use after fre e attempt 1:34873 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTextElement use after fre e attempt 1:37633 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTitleElement object use a fter free attempt 1:35172 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTitleElement object use-a fter-free attempt 1:34422 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTitleElement use after free attempt 1:34437 Drop and generate BROWSER-IE Microsoft Internet Explorer CTransientLookaside object use after free attempt 1:32168 Drop and generate BROWSER-IE Microsoft Internet Explorer CTravelEntry use after fre e attempt 1:43758 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer CTravelEntry use after fre e attempt 1:38085 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTree Node use after free attempt 1:29711 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreeDataPos object use af ter free attempt 1:30125 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreeDataPos use-after-fre e remote code execution attempt 1:33421 Drop and generate

events

events

BROWSER-IE Microsoft Internet Explorer CTreeNode interpreted as C GeneratedTreeNode remote code execution attempt 1:33718

Drop and generate events

BROWSER-IE Microsoft Internet Explorer CTreeNode object CSS text overflow attempt 1:27608 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreeNode object used afte r free attempt 1:33356 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreeNode onmousemove use- after-free attempt 1:31196 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreeNode row element remo val remote code execution attempt 1:36699 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreeNode type confusion attempt 1:35119 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreeNode undefined before Element use-after-free attempt 1:34725 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreeNode use after free attempt 1:33317 Drop and generate

events

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CTreeNode use after free m emory corruption attempt 1:26888 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreeNode use-after-free attempt 1:35012 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreeNode use-after-free attempt 1:33741 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos deleted object ac cess attempt 1:29667 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos object use-after- free attempt 1:27843 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos remote code execu tion attempt 1:38094 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:38067 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:38069 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:47291 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:47292 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:47293 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:47294 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos type confusion at tempt 1:40312 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos use after free at tempt 1:33419 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos use after free at tempt 1:30123 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CTreePos use after free at tempt 1:36944 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreePos use after free me mory corruption attempt 1:25776 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreePos use after free me mory corruption attempt 1:25777 Drop and generate BROWSER-IE Microsoft Internet Explorer CTreePos use-after-free at tempt 1:33347 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer CTsfTextStore use-after-free attempt 1:36738 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer CUListElement use-after-free attempt 1:36691 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer custom cursor file use aft er free attempt 1:25771 Drop and generate BROWSER-IE Microsoft Internet Explorer CViewportChangeInvalidatio n use after free attempt 1:28862 Drop and generate BROWSER-IE Microsoft Internet Explorer CWindow object use after f ree attempt 1:36417 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer DataView use-after-free at tempt 1:34727 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DataView use-after-free at tempt 1:42032 Drop and generate

BROWSER-IE Microsoft Internet Explorer DataView use-after-free at tempt 1:42038 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DataView use-after-free at tempt 1:37969 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DCOM sandbox escape attemp t 1:32139 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DCOMTextNode object use af ter free attempt 1:26636 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer dd element use after free attempt 1:34415 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted button use after f ree attempt 1:25125 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted button use after f ree attempt 1:25126 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted button use after f ree attempt 1:25127 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted button use after f ree attempt 1:25128 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted button use after f ree attempt 1:25129 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted button use after f ree attempt 1:25234 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted object access atte mpt detected 1:29706 Drop and generate BROWSER-IE Microsoft Internet Explorer deleted object access memo ry corruption attempt 1:29741 Drop and generate BROWSER-IE Microsoft Internet Explorer deleted object memory corruption attempt 1:29716 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer deleted object memory corruption attempt 1:28204 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted object memory corruption attempt 1:30956 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer deleted object memory corruption attempt 1:28490 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DirectX information disclosure attempt 1:48370 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DirectX information disclosure attempt 1:48371 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer display node use after fre e attempt 1:27133 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DOMAttrModified event use after free attempt 1:41583 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer DOMNodeInserted use-after- free attempt 1:34409 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer double-free memory corrupt ion attempt 1:27100 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer double-free memory corrupt ion attempt 1:26869 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer double-free memory corrupt ion attempt 1:26871 Drop and generate BROWSER-IE Microsoft Internet Explorer drag and drop API remote c ode execution attempt 1:39207 Drop and generate BROWSER-IE Microsoft Internet Explorer dximagetransform.microsoft .shadow out of bounds array access attempt 1:33348 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer Edge text node table-cell use after free attempt 1:39505 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer element attribute use afte r free attempt 1:32138 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer element attribute use afte r free attempt 1:35963 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Element object use-after-f ree attempt 1:34419 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer element type confusion use after free attempt 1:32720 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer embedded media player use after free attempt 1:38079 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer embedded media player use after free attempt 1:38080 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer embedSWF use after free ex ploit attempt 1:46243 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer embedSWF use after free ex ploit attempt 1:46244 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer embedSWF use after free ex ploit attempt 1:46245 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer embedSWF use after free ex ploit attempt 1:46246 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer EMF file integer overflow attempt 1:38772 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer EMF file integer overflow attempt 1:38773 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer EPM brokercreatefile file access bypass attempt 1:43497 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer EventListener use after free attempt 1:36443 Drop and generate BROWSER-IE Microsoft Internet Explorer execCommand CTreePos memor y corruption attempt 1:28494 Drop and generate BROWSER-IE Microsoft Internet Explorer failed large copy clonenod e attempt 1:30497 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer flexbox use after free att empt 1:36942 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer font element out of bounds read attempt 1:40108 Drop and generate BROWSER-IE Microsoft Internet Explorer fontFamily attribute delet ed object access memory corruption attempt 1:29709 Drop and generate BROWSER-IE Microsoft Internet Explorer FormatContext Use after free attempt 1:32155 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer fragmented CtxtBlk heap ov erflow attempt 1:36671 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer freed CTreePos object use- after-free attempt 1:28492 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer generic use after free att empt 1:28523 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer GetClassObject use after f ree attempt 1:30503 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer GetClassObject use after f ree attempt 1:30504 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer GetClassObject use after f ree attempt 1:30505 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer GetClassObject use after f ree attempt 1:28875 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer GetClassObject use after f ree attempt 1:28876 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer GETDISPID invalid pointer access attempt 1:38065 Drop and generate BROWSER-IE Microsoft Internet Explorer GetPlainText negative star t index out of bounds write attempt 1:36673 Drop and generate BROWSER-IE Microsoft Internet Explorer hgroup element DOM reset u se after free attempt 1:27829 Drop and generate BROWSER-IE Microsoft Internet Explorer htc file use after free at tempt 1:26129 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer html reload loop attempt 1 :26633 Generate events

BROWSER-IE Microsoft Internet Explorer htmlFile ActiveX control u niversal XSS attempt 1:42204 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Hyphenator object use afte r free attempt 1:33333 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer iCalendar cross site scrip ting attempt 1:36917 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer ieframe.dll ActiveX clsid access 1:36437 Drop and generate BROWSER-IE Microsoft Internet Explorer iertutil.dll long UNC redi rect out of bounds read attempt 1:40787 Drop and generate BROWSER-IE Microsoft Internet Explorer iertutil.dll long UNC redi rect out of bounds read attempt 1:39810 Drop and generate BROWSER-IE Microsoft Internet Explorer iframe execCommand use aft er free attempt 1:27845 Drop and generate BROWSER-IE Microsoft Internet Explorer IFRAME object constructor cross site scripting attempt 1:37602 Drop and generate BROWSER-IE Microsoft Internet Explorer iframe type confusion atte mpt 1:40378 Drop and generate

events

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer iframe use after free atte mpt 1:25788 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer improper object cast memor y corruption attempt 1:31388 Drop and generate BROWSER-IE Microsoft Internet Explorer incorrect array element re ad information disclosure attempt 1:34089 Drop and generate BROWSER-IE Microsoft Internet Explorer innerHTML use after free attempt 1:32153 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer InsertElementInternal out of bounds indexed array remote code execution attempt 1:33312

Drop and generate events

BROWSER-IE Microsoft Internet Explorer InsertSanitizedTextEx use after free attempt 1:38465 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer InsertSelectDropdown use a fter free attempt 1:39833 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer integer overflow exploit attempt 1:31809 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer invalid memory access atte mpt 1:36018 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer invalid table grid memory corruption attempt 1:36938 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer invalid TableRow use after free attempt 1:36920 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer javascript apply method ty pe confusion attempt 1:27832 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer javascript argument type c onfusion attempt 1:36980 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer javascript call method typ e confusion attempt 1:27831 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer javascript call method typ e confusion attempt 1:28231 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer JavaScript memory corruption attempt 1:46229 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer javascript memory corruption attempt 1:46228 Drop and generate BROWSER-IE Microsoft Internet Explorer JScript.Compact insertBefo re memory corruption attempt 1:35990 Drop and generate BROWSER-IE Microsoft Internet Explorer justifying text with an in correct type use after free attempt 1:31788 Drop and generate BROWSER-IE Microsoft Internet Explorer kbd element use-after-free attempt 1:31619 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer LayoutLineBoxFullShort use after free attempt 1:34778 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer list element use after fre e attempt 1:29731 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer mapi32x.dll dll-load explo it attempt 1:37257 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer margin overflow use after free attempt 1:31634 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:47484 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:47485 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:34383 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:46944 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:46945 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:44512 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:43155 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:47730 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:47731 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:47738 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:47739 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory corruption attempt 1:44526 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer memory leak exploit attemp t 1:33422 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer merged stylesheet array us e after free attempt 1:27620 Drop and generate

events

1:27615 events

BROWSER-IE Microsoft Internet Explorer mshtml InsertRange out of bounds write access 1:38117 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer mshtml.dll cached object u se after free attempt 1:39828 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer mshtml.dll invalid resize use after free attempt 1:39499 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer mshtml.dll null pointer de reference attempt 1:38763 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer msSaveBlob use after free attempt 1:40653 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer MSXML IDispatch use after free attempt 1:40149 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer MSXML use after free attempt 1:47747 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer MSXML use after free attempt 1:47748 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Nested Tables use after free attempt 1:30129 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer NodeFilter use after free attempt 1:32691 Drop and generate BROWSER-IE Microsoft Internet Explorer nonexistent attribute remo val memory corruption attempt 1:36811 Drop and generate BROWSER-IE Microsoft Internet Explorer nonexistent attribute remo val memory corruption attempt 1:36812 Drop and generate BROWSER-IE Microsoft Internet Explorer nonexistent attribute remo val memory corruption attempt 1:36813 Drop and generate BROWSER-IE Microsoft Internet Explorer nth-child use after free attempt 1:30501 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer null object access attempt 1:26569 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer null object access attempt 1:26668 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer object property change use after free attempt 1:41405 Drop and generate BROWSER-IE Microsoft Internet Explorer object type confusion remo te code execution attempt 1:32424 Drop and generate BROWSER-IE Microsoft Internet Explorer object use after free atte mpt 1:44349 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer object use after free atte mpt 1:46220 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer object use after free atte mpt 1:46221 Drop and generate BROWSER-IE Microsoft Internet Explorer onbeforeeditfocus element attribute use after free attempt 1:25772 Drop and generate BROWSER-IE Microsoft Internet Explorer onbeforeeditfocus element attribute use after free attempt 1:31485 Drop and generate BROWSER-IE Microsoft Internet Explorer OnMove use after free atte mpt 1:30140 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer OnMove use after free atte mpt 1:30142 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer onreadystatechange use aft er free attempt 1:32317 Generate events

BROWSER-IE Microsoft Internet Explorer onreadystatechange use aft er free attempt 1:31621 Generate events BROWSER-IE Microsoft Internet Explorer onscroll use after free at tempt 1:29988

BROWSER-IE Microsoft Internet Explorer onscroll use after free at tempt 1:26882 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer onscroll use after free at tempt 1:26883 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer onscroll use after free at tempt 1:26884 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bound write access attempt 1:38096 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds array access attempt 1:33730 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds array access attempt 1:33775 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds array access attempt 1:33776 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds array access attempt 1:34723 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds array memory access attempt 1:36008 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds memory acces s attempt 1:34790 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds read attempt 1:40988 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer out of bounds read attempt 1:40989 Drop and generate BROWSER-IE Microsoft Internet Explorer overlapping object boundar ies memory corruption attempt 1:29733 Drop and generate BROWSER-IE Microsoft Internet Explorer overlapping object boundar ies memory corruption attempt 1:32364 Drop and generate BROWSER-IE Microsoft Internet Explorer page layout use after free attempt 1:47310 Drop and generate

events

events

events

events

BROWSER-IE Microsoft Internet Explorer page layout use after free attempt 1:47311 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer page layout use after free attempt 1:39812 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer pastHTML use after free 1: 30120 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer pElement member use after free attempt 1:27154 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer pre-line use after free at tempt 1:25775 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer PreviousTreePos use after free attempt 1:27132 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer prototype type confusion attempt 1:46594 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer prototype type confusion attempt 1:46595 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer range markup switch use af ter free attempt 1:27839 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer range use after free attempt 1:34381 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer recordset use after free attempt 1:42156 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer recordset use after free attempt 1:42157 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer RegExp object use after free attempt 1:36450 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Regexp use after free atte mpt 1:46554 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Regexp use after free atte mpt 1:46555 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer remote code execution atte mpt 1:30499 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Remove Format use after free attempt 1:30108 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer RemoveSplice use-after-fre e attempt 1:31190 Drop and generate BROWSER-IE Microsoft Internet Explorer replaceChild function memo ry corruption attempt 1:35114 Drop and generate BROWSER-IE Microsoft Internet Explorer request for mapi32x.dll ov er SMB attempt 1:37258 Drop and generate BROWSER-IE Microsoft Internet Explorer ruby element in media elem ent use after free attempt 1:30131 Drop and generate BROWSER-IE Microsoft Internet Explorer ruby text tag heap-based b uffer overflow attempt 1:30144 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer runtimeStyle memory corrup tion attempt 1:26641 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer saveHistory use after free attempt 1:26132 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer saveHistory use after free attempt 1:26135 Drop and generate BROWSER-IE Microsoft Internet Explorer SComputedStyle destructor out of bounds read attempt 1:36950 Drop and generate BROWSER-IE Microsoft Internet Explorer scripting engine buffer ov erflow attempt 1:39236 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer scripting engine memory co rruption attempt 1:44510 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer scripting engine memory co rruption attempt 1:45138 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer scripting engine memory co rruption attempt 1:45877 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer scripting engine memory co rruption attempt 1:45878 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer scripting engine memory co rruption attempt 1:45144 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer scripting engine memory co rruption attempt 1:45146 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer select use after free atte mpt 1:36982 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer selectall use after free attempt 1:29735 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer setCapture use after free attempt 1:27126 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer setEndPoint use after free attempt 1:30118 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer setInterval focus use afte r free attempt 1:26629 Drop and generate

BROWSER-IE Microsoft Internet Explorer SLayoutRun use-after-free attempt 1:33358 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer STextBlockPosition use aft er free attempt 1:28151 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer StrCmpNICW string object u se after free attempt 1:37604 Drop and generate BROWSER-IE Microsoft Internet Explorer string type confusion remo te code execution attempt 1:38088 Drop and generate BROWSER-IE Microsoft Internet Explorer style object stylesheet us e after free attempt 1:36693 Drop and generate BROWSER-IE Microsoft Internet Explorer style type confusion remot e code execution attempt 1:33412 Drop and generate BROWSER-IE Microsoft Internet Explorer style-image-url use after free attempt 1:31786 Drop and generate BROWSER-IE Microsoft Internet Explorer superscript invalid parame ter denial of service attempt 1:32161 Drop and generate BROWSER-IE Microsoft Internet Explorer superscript use after free attempt 1:26849 Drop and generate

events

events

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer SVG handling use after fre e attempt 1:29671 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer SVG handling use after fre e attempt 1:29672 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer SVG handling use after fre e attempt 1:30079 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer SVG handling use after fre e attempt 1:30080 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer SVG object use after free attempt 1:25792 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer svg use after free attempt 1:33359 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer swap node user after free 1:29678 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer table cell out-of-bounds a ccess attempt 1:33743 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer table column resize use-af ter-free attempt 1:35182 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer table column-count integer overflow attempt 1:27156 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer table element modification use after free attempt 1:36695 Drop and generate BROWSER-IE Microsoft Internet Explorer table layout cache arbitra ry code execution attempt 1:35536 Drop and generate BROWSER-IE Microsoft Internet Explorer table sub structure use af ter free attempt 1:28866 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer TableCellLayoutArray use-a fter-free attempt 1:38098 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer TableGridBlock object use after free attempt 1:34750 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer TableGridBlock use after f ree attempt 1:34432 Drop and generate BROWSER-IE Microsoft Internet Explorer TableGridBoxBuilder Update ColumnSize out of bounds read attempt 1:36956 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer text node use after free attempt 1:29717 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer textarea parent use-after- free attempt 1:34767 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer textarea type confusion at tempt 1:41954 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer TextBlock object use after free attempt 1:37009 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer TextBlock out of bounds re ad attempt 1:36936 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer TextData object use after free attempt 1:34074 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer TextNode object use after free attempt 1:34745 Drop and generate BROWSER-IE Microsoft Internet Explorer textTransform out-of-bound s memory access attempt 1:39514 Drop and generate BROWSER-IE Microsoft Internet Explorer title integer overflow att empt 1:40986 Drop and generate BROWSER-IE Microsoft Internet Explorer TreeComputedContent object use after free attempt 1:35199 Drop and generate BROWSER-IE Microsoft Internet Explorer TreeNode use after free at tempt 1:27605 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer type confusion vulnerabili ty attempt 1:42165 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer UIAnimaation.dll use after free attempt 1:40703 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer UIAnimaation.dll use after free attempt 1:40704 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer undo use after free attemp t 1:28504 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer uninitialized object use a fter free attempt 1:31382 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer uninitialized pointer atte mpt 1:38776 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer uninitialized pointer use exploit attempt 1:33323 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Use after free attempt 1:3 1625 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:3 3707 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:3 1198 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:2 7150 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:2 7151 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:2 7171 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:2 9721 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:2 8873 Drop and generate

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:3 9763 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:4 5121 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free attempt 1:3 2441 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use after free memory corruption attempt 1:30127 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use asm memory corruption attempt 1:41555 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer use of rtf file in clipboa rd attempt 1:32703 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer vbscript csession close us e after free attempt 1:39201 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript engine memory cor ruption attempt 1:47591 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript engine memory cor ruption attempt 1:47592 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript Engine remote cod e execution attempt 1:48368 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript Engine remote cod e execution attempt 1:48369 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript Engine remote cod e execution attempt 1:48372 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript Engine remote cod e execution attempt 1:48373 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript engine use after free attempt 1:37283 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript engine use after free attempt 1:36922 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript engine use after free attempt 1:38308 Drop and generate BROWSER-IE Microsoft Internet Explorer VBScript out of bounds mem ory access remote code execution attempt 1:39211 Drop and generate BROWSER-IE Microsoft Internet Explorer VBScript remote code execu tion attempt 1:46548 Drop and generate

events

events

events

BROWSER-IE Microsoft Internet Explorer VBScript remote code execu tion attempt 1:46549 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript remote code execu tion attempt 1:46745 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VBScript remote code execu tion attempt 1:46746 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Vbscript String out of bou nds write 1:46198 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer Vbscript String out of bou nds write 1:46199 Drop and generate BROWSER-IE Microsoft Internet Explorer VBScript toString redim ar ray use after free attempt 1:38841 Drop and generate BROWSER-IE Microsoft Internet Explorer VBScript toString redim ar ray use after free attempt 1:39680 Drop and generate BROWSER-IE Microsoft Internet Explorer vbscript variable type con fusion attempt 1:40385 Drop and generate BROWSER-IE Microsoft Internet Explorer VML array with negative le ngth memory corruption attempt 1:26638 Drop and generate

events

events

events

events

events

BROWSER-IE Microsoft Internet Explorer VML use after free attempt 1:30794 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VML use after free attempt 1:32362 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer VML use after free attempt 1:30894 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer window scroll integer over flow attempt 1:35499 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer window scroll integer over flow attempt 1:36069 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer WindowedMarkupContext use after free attempt 1:31219 Drop and generate

events

BROWSER-IE Microsoft Internet Explorer XMLDOM double free corrupt ion attempt 1:35866 Drop and generate

events

BROWSER-IE Microsoft Windows Edge array out of bounds write 1:434 92 Drop and generate

events

BROWSER-IE Microsoft Windows Edge AudioContext use after free att empt 1:42781 Drop and generate

events

BROWSER-IE Microsoft Windows Edge emodel use after free attempt 1 :40372 Drop and generate

events

BROWSER-IE Microsoft Windows Edge function.apply use afterfree at tempt 1:40423 Drop and generate

events

BROWSER-IE Microsoft Windows Edge memory corruption attempt 1:443 31 Drop and generate

events

BROWSER-IE Microsoft Windows Edge use-after-free attempt 1:46206 Drop and generate

events

BROWSER-IE Microsoft Windows Edge use-after-free attempt 1:46207 Drop and generate

events

BROWSER-IE Microsoft Windows Internet Explorer MSHTML.dll type co nfusion attempt 1:39839 Drop and generate

events

BROWSER-IE scripting engine memory corruption vulnerability attempt 1:44508 Drop and generate

events

BROWSER-IE SFVRT-1021 attack attempt 3:38671 Drop and generate

events

BROWSER-IE VBScript ADODB.Connection object use after free attemp t 1:40132 Drop and generate

events

BROWSER-IE VBScript ADODB.Connection object use after free attemp t 1:40133 Drop and generate

events

BROWSER-IE VBScript RegEx use-after-free attempt 1:32709 Drop and generate

events

BROWSER-OTHER Cisco WebEx extension command execution attempt 1:4 1407 Drop and generate

events

BROWSER-OTHER Microsoft Edge url spoofing attempt 1:47119 Drop and generate

events

BROWSER-OTHER Microsoft Edge url spoofing attempt 1:47120 Drop and generate

events

BROWSER-OTHER Novell Messenger Client nim URI handler buffer over flow attempt 1:26489 Drop and generate

events

BROWSER-PLUGINS Adobe Reader 11 messageHandler ActiveX access att empt 1:31407 Drop and generate

events

BROWSER-PLUGINS Adobe Reader 11 messageHandler ActiveX access att empt 1:31409 Drop and generate BROWSER-PLUGINS Advantech WebAccess AspVCObj.AspDataDriven Interf aceFilter ActiveX clsid access 1:36109 Drop and generate

events

events

BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function ca ll attempt 1:27869 Drop and generate

events

BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function ca ll attempt 1:27870 Drop and generate

events

BROWSER-PLUGINS Java Applet sql.DriverManager fakedriver exploit attempt 1:26898 Drop and generate BROWSER-PLUGINS Microsoft Internet Explorer Adobe Reader Extensio n race condition attempt 1:31017 Drop and generate BROWSER-PLUGINS Microsoft Silverlight GetChar out of bounds read attempt 1:40813 Drop and generate

events

events

events

BROWSER-PLUGINS Microsoft Silverlight GetChar out of bounds read attempt 1:37267 Drop and generate BROWSER-PLUGINS Microsoft Silverlight ScriptObject untrusted poin ter dereference attempt 1:28579 Drop and generate BROWSER-PLUGINS Microsoft Silverlight ScriptObject untrusted poin ter dereference attempt 1:28580 Drop and generate BROWSER-PLUGINS Microsoft Silverlight ScriptObject untrusted poin ter dereference attempt 1:28581 Drop and generate BROWSER-PLUGINS Microsoft Silverlight ScriptObject untrusted poin ter dereference attempt 1:37801 Drop and generate BROWSER-PLUGINS Microsoft XML Core Services ActiveX control use a fter free attempt 1:38463 Drop and generate

events

events

events

events

events

events

BROWSER-PLUGINS Oracle Java Security Slider feature bypass attemp t 1:27766 Generate events

BROWSER-WEBKIT Apple WebKit memory corruption attempt 1:47022 Drop and generate

events

BROWSER-WEBKIT Apple WebKit memory corruption attempt 1:47023 Drop and generate

events

DCE2\_EVENT CL\_BAD\_MAJ\_VERSION 133:40 Generate events

DCE2\_EVENT CL\_BAD\_PDU\_TYPE 133:41 Generate events

DCE2\_EVENT CL\_BAD\_SEQ\_NUM 133:43 Generate events

DCE2\_EVENT CL\_DATA\_LT\_HDR 133:42 Generate events

DCE2\_EVENT CO\_ALTER\_CHANGE\_BYTE\_ORDER 133:36 Generate events

DCE2\_EVENT CO\_BAD\_MAJ\_VERSION 133:27 Generate events

DCE2\_EVENT CO\_BAD\_MIN\_VERSION 133:28 Generate events

DCE2\_EVENT CO\_BAD\_PDU\_TYPE 133:29 Generate events

DCE2\_EVENT CO\_FLEN\_LT\_HDR 133:30 Generate events

DCE2\_EVENT CO\_FLEN\_LT\_SIZE 133:31 Generate events

DCE2\_EVENT CO\_FRAG\_DIFF\_CALL\_ID 133:37 Generate events

DCE2\_EVENT CO\_FRAG\_DIFF\_CTX\_ID 133:39 Generate events

DCE2\_EVENT CO\_FRAG\_DIFF\_OPNUM 133:38 Generate events

DCE2\_EVENT CO\_FRAG\_GT\_MAX\_XMIT\_FRAG 133:35 Generate events

DCE2\_EVENT CO\_FRAG\_LT\_MAX\_XMIT\_FRAG 133:34 Generate events

DCE2\_EVENT CO\_ZERO\_CTX\_ITEMS 133:32 Generate events

DCE2\_EVENT CO\_ZERO\_TSYNS 133:33 Generate events

DCE2\_EVENT SMB\_BAD\_BCC 133:6 Generate events

DCE2\_EVENT SMB\_BAD\_FORMAT 133:7 Generate events

DCE2\_EVENT SMB\_BAD\_ID 133:4 Generate events

DCE2\_EVENT SMB\_BAD\_NBSS\_TYPE 133:2 Generate events

DCE2\_EVENT SMB\_BAD\_OFF 133:8 Generate events

DCE2\_EVENT SMB\_BAD\_TYPE 133:3 Generate events

DCE2\_EVENT SMB\_BAD\_WCT 133:5 Generate events

DCE2\_EVENT SMB\_BCC\_LT\_DSIZE 133:16 Generate events

DCE2\_EVENT SMB\_CHAIN\_OPEN\_CLOSE 133:25 Generate events

DCE2\_EVENT SMB\_CHAIN\_SS\_LOGOFF 133:23 Generate events

DCE2\_EVENT SMB\_CHAIN\_TC\_TDIS 133:24 Generate events

DCE2\_EVENT SMB\_DCNT\_MISMATCH 133:49 Generate events

DCE2\_EVENT SMB\_DCNT\_ZERO 133:48 Generate events

DCE2\_EVENT SMB\_DEPR\_COMMAND\_USED 133:53 Generate events

DCE2\_EVENT SMB\_DEPR\_DIALECT\_NEGOTIATED 133:52 Generate events

DCE2\_EVENT SMB\_DSENT\_GT\_TDCNT 133:15 Generate events

DCE2\_EVENT SMB\_EVASIVE\_FILE\_ATTRS 133:57 Generate events

DCE2\_EVENT SMB\_EXCESSIVE\_CHAINING 133:20 Generate events

DCE2\_EVENT SMB\_EXCESSIVE\_READS 133:19 Generate events

DCE2\_EVENT SMB\_EXCESSIVE\_TREE\_CONNECTS 133:18 Generate events

DCE2\_EVENT SMB\_INVALID\_DSIZE 133:17 Generate events

DCE2\_EVENT SMB\_INVALID\_SETUP\_COUNT 133:55 Generate events

DCE2\_EVENT SMB\_INVALID\_SHARE 133:26 Generate events

DCE2\_EVENT SMB\_MAX\_REQS\_EXCEEDED 133:50 Generate events

DCE2\_EVENT SMB\_MULT\_CHAIN\_SS 133:21 Generate events

DCE2\_EVENT SMB\_MULT\_CHAIN\_TC 133:22 Generate events

DCE2\_EVENT SMB\_MULTIPLE\_NEGOTIATIONS 133:56 Generate events

DCE2\_EVENT SMB\_NB\_LT\_BCC 133:12 Generate events

DCE2\_EVENT SMB\_NB\_LT\_COM 133:11 Generate events

DCE2\_EVENT SMB\_NB\_LT\_DSIZE 133:13 Generate events

DCE2\_EVENT SMB\_NB\_LT\_SMBHDR 133:10 Generate events

DCE2\_EVENT SMB\_REQS\_SAME\_MID 133:51 Generate events

DCE2\_EVENT SMB\_TDCNT\_LT\_DSIZE 133:14 Generate events

DCE2\_EVENT SMB\_TDCNT\_ZERO 133:9 Generate events

DCE2\_EVENT SMB\_UNUSUAL\_COMMAND\_USED 133:54 Generate events

DNS\_EVENT\_EXPERIMENTAL\_TYPES 131:2 Generate events

DNS\_EVENT\_OBSOLETE\_TYPES 131:1 Generate events

EXPLOIT-KIT Angler exploit kit Adobe Flash download 1:33184 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Adobe Flash encoded shellcode dete cted 1:31899 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download 1 :33186 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download 1 :33271 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download 1 :33272 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download 1 :33286 Drop and generate

events

EXPLOIT-KIT Angler exploit kit browser version detection attempt 1:36071 Drop and generate

events

EXPLOIT-KIT Angler Exploit Kit email gate 1:38682 Drop and generate

events

EXPLOIT-KIT Angler exploit kit encrypted binary download 1:33185

EXPLOIT-KIT Angler exploit kit Flash exploit file download attemp t 3:38285 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Flash exploit file download 3:3824 4 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Flash exploit file download 3:3824 5 Drop and generate

events

EXPLOIT-KIT Angler exploit kit index uri request attempt 1:37871 Drop and generate

events

EXPLOIT-KIT Angler exploit kit index uri request attempt 1:36636 Drop and generate

events

EXPLOIT-KIT Angler exploit kit index uri request attempt 1:38161 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Internet Explorer encoded shellcod e detected 1:31900 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page - base64 encoded xml/ jnlp statement 1:30852 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:36808 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:32390 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:33183 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:33292 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:31898 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:34969 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:34970 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:35256 Drop and generate

events

EXPLOIT-KIT Angler exploit kit landing page detected 1:36457 Drop and generate

events

EXPLOIT-KIT Angler exploit kit obfuscated Flash actionscript clas sname detected 1:35109 Drop and generate

events

EXPLOIT-KIT Angler exploit kit Oracle Java encoded shellcode dete cted 1:31901 Drop and generate

events

EXPLOIT-KIT Angler exploit kit outbound Adobe Flash request 1:331 82 Drop and generate

events

EXPLOIT-KIT Angler exploit kit outbound Oracle Java request 1:323 99 Drop and generate

events

EXPLOIT-KIT Angler exploit kit outbound uri structure 1:33663 Drop and generate

events

EXPLOIT-KIT Angler exploit kit outbound uri structure 1:38437 Drop and generate

events

EXPLOIT-KIT Angler exploit kit questions uri request attempt 1:38 438 Drop and generate

events

EXPLOIT-KIT Angler exploit kit redirect page detected 1:38521 Drop and generate

events

EXPLOIT-KIT Angler exploit kit redirection page 1:31370 Drop and generate

events

EXPLOIT-KIT Angler exploit kit relay traffic detected 1:36332 Drop and generate

events

EXPLOIT-KIT Angler exploit kit search uri request attempt 1:36635 Drop and generate

events

EXPLOIT-KIT Angler exploit kit view uri request attempt 1:37873 Drop and generate

events

EXPLOIT-KIT Angler exploit kit view uri request attempt 1:38163 Drop and generate

events

EXPLOIT-KIT Angler exploit kit view uri request attempt 1:37957 Drop and generate

events

EXPLOIT-KIT Angler exploit kit viewthread uri request attempt 1:3 8162 Drop and generate

events

EXPLOIT-KIT Angler exploit kit viewthread uri request attempt 1:3 7958 Drop and generate

events

EXPLOIT-KIT Angler exploit kit viewtopic uri request attempt 1:36 637 Drop and generate

events

EXPLOIT-KIT Angler landing page detected 1:38555 Drop and generate

events

EXPLOIT-KIT Blackholev2 exploit kit url structure detected 1:2504 3 Drop and generate

events

EXPLOIT-KIT Blackholev2/Cool exploit kit landing page 1:27877 Drop and generate

events

EXPLOIT-KIT Blackholev2/Cool exploit kit landing page 1:27878 Drop and generate

events

EXPLOIT-KIT Blackholev2/Cool exploit kit outbound portable execut able request 1:27110 Generate events

EXPLOIT-KIT Blackholev2/Darkleech exploit kit landing page reques t 1:27865 Drop and generate

events

EXPLOIT-KIT Blackholev2/Darkleech exploit kit landing page 1:2786 6 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call attempt 1:21679 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21678 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21680 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21681 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21682 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21683 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21684 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21685 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:21686 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:28196 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:28197 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:28198 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit module call 1:28199 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit outbound connection 1:31230 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit outbound connection 1:31231 Drop and generate

events

EXPLOIT-KIT Bleeding Life exploit kit outbound jar request 1:3123 2 Drop and generate

events

EXPLOIT-KIT CK exploit kit landing page 1:32803 Drop and generate

events

EXPLOIT-KIT CottonCastle exploit kit Adobe flash outbound connect ion 1:31276 Drop and generate

events

EXPLOIT-KIT CottonCastle exploit kit decryption page outbound req uest 1:31279 Drop and generate

events

EXPLOIT-KIT CottonCastle exploit kit encrypted binary download 1: 31274 Drop and generate

events

EXPLOIT-KIT CottonCastle exploit kit landing page 1:31275 Drop and generate

events

EXPLOIT-KIT CottonCastle exploit kit Oracle Java outbound connect ion 1:31277 Drop and generate

events

EXPLOIT-KIT CottonCastle exploit kit Oracle java outbound connect ion 1:31278 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - Java exploit download 1:26038 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - Java exploit download 1:26039 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - Java Exploit 1:26036 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - java on 1:26035 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - Portable Executable download attempt 1:26040 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - Portable Executable download attempt 1:26041 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - Portable Executable download attempt 1:26043 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - redirection attempt 1:26044 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - setup 1:26045 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - stats access 1:26034 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit - stats loaded 1:26042 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit outbound connection 1:24232 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit outbound connection 1:24233 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit outbound connection 1:24234 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit redirection attempt 1:24231 Drop and generate

events

EXPLOIT-KIT Crimeboss exploit kit redirection attempt 1:26226 Drop and generate

events

EXPLOIT-KIT Crimepack exploit kit control panel access 1:21096 Drop and generate

events

EXPLOIT-KIT Crimepack exploit kit malicious pdf request 1:21099 Drop and generate

events

EXPLOIT-KIT Crimepack exploit kit post-exploit download request 1 :21097 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Java Exploit download 1:24787 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Java Exploit request structure 1:24 786 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Java Exploit request structure 1:27 274 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Java V5 exploit download 1:25823 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Java V6 exploit download 1:25046 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Java V7 exploit download 1:25047 Drop and generate

events

EXPLOIT-KIT CritX exploit kit landing page - redirection to Adobe Flash exploit 1:30967 Drop and generate

events

EXPLOIT-KIT CritX exploit kit landing page - redirection to Adobe Flash exploit 1:30976 Drop and generate

events

EXPLOIT-KIT CritX exploit kit landing page - redirection to font exploit 1:30968 Drop and generate EXPLOIT-KIT CritX exploit kit landing page - redirection to Micro soft Internet Explorer exploit 1:30966 Drop and generate EXPLOIT-KIT CritX exploit kit landing page - redirection to Oracl e Java exploit 1:30965 Drop and generate

events

events

events

EXPLOIT-KIT CritX exploit kit landing page - redirection to Oracl e Java exploit 1:30975 Drop and generate

events

EXPLOIT-KIT CritX exploit kit landing page detected 1:31692 Drop and generate

events

EXPLOIT-KIT CritX exploit kit malicious payload retrieval 1:25824 Drop and generate

events

EXPLOIT-KIT CritX exploit kit malicious PDF retrieval 1:25822 Drop and generate

events

EXPLOIT-KIT CritX exploit kit outbound jar request 1:29165 Generate events

EXPLOIT-KIT CritX exploit kit outbound request for Adobe Flash la nding page 1:30970 Generate events

EXPLOIT-KIT CritX exploit kit outbound request for Oracle Java la nding page 1:30971 Generate events

EXPLOIT-KIT CritX exploit kit payload download attempt 1:29166 Generate events

EXPLOIT-KIT CritX exploit kit payload download attempt 1:29167 Generate events

EXPLOIT-KIT CritX exploit kit payload request 1:30973 Drop and generate

events

EXPLOIT-KIT CritX exploit kit PDF Exploit download attempt 1:2478 9 Drop and generate

events

EXPLOIT-KIT CritX exploit kit PDF Exploit request structure 1:247 88 Drop and generate

events

EXPLOIT-KIT CritX exploit kit PDF Library exploit download 1:2504 8 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Portable Executable download 1:2479 1 Drop and generate

events

EXPLOIT-KIT CritX exploit kit Portable Executable request 1:24790 Drop and generate

events

EXPLOIT-KIT CritX exploit kit redirection page 1:26323 Drop and generate

events

EXPLOIT-KIT DarkLeech iframe injection tool detected 1:37361 Drop and generate

events

EXPLOIT-KIT DoloMalo exploit kit packer detected 1:37016 Drop and generate

events

EXPLOIT-KIT DotkaChef/Rmayana exploit kit redirection attempt 1:2 8138 Drop and generate

events

EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit landing page 1 :26949 Drop and generate EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit Malvertising C ampaign URI request 1:26951 Drop and generate EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit Zeroaccess dow nload attempt 1:27113 Drop and generate

events

events

events

EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit Zeroaccess dow nload 1:27876 Drop and generate

events

EXPLOIT-KIT Eleanore exploit kit exploit fetch request 1:21069 Drop and generate

events

EXPLOIT-KIT Eleanore exploit kit landing page 1:21068 Drop and generate

events

EXPLOIT-KIT Eleanore exploit kit pdf exploit page request 1:21070 Drop and generate

events

EXPLOIT-KIT Eleanore exploit kit post-exploit page request 1:2107 1 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - IFRAMEr injection tool 1:28022 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:27242 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:28016 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:28017 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:28018 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:28019 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:28020 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit in dicator 1:28021 Drop and generate

events

EXPLOIT-KIT embedded iframe redirection - possible exploit kit re direction 1:25558 Drop and generate

events

EXPLOIT-KIT Fake transaction redirect page to exploit kit 1:23141 Drop and generate

events

EXPLOIT-KIT FakeFlash update attempt 1:46662 Drop and generate

events

EXPLOIT-KIT Flashpack/Safe/CritX exploit kit executable download 1:26891 Drop and generate

events

EXPLOIT-KIT Flashpack/Safe/CritX exploit kit jar file download 1: 26892 Drop and generate

events

EXPLOIT-KIT Flashpack/Safe/CritX exploit kit Java V6 exploit down load 1:26894 Drop and generate

events

EXPLOIT-KIT Flashpack/Safe/CritX exploit kit Java V7 exploit down load 1:26895 Drop and generate

events

EXPLOIT-KIT Flashpack/Safe/CritX exploit kit malware download 1:2 6897 Drop and generate

events

EXPLOIT-KIT Flashpack/Safe/CritX exploit kit Plugin detection res ponse 1:26896 Drop and generate

events

EXPLOIT-KIT Flim exploit kit landing page 1:26961 Drop and generate

events

EXPLOIT-KIT Flim exploit kit portable executable download 1:26962 Drop and generate

events

EXPLOIT-KIT g01pack exploit kit redirection attempt 1:28015 Drop and generate

events

EXPLOIT-KIT Glazunov exploit kit landing page 1:28428 Drop and generate

events

EXPLOIT-KIT Glazunov exploit kit outbound jnlp download attempt 1 :28429 Drop and generate

events

EXPLOIT-KIT Glazunov exploit kit zip file download 1:28430 Drop and generate

events

EXPLOIT-KIT Gong Da exploit kit Java exploit requested 1:27704 Drop and generate

events

EXPLOIT-KIT Gong Da exploit kit Java exploit requested 1:27705 Drop and generate

events

EXPLOIT-KIT Gong Da exploit kit landing page 1:31988 Drop and generate

events

EXPLOIT-KIT Gong Da exploit kit landing page 1:27702 Drop and generate

events

EXPLOIT-KIT Gong da exploit kit landing page 1:37919 Drop and generate

events

EXPLOIT-KIT Gong Da exploit kit redirection page received 1:26013 Drop and generate

events

EXPLOIT-KIT GongDa landing page detected 1:36798 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit encrypted binary download 1 :29360 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit iframe redirection 1:27273 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit landing page 1:29361 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit landing page 1:30316 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit landing page 1:30317 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit malicious portable executab le file request 1:30319 Drop and generate

events

EXPLOIT-KIT Goon/Infinity exploit kit payload download attempt 1: 28795 Drop and generate

events

EXPLOIT-KIT Goon/Infinity/Rig exploit kit encrypted binary downlo ad 1:30934 Drop and generate

events

EXPLOIT-KIT Goon/Infinity/Rig exploit kit landing page - specific structure 1:30935 Drop and generate

events

EXPLOIT-KIT Goon/Infinity/Rig exploit kit outbound uri structure 1:30936 Drop and generate

events

EXPLOIT-KIT Hanjuan exploit kit encrypted binary download 1:31699 Drop and generate

events

EXPLOIT-KIT Hanjuan exploit kit landing page detection 1:31700 Drop and generate

events

EXPLOIT-KIT Hello/LightsOut exploit kit - exploit targeting Java before v1.7.17 1:30004 Drop and generate

events

EXPLOIT-KIT Hello/LightsOut exploit kit - exploit targeting Java v1.6.32 and older 1:30009 Drop and generate EXPLOIT-KIT Hello/LightsOut exploit kit - exploit targeting Micro soft Internet Explorer 6 on Windows XP 1:30006 Drop and generate

events

events

EXPLOIT-KIT Hello/LightsOut exploit kit - exploit targeting Micro soft Internet Explorer 7 on Windows XP with Java before v1.7.17 1:30007

Drop and generate events

EXPLOIT-KIT Hello/LightsOut exploit kit - exploit targeting Micro soft Internet Explorer 8 on Windows XP 1:30008 Drop and generate

events

EXPLOIT-KIT Hello/LightsOut exploit kit Java download attempt 1:3 0002 Drop and generate

events

EXPLOIT-KIT Hello/LightsOut exploit kit landing page detected 1:3 0001 Drop and generate

events

EXPLOIT-KIT Hello/LightsOut exploit kit payload download attempt 1:30003 Drop and generate

events

EXPLOIT-KIT Hellspawn exploit kit landing page detected 1:32554 Drop and generate

events

EXPLOIT-KIT Hellspawn exploit kit outbound Oracle Java jar reques t 1:32555 Generate events

EXPLOIT-KIT HiMan exploit kit Flash Exploit landing page 1:28963 Drop and generate

events

EXPLOIT-KIT Himan exploit kit landing page 1:28307 Drop and generate

events

EXPLOIT-KIT HiMan exploit kit outbound exploit retrieval connecti on 1:28967 Drop and generate

events

EXPLOIT-KIT HiMan exploit kit outbound flash exploit retrieval at tempt 1:28968 Drop and generate

events

EXPLOIT-KIT HiMan exploit kit outbound payload retreival - specif ic string 1:28969 Drop and generate

events

EXPLOIT-KIT HiMan exploit kit outbound POST connection 1:28966 Drop and generate

events

EXPLOIT-KIT Himan exploit kit payload - Adobe Reader compromise 1 :28308 Drop and generate

events

EXPLOIT-KIT Himan exploit kit payload - Oracle Java compromise 1: 28309 Drop and generate

events

EXPLOIT-KIT Himan exploit kit payload - Oracle Java compromise 1: 28310 Drop and generate

events

EXPLOIT-KIT Hunter exploit kit landing page detected 1:36543 Drop and generate

events

EXPLOIT-KIT iFramer injection - specific structure 1:26540 Drop and generate

events

EXPLOIT-KIT iFramer injection - specific structure 1:26617 Drop and generate

events

EXPLOIT-KIT IFRAMEr injection detection - leads to exploit kit 1: 26338 Drop and generate

events

EXPLOIT-KIT iFRAMEr successful cnt.php redirection 1:28796 Generate events

EXPLOIT-KIT IFRAMEr Tool embedded javascript attack method - spec ific structure 1:27734 Drop and generate

events

EXPLOIT-KIT iFramer toolkit injected iframe detected - specific s tructure 1:27271 Drop and generate

events

EXPLOIT-KIT Impact exploit kit landing page 1:26252 Drop and generate

events

EXPLOIT-KIT Impact/Stamp exploit kit landing page 1:26599

EXPLOIT-KIT Impact/Stamp exploit kit landing page 1:26600 Drop and generate

events

EXPLOIT-KIT Java User-Agent downloading Portable Executable - Pos sible exploit kit 1:25042 Drop and generate

events

EXPLOIT-KIT JDB exploit kit landing page retrieval 1:25559 Drop and generate

events

EXPLOIT-KIT JDB exploit kit landing page 1:25560 Drop and generate

events

EXPLOIT-KIT JDB exploit kit landing page 1:25561 Drop and generate

events

EXPLOIT-KIT KaiXin exploit kit attack vector attempt 1:24667 Drop and generate

events

EXPLOIT-KIT KaiXin exploit kit attack vector attempt 1:24668 Drop and generate

events

EXPLOIT-KIT KaiXin exploit kit Java Class download 1:24793 Drop and generate

events

EXPLOIT-KIT known malicious javascript packer detected 1:32804 Drop and generate

events

EXPLOIT-KIT Known malicious redirection attempt 1:38254 Drop and generate

events

EXPLOIT-KIT Kore exploit kit landing page 1:27695 Drop and generate

events

EXPLOIT-KIT Kore exploit kit landing page 1:27696 Drop and generate

events

EXPLOIT-KIT Kore exploit kit outbound payload download attempt 1: 27873 Drop and generate

events

EXPLOIT-KIT Kore exploit kit successful Java exploit 1:27697 Drop and generate

events

EXPLOIT-KIT Magnitude exploit kit embedded redirection attempt 1: 28413 Drop and generate

events

EXPLOIT-KIT Magnitude exploit kit Internet Explorer exploit attempt 1:37918 Drop and generate

events

EXPLOIT-KIT Magnitude exploit kit landing page 1:30766 Drop and generate

events

EXPLOIT-KIT Magnitude exploit kit Microsoft Internet Explorer Pay load request 1:29189 Generate events

EXPLOIT-KIT Magnitude exploit kit Oracle Java payload request 1:3 0767 Drop and generate

events

EXPLOIT-KIT Magnitude exploit kit Oracle Java payload request 1:3 0768 Drop and generate

events

EXPLOIT-KIT Magnitude/Nuclear exploit kit landing page 1:28236 Drop and generate

events

EXPLOIT-KIT Magnitude/Nuclear exploit kit outbound pdf download attempt 1:28237 Generate events

EXPLOIT-KIT Magnitude/Popads/Nuclear exploit kit jnlp request 1:2 8029 Drop and generate

events

EXPLOIT-KIT Malicious iFrame redirection injection attempt 1:3754 8 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit 32-alpha jar request 1:25798 Generate events

EXPLOIT-KIT Multiple exploit kit binkey xored binary download att empt 1:28797 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit flash file download 1:31902 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit flash file download 1:31903 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit jar file dropped 1:25803 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit java payload detection 1:26509 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit landing page - specific structur e 1:26535 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit landing page - specific structur e 1:26653 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit landing page 1:27738 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit malicious jar archive download 1 :25302 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit malicious jar file downloaded wh en exe is declared 1:27108 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - about.dll 1: 27894 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - about.exe 1: 25386 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - calc.dll 1:2 7897 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - calc.exe 1:2 5385 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - contacts.dll 1:27896 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - contacts.exe 1:25384 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - info.dll 1:2 6508 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - info.dll 1:2 7895 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - info.exe 1:2 5383 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - readme.dll 1 :27898 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Payload detection - readme.exe 1 :25387 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit payload download - scandsk.exe 1 :29447 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit payload download 1:28593 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Portable Executable downloaded w hen mp3 is declared 1:27005 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit possibly malicious iframe embedd ed into a webpage 1:28798 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit redirection gate 1:30920 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit redirection page 1:27739 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit Silverlight exploit download 1:2 8612 Drop and generate

events

EXPLOIT-KIT Multiple exploit kit single digit exe detection 1:284 23 Drop and generate

EXPLOIT-KIT Nailed exploit kit Firefox exploit download - autopwn 1:27080 Drop and generate

events

EXPLOIT-KIT Nailed exploit kit flash remote code execution exploi t download - autopwn 1:27082 Drop and generate

events

EXPLOIT-KIT Nailed exploit kit Internet Explorer exploit download - autopwn 1:27081 Drop and generate EXPLOIT-KIT Nailed exploit kit jmxbean remote code execution expl oit download - autopwn 1:27083 Drop and generate EXPLOIT-KIT Nailed exploit kit landing page - specific structure 1:27078 Drop and generate

events

events

events

EXPLOIT-KIT Nailed exploit kit landing page stage 2 1:27079 Drop and generate

events

EXPLOIT-KIT Nailed exploit kit rhino remote code execution exploi t download - autopwn 1:27084 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit gate detected 1:36492 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit initial outbound request - gener ic detection 1:28911 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit landing page detected 1:36535 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit landing page 1:37207 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit landing page 1:27026 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit landing page 1:26095 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit landing page 1:26096 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit outbound plugin detection respon se - generic detection 1:28474 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit outbound request - generic detec tion 1:28475 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit outbound request by Java - gener ic detection 1:28476 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit plugin detection page 1:27783 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit redirection attempt 1:38275 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit redirection page 1:26099 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit redirection page 1:26100 Drop and generate

events

EXPLOIT-KIT Neutrino exploit kit redirection received 1:28213 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit Adobe Flash download 1:32995 Drop and generate

events

EXPLOIT-KIT Nuclear Exploit Kit back end communications attempt 1 :38592 Drop and generate

events

EXPLOIT-KIT Nuclear Exploit Kit back end communications attempt 1 :38593 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit flash file download 1:33981 Drop and generate

EXPLOIT-KIT Nuclear exploit kit landing page - specific structure 1:26342 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page detected 1:33982 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page detected 1:35845 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page detected 1:24888 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page detected 1:32388 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page detection 1:31734 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page 1:26341 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit landing page 1:26343 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit Microsoft Internet Explorer vulne rability request 1:28594 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit Microsoft Internet Explorer vulne rability request 1:28424 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit obfuscated file download 1:33983 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit Oracle Java jar file retrieval 1: 28595 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound connection 1:29186 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound jar request 1:30219 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound Microsoft Silverlight ex ploit request 1:32876 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound Oracle Java request 1:32 389 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound payload request 1:30220 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound PDF request 1:30937 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound pdf request 1:29187 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound structure 1:32386 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit outbound uri request attempt 1:37 528 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit payload delivery 1:32879 Drop and generate

events

EXPLOIT-KIT Nuclear exploit kit payload request 1:28596 Drop and generate

events

EXPLOIT-KIT Nuclear landing page detected 1:37550 Drop and generate

events

EXPLOIT-KIT Nuclear landing page detected 1:37551 Drop and generate

events

EXPLOIT-KIT Nuclear Pack exploit kit binary download 1:23157 Drop and generate

events

EXPLOIT-KIT Nuclear/Magnitude exploit kit Adobe Flash exploit dow nload attempt 1:28108 Drop and generate

events

EXPLOIT-KIT Nuclear/Magnitude exploit kit Oracle Java exploit dow nload attempt 1:28414 Drop and generate

events

EXPLOIT-KIT Nuclear/Magnitude exploit kit post Java compromise do wnload attempt 1:28111 Drop and generate

events

EXPLOIT-KIT Oracle Java Jar file downloaded when zip is defined 1 :26292 Drop and generate

events

EXPLOIT-KIT Portable Executable downloaded with bad DOS stub 1:26 526 Drop and generate

events

EXPLOIT-KIT Possible exploit kit post compromise activity - StrRe verse 1:21874 Drop and generate

events

EXPLOIT-KIT Possible exploit kit post compromise activity - taskk ill 1:21875 Drop and generate

events

EXPLOIT-KIT Private exploit kit landing page 1:27141 Drop and generate

events

EXPLOIT-KIT Private exploit kit landing page 1:27142 Drop and generate

events

EXPLOIT-KIT Private exploit kit landing page 1:27143 Drop and generate

events

EXPLOIT-KIT Private exploit kit outbound traffic 1:27144 Generate events

EXPLOIT-KIT ProPack exploit kit outbound connection attempt 1:249 77 Drop and generate

events

EXPLOIT-KIT ProPack exploit kit outbound connection 1:24979 Drop and generate

events

EXPLOIT-KIT ProPack exploit kit outbound payload request 1:24978 Drop and generate

events

EXPLOIT-KIT Pseudo-Darkleech gate redirect attempt 1:39677 Drop and generate

events

EXPLOIT-KIT Qadars exploit kit attempt 1:48440 Drop and generate

events

EXPLOIT-KIT Rawin exploit kit outbound java retrieval 1:26985 Drop and generate

events

EXPLOIT-KIT Red Dot executable retrieval attempt 1:25540 Drop and generate

events

EXPLOIT-KIT Red Dot java retrieval attempt 1:25539 Drop and generate

events

EXPLOIT-KIT Red Dot landing page 1:25538 Drop and generate

events

EXPLOIT-KIT redirect to malicious java archive attempt 1:25301 Drop and generate

events

EXPLOIT-KIT redirection to driveby download 1:25948 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit encrypted binary download 1:26805 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit java exploit delivery 1:26348 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit Java Exploit request to .class fil e 1:23219 Generate events

EXPLOIT-KIT Redkit exploit kit java exploit request 1:26377 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit Java Exploit Requested - 5 digit j ar 1:23220 Generate events

EXPLOIT-KIT Redkit exploit kit landing page Received - applet and 5 digit jar attempt 1:23222 Generate events

EXPLOIT-KIT Redkit exploit kit landing page Received - applet and flowbit 1:23225 Generate events

EXPLOIT-KIT Redkit exploit kit landing page redirection 1:26344 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit landing page 1:26383 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit landing page 1:26384 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit landing page 1:26345 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit landing page 1:25988 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit landing page 1:26807 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit obfuscated portable executable 1:2 6349 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit payload request 1:29864 Drop and generate

events

EXPLOIT-KIT Redkit exploit kit redirection attempt 1:25255 Drop and generate

events

EXPLOIT-KIT Redkit Repeated Exploit Request Pattern 1:23218 Generate events

EXPLOIT-KIT Rig Exploit Kit landing page obfuscation detected 1:4 1092 Drop and generate

events

EXPLOIT-KIT Rig exploit kit outbound communication 1:33905 Drop and generate

events

EXPLOIT-KIT Rig exploit kit outbound communication 1:33906 Drop and generate

events

EXPLOIT-KIT Rig exploit kit outbound communication 1:40753 Drop and generate

events

EXPLOIT-KIT Rig exploit kit outbound Microsoft Silverlight reques t 1:31369 Drop and generate

events

EXPLOIT-KIT RIG exploit kit shellcode detected 1:43931 Drop and generate

events

EXPLOIT-KIT Rig Exploit Kit URL outbound communication 1:42806 Drop and generate

events

EXPLOIT-KIT Rig exploit kit URL outbound communication 1:41783 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit Atomic exploit download - specific -structure 1:28608 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit exploit payload retrieve attempt 1 :28450 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit exploit request 1:26293 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit jar download detection 1:26537 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit landing page received 1:26538 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit logo transfer 1:21510 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit obfuscated exploit payload downloa d 1:28609 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit outbound connection attempt 1:2861 1 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit pdf download detection 1:26539 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit redirection structure 1:26511 Drop and generate

events

EXPLOIT-KIT Sakura exploit kit successful redirection 1:28038 Drop and generate

events

EXPLOIT-KIT Sakura exploit outbound connection attempt 1:28449 Drop and generate

events

EXPLOIT-KIT Scanbox exploit kit enumeration code detected 1:31857 Drop and generate

events

EXPLOIT-KIT Scanbox exploit kit exfiltration attempt 1:36201 Drop and generate

events

EXPLOIT-KIT Scanbox exploit kit exfiltration attempt 1:31859 Drop and generate

events

EXPLOIT-KIT SET java applet load attempt 1:23106 Drop and generate

events

EXPLOIT-KIT Sibhost exploit kit outbound JAR download attempt 1:2 4841 Drop and generate

events

EXPLOIT-KIT Sibhost exploit kit 1:26020 Drop and generate

events

EXPLOIT-KIT SofosFO/Stamp exploit kit plugin detection page 1:303 06 Drop and generate

events

EXPLOIT-KIT SPL2 exploit kit jar exploit download 1:29003 Drop and generate

events

EXPLOIT-KIT SPL2 exploit kit landing page detection 1:29001 Drop and generate

events

EXPLOIT-KIT SPL2 exploit kit Silverlight plugin outbound connecti on attempt 1:29002 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit jar exploit download - specific str ucture 1:29129 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit jar file request 1:25801 Generate events

EXPLOIT-KIT Stamp exploit kit landing page 1:30133 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit landing page 1:26536 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit malicious payload delivery - specif ic string 1:30134 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit malicious payload download attempt 1:29130 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit PDF exploit retrieval attempt 1:291 31 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit pdf request 1:25799 Generate events

EXPLOIT-KIT Stamp exploit kit plugin detection page 1:29128 Drop and generate

events

EXPLOIT-KIT Stamp exploit kit portable executable download 1:2653 4 Generate events

EXPLOIT-KIT Styx exploit kit fonts download page 1:29445 Drop and generate

events

EXPLOIT-KIT Styx exploit kit jar outbound connection 1:29446 Generate events

EXPLOIT-KIT Styx exploit kit jar outbound connection 1:25137 Generate events

EXPLOIT-KIT Styx exploit kit landing page request 1:29452 Drop and generate

events

EXPLOIT-KIT Styx exploit kit landing page with payload 1:27813 Drop and generate

events

EXPLOIT-KIT Styx exploit kit landing page 1:29448 Drop and generate

events

EXPLOIT-KIT Styx exploit kit landing page 1:29449 Drop and generate

events

EXPLOIT-KIT Styx exploit kit landing page 1:26090 Drop and generate

events

EXPLOIT-KIT Styx exploit kit landing page 1:27935 Drop and generate

events

EXPLOIT-KIT Styx exploit kit malicious redirection attempt 1:2781 5 Drop and generate

events

EXPLOIT-KIT Styx exploit kit outbound connection attempt 1:29450 Drop and generate

events

EXPLOIT-KIT Styx exploit kit outbound pdf request 1:28477 Generate events

EXPLOIT-KIT Styx exploit kit plugin detection connection jlnp 1:2 7041 Drop and generate

events

EXPLOIT-KIT Styx exploit kit plugin detection connection jorg 1:2 7040 Drop and generate

events

EXPLOIT-KIT Styx exploit kit plugin detection connection jovf 1:2 7042 Drop and generate

events

EXPLOIT-KIT Styx exploit kit plugin detection connection 1:25136 Drop and generate

events

EXPLOIT-KIT Styx exploit kit portable executable download request 1:25140 Drop and generate

events

EXPLOIT-KIT Styx exploit kit portable executable download 1:27936 Drop and generate

events

EXPLOIT-KIT Styx exploit kit redirection page 1:26297 Drop and generate

events

EXPLOIT-KIT Sundown exploit kit landing page detected 1:40233 Drop and generate

events

EXPLOIT-KIT Sundown Exploit Kit redirection attempt 1:41035 Drop and generate

events

EXPLOIT-KIT Suspicious StrReverse - Scripting.FileSystemObject 1: 23149 Drop and generate

events

EXPLOIT-KIT Suspicious StrReverse - Shell 1:23148 Drop and generate

events

EXPLOIT-KIT Suspicious taskkill script - StrReverse 1:23147 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit java compromise successful 1 :28264 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page - JAR redirecti on 1:24840 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page - specific stru cture 1:25389 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page - specific stru cture 1:25390 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page - specific stru cture 1:24839 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page - specific stru cture 1:25044 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page attempt 1:28265 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page in.php base64 u ri 1:26834 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page 1:26232 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit landing page 1:26233 Drop and generate

events

EXPLOIT-KIT Sweet Orange exploit kit outbound connection on non-s tandard port 1:31769 Generate events

EXPLOIT-KIT TDS redirection - may lead to exploit kit 1:26350 Drop and generate

events

EXPLOIT-KIT Teletubbies exploit kit exploit attempt for Adobe Acr obat Reader 8 1:27879 Generate events

EXPLOIT-KIT Teletubbies exploit kit exploit attempt for Adobe Acr obat Reader 9 1:27880 Generate events

EXPLOIT-KIT Teletubbies exploit kit exploit attempt for Adobe Acr obat Reader 1:27892 Generate events

EXPLOIT-KIT Teletubbies exploit kit exploit attempt for Adobe Fla sh Player 1:27881 Generate events

EXPLOIT-KIT Teletubbies exploit kit exploit attempt for Adobe Fla sh Player 1:27882 Generate events

EXPLOIT-KIT Teletubbies exploit kit exploit attempt for Oracle Ja va 1:27883 Generate events

EXPLOIT-KIT Teletubbies exploit kit payload download 1:27885 Generate events

EXPLOIT-KIT Teletubbies exploit kit payload download 1:27886 Generate events

EXPLOIT-KIT Teletubbies exploit kit payload download 1:27887 Generate events

EXPLOIT-KIT Teletubbies exploit kit payload download 1:27888 Generate events

EXPLOIT-KIT Teletubbies exploit kit payload download 1:27889 Generate events

EXPLOIT-KIT Teletubbies exploit kit payload download 1:27893 Generate events

EXPLOIT-KIT Teletubbies exploit kit secondary payload 1:27890 Generate events

EXPLOIT-KIT Teletubbies exploit kit secondary payload 1:27891 Generate events

EXPLOIT-KIT Terror EK dll download attempt 1:45923 Drop and generate

events

EXPLOIT-KIT Terror EK exe download attempt 1:45922 Drop and generate

events

EXPLOIT-KIT Terror EK page access attempt 1:45925 Drop and generate

events

EXPLOIT-KIT TERROR exploit kit FlashVars parameter shellcode 1:43 932 Drop and generate

events

EXPLOIT-KIT Topic exploit kit outbound connection - 1 1:26956 Drop and generate

events

EXPLOIT-KIT Topic exploit kit outbound connection - 2 1:26957 Drop and generate

events

EXPLOIT-KIT Topic exploit kit outbound connection - 3 1:26958 Drop and generate

events

EXPLOIT-KIT Topic exploit kit outbound connection - 4 1:26959 Drop and generate

events

EXPLOIT-KIT Unix.Backdoor.Cdorked possible blackhole request atte mpt 1:26527 Drop and generate

events

EXPLOIT-KIT Unknown exploit kit redirection page 1:24344 Drop and generate

events

EXPLOIT-KIT unknown exploit kit script injection attempt 1:26591 Drop and generate

events

EXPLOIT-KIT Unknown Malvertising exploit kit Hostile Jar pipe.cla ss 1:27085 Drop and generate

events

EXPLOIT-KIT Unknown Malvertising exploit kit stage-1 redirect 1:2 7086 Drop and generate

events

EXPLOIT-KIT URI request for known malicious URI /stat2.php 1:2055 8 Drop and generate

events

EXPLOIT-KIT Whitehole exploit kit Java exploit retrieval 1:25805 Drop and generate

events

EXPLOIT-KIT Whitehole exploit kit landing page 1:25806 Drop and generate

events

EXPLOIT-KIT Whitehole exploit kit malicious jar download attempt 1:25804 Drop and generate

events

EXPLOIT-KIT WhiteLotus exploit kit plugin outbound detection 1:30 312 Drop and generate

events

EXPLOIT-KIT X2O exploit kit landing page 1:28194 Drop and generate

events

EXPLOIT-KIT X2O exploit kit landing page 1:27911 Drop and generate

events

EXPLOIT-KIT X2O exploit kit landing page 1:27912 Drop and generate

events

EXPLOIT-KIT X2O exploit kit post java exploit download attempt 1: 28195 Drop and generate

events

EXPLOIT-KIT Zuponcic exploit kit landing page 1:26960 Drop and generate

events

EXPLOIT-KIT Zuponcic exploit kit Oracle Java file download 1:2576 4 Drop and generate

events

FILE-EXECUTABLE Adobe Reader AcroBroker registry value out of bou nds attempt 1:34466 Drop and generate

events

FILE-EXECUTABLE Ichitaro JSMISC32.dll dll-load exploit attempt 1: 26070 Drop and generate FILE-EXECUTABLE Invincea Dell Protected Workspace InvProtectDrv s andbox escape attempt 1:41312 Drop and generate FILE-EXECUTABLE Invincea-X SboxDrv.sys local privilege escalation attempt 1:41306 Drop and generate

events

events

events

FILE-EXECUTABLE Microsoft CLFS.sys information leak attempt 1:409 36 Drop and generate

events

FILE-EXECUTABLE Microsoft CLFS.sys information leak attempt 1:409 37 Drop and generate

events

FILE-EXECUTABLE Microsoft Windows NTFS privilege escalation attempt 1:48057 Drop and generate

events

FILE-EXECUTABLE Microsoft Windows NTFS privilege escalation attempt 1:48058 Drop and generate

events

FILE-EXECUTABLE Microsoft Windows Win32k privilege escalation att empt 1:47503 Drop and generate

events

FILE-EXECUTABLE Microsoft Windows Win32k privilege escalation att empt 1:47504 Drop and generate

events

FILE-EXECUTABLE Norton Antivirus ASPack heap corruption attempt 3 :39379 Drop and generate

events

FILE-EXECUTABLE Nvidia Windows kernel mode driver denial of servi ce attempt 1:40934 Drop and generate

events

FILE-EXECUTABLE Win.Ransomware.Rapid download attempt 1:46396 Drop and generate

events

FILE-EXECUTABLE Win.Ransomware.Rapid download attempt 1:46397 Drop and generate

events

FILE-EXECUTABLE Win.Trojan.CoinMiner attempted download 1:45548 Drop and generate

events

FILE-FLASH Acrobat Flash FileReference class use-after-free memor y corruption attempt 1:41160 Drop and generate

events

FILE-FLASH Acrobat Flash FileReference class use-after-free memor y corruption attempt 1:41165 Drop and generate

events

FILE-FLASH Acrobat Flash WorkerDomain memory corruption attempt 1 :41014 Drop and generate

events

FILE-FLASH Adobe Acrobat Reader profile use after free attempt 1: 43395 Drop and generate

events

FILE-FLASH Adobe ActionScript malformed pushwith opcode attempt 1 :32764 Drop and generate

events

FILE-FLASH Adobe Adobe Flash Player ActionExtends use after free attempt 1:40738 Drop and generate

events

FILE-FLASH Adobe AS3 decompressed pcre assertion out of bounds co rruption attempt 1:31351 Drop and generate

events

FILE-FLASH Adobe AS3 decompressed pcre assertion out of bounds co rruption attempt 1:31353 Drop and generate

events

FILE-FLASH Adobe AS3 pcre assertion out of bounds corruption atte mpt 1:31347 Drop and generate

events

FILE-FLASH Adobe AS3 simplified pcre assertion out of bounds corruption attempt 1:31349 Drop and generate

events

FILE-FLASH Adobe Flash AWM2 out of bounds corruption attempt 1:33 176 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:32097 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:37644 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36160 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36161 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36162 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36163 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36164 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36165 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36166 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36167 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:36168 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:37708 Drop and generate

events

FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow att empt 1:37709 Drop and generate

events

FILE-FLASH Adobe Flash custom TextField filter use after free att empt 1:34853 Drop and generate

events

FILE-FLASH Adobe Flash FPU stack corruption attempt 1:34816 Drop and generate

events

FILE-FLASH Adobe Flash malformed pixel bytecode attempt 1:34272 Drop and generate

events

FILE-FLASH Adobe Flash malformed pixel bytecode attempt 1:34274 Drop and generate

events

FILE-FLASH Adobe Flash malformed regular expression exploit attempt 1:28619 Drop and generate

events

FILE-FLASH Adobe Flash malformed regular expression exploit attempt 1:28699 Drop and generate

events

FILE-FLASH Adobe Flash malformed regular expression exploit attempt 1:28700 Drop and generate

events

FILE-FLASH Adobe Flash malformed regular expression exploit attempt 1:25676 Drop and generate

events

FILE-FLASH Adobe Flash malformed regular expression exploit attempt 1:30754 Drop and generate

events

FILE-FLASH Adobe Flash MovieClip proto chain manipulation targeti ng constructor use after free attempt 1:40734 Drop and generate FILE-FLASH Adobe Flash Player Primetime SDK AdvertisingMetadata type confustion attempt 1:40736 Drop and generate FILE-FLASH Adobe Flash Player ABRControlParameters access memory corruption attempt 1:39689 Drop and generate FILE-FLASH Adobe Flash Player ABRControlParameters access memory corruption attempt 1:39691 Drop and generate FILE-FLASH Adobe Flash Player ABRControlParameters access memory corruption attempt 1:39692 Drop and generate FILE-FLASH Adobe Flash Player ABRControlParameters access memory corruption attempt 1:39693 Drop and generate FILE-FLASH Adobe Flash Player ABRControlParameters access memory corruption attempt 1:39694 Drop and generate FILE-FLASH Adobe Flash Player ActionPush out of bounds read attempt 1:42800 Drop and generate

events

events

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player ActionScript 3 URLRequest class use after free attempt 1:37793 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript AVSS memory corruption attempt 1:34502 Drop and generate FILE-FLASH Adobe Flash Player ActionScript bytecode object type c onfusion information disclosure attempt 1:29835 Drop and generate FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt - dear chu.rar 1:20779 Drop and generate FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt - economy.rar 1:20778 Drop and generate FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt - namelist.xls 1:20780 Drop and generate FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt 1:28695 Drop and generate

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt 1:28696 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt 1:20131 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript callMethod type confus ion attempt 1:20781 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript constructor use after free attempt 1:37772 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript constructor use after free attempt 1:37774 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript memory corruption atte mpt 1:33899 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript memory corruption atte mpt 1:33901 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript ProgressBar use after free attempt 1:36897 Drop and generate FILE-FLASH Adobe Flash Player ActionScript user-supplied PCM resa mpling integer overflow attempt 1:27267 Drop and generate FILE-FLASH Adobe Flash Player ActionScript worker use after free attempt 1:36507 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player ActionScript worker use after free attempt 1:33459 Drop and generate

events

FILE-FLASH Adobe Flash Player ActionScript worker use after free attempt 1:33460 Drop and generate

events

FILE-FLASH Adobe Flash Player AdBreakPlacement object memory corruption attempt 1:39554 Drop and generate

events

FILE-FLASH Adobe Flash Player addCallback use after free attempt 1:40740 Drop and generate

events

FILE-FLASH Adobe Flash Player addProperty use after free attempt 1:38996 Drop and generate

events

FILE-FLASH Adobe Flash Player addProperty use after free attempt 1:38997 Drop and generate

events

FILE-FLASH Adobe Flash Player AdTimelineItem object memory corrup tion attempt 1:39548 Drop and generate

events

FILE-FLASH Adobe Flash Player AdvertisingMetadata use after free attempt 1:43382 Drop and generate

events

FILE-FLASH Adobe Flash Player allocator use-after-free attempt 1: 42206 Drop and generate

events

FILE-FLASH Adobe Flash Player and AIR type confusion remote code execution attempt 1:29047 Drop and generate

events

FILE-FLASH Adobe Flash Player and AIR type confusion remote code execution attempt 1:29049 Drop and generate

events

FILE-FLASH Adobe Flash Player and AIR type confusion remote code execution attempt 1:29051 Drop and generate

events

FILE-FLASH Adobe Flash Player and AIR type confusion remote code execution attempt 1:29054 Drop and generate

events

FILE-FLASH Adobe Flash Player and AIR type confusion remote code execution attempt 1:36527 Drop and generate

events

FILE-FLASH Adobe Flash Player and AIR type confusion remote code execution attempt 1:36528 Drop and generate

events

FILE-FLASH Adobe Flash Player applyFilter memory corruption attempt 1:43479 Drop and generate

events

FILE-FLASH Adobe Flash Player array type confusion attempt 1:4458 3 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 actionExtends use-after-free at tempt 1:36827 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 actionExtends use-after-free at tempt 1:36829 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 actionExtends use-after-free at tempt 1:36830 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 custom getter addProperty use a fter free attempt 1:40218 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 setInterval use after free atte mpt 1:38185 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 setInterval use after free atte mpt 1:38186 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 setTransform use-after-free att empt 1:37128 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 TextField antiAliasType use aft er free attempt 1:41485 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 TextField gridFitType use after free attempt 1:36844 Drop and generate

events

FILE-FLASH Adobe Flash Player AS2 valueOf function assignment wit h removeTextField use after free attempt 1:36873 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 multiple axis attributes intege r overflow attempt 1:38181 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 multiple axis attributes intege r overflow attempt 1:38182 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:36124 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:36125 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:36128 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:36819 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:36820 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:35449 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:35450 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 opaqueBackground use-after-free attempt 1:35453 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 regex sign-extension denial of service attempt 1:33300 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 regex sign-extension denial of service attempt 1:33301 Drop and generate

events

FILE-FLASH Adobe Flash Player AS3 regex sign-extension denial of service attempt 1:39560 Drop and generate FILE-FLASH Adobe Flash Player AS3 regular expression grouping dep th denial of service attempt 1:32534 Drop and generate FILE-FLASH Adobe Flash Player AS3 regular expression grouping dep th denial of service attempt 1:32535 Drop and generate FILE-FLASH Adobe Flash Player AS3 regular expression grouping dep th denial of service attempt 1:32536 Drop and generate FILE-FLASH Adobe Flash Player ASnative custom getter use after free attempt 1:37768 Drop and generate

events

events

events

events

events

FILE-FLASH Adobe Flash Player ASnative custom getter use after free attempt 1:37771 Drop and generate

events

FILE-FLASH Adobe Flash Player ASnative memory corruption attempt 1:37780 Drop and generate

events

FILE-FLASH Adobe Flash Player ASnative MovieClip type confusion attempt 1:46598 Drop and generate

events

FILE-FLASH Adobe Flash Player ASnative MovieClip type confusion attempt 1:46599 Drop and generate FILE-FLASH Adobe Flash Player ASnative previously set SharedObjec t variable set attempt 1:35642 Drop and generate FILE-FLASH Adobe Flash Player ASnative previously set SharedObjec t variable set attempt 1:35644 Drop and generate FILE-FLASH Adobe Flash Player ASnative previously set SharedObjec t variable set attempt 1:35691 Drop and generate FILE-FLASH Adobe Flash Player ASnative previously set SharedObjec t variable set attempt 1:35693 Drop and generate

events

events

events

events

events

FILE-FLASH Adobe Flash player ASNative textField use after free attempt 1:37679 Drop and generate

events

FILE-FLASH Adobe Flash Player ASnative use after free attempt 1:3 7789 Drop and generate

events

FILE-FLASH Adobe Flash Player ASnative use after free attempt 1:3 7790 Drop and generate

events

FILE-FLASH Adobe Flash Player assertion out of bounds corruption attempt 1:36597 Drop and generate

events

FILE-FLASH Adobe Flash Player assertion out of bounds corruption attempt 1:36599 Drop and generate

events

FILE-FLASH Adobe Flash Player ASSetNative use-after-free attempt 1:39030 Drop and generate

events

FILE-FLASH Adobe Flash Player ASSetNative use-after-free attempt 1:39032 Drop and generate

events

FILE-FLASH Adobe Flash Player ASSetNativeAccessor use after free attempt 1:38792 Drop and generate FILE-FLASH Adobe Flash Player asynchronous shader changes memory corruption attempt 1:34561 Drop and generate FILE-FLASH Adobe Flash Player asynchronous shader changes memory corruption attempt 1:34563 Drop and generate FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:37925 Drop and generate

events

events

events

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:37926 Drop and generate

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:37927 Drop and generate

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:37722 Drop and generate

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:32226 Drop and generate

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:32228 Drop and generate

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:40009 Drop and generate

events

FILE-FLASH Adobe Flash Player atomicCompareAndSwapLength integer overflow attempt 1:36875 Drop and generate

events

FILE-FLASH Adobe Flash Player attachsound use-after-free attempt 1:36861 Drop and generate

events

FILE-FLASH Adobe Flash Player attachsound use-after-free attempt 1:36863 Drop and generate

events

FILE-FLASH Adobe Flash Player AuditudeSettings stack overflow att empt 1:42012 Drop and generate FILE-FLASH Adobe Flash Player AuthorizedFeaturesLoader object mem ory corruption attempt 1:34186 Drop and generate FILE-FLASH Adobe Flash Player AuthorizedFeaturesLoader object mem ory corruption attempt 1:34187 Drop and generate FILE-FLASH Adobe Flash Player AVC parser integer overflow attempt 1:34264 Drop and generate

events

events

events

events

FILE-FLASH Adobe Flash Player AVC parser integer overflow attempt 1:34265 Drop and generate

events

FILE-FLASH Adobe Flash Player avc\_core out of bounds memory acces s attempt 1:36287 Drop and generate

events

FILE-FLASH Adobe Flash Player AVM domain memory range integer ove rflow attempt 1:37195 Drop and generate

events

FILE-FLASH Adobe Flash Player AVSegmentedSource caption unlink us e-after-free attempt 1:33918 Drop and generate

events

FILE-FLASH Adobe Flash Player AVSegmentedSource caption unlink us e-after-free attempt 1:33919 Drop and generate FILE-FLASH Adobe Flash Player AVSegmentedSource null pointer atte mpt 1:36358 Drop and generate

events

events

FILE-FLASH Adobe Flash Player AVSegmentedSource use after free at tempt 1:40742 Drop and generate

events

FILE-FLASH Adobe Flash Player AVSS null pointer attempt 1:36351 Drop and generate

events

FILE-FLASH Adobe Flash Player AVSS null pointer attempt 1:36352 Drop and generate

events

FILE-FLASH Adobe Flash Player AVSS null pointer attempt 1:36353 Drop and generate

events

FILE-FLASH Adobe Flash Player beginGradientFill color array out o f bounds read attempt 1:42794 Drop and generate

events

FILE-FLASH Adobe Flash Player bitmap handling memory corruption attempt 1:35666 Drop and generate

events

FILE-FLASH Adobe Flash Player bitmap heap overflow attempt 1:3883 5 Drop and generate

events

FILE-FLASH Adobe Flash Player bitmap hitTest integer overflow att empt 1:44887 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData applyFilter heap overflo w attempt 1:35578 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData applyFilter heap overflo w attempt 1:35579 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData applyFilter integer over flow attempt 1:41010 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData method memory corruption attempt 1:37764 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData method memory corruption attempt 1:37765 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData object out of bounds acc ess attempt 1:43416 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData object out of bounds acc ess attempt 1:43417 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData object use after free at tempt 1:35584 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData object use after free at tempt 1:35586 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData out of bounds memory acc ess attempt 1:42809 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData use-after-free attempt 1 :35217 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData use-after-free attempt 1 :35219 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData.applyFilter access viola tion attempt 1:38203 Drop and generate

events

FILE-FLASH Adobe Flash Player BitmapData.copyChannel access viola tion attempt 1:38199 Drop and generate FILE-FLASH Adobe Flash Player BitmapData.paletteMap size mismatch integer overflow attempt 1:38213 Drop and generate FILE-FLASH Adobe Flash Player BitmapData.paletteMap size mismatch integer overflow attempt 1:38215 Drop and generate

events

events

events

FILE-FLASH Adobe flash player BitmapData.paletteMap use after fre e attempt 1:35465 Drop and generate

events

FILE-FLASH Adobe Flash Player BlurFilter memory corruption attemp t 1:37738 Drop and generate

events

FILE-FLASH Adobe Flash Player BlurFilter memory corruption attemp t 1:37740 Drop and generate

events

FILE-FLASH Adobe Flash Player broker arbitrary file write attempt 1:41472 Drop and generate

events

FILE-FLASH Adobe Flash Player broker arbitrary file write attempt 1:41473 Drop and generate

events

FILE-FLASH Adobe Flash Player BrokerExtTextOutW invalid string an d length parameter sandbox escape attempt 1:33977 Drop and generate FILE-FLASH Adobe Flash Player buffer overflow attempt 1:29926 Generate events

events

FILE-FLASH Adobe Flash Player buildTraitsBindings null pointer de reference attempt 1:35271 Drop and generate

events

FILE-FLASH Adobe Flash Player buildTraitsBindings null pointer de reference attempt 1:35273 Drop and generate

events

FILE-FLASH Adobe Flash Player button pointer exploit attempt 1:35 582 Drop and generate FILE-FLASH Adobe Flash Player Button.filters type confusion remot e code execution attempt 1:34520 Drop and generate FILE-FLASH Adobe Flash Player Button.filters type confusion remot e code execution attempt 1:34522 Drop and generate FILE-FLASH Adobe Flash Player byte array double free attempt 1:34 166 Drop and generate

events

events

events

events

FILE-FLASH Adobe Flash Player byte array double free attempt 1:34 168 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array memory corruption attemp t 1:37083 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array memory corruption attemp t 1:37085 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:36880 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:36883 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:33261 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:33262 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:33263 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:33264 Drop and generate

events

FILE-FLASH Adobe Flash Player byte array uncompress information d isclosure attempt 1:33265 Drop and generate

events

FILE-FLASH Adobe Flash Player ByteArray shading memory leak attempt 1:34538 Drop and generate

events

FILE-FLASH Adobe Flash Player ByteArray shading memory leak attempt 1:45743 Drop and generate

events

FILE-FLASH Adobe Flash Player ByteArray shading memory leak attempt 1:45744 Drop and generate

events

FILE-FLASH Adobe Flash Player ByteArray type confusion memory cor ruption attempt 1:39552 Drop and generate

events

FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33369 Drop and generate

events

FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33371 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33373 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33375 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33377 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33379 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33381 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33383 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33385 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33387 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33389 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33391 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33393 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33395 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33397 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33399 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33401 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33403 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33405 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33407 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:33409 Drop and generate FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory u se after free attempt 1:35048 Drop and generate FILE-FLASH Adobe Flash Player ByteArray writeByte buffer overflow attempt 1:36257 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player ByteArray writeByte buffer overflow attempt 1:36259 Drop and generate

events

FILE-FLASH Adobe Flash Player Camera use after free attempt 1:420 06 Drop and generate

events

FILE-FLASH Adobe Flash Player canvas out of bounds read attempt 1 :37240 Drop and generate

events

FILE-FLASH Adobe Flash Player CFF FeatureCount integer overflow attempt 1:25681 Drop and generate

events

FILE-FLASH Adobe Flash Player class confusion memory corruption c ompressed file attempt 1:33203 Drop and generate

events

FILE-FLASH Adobe Flash Player class scope bypass attempt 1:36311 Drop and generate

events

FILE-FLASH Adobe Flash Player class scope bypass attempt 1:36312 Drop and generate

events

FILE-FLASH Adobe Flash Player Compressed File object type confusi on attempt 1:33541 Drop and generate FILE-FLASH Adobe Flash Player compressed microphone object codec denial of service attempt 1:32542 Drop and generate FILE-FLASH Adobe Flash Player concurrent worker thread terminate use-after-free attempt 1:34819 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player concurrent worker thread terminate use-after-free attempt 1:34821 Drop and generate

events

FILE-FLASH Adobe Flash Player ContentFactory memory corruption at tempt 1:38830 Drop and generate

events

FILE-FLASH Adobe Flash Player ContentFactory memory corruption at tempt 1:38831 Drop and generate

events

FILE-FLASH Adobe Flash Player convolution filter use-after-free attempt 1:37668 Drop and generate

events

FILE-FLASH Adobe Flash Player convolution filter use-after-free attempt 1:37670 Drop and generate

events

FILE-FLASH Adobe Flash Player convolution filter use-after-free attempt 1:34190 Drop and generate

events

FILE-FLASH Adobe Flash Player convolution filter use-after-free attempt 1:34191 Drop and generate

events

FILE-FLASH Adobe Flash Player ConvolutionFilter memory corruption attempt 1:42796 Drop and generate

events

FILE-FLASH Adobe Flash Player corrupt glyph array out of bounds attempt 1:35662 Drop and generate FILE-FLASH Adobe Flash Player corrupt PNG image load out of bound s memory access attempt 1:46254 Drop and generate FILE-FLASH Adobe Flash Player corrupt PNG image load out of bound s memory access attempt 1:46255 Drop and generate FILE-FLASH Adobe Flash Player corrupt PNG image load out of bound s memory access attempt 1:38982 Drop and generate FILE-FLASH Adobe Flash Player CreateTextField use-after-free atte mpt 1:35607 Drop and generate

events

events

events

events

events

FILE-FLASH Adobe Flash Player CreateTextField use-after-free atte mpt 1:35609 Drop and generate

events

FILE-FLASH Adobe Flash Player custom object garbage collection us e after free attempt 1:42044 Drop and generate

events

FILE-FLASH Adobe Flash Player custom object garbage collection us e after free attempt 1:42045 Drop and generate

events

FILE-FLASH Adobe Flash Player custom toString and valueOf functio n attempt 1:41740 Drop and generate

events

FILE-FLASH Adobe Flash Player custom toString function attempt 1: 43420 Drop and generate

events

FILE-FLASH Adobe Flash Player custom toString function attempt 1: 41411 Drop and generate

events

FILE-FLASH Adobe Flash Player custom valueOf function attempt 1:4 1708 Drop and generate

events

FILE-FLASH Adobe Flash Player dangling bytearray pointer code execution attempt 1:35946 Drop and generate

events

FILE-FLASH Adobe Flash Player dangling bytearray pointer code execution attempt 1:35947 Drop and generate

events

FILE-FLASH Adobe Flash Player dangling bytearray pointer code execution attempt 1:35948 Drop and generate

events

FILE-FLASH Adobe Flash Player dangling bytearray pointer code execution attempt 1:35949 Drop and generate

events

FILE-FLASH Adobe Flash Player dangling bytearray pointer code execution attempt 1:37629 Drop and generate

events

FILE-FLASH Adobe Flash Player dangling bytearray pointer code execution attempt 1:37631 Drop and generate

events

FILE-FLASH Adobe Flash Player Date with invalid parameter toTimeS tring attempt 1:37220 Drop and generate FILE-FLASH Adobe Flash Player decompressed microphone object code c denial of service attempt 1:32540 Drop and generate FILE-FLASH Adobe Flash Player DefineBitsJPEG2 invalid length memo ry corruption attempt 1:42930 Drop and generate FILE-FLASH Adobe Flash Player DefineFont3 tag overly large NumGly phs out of bounds read attempt 1:45546 Drop and generate FILE-FLASH Adobe Flash Player DefineFont3 tag overly large NumGly phs out of bounds read attempt 1:45547 Drop and generate FILE-FLASH Adobe Flash Player DefineText buffer overflow attempt 1:36367 Drop and generate

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player DefineText buffer overflow attempt 1:36369 Drop and generate

events

FILE-FLASH Adobe Flash Player DeleteRangeTimelineOperation type c onfusion attempt 1:38874 Drop and generate

events

FILE-FLASH Adobe Flash Player determinePreferredLocales memory co rruption attempt 1:44891 Drop and generate FILE-FLASH Adobe Flash Player determinePreferredLocales out of bo unds memory read attempt 1:43405 Drop and generate FILE-FLASH Adobe Flash Player DisplacementMapFilter mapBitmap use after free attempt 1:37115 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player DisplacementMapFilter use-after-fre e attempt 1:40168 Drop and generate

events

FILE-FLASH Adobe Flash Player display list structure memory corru ption attempt 1:41138 Drop and generate

events

FILE-FLASH Adobe Flash Player display list use after free attempt 1:36187 Drop and generate

events

FILE-FLASH Adobe Flash Player display list use after free attempt 1:36189 Drop and generate

events

FILE-FLASH Adobe Flash Player display object mask use after free attempt 1:42815 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayList memory corruption attempt 1:36339 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayList memory corruption attempt 1:36341 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayList memory corruption attempt 1:36343 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayList memory corruption attempt 1:36345 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayObject use after free attemp t 1:43412 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayObject use after free attemp t 1:43414 Drop and generate

events

FILE-FLASH Adobe Flash Player DisplayObject use after free attemp t 1:42818 Drop and generate

events

FILE-FLASH Adobe Flash Player DRMManager memory corruption attemp t 1:40151 Drop and generate

events

FILE-FLASH Adobe Flash Player duplicateMovieClip use after free attempt 1:38411 Drop and generate

events

FILE-FLASH Adobe Flash Player EAC3 memory corruption attempt 1:34 156 Drop and generate

events

FILE-FLASH Adobe Flash Player EAC3 memory corruption attempt 1:34 158 Drop and generate

events

FILE-FLASH Adobe Flash Player event handler out of bounds memory access attempt 1:40583 Drop and generate

events

FILE-FLASH Adobe Flash Player ExecPolicy invalid string table loo kup attempt 1:39301 Drop and generate

events

FILE-FLASH Adobe Flash Player Exploit Kit decryption key detected 1:36193 Drop and generate

events

FILE-FLASH Adobe Flash Player ExportAssets count memory corruptio n attempt 1:38425 Drop and generate

events

FILE-FLASH Adobe Flash Player ExportAssets count memory corruptio n attempt 1:38426 Drop and generate

events

FILE-FLASH Adobe Flash Player extended BitmapFilter class denial of service attempt 1:33497 Drop and generate

events

FILE-FLASH Adobe Flash Player extended BitmapFilter class denial of service attempt 1:33498 Drop and generate

events

FILE-FLASH Adobe Flash Player faulty x64 support out of bounds re ad attempt 1:38837 Drop and generate

events

FILE-FLASH Adobe Flash Player file API validation bypass attempt 1:36838 Drop and generate

events

FILE-FLASH Adobe Flash Player FileReference constructor type conf usion attempt 1:35658 Drop and generate

events

FILE-FLASH Adobe Flash Player FileReference constructor type conf usion attempt 1:35660 Drop and generate

events

FILE-FLASH Adobe Flash Player FileReference type confusion attemp t 1:39956 Drop and generate

events

FILE-FLASH Adobe Flash Player FileReference type confusion attemp t 1:38881 Drop and generate

events

FILE-FLASH Adobe Flash Player FileReference type confusion attemp t 1:38882 Drop and generate

events

FILE-FLASH Adobe Flash Player FileReferenceList.browse type confu sion attempt 1:41332 Drop and generate

events

FILE-FLASH Adobe Flash Player flash settings manager double free attempt 1:34255 Drop and generate

events

FILE-FLASH Adobe Flash Player flash settings manager double free attempt 1:34256 Drop and generate

events

FILE-FLASH Adobe Flash Player flash settings manager double free attempt 1:34257 Drop and generate

events

FILE-FLASH Adobe Flash Player FlashUtil memory corruption attempt 1:33091 Drop and generate

events

FILE-FLASH Adobe Flash Player FLV invalid tag buffer overflow att empt 1:42792 Drop and generate

events

FILE-FLASH Adobe Flash Player FLV tag datasize buffer overflow at tempt 1:34270 Drop and generate

events

FILE-FLASH Adobe Flash Player FrameLabel memory corruption attemp t 1:40442 Drop and generate

events

FILE-FLASH Adobe Flash Player garbage collection use after free attempt 1:41627 Drop and generate

events

FILE-FLASH Adobe Flash Player getBounds method use after free att empt 1:37231 Drop and generate

events

FILE-FLASH Adobe Flash Player GetConsoleMode input action variabl e corruption attempt 1:36848 Drop and generate

events

FILE-FLASH Adobe Flash Player GIF sprite kernel memory leak attempt 1:34542 Drop and generate

events

FILE-FLASH Adobe Flash Player GIF sprite kernel memory leak attempt 1:34543 Drop and generate

events

FILE-FLASH Adobe Flash Player globalToLocal use-after-free attemp t 1:36850 Drop and generate

events

FILE-FLASH Adobe Flash Player globalToLocal use-after-free attemp t 1:36852 Drop and generate

events

FILE-FLASH Adobe Flash Player GlyphOffset memory disclosure attempt 1:28587 Drop and generate

events

FILE-FLASH Adobe Flash Player heap buffer overflow attempt 1:2726 5 Drop and generate FILE-FLASH Adobe Flash Player heap memory disclosure via custom v alueOf handler attempt 1:37169 Drop and generate FILE-FLASH Adobe Flash Player heap memory disclosure via custom v alueOf handler attempt 1:37171 Drop and generate FILE-FLASH Adobe Flash Player heap memory disclosure via custom v alueOf handler attempt 1:37173 Drop and generate FILE-FLASH Adobe Flash Player heap memory disclosure via custom v alueOf handler attempt 1:37175 Drop and generate FILE-FLASH Adobe Flash Player heap overflow using special charact ers with regex options attempt 1:33465 Drop and generate FILE-FLASH Adobe Flash Player heap overflow using special charact ers with regex options attempt 1:33467 Drop and generate FILE-FLASH Adobe Flash Player hitTest BitmapData object integer o verflow attempt 1:38165 Drop and generate

events

events

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player hitTest BitmapData object integer o verflow attempt 1:38166 Drop and generate

events

FILE-FLASH Adobe Flash Player hitTest BitmapData object integer o verflow attempt 1:38169 Drop and generate FILE-FLASH Adobe Flash Player HTML & Javascript SWF use-after-fre e execution attempt 1:26000 Drop and generate FILE-FLASH Adobe Flash Player HTML & Javascript SWF use-after-fre e execution attempt 1:26002 Drop and generate FILE-FLASH Adobe Flash Player HTML & Javascript SWF use-after-fre e execution attempt 1:26004 Drop and generate FILE-FLASH Adobe Flash Player HTML & Javascript SWF use-after-fre e execution attempt 1:26006 Drop and generate FILE-FLASH Adobe Flash Player HTML focus with no data denial of s ervice attempt 1:32544 Drop and generate

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player improper display list handling memo ry corruption attempt 1:37344 Drop and generate

events

FILE-FLASH Adobe Flash Player improper display list handling memo ry corruption attempt 1:37345 Drop and generate

events

FILE-FLASH Adobe Flash Player incorrect codec denial of service attempt 1:32552 Drop and generate

events

FILE-FLASH Adobe Flash Player incorrect reference to IExternaliza ble object attempt 1:35671 Drop and generate

events

FILE-FLASH Adobe Flash Player incorrect reference to IExternaliza ble object attempt 1:35673 Drop and generate

events

FILE-FLASH Adobe Flash Player integer overflow attempt 1:39438 Drop and generate

events

FILE-FLASH Adobe Flash Player integer overflow attempt 1:39439 Drop and generate

events

FILE-FLASH Adobe Flash Player integer overflow attempt 1:34553 Drop and generate

events

FILE-FLASH Adobe Flash Player integer overflow attempt 1:34555 Drop and generate

events

FILE-FLASH Adobe Flash Player integer underflow attempt 1:37806 Drop and generate

events

FILE-FLASH Adobe Flash Player integer underflow attempt 1:37808 Drop and generate

events

FILE-FLASH Adobe Flash Player integer underflow attempt 1:29631 Drop and generate

events

FILE-FLASH Adobe Flash Player integer underflow attempt 1:29634 Drop and generate

events

FILE-FLASH Adobe Flash Player integer underflow attempt 1:38311 Drop and generate

events

FILE-FLASH Adobe Flash Player integer underflow attempt 1:39458 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid BitmapData use after free attempt 1:34582 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid instruction memory corruption attempt 1:29551 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid instruction memory corruption attempt 1:29552 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid package script information use after free attempt 1:41705 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid parent pointer use after free attempt 1:37350 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid sourceRect copyPixels heap corruption attempt 1:37756 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid sourceRect copyPixels heap corruption attempt 1:37758 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid vector length memory corrup tion attempt 1:36371 Drop and generate

events

FILE-FLASH Adobe Flash Player invalid vector length memory corrup tion attempt 1:36372 Drop and generate

events

FILE-FLASH Adobe Flash Player JPEG handling memory corruption att empt 1:39656 Drop and generate

events

FILE-FLASH Adobe Flash Player JPEG-XR decode buffer overflow atte mpt 1:38407 Drop and generate

events

FILE-FLASH Adobe Flash Player JSON stringify memory corruption at tempt 1:34795 Drop and generate

events

FILE-FLASH Adobe Flash Player list filter memory corruption attempt 1:37747 Drop and generate FILE-FLASH Adobe Flash Player loadPCMFromByteArray exception null pointer access attempt 1:39567 Drop and generate FILE-FLASH Adobe Flash Player loadPCMFromByteArray exception null pointer access attempt 1:37652 Drop and generate FILE-FLASH Adobe Flash Player loadSound method use-after-free mem ory corruption attempt 1:38847 Drop and generate FILE-FLASH Adobe Flash Player loadSound type confusion attempt 1: 35813 Drop and generate

events

events

events

events

events

FILE-FLASH Adobe Flash Player loadSound type confusion attempt 1: 35815 Drop and generate

events

FILE-FLASH Adobe Flash Player loadSound use after free attempt 1: 39275 Drop and generate

events

FILE-FLASH Adobe Flash Player loadSound use after free attempt 1: 39283 Drop and generate

events

FILE-FLASH Adobe Flash Player loadSound use after free attempt 1: 39285 Drop and generate

events

FILE-FLASH Adobe Flash Player LoadVars decode use after free atte mpt 1:37208 Drop and generate

events

FILE-FLASH Adobe Flash Player LoadVars decode use after free atte mpt 1:37209 Drop and generate

events

FILE-FLASH Adobe Flash Player LoadVars use-after-free attempt 1:4 0780 Drop and generate

events

FILE-FLASH Adobe Flash Player LoadVars use-after-free attempt 1:3 7776 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-file-access security byp ass attempt 1:31839 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-file-access security byp ass attempt 1:31840 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-filesystem sandbox escap e attempt 1:40178 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-filesystem sandbox escap e attempt 1:40180 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-filesystem security bypa ss attempt 1:39540 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-filesystem security bypa ss attempt 1:39541 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-filesystem security bypa ss attempt 1:39543 Drop and generate

events

FILE-FLASH Adobe Flash Player local-with-filesystem security bypa ss attempt 1:39544 Drop and generate

events

FILE-FLASH Adobe Flash Player M3U8 parser logic memory corruption attempt 1:37177 Drop and generate

events

FILE-FLASH Adobe Flash Player M3U8 parser logic memory corruption attempt 1:37178 Drop and generate FILE-FLASH Adobe Flash Player malformed ActionSetTarget record in formation disclosure attempt 1:47127 Drop and generate FILE-FLASH Adobe Flash Player malformed ActionSetTarget record in formation disclosure attempt 1:47128 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player malformed ATF file length heap over flow attempt 1:41156 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed ATF file length load buff er overflow attempt 1:39308 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed ATF header integer overfl ow attempt 1:32567 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed ATF header integer overfl ow attempt 1:32568 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed ATF heap overflow attempt 1:39273 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed CEA-708 packet denial of service attempt 1:34251 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed DefineSprite tag memory c orruption attempt 1:41644 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed FLV file buffer overflow attempt 1:34988 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed HTML text null dereferenc e attempt 1:30535 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed HTML text null dereferenc e attempt 1:30536 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed HTML text null dereferenc e attempt 1:26687 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed JPEG information leak att empt 1:32592 Drop and generate FILE-FLASH Adobe Flash Player malformed JPEG-XR out of bounds mem ory access attempt 1:39281 Drop and generate FILE-FLASH Adobe Flash Player malformed mp4 tag memory corruption attempt 1:33998 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player malformed placeObject2 memory corru ption attempt 1:40158 Drop and generate FILE-FLASH Adobe Flash Player malformed pushcode type confusion r emote code execution attempt 1:32749 Drop and generate FILE-FLASH Adobe Flash Player malformed pushcode type confusion r emote code execution attempt 1:32750 Drop and generate FILE-FLASH Adobe Flash Player malformed regular expression use af ter free attempt 1:39299 Drop and generate

events

events

events

events

FILE-FLASH Adobe Flash Player malformed tag out of bounds read at tempt 1:39538 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed tag parsing memory corrup tion attempt 1:39565 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed TagTypeAndLength field at tempt 1:39591 Drop and generate

events

FILE-FLASH Adobe Flash Player malformed VideoFrame memory corrupt ion attempt 1:40153 Drop and generate FILE-FLASH Adobe Flash Player MediaPlayerItemLoader out of bounds memory access attempt 1:39701 Drop and generate FILE-FLASH Adobe Flash Player memory corruption attempt 1:31023 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player memory corruption attempt 1:31025 Drop and generate

events

FILE-FLASH Adobe Flash Player memory corruption attempt 1:28589 Drop and generate

events

FILE-FLASH Adobe Flash Player memory corruption attempt 1:43530 Drop and generate

events

FILE-FLASH Adobe Flash Player memory leak ASLR bypass attempt 1:3 1723 Drop and generate

events

FILE-FLASH Adobe Flash Player memory leak ASLR bypass attempt 1:3 1726 Drop and generate

events

FILE-FLASH Adobe Flash Player message handler array length overfl ow attempt 1:36586 Drop and generate

events

FILE-FLASH Adobe Flash Player message handler array length overfl ow attempt 1:36588 Drop and generate

events

FILE-FLASH Adobe Flash Player MessageChannel type confusion attempt 1:41623 Drop and generate

events

FILE-FLASH Adobe Flash Player MessageChannel use after free attempt 1:33501 Drop and generate

events

FILE-FLASH Adobe Flash Player MessageChannel use after free attempt 1:33503 Drop and generate

events

FILE-FLASH Adobe Flash Player Microsoft Internet Explorer sandbox escape attempt 1:31284 Drop and generate

events

FILE-FLASH Adobe Flash Player MMgc use-after-free attempt 1:31732 Drop and generate

events

FILE-FLASH Adobe Flash Player movie signed integer memory corrupt ion attempt 1:36295 Drop and generate

events

FILE-FLASH Adobe Flash Player movieclip attachbitmap use-after-free attempt 1:45459 Drop and generate

events

FILE-FLASH Adobe Flash Player movieclip duplicateMovieClip use-af ter-free attempt 1:45615 Drop and generate

events

FILE-FLASH Adobe Flash Player movieclip duplicateMovieClip use-af ter-free attempt 1:45616 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip method loop use-after-fre e attempt 1:39550 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip method use after free att empt 1:37229 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip object corruption use aft er free attempt 1:36842 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip object use-after-free att empt 1:39316 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip object use-after-free att empt 1:37103 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip object use-after-free att empt 1:37105 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip setMask use after free at tempt 1:37216 Drop and generate

events

FILE-FLASH Adobe Flash Player MovieClip setMask use after free at tempt 1:37217 Drop and generate

events

FILE-FLASH Adobe Flash Player MP3 ID3 data parsing heap buffer ov erflow attempt 1:37121 Drop and generate

events

FILE-FLASH Adobe Flash Player MP3 ID3 data parsing heap buffer ov erflow attempt 1:37122 Drop and generate

events

FILE-FLASH Adobe Flash Player MP3 ID3 data parsing heap buffer ov erflow attempt 1:37125 Drop and generate

events

FILE-FLASH Adobe Flash Player MP3 ID3 data parsing heap buffer ov erflow attempt 1:37149 Drop and generate

events

FILE-FLASH Adobe Flash Player MP4 atom parser memory corruption attempt 1:44348 Drop and generate

events

FILE-FLASH Adobe Flash Player mp4 trex tag heap corruption attemp t 1:34020 Drop and generate

events

FILE-FLASH Adobe Flash Player MPD use-after-free attempt 1:38205 Drop and generate

events

FILE-FLASH Adobe Flash Player MPD use-after-free attempt 1:38207 Drop and generate

events

FILE-FLASH Adobe Flash Player MPEG-4 AVC decoding out of bounds r ead attempt 1:43393 Drop and generate

events

FILE-FLASH Adobe Flash Player MSIMG32.dll dll-load exploit attemp t 1:38873 Drop and generate

events

FILE-FLASH Adobe Flash Player multiple script render display use after free attempt 1:37199 Drop and generate

events

FILE-FLASH Adobe Flash Player multiple scripts display rendering use-after-free attempt 1:38401 Drop and generate FILE-FLASH Adobe Flash Player NetConnection and NetStream type co nfusion exploit attempt 1:34807 Drop and generate FILE-FLASH Adobe Flash Player NetConnection and NetStream type co nfusion exploit attempt 1:34809 Drop and generate FILE-FLASH Adobe Flash Player NetConnection AS2 arbitrary code ex ecution attempt 1:33967 Drop and generate

events

events

events

events

FILE-FLASH Adobe Flash Player NetConnection AS2 arbitrary code ex ecution attempt 1:33968 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection AS2 arbitrary code ex ecution attempt 1:34354 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection AS2 arbitrary code ex ecution attempt 1:34355 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection AS2 arbitrary code ex ecution attempt 1:36143 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection AS2 arbitrary code ex ecution attempt 1:36144 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection object type confusion overflow attempt 1:39291 Drop and generate FILE-FLASH Adobe Flash Player NetConnection proxyType invalid val ue out of bounds read attempt 1:40998 Drop and generate FILE-FLASH Adobe Flash Player NetConnection to ColorMatrixFilter object type confusion attempt 1:38413 Drop and generate FILE-FLASH Adobe Flash Player NetConnection to ColorMatrixFilter object type confusion attempt 1:38414 Drop and generate FILE-FLASH Adobe Flash Player NetConnection type confusion attemp t 1:41418 Drop and generate

events

events

events

events

events

FILE-FLASH Adobe Flash Player NetConnection type confusion attemp t 1:35275 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection type confusion attemp t 1:35277 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection use after free attemp t 1:41012 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection use-after-free attemp t 1:35599 Drop and generate

events

FILE-FLASH Adobe Flash Player NetConnection use-after-free attemp t 1:35601 Drop and generate

events

FILE-FLASH Adobe Flash Player NetStream type confusion attempt 1: 40159 Drop and generate

events

FILE-FLASH Adobe Flash Player NetStream use after free attempt 1: 42214 Drop and generate

events

FILE-FLASH Adobe Flash Player Netstream Video null pointer derefe rence attempt 1:36318 Drop and generate

events

FILE-FLASH Adobe Flash Player NetStream.appendBytes use after fre e attempt 1:36289 Drop and generate

events

FILE-FLASH Adobe Flash Player NetStream.appendBytes use after fre e attempt 1:36291 Drop and generate

events

FILE-FLASH Adobe Flash Player object Filters type confusion use a fter free attempt 1:37069 Drop and generate

events

FILE-FLASH Adobe Flash Player object hasOwnProperty use after fre e attempt 1:37236 Drop and generate

events

FILE-FLASH Adobe Flash Player object hasOwnProperty use after fre e attempt 1:37237 Drop and generate

events

FILE-FLASH Adobe Flash Player object type confusion attempt 1:344 77 Drop and generate

events

FILE-FLASH Adobe Flash Player object type confusion attempt 1:335 39 Drop and generate

events

FILE-FLASH Adobe Flash Player object.addProperty method use after free attempt 1:37203 Drop and generate

events

FILE-FLASH Adobe Flash Player object.addProperty method use after free attempt 1:37205 Drop and generate FILE-FLASH Adobe Flash Player On2 VP6 video codec fragment read a ccess violation attempt 1:36229 Drop and generate FILE-FLASH Adobe Flash Player OpportunityGenerator.update memory corruption attempt 1:38971 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player OpportunityGenerator.update memory corruption attempt 1:38973 Drop and generate

events

FILE-FLASH Adobe Flash Player out of bounds memory access attempt 1:46949 Drop and generate

events

FILE-FLASH Adobe Flash Player out of bounds memory access attempt 1:46950 Drop and generate

events

FILE-FLASH Adobe Flash Player out of bounds write attempt 1:46917 Drop and generate

events

FILE-FLASH Adobe Flash Player out of bounds write attempt 1:46918 Drop and generate

events

FILE-FLASH Adobe Flash Player out of bounds write attempt 1:46919 Drop and generate

events

FILE-FLASH Adobe Flash Player out of bounds write attempt 1:46920 Drop and generate

events

FILE-FLASH Adobe Flash Player out of scope newclass memory corrup tion attempt 1:33505 Drop and generate

events

FILE-FLASH Adobe Flash Player out of scope newclass memory corrup tion attempt 1:33507 Drop and generate

events

FILE-FLASH Adobe Flash Player Ovector out of bounds stack corrupt ion attempt 1:33490 Drop and generate

events

FILE-FLASH Adobe Flash Player Ovector out of bounds stack corrupt ion attempt 1:36398 Drop and generate

events

FILE-FLASH Adobe Flash Player overly large bitmap integer overflo w attempt 1:37223 Drop and generate

events

FILE-FLASH Adobe Flash Player oversize source bitmap memory corru ption attempt 1:37162 Drop and generate

events

FILE-FLASH Adobe Flash Player paletteMap integer overflow attempt 1:33923 Drop and generate

events

FILE-FLASH Adobe Flash Player paletteMap integer overflow attempt 1:33925 Drop and generate FILE-FLASH Adobe Flash Player parseFloat stack overflow remote co de execution attempt 1:32782 Drop and generate FILE-FLASH Adobe Flash Player parseFloat stack overflow remote co de execution attempt 1:32783 Drop and generate FILE-FLASH Adobe Flash Player PCRE control character denial of se rvice attempt 1:33533 Drop and generate

events

events

events

events

FILE-FLASH Adobe Flash Player PCRE control character denial of se rvice attempt 1:33536 Drop and generate

events

FILE-FLASH Adobe Flash Player PCRE engine find\_recurse out-of-bou nds read attempt 1:36581 Drop and generate

events

FILE-FLASH Adobe Flash Player PCRE engine find\_recurse out-of-bou nds read attempt 1:36582 Drop and generate

events

FILE-FLASH Adobe Flash Player PCRE parsing out of bounds read att empt 1:37111 Drop and generate

events

FILE-FLASH Adobe Flash Player PCRE parsing out of bounds read att empt 1:37112 Drop and generate

events

FILE-FLASH Adobe Flash Player PCRE regex compilation memory corru ption attempt 1:33469 Drop and generate

events

FILE-FLASH Adobe Flash Player Point object integer overflow attempt 1:37752 Drop and generate

events

FILE-FLASH Adobe Flash Player Point object integer overflow attempt 1:37754 Drop and generate

events

FILE-FLASH Adobe Flash Player Point object integer overflow attempt 1:37735 Drop and generate

events

FILE-FLASH Adobe Flash Player Point object integer overflow attempt 1:37736 Drop and generate

events

FILE-FLASH Adobe Flash Player pre-compile regex length denial of service attempt 1:33077 Drop and generate

events

FILE-FLASH Adobe Flash Player pre-compile regex length denial of service attempt 1:33078 Drop and generate FILE-FLASH Adobe Flash Player Primetime MediaPlayerItemLoader Blu rFilter object out of bounds write attempt 1:46247 Drop and generate FILE-FLASH Adobe Flash Player Primetime MediaPlayerItemLoader Blu rFilter object out of bounds write attempt 1:46248 Drop and generate FILE-FLASH Adobe Flash Player Primetime MediaPlayerItemLoader QOS Provider object use after free attempt 1:41004 Drop and generate FILE-FLASH Adobe Flash Player Primetime SDK out of bounds read at tempt 1:41002 Drop and generate FILE-FLASH Adobe Flash Player Primetime SDK ShimContentResolver m emory corruption attempt 1:41357 Drop and generate FILE-FLASH Adobe Flash Player Primetime SDK ShimContentResolver o ut of bounds memory access attempt 1:39289 Drop and generate FILE-FLASH Adobe Flash Player Primetime SDK ShimContentResolver o ut of bounds memory access attempt 1:39304 Drop and generate FILE-FLASH Adobe Flash Player Primetime TVSDK memory corruption attempt 1:42052 Drop and generate

events

events

events

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player PrintJobOptions use-after-free atte mpt 1:39711 Drop and generate

events

FILE-FLASH Adobe Flash Player PSDK EventDispatch removeEventListe ner use after free attempt 1:41629 Drop and generate FILE-FLASH Adobe Flash Player PSDK Metadata memory corruption att empt 1:44902 Drop and generate

events

events

FILE-FLASH Adobe Flash Player PSDK use-after-free attempt 1:39019 Drop and generate

events

FILE-FLASH Adobe Flash Player PSDK use-after-free attempt 1:39021 Drop and generate

events

FILE-FLASH Adobe Flash Player QOSProvider use-after-free attempt 1:40502 Drop and generate

events

FILE-FLASH Adobe Flash Player raster pointer null pointer derefer ence attempt 1:35741 Drop and generate

events

FILE-FLASH Adobe Flash Player raster pointer null pointer derefer ence attempt 1:35743 Drop and generate

events

FILE-FLASH Adobe Flash Player rectangle auxiliary method integer overflow attempt 1:37760 Drop and generate

events

FILE-FLASH Adobe Flash Player rectangle auxiliary method integer overflow attempt 1:37761 Drop and generate

events

FILE-FLASH Adobe Flash Player Rectangle constructor use after fre e attempt 1:39727 Drop and generate

events

FILE-FLASH Adobe Flash Player Rectangle constructor use after fre e attempt 1:44016 Drop and generate

events

FILE-FLASH Adobe Flash Player rectangle memory access violation attempt 1:37795 Drop and generate

events

FILE-FLASH Adobe Flash Player rectangle memory access violation attempt 1:37797 Drop and generate

events

FILE-FLASH Adobe Flash Player rectangle width integer overflow at tempt 1:38238 Drop and generate

events

FILE-FLASH Adobe Flash Player rectangle width integer overflow at tempt 1:38239 Drop and generate

events

FILE-FLASH Adobe Flash Player recursion calls stack overflow atte mpt 1:38197 Drop and generate

events

FILE-FLASH Adobe Flash Player recursion check stack overflow atte mpt 1:36573 Drop and generate

events

FILE-FLASH Adobe Flash Player recursion check stack overflow atte mpt 1:36574 Drop and generate

events

FILE-FLASH Adobe Flash Player regex denial of service attempt 1:3 2301 Drop and generate

events

FILE-FLASH Adobe Flash Player regex denial of service attempt 1:3 2303 Drop and generate

events

FILE-FLASH Adobe Flash Player regex denial of service attempt 1:3 2305 Drop and generate

events

FILE-FLASH Adobe Flash Player regex denial of service attempt 1:3 2307 Drop and generate

events

FILE-FLASH Adobe Flash Player RegExp compilation heap overflow at tempt 1:31847 Drop and generate

events

FILE-FLASH Adobe Flash Player RegExp compilation heap overflow at tempt 1:31848 Drop and generate

events

FILE-FLASH Adobe Flash Player RegExp zero length assertion heap o verflow attempt 1:34162 Drop and generate

events

FILE-FLASH Adobe Flash Player remote memory corruption attempt 1: 26982 Drop and generate

events

FILE-FLASH Adobe Flash Player remote memory corruption attempt 1: 28568 Drop and generate

events

FILE-FLASH Adobe Flash Player removeChildren use-after-free attempt 1:36321 Drop and generate

events

FILE-FLASH Adobe Flash Player removeChildren use-after-free attempt 1:36323 Drop and generate

events

FILE-FLASH Adobe Flash Player removeMovieClip callback use after free attempt 1:38824 Drop and generate

events

FILE-FLASH Adobe Flash Player removeMovieClip callback use after free attempt 1:38826 Drop and generate

events

FILE-FLASH Adobe Flash Player removeMovieClip use after free atte mpt 1:37247 Drop and generate

events

FILE-FLASH Adobe Flash Player removeMovieClip use after free atte mpt 1:37248 Drop and generate

events

FILE-FLASH Adobe Flash Player removeMovieClip use after free atte mpt 1:37249 Drop and generate

events

FILE-FLASH Adobe Flash Player removeMovieClip use after free atte mpt 1:37234 Drop and generate

events

FILE-FLASH Adobe Flash Player request for MSIMG32.dll over SMB at tempt 1:38872 Drop and generate FILE-FLASH Adobe Flash Player Resolution Opportunity parameter me mory corruption attempt 1:42096 Drop and generate FILE-FLASH Adobe Flash player retrieveResolvers memory corruption attempt 1:39297 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player same origin policy security bypass attempt 1:39310 Drop and generate

events

FILE-FLASH Adobe Flash Player scale9Grid use after free attempt 1 :35820 Drop and generate

events

FILE-FLASH Adobe Flash Player scale9Grid use after free attempt 1 :35822 Drop and generate

events

FILE-FLASH Adobe Flash Player scale9Grid use after free attempt 1 :35823 Drop and generate

events

FILE-FLASH Adobe Flash Player secret cookie location disclosure attempt 1:35574 Drop and generate

events

FILE-FLASH Adobe Flash Player secret cookie location disclosure attempt 1:35576 Drop and generate

events

FILE-FLASH Adobe Flash Player selection.setFocus use after free attempt 1:39023 Drop and generate

events

FILE-FLASH Adobe Flash Player selection.setFocus use after free attempt 1:39024 Drop and generate

events

FILE-FLASH Adobe Flash Player selection.setFocus use after free attempt 1:37107 Drop and generate

events

FILE-FLASH Adobe Flash Player selection.setFocus use after free attempt 1:37109 Drop and generate

events

FILE-FLASH Adobe Flash Player Selection.SetSelection use-after-free attempt 1:45613 Drop and generate

events

FILE-FLASH Adobe Flash Player Selection.SetSelection use-after-free attempt 1:45614 Drop and generate

events

FILE-FLASH Adobe Flash Player sentEvent use after free attempt 1: 40581 Drop and generate

events

FILE-FLASH Adobe Flash Player setCuePointTags memory corruption attempt 1:34506 Drop and generate

events

FILE-FLASH Adobe Flash Player setglobalslot malformed bytecode re mote code execution attempt 1:32558 Drop and generate FILE-FLASH Adobe Flash Player setglobalslot malformed bytecode re mote code execution attempt 1:32560 Drop and generate FILE-FLASH Adobe Flash Player setInterval use-after-free memory c orruption attempt 1:38193 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player setMetadata memory corruption attempt 1:39009 Drop and generate

events

FILE-FLASH Adobe Flash Player setMetadata memory corruption attempt 1:39011 Drop and generate

events

FILE-FLASH Adobe Flash Player SetSlot type confusion attempt 1:37 142 Drop and generate

events

FILE-FLASH Adobe Flash Player SetSlot type confusion attempt 1:37 144 Drop and generate

events

FILE-FLASH Adobe Flash Player setSubscribedTags memory corruption attempt 1:34504 Drop and generate FILE-FLASH Adobe Flash Player setSubscribedTagsForBackgroundManif est memory corruption attempt 1:34508 Drop and generate FILE-FLASH Adobe Flash Player Shader Channel integer overflow att empt 1:34848 Drop and generate

events

events

events

FILE-FLASH Adobe Flash Player Shader Channel integer overflow att empt 1:34850 Drop and generate

events

FILE-FLASH Adobe Flash Player ShaderParameter integer overflow at tempt 1:37071 Drop and generate

events

FILE-FLASH Adobe Flash Player ShaderParameter integer overflow at tempt 1:37072 Drop and generate

events

FILE-FLASH Adobe Flash Player ShaderParameter integer overflow at tempt 1:37073 Drop and generate

events

FILE-FLASH Adobe Flash Player ShaderParameter out of bounds write attempt 1:34855 Drop and generate

events

FILE-FLASH Adobe Flash Player ShaderParameter out of bounds write attempt 1:36299 Drop and generate

events

FILE-FLASH Adobe Flash Player ShaderParameter out of bounds write attempt 1:36301 Drop and generate

events

FILE-FLASH Adobe Flash Player shared byte array memory corruption attempt 1:34302 Drop and generate

events

FILE-FLASH Adobe Flash Player shared byte array memory corruption attempt 1:34303 Drop and generate FILE-FLASH Adobe Flash Player SharedObject array.prototype.push u se after free attempt 1:35290 Drop and generate FILE-FLASH Adobe Flash Player SharedObject array.prototype.push u se after free attempt 1:35292 Drop and generate FILE-FLASH Adobe Flash Player SharedObject array.prototype.push u se after free attempt 1:35294 Drop and generate FILE-FLASH Adobe Flash Player SharedObject send stack buffer over flow attempt 1:37156 Drop and generate

events

events

events

events

events

FILE-FLASH Adobe Flash Player SharedObject send stack buffer over flow attempt 1:37157 Drop and generate

events

FILE-FLASH Adobe Flash Player SharedObject type confusion attempt 1:35296 Drop and generate

events

FILE-FLASH Adobe Flash Player SharedObject use after free attempt 1:35754 Drop and generate

events

FILE-FLASH Adobe Flash Player SharedObject use after free attempt 1:44173 Drop and generate

events

FILE-FLASH Adobe Flash Player ShimContentFactory uninitialized po inter use attempt 1:39271 Drop and generate FILE-FLASH Adobe Flash Player ShimContentResolver out of bounds m emory access attempt 1:39287 Drop and generate FILE-FLASH Adobe Flash Player ShimContentResolver out of bounds m emory access attempt 1:41679 Drop and generate FILE-FLASH Adobe Flash Player ShimContentResolver out of bounds m emory access attempt 1:40166 Drop and generate FILE-FLASH Adobe Flash Player ShimOpportunityGenerator out of bou nds memory access attempt 1:39318 Drop and generate FILE-FLASH Adobe Flash Player si32 integer overflow attempt 1:381 91 Drop and generate

events

events

events

events

events

events

FILE-FLASH Adobe Flash Player SimpleButton constructor type confu sion attempt 1:37352 Drop and generate

events

FILE-FLASH Adobe Flash Player slow script invalid pointer derefer ence attempt 1:35618 Drop and generate

events

FILE-FLASH Adobe Flash Player SMB sandbox bypass attempt 1:44002 Drop and generate

events

FILE-FLASH Adobe Flash Player sortOn heap overflow attempt 1:2617 2 Drop and generate

events

FILE-FLASH Adobe Flash Player sound class type confusion attempt 1:34151 Drop and generate

events

FILE-FLASH Adobe Flash Player sound class type confusion attempt 1:34153 Drop and generate

events

FILE-FLASH Adobe Flash Player sound object use-after-free attempt 1:39306 Drop and generate

events

FILE-FLASH Adobe Flash Player Sound.extract integer overflow atte mpt 1:34276 Drop and generate

events

FILE-FLASH Adobe Flash Player Sound.extract integer overflow atte mpt 1:34278 Drop and generate

events

FILE-FLASH Adobe Flash Player SoundURLStream memory corruption at tempt 1:37092 Drop and generate

events

FILE-FLASH Adobe Flash Player SoundURLStream memory corruption at tempt 1:37093 Drop and generate

events

FILE-FLASH Adobe Flash Player Stage align use aftre free attempt 1:39558 Drop and generate

events

FILE-FLASH Adobe Flash Player stage object use-after-free attempt 1:33290 Drop and generate

events

FILE-FLASH Adobe Flash Player string concatenation integer overfl ow attempt 1:32572 Drop and generate

events

FILE-FLASH Adobe Flash Player string concatenation integer overfl ow attempt 1:32573 Drop and generate

events

FILE-FLASH Adobe Flash Player string concatenation integer overfl ow attempt 1:32574 Drop and generate

events

FILE-FLASH Adobe Flash Player string concatenation memory corrupt ion attempt 1:32236 Drop and generate

events

FILE-FLASH Adobe Flash Player string concatenation memory corrupt ion attempt 1:32238 Drop and generate

events

FILE-FLASH Adobe Flash Player String null check memory corruption attempt 1:37181 Drop and generate

events

FILE-FLASH Adobe Flash Player StyleSheets use after free attempt 1:41353 Drop and generate

events

FILE-FLASH Adobe Flash Player swapDepths use after free attempt 1 :39651 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF ActionScript exploit attempt 1: 30845 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF buffer overflow attempt 1:36878 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF buffer overflow attempt 1:33509 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF buffer overflow attempt 1:33510 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF dereference attempt 1:35571 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF object type mismatch attempt 1: 33975 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF use-after-free attempt 1:33554 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF use-after-free attempt 1:33555 Drop and generate

events

FILE-FLASH Adobe Flash Player SWF-based shellcode download attemp t 1:26008 Drop and generate

events

FILE-FLASH Adobe Flash Player text field mask use after free atte mpt 1:34247 Drop and generate

events

FILE-FLASH Adobe Flash Player text field mask use after free atte mpt 1:34249 Drop and generate

events

FILE-FLASH Adobe Flash Player text handling memory corruption att empt 1:44351 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField filter use-after-free att empt 1:34172 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField filter use-after-free att empt 1:34174 Drop and generate

events

FILE-FLASH Adobe Flash Player textfield filter use-after-free att empt 1:35267 Drop and generate

events

FILE-FLASH Adobe Flash Player textfield filter use-after-free att empt 1:35269 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField filters use-after-free at tempt 1:35650 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField filters use-after-free at tempt 1:35651 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField filters use-after-free at tempt 1:37118 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField object event handler use after free attempt 1:41673 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField object Type Confusion Att empt 1:37748 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField use after free attempt 1: 42010 Drop and generate

events

FILE-FLASH Adobe Flash Player TextField use after free attempt 1: 40746 Drop and generate

events

FILE-FLASH Adobe Flash Player TextFormat.tabStops use after free attempt 1:37187 Drop and generate

events

FILE-FLASH Adobe Flash Player TextFormat.tabStops use after free attempt 1:37189 Drop and generate

events

FILE-FLASH Adobe Flash Player TextFormat.tabStops use after free attempt 1:37191 Drop and generate

events

FILE-FLASH Adobe Flash Player TextFormat.tabStops use after free attempt 1:37193 Drop and generate

events

FILE-FLASH Adobe Flash Player TextLine memory corruption attempt 1:37742 Drop and generate

events

FILE-FLASH Adobe Flash Player TextLine memory corruption attempt 1:37744 Drop and generate

events

FILE-FLASH Adobe Flash Player textLine use-after-free attempt 1:3 6590 Drop and generate

events

FILE-FLASH Adobe Flash Player textLine use-after-free attempt 1:3 6592 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 35364 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 35366 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 34240 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 34242 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 34244 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 34803 Drop and generate

events

FILE-FLASH Adobe Flash Player thread write double-free attempt 1: 34805 Drop and generate

events

FILE-FLASH Adobe Flash Player TimedEvent memory corruption attemp t 1:39563 Drop and generate

events

FILE-FLASH Adobe Flash Player toString type confusion memory corruption attempt 1:44552 Drop and generate

events

FILE-FLASH Adobe Flash Player toString type confusion memory corruption attempt 1:38429 Drop and generate

events

FILE-FLASH Adobe Flash Player toString type confusion memory corruption attempt 1:38430 Drop and generate

events

FILE-FLASH Adobe Flash Player toString type confusion memory corruption attempt 1:38433 Drop and generate

events

FILE-FLASH Adobe Flash Player toString type confusion memory corruption attempt 1:38455 Drop and generate

events

FILE-FLASH Adobe Flash Player toString with script objects use af ter free attempt 1:36836 Drop and generate

events

FILE-FLASH Adobe Flash Player Transform Class Matrix AS2 use afte r free attempt 1:38403 Drop and generate

events

FILE-FLASH Adobe Flash Player Transform Class Matrix AS2 use afte r free attempt 1:38405 Drop and generate

events

FILE-FLASH Adobe Flash Player Transform getter use after free att empt 1:39658 Drop and generate

events

FILE-FLASH Adobe Flash Player Transform object use after free att empt 1:39571 Drop and generate

events

FILE-FLASH Adobe Flash Player URLRequestHeaders null pointer dere ference denial of service attempt 1:33484 Drop and generate

events

FILE-FLASH Adobe Flash Player URLRequestHeaders null pointer dere ference denial of service attempt 1:33485 Drop and generate FILE-FLASH Adobe Flash Player URLStream use after free attempt 1: 37165 Drop and generate

events

events

FILE-FLASH Adobe Flash Player URLStream use after free attempt 1: 37168 Drop and generate

events

FILE-FLASH Adobe Flash Player URLStreamObject out of bounds read attempt 1:36263 Drop and generate

events

FILE-FLASH Adobe Flash Player URLStreamObject out of bounds read attempt 1:36264 Drop and generate

events

FILE-FLASH Adobe Flash Player use after free attempt 1:38219 Drop and generate

events

FILE-FLASH Adobe Flash Player use after free attempt 1:38221 Drop and generate

events

FILE-FLASH Adobe Flash Player use after free attempt 1:46262 Drop and generate

events

FILE-FLASH Adobe Flash Player use after free attempt 1:46263 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35223 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35225 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35227 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35228 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35231 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35233 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35235 Drop and generate

events

FILE-FLASH Adobe Flash Player valueOf and toString use after free attempt 1:35237 Drop and generate

events

FILE-FLASH Adobe Flash Player Vector.String class out-of-bounds r ead attempt 1:47531 Drop and generate

events

FILE-FLASH Adobe Flash Player Vector.String class out-of-bounds r ead attempt 1:47532 Drop and generate

events

FILE-FLASH Adobe Flash Player video decode use after free attempt 1:36297 Drop and generate

events

FILE-FLASH Adobe Flash Player visual blend out of bounds read att empt 1:41158 Drop and generate

events

FILE-FLASH Adobe Flash Player worker shared object use-after-free attempt 1:32359 Drop and generate

events

FILE-FLASH Adobe Flash Player worker shared object use-after-free attempt 1:29928 Drop and generate

events

FILE-FLASH Adobe Flash Player worker shared object use-after-free attempt 1:29929 Drop and generate

events

FILE-FLASH Adobe Flash Player worker shared object user-after-fre e attempt 1:37684 Drop and generate

events

FILE-FLASH Adobe Flash Player writeExternal type confusion attemp t 1:43453 Drop and generate

events

FILE-FLASH Adobe Flash Player writeExternal type confusion attemp t 1:36859 Drop and generate

events

FILE-FLASH Adobe Flash Player writeExternal type confusion attemp t 1:36549 Drop and generate

events

FILE-FLASH Adobe Flash Player writeExternal type confusion attemp t 1:36551 Drop and generate

events

FILE-FLASH Adobe Flash Player writeExternal type confusion attemp t 1:36552 Drop and generate

events

FILE-FLASH Adobe Flash Player writeExternal type confusion attemp t 1:36554 Drop and generate

events

FILE-FLASH Adobe Flash Player XML pointer wrong parent reference 1:35646 Drop and generate

events

FILE-FLASH Adobe Flash Player XML pointer wrong parent reference 1:35648 Drop and generate

events

FILE-FLASH Adobe Flash Player XML property delete out of bounds m emory write attempt 1:35654 Drop and generate

events

FILE-FLASH Adobe Flash Player XML property delete out of bounds m emory write attempt 1:35656 Drop and generate

events

FILE-FLASH Adobe Flash Player XMLSocket destroy function type con fusion attempt 1:35759 Drop and generate

events

FILE-FLASH Adobe Flash Player XMLSocket destroy function type con fusion attempt 1:35761 Drop and generate

events

FILE-FLASH Adobe Flash Standalone Player ASSetPropFlags use after free attempt 1:37201 Drop and generate

events

FILE-FLASH Adobe Flash TextFormat.setTabStops use-after-free atte mpt 1:39269 Drop and generate

events

FILE-FLASH Adobe Flash valueOf memory leak attempt 1:31678 Drop and generate

events

FILE-FLASH Adobe Primetime SDK object type confusion overflow att empt 1:39279 Drop and generate

events

FILE-FLASH Adobe PSDK DRM Manager memory corruption attempt 1:463 24 Drop and generate

events

FILE-FLASH Adobe PSDK DRM Manager memory corruption attempt 1:455 93 Drop and generate

events

FILE-FLASH Adobe PSDK DRM Manager memory corruption attempt 1:455 94 Drop and generate

events

FILE-FLASH Adobe PSDK DRM Manager memory corruption attempt 1:455 95 Drop and generate

events

FILE-FLASH Adobe PSDK DRM Manager memory corruption attempt 1:456 83 Drop and generate

events

FILE-FLASH Adobe Standalone Flash Player AS3 NetStream object use after free attempt 1:40438 Drop and generate

events

FILE-FLASH Adobe Standalone Flash Player AS3 Primetime timeline S himContentResolver out of bounds read attempt 1:40452

Drop and generate events

FILE-FLASH Adobe Standalone Flash Player ASnative object use afte r free attempt 1:38177 Drop and generate

events

FILE-FLASH Adobe Standalone Flash Player ASnative object use afte r free attempt 1:38179 Drop and generate

events

FILE-FLASH Adobe Standalone Flash Player BlendMode memory corrupt ion attempt 1:42807 Drop and generate FILE-FLASH Adobe Standalone Flash Player IExternalizable deserial ization use after free attempt 1:40544 Drop and generate FILE-FLASH Adobe Standalone Flash Player IExternalizable deserial ization use after free attempt 1:40798 Drop and generate

events

events

events

FILE-FLASH Adobe Standalone Flash Player texfield getter use afte r free attempt 1:38173 Drop and generate

events

FILE-FLASH Adobe Standalone Flash Player texfield getter use afte r free attempt 1:38175 Drop and generate

events

FILE-FLASH Angler exploit kit Adobe Flash SWF exploit download 1: 38629 Drop and generate

events

FILE-FLASH Angler exploit kit Adobe Flash SWF exploit download 1: 38631 Drop and generate

events

FILE-FLASH Google Chrome pepflashplayer SurfaceFilterList use-aft er-free attempt 1:35588 Drop and generate

events

FILE-FLASH Google Chrome pepflashplayer SurfaceFilterList use-aft er-free attempt 1:35589 Drop and generate

events

FILE-FLASH Nuclear exploit kit Adobe Flash SWF exploit download 1 :38633 Drop and generate

events

FILE-FLASH Nuclear exploit kit Adobe Flash SWF exploit download 1 :38635 Drop and generate

events

FILE-IDENTIFY Adobe Flash Player embedded compact font detected 1 :25680 Generate events

FILE-IDENTIFY Microsoft emf file download request 1:2435 Generate events

FILE-IDENTIFY Obfuscated .wsf download attempt 1:37130 Drop and generate

events

FILE-IDENTIFY Obfuscated .wsf download attempt 1:37132 Drop and generate

events

FILE-IMAGE Adobe Acrobat EmfPlusDrawImagePoints out of bounds rea d attempt 1:47827 Drop and generate

events

FILE-IMAGE Adobe Acrobat EmfPlusDrawImagePoints out of bounds rea d attempt 1:47828 Drop and generate

events

FILE-IMAGE Adobe Acrobat GIF to PDF conversion heap overflow atte mpt 1:35751 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF EmfPlusFont memory corruption at tempt 1:44969 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF EMR\_STRETCHDIBITS memory corrupt ion attempt 1:44880 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF file EmfPlusDrawImagePoints heap overflow attempt 1:47210 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF file EmfPlusDrawImagePoints heap overflow attempt 1:47211 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF out of bounds read attempt 1:479 81 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF out of bounds read attempt 1:479 82 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF out of bounds read attempt 1:479 79 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF out of bounds read attempt 1:479 80 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF out of bounds write attempt 1:44 929 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF pointer out of bounds read attempt 1:47997 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF pointer out of bounds read attempt 1:47998 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF pointer out of bounds write atte mpt 1:47995 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro EMF pointer out of bounds write atte mpt 1:47996

FILE-IMAGE Adobe Acrobat Pro integer overflow attempt 1:48009 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro integer overflow attempt 1:48010 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro invalid APP13 marker size attempt 1: 44912 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro JPEG Huffman table memory corruption attempt 1:48219 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro JPEG Huffman table memory corruption attempt 1:48220 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro malformed CommentExtension attempt 1 :44861 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro malformed GIF memory corruption atte mpt 1:42218 Drop and generate FILE-IMAGE Adobe Acrobat Pro malformed JPEG APP2 marker memory co rruption attempt 1:48043 Drop and generate FILE-IMAGE Adobe Acrobat Pro malformed JPEG APP2 marker memory co rruption attempt 1:48044 Drop and generate FILE-IMAGE Adobe Acrobat Pro malformed TIF tag entry out of bound s read attempt 1:47953 Drop and generate

events

events

events

events

FILE-IMAGE Adobe Acrobat Pro malformed TIF tag entry out of bound s read attempt 1:47954 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro malformed TIF tag entry out of bound s read attempt 1:47955 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro malformed TIF tag entry out of bound s read attempt 1:47956 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45788 Drop and generate

events

FILE-IMAGE Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45789 Drop and generate

events

FILE-IMAGE Adobe Acrobat Reader DC TIFF orientation heap buffer o verflow attempt 1:35360 Drop and generate

events

FILE-IMAGE Adobe Acrobat Reader DC TIFF orientation heap buffer o verflow attempt 1:35362 Drop and generate

events

FILE-IMAGE Adobe Acrobat Reader JPEG 2000 tile memory corruption attempt 1:43908 Drop and generate

events

FILE-IMAGE Adobe Acrobat Reader JPEG 2000 tile memory corruption attempt 1:43909 Drop and generate

events

FILE-IMAGE Adobe Acrobat Reader overly large segment size out of bounds read attempt 1:42324 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF ICC tag heap buffer overflow attemp t 1:41391 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF ICC tag heap buffer overflow attemp t 1:41393 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF ICC tag heap buffer overflow attemp t 1:41395 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF ICC tag heap buffer overflow attemp t 1:41397 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF malformed YCbCrCoefficients values attempt 1:45791 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF malformed YCbCrCoefficients values attempt 1:45792 Drop and generate FILE-IMAGE Adobe Acrobat TIFF malformed YCbCrCoefficients values memory corruption attempt 1:44959 Drop and generate

events

events

FILE-IMAGE Adobe Acrobat TIFF PhotometricInterpretation heap buff er overflow attempt 1:41182 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF Software tag heap buffer overflow attempt 1:41198 Drop and generate

events

FILE-IMAGE Adobe Acrobat TIFF Software tag heap buffer overflow attempt 1:41200 Drop and generate

events

FILE-IMAGE Adobe Acrobat XPS heap overflow attempt 1:47941 Drop and generate

events

FILE-IMAGE Adobe Acrobat XPS heap overflow attempt 1:47942 Drop and generate

events

FILE-IMAGE Adobe Acrobat XPS out-of-bounds read attempt 1:46688 Drop and generate

events

FILE-IMAGE Adobe Acrobat XPS out-of-bounds read attempt 1:46689 Drop and generate

events

FILE-IMAGE Adobe Acrobat XPS unicode glyph pointer out of bounds 1:44884 Drop and generate

events

FILE-IMAGE Adobe Flash Player element array stack overflow attemp t 1:34133 Drop and generate

events

FILE-IMAGE Adobe Reader EMF EMR\_MOVETOEX memory corruption attemp t 1:43865 Drop and generate

events

FILE-IMAGE Apple Core Graphics BMP img\_decode\_read memory corrupt ion attempt 1:39683 Drop and generate

events

FILE-IMAGE BMP extremely large xpos opcodes 1:26664 Drop and generate

events

FILE-IMAGE Corel PHOTO-PAINT X8 GIF Filter Code Execution Vulnera bility attempt 1:42140 Drop and generate

events

FILE-IMAGE GDI+ malformed EMF comment heap access violation attempt 1:41970 Drop and generate

events

FILE-IMAGE GDI+ malformed EMF comment heap access violation attempt 1:41971 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39090 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39091 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39092 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39093 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39094 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39095 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39096 Drop and generate

events

FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command inject ion attempt 1:39097 Drop and generate

events

FILE-IMAGE ImageMagick LibTIFF invalid SamplesPerPixel buffer ove rflow attempt 1:40914 Drop and generate

events

FILE-IMAGE ImageMagick PostScript decode delegate command injecti on attempt 1:41120 Drop and generate

events

FILE-IMAGE ImageMagick PostScript decode delegate command injecti on attempt 1:41121 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38871 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38945 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38946 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38947 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38948 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39000 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39001 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39002 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39003 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39004 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39005 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:39006 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38743 Drop and generate

events

FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attemp t 1:38744 Drop and generate

events

FILE-IMAGE libBPG restore\_tqb\_pixel out of bounds write attempt 1 :41310 Drop and generate

events

FILE-IMAGE libpng malformed chunk denial of service attempt 3:147 72 Drop and generate

events

FILE-IMAGE Microsoft Graphics component WMF code execution attemp t 1:48374 Drop and generate

events

FILE-IMAGE Microsoft Graphics component WMF code execution attemp t 1:48375 Drop and generate FILE-IMAGE Microsoft Multiple Products potentially malicious PNG detected - large or invalid chunk size 3:29944 Drop and generate FILE-IMAGE Microsoft Windows asycfilt.dll malformed jpeg buffer o verread attempt 1:40645 Drop and generate

events

events

events

FILE-IMAGE Microsoft Windows asycfilt.dll malformed jpeg buffer o verread attempt 1:40646 Drop and generate

events

FILE-IMAGE Microsoft Windows malformed TIFF remote code execution attempt 1:47764 Drop and generate

events

FILE-IMAGE Microsoft Windows malformed TIFF remote code execution attempt 1:47765 Drop and generate

events

FILE-IMAGE OpenOffice TIFF file in big endian format parsing inte ger overflow attempt 3:15976 Drop and generate

events

FILE-IMAGE OpenOffice TIFF file in little endian format parsing i nteger overflow attempt 3:15975 Drop and generate

events

FILE-IMAGE Trimble SketchUp corrupt BMP RLE4 heap buffer overflow attempt 1:36307 Drop and generate

events

FILE-IMAGE Trimble SketchUp corrupt BMP RLE4 heap buffer overflow attempt 1:36308 Drop and generate

events

FILE-IMAGE XnView PCT file processing buffer overflow attempt 1:3 1039 Drop and generate

events

FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp integer ove rflow attempt 1:26195 Drop and generate

events

FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp integer ove rflow attempt 1:29605 Drop and generate FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp storeImageA rray memory corruption attempt 1:27621 Drop and generate FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp storeImageA rray memory corruption attempt 1:28276 Drop and generate FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp storeImageA rray memory corruption attempt 1:27672 Drop and generate FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp storeImageA rray memory corruption attempt 1:27674 Drop and generate FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp storeImageA rray memory corruption attempt 1:27676 Drop and generate FILE-JAVA Oracle Java 2D ImagingLib ConvolveOp integer overflow attempt 1:26197 Drop and generate

events

events

events

events

events

events

events

FILE-JAVA Oracle Java 2D ImagingLib LookupOp integer overflow att empt 1:26196 Drop and generate

events

FILE-JAVA Oracle Java and JavaFX JPEGImageReader memory corruptio n attempt 1:29218 Drop and generate

events

FILE-JAVA Oracle Java Applet disable security manager attempt 1:2 7076 Drop and generate

events

FILE-JAVA Oracle Java Applet ProviderSkeleton sandbox bypass atte mpt 1:27188 Drop and generate

events

FILE-JAVA Oracle Java Applet ProviderSkeleton sandbox bypass atte mpt 1:27190 Drop and generate

events

FILE-JAVA Oracle Java Applet Rhino script engine remote code exec ution attempt 1:20831 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:25121 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:25122 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:25123 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:24201 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:31511 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:23273 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:23274 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:23275 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:23276 Drop and generate

events

FILE-JAVA Oracle Java field bytecode verifier cache code executio n attempt 1:23277 Drop and generate

events

FILE-JAVA Oracle Java font rendering remote code execution attemp t 1:26716 Drop and generate

events

FILE-JAVA Oracle Java Gmbal package sandbox breach attempt 1:2618 5 Drop and generate

events

FILE-JAVA Oracle Java ImagingLib buffer overflow attempt 1:28926 Drop and generate

events

FILE-JAVA Oracle Java ImagingLib buffer overflow attempt 1:27786 Drop and generate

events

FILE-JAVA Oracle Java IntegerInterleavedRaster integer overflow attempt 1:27691 Drop and generate

events

FILE-JAVA Oracle Java IntegerInterleavedRaster integer overflow attempt 1:31540 Drop and generate

events

FILE-JAVA Oracle Java IntegerInterleavedRaster integer overflow attempt 1:27750 Drop and generate

events

FILE-JAVA Oracle Java IntegerInterleavedRaster.verify method inte ger overflow attempt 1:28915 Drop and generate

events

FILE-JAVA Oracle Java JMX class arbitrary code execution attempt 1:25831 Drop and generate

events

FILE-JAVA Oracle Java JMX class arbitrary code execution attempt 1:25472 Drop and generate

events

FILE-JAVA Oracle Java JMX class arbitrary code execution attempt 1:25473 Drop and generate

events

FILE-JAVA Oracle Java JRE sandbox Atomic breach attempt 1:21664 Drop and generate

events

FILE-JAVA Oracle Java JRE sandbox Atomic breach attempt 1:21665 Drop and generate

events

FILE-JAVA Oracle Java JRE sandbox Atomic breach attempt 1:21666 Generate events

FILE-JAVA Oracle Java JRE sandbox Atomic breach attempt 1:21667 Generate events

FILE-JAVA Oracle Java malicious class download attempt 1:25830 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24769 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24037 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24125 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24084 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24020 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24022 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24024 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24026 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24063 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24065 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24055 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24057 Drop and generate

events

FILE-JAVA Oracle Java privileged protection domain exploitation attempt 1:24028 Generate events

FILE-JAVA Oracle Java ServiceLoader exception handling exploit at tempt 1:37664 Drop and generate

events

FILE-JAVA Oracle Java ServiceLoader exception handling exploit at tempt 1:32234 Drop and generate

events

FILE-JAVA Oracle Java ShortComponentRaster integer overflow attempt 1:29490 Drop and generate FILE-JAVA Oracle Java sun.awt.image.ImageRepresentation.setPixels integer overflow attempt 1:29268 Drop and generate FILE-JAVA Oracle Java sun.tracing.ProviderSkeleton sandbox bypass attempt 1:31366 Drop and generate

events

events

events

FILE-JAVA Oracle Java System.arraycopy race condition attempt 1:3 6240 Drop and generate

events

FILE-JAVA Oracle Java VersionHelper loadClass sandbox bypass atte mpt 1:35467 Drop and generate

events

FILE-JAVA Oracle Java VersionHelper loadClass sandbox bypass atte mpt 1:35468 Drop and generate

events

FILE-JAVA Oracle Java VersionHelper loadClass sandbox bypass atte mpt 1:35469 Drop and generate

events

FILE-MULTIMEDIA Adobe Acrobat Professional EMF malformed brush ob ject attempt 1:43999 Drop and generate

events

FILE-MULTIMEDIA Adobe Acrobat Professional EMF malformed EMR\_COMM ENT record out of bounds access attempt 1:43940

FILE-MULTIMEDIA Adobe Acrobat Professional EMF malformed EMR\_POLY BEZIERTO16 out of bounds access attempt 1:43967

Drop and generate events

Drop and generate events

FILE-MULTIMEDIA Adobe Flash pixel bender buffer overflow attempt 1:37937 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash pixel bender buffer overflow attempt 1:37939 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash pixel bender buffer overflow attempt 1:31519 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash pixel bender buffer overflow attempt 1:31520 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash pixel bender buffer overflow attempt 1:31521 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash pixel bender buffer overflow attempt 1:30876 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player AVC parser integer overflow at tempt 1:34268 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player ID3 tag integer overflow attempt 1:36113 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player malformed mp4 atom use-after-f ree attempt 1:38217 Drop and generate FILE-MULTIMEDIA Adobe Flash Player malformed mp4 CABAC encoding o ut of bounds read attempt 1:36512 Drop and generate FILE-MULTIMEDIA Adobe Flash Player malformed mp4 out of bounds wr ite attempt 1:38209 Drop and generate

events

events

events

FILE-MULTIMEDIA Adobe Flash Player malformed MP4-AVC out-of-bound s read attempt 1:47533 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player malformed MP4-AVC out-of-bound s read attempt 1:47534 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player memory corruption attempt 1:30 150 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player memory corruption attempt 1:29 061 Drop and generate FILE-MULTIMEDIA Adobe Flash Player MP4 malformed avc atom memory corruption attempt 1:33473 Drop and generate

events

FILE-MULTIMEDIA Adobe Flash Player MP4 zero length atom titl fiel d attempt 1:21340 Drop and generate

events

FILE-MULTIMEDIA Adobe Professional EMF malformed EMR\_BITBLT recor d out of bounds access attempt 1:43888 Drop and generate FILE-MULTIMEDIA Apple Quicktime crgn atom parsing stack buffer ov erflow attempt 3:13897 Drop and generate

events

events

FILE-MULTIMEDIA Apple QuickTime enof atom parsing heap buffer ove rflow attempt 1:27102 Drop and generate

events

FILE-MULTIMEDIA Apple QuickTime mdat atom corruption out of bound s read attempt 1:35717 Drop and generate

events

FILE-MULTIMEDIA Apple QuickTime mdat atom corruption out of bound s read attempt 1:35715 Drop and generate

events

FILE-MULTIMEDIA Chrome Pepper Flash Player SampleCount heap overf low attempt 1:41745 Drop and generate

events

FILE-MULTIMEDIA libvorbis VORBIS audio data out of bounds write attempt 1:48105 Drop and generate

events

FILE-MULTIMEDIA libvorbis VORBIS audio data out of bounds write attempt 1:48106 Drop and generate

events

FILE-MULTIMEDIA Matroska libmatroska ebml unicode string out of b ounds read attempt 1:35725 Drop and generate

events

FILE-MULTIMEDIA Microsoft Windows DirectShow MPEG heap overflow attempt 1:25795 Drop and generate

events

FILE-MULTIMEDIA RealNetworks RealPlayer wav chunk string overflow attempt 3:17700 Drop and generate

events

FILE-MULTIMEDIA TRUFFLEHUNTER TALOS-CAN-0043 attack attempt 3:358 34 Drop and generate

events

FILE-OFFICE Adobe Flash Player ActiveX security bypass attempt 1: 47568 Drop and generate

events

FILE-OFFICE Adobe Flash Player ActiveX security bypass attempt 1: 47569 Drop and generate

events

FILE-OFFICE AntennaHouse DMC HTMLFilter AddSst heap overflow atte mpt 1:41726 Drop and generate

events

FILE-OFFICE AntennaHouse HTMLFilter DHFSummary remote code execut ion attempt 1:40931 Drop and generate FILE-OFFICE AntennaHouse HTMLFilter Doc\_SetSummary remote code ex ecution attempt 1:40927 Drop and generate FILE-OFFICE AntennaHouse HTMLFilter GetFontTable remote code exec ution attempt 1:40929 Drop and generate

events

events

events

FILE-OFFICE Document Foundation LibreOffice RTF stylesheet use af ter free attempt 1:39148 Drop and generate

events

FILE-OFFICE Download of PowerPoint 95 file 1:15503 Drop and generate

events

FILE-OFFICE Fin7 Maldoc campaign exploitation attempt 1:44430 Drop and generate

events

FILE-OFFICE Fin7 Maldoc campaign exploitation attempt 1:44432 Drop and generate

events

FILE-OFFICE Ichitaro Office JTD Figure handling code execution at tempt 1:41110 Drop and generate

events

FILE-OFFICE Microsoft Access memory corruption attempt 1:31534 Drop and generate

events

FILE-OFFICE Microsoft Access memory corruption attempt 1:31535 Drop and generate

FILE-OFFICE Microsoft Excel out of bounds read attempt 1:46178 Drop and generate

events

FILE-OFFICE Microsoft Excel out of bounds read attempt 1:46179 Drop and generate

events

FILE-OFFICE Microsoft Excel remote code execution attempt 1:4655 6 Drop and generate

events

FILE-OFFICE Microsoft Excel remote code execution attempt 1:46557 Drop and generate

events

FILE-OFFICE Microsoft Excel remote code execution attempt 1:46552 Drop and generate

events

FILE-OFFICE Microsoft Excel remote code execution attempt 1:46553 Drop and generate

events

FILE-OFFICE Microsoft Excel use after free remote code execution attempt 1:46180 Drop and generate

events

FILE-OFFICE Microsoft Excel use after free remote code execution attempt 1:46181 Drop and generate

events

FILE-OFFICE Microsoft Excel use after free remote code execution attempt 1:46208 Drop and generate

events

FILE-OFFICE Microsoft Excel use after free remote code execution attempt 1:46209 Drop and generate

events

FILE-OFFICE Microsoft JET Database remote code execution attempt 1:46233 Drop and generate

events

FILE-OFFICE Microsoft JET Database remote code execution attempt 1:46234 Drop and generate

events

FILE-OFFICE Microsoft Office 2016 arbitrary pointer dereference v ulnerability attempt 1:40711 Drop and generate

events

FILE-OFFICE Microsoft Office Access Jet Database Engine integer o verflow attempt 1:43847 Drop and generate

events

FILE-OFFICE Microsoft Office api-ms-win-core-winrt-l1-1-0.dll dll -load exploit attempt 1:37264 Drop and generate

events

FILE-OFFICE Microsoft Office directory entry remote code executio n attempt 1:48378 Drop and generate

events

FILE-OFFICE Microsoft Office directory entry remote code executio n attempt 1:48379 Drop and generate

events

FILE-OFFICE Microsoft Office document with auto-start VBA macro d etected 1:38639 Drop and generate

events

FILE-OFFICE Microsoft Office docx heap out of bounds read attempt 1:46558 Drop and generate

events

FILE-OFFICE Microsoft Office docx heap out of bounds read attempt 1:46559 Drop and generate

events

FILE-OFFICE Microsoft Office elsext.dll dll-load exploit attempt 1:36999 Drop and generate

events

FILE-OFFICE Microsoft Office EPS file containing embedded PE 1:42 901 Drop and generate

events

FILE-OFFICE Microsoft Office EPS restore command use after free attempt 1:42900 Drop and generate

events

FILE-OFFICE Microsoft Office EPS restore command use after free attempt 1:42902 Drop and generate

events

FILE-OFFICE Microsoft Office Equation Editor object stack buffer overflow attempt 1:45133 Drop and generate

events

FILE-OFFICE Microsoft Office Equation Editor object stack buffer overflow attempt 1:45134 Drop and generate

FILE-OFFICE Microsoft Office Equation Editor Package objclass RTF evasion attempt 1:45512 Drop and generate

events

FILE-OFFICE Microsoft Office Excel out of bounds memory attempt 1:42161 Drop and generate

events

FILE-OFFICE Microsoft Office Excel bad file pointer memory corrup tion attempt 1:36002 Drop and generate

events

FILE-OFFICE Microsoft Office Excel blip image use after free atte mpt 1:32683 Drop and generate

events

FILE-OFFICE Microsoft Office Excel c legend remote code execution attempt 1:35176 Drop and generate

events

FILE-OFFICE Microsoft Office Excel CrtMlFrt record out of bounds read attempt 1:40944 Drop and generate

events

FILE-OFFICE Microsoft Office Excel ddeService command execution attempt 1:47175 Drop and generate

events

FILE-OFFICE Microsoft Office Excel ddeService command execution attempt 1:47176 Drop and generate

events

FILE-OFFICE Microsoft Office Excel ddeService command execution attempt 1:40959 Drop and generate

events

FILE-OFFICE Microsoft Office Excel drawing cell reuse use-after-f ree attempt 1:46192 Drop and generate

events

FILE-OFFICE Microsoft Office Excel drawing cell reuse use-after-f ree attempt 1:46193 Drop and generate

events

FILE-OFFICE Microsoft Office Excel empty bookViews element denial of service attempt 1:39524 Drop and generate

events

FILE-OFFICE Microsoft Office Excel empty bookViews element denial of service attempt 1:47055 Drop and generate

events

FILE-OFFICE Microsoft Office Excel empty bookViews element denial of service attempt 1:47056 Drop and generate

events

FILE-OFFICE Microsoft Office Excel fileVersion use-after-free att empt 1:36425 Drop and generate

events

FILE-OFFICE Microsoft Office Excel formula length heap corruption attempt 1:37592 Drop and generate

events

FILE-OFFICE Microsoft Office Excel graphics remote code execution attempt 1:46182 Drop and generate

events

FILE-OFFICE Microsoft Office Excel graphics remote code execution attempt 1:46183 Drop and generate

events

FILE-OFFICE Microsoft Office Excel invalid external defined names read AV attempt 1:27824 Drop and generate

events

FILE-OFFICE Microsoft Office Excel invalid signed integer attempt 1:40725 Drop and generate

events

FILE-OFFICE Microsoft Office Excel IPMT record buffer overflow at tempt 1:25293 Drop and generate

events

FILE-OFFICE Microsoft Office Excel IPMT record buffer overflow at tempt 1:25294 Drop and generate

events

FILE-OFFICE Microsoft Office Excel LPenHelper out of bounds write attempt 1:40075 Drop and generate

events

FILE-OFFICE Microsoft Office Excel LPenHelper use after free atte mpt 1:40717 Drop and generate

events

FILE-OFFICE Microsoft Office Excel malformed binary format use af ter free attempt 1:36429 Drop and generate

events

FILE-OFFICE Microsoft Office Excel malformed spreadsheet use-afte r-free attempt 1:45123 Drop and generate

FILE-OFFICE Microsoft Office Excel malformed XLS out of bounds me mory read attempt 1:39223 Drop and generate

events

FILE-OFFICE Microsoft Office Excel malicious cce value following a PtgMemFunc token 1:40459 Drop and generate

events

FILE-OFFICE Microsoft Office Excel MdCallBack out of bounds read attempt 1:36751 Drop and generate

events

FILE-OFFICE Microsoft Office Excel MSO reference count use after free attempt 1:36924 Drop and generate

events

FILE-OFFICE Microsoft Office Excel mso20win32client use after fre e attempt 1:37259 Drop and generate

events

FILE-OFFICE Microsoft Office Excel msxml6 ParseElementN use after free attempt 1:38481 Drop and generate

events

FILE-OFFICE Microsoft Office Excel named range cell content use-a fter-free attempt 1:46196 Drop and generate

events

FILE-OFFICE Microsoft Office Excel named range cell content use-a fter-free attempt 1:46197 Drop and generate FILE-OFFICE Microsoft Office Excel OLESS directory entry type con fusion remote code execution attempt 1:35996 Drop and generate FILE-OFFICE Microsoft Office Excel Ordinal43 out of bounds read attempt 1:40082 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office Excel out of bounds memory access at tempt 1:35137 Drop and generate

events

FILE-OFFICE Microsoft Office Excel out of bounds read attempt 1:3 6974 Drop and generate FILE-OFFICE Microsoft Office Excel PtgMemFunc zero-value cce-fiel d read access violation attempt 1:27820 Drop and generate FILE-OFFICE Microsoft Office Excel RealTimeData record memory cor ruption attempt 1:28544 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office Excel remote code execution attempt 1:32718 Drop and generate

events

FILE-OFFICE Microsoft Office Excel remote code execution attempt 1:46184 Drop and generate

events

FILE-OFFICE Microsoft Office Excel remote code execution attempt 1:46185 Drop and generate

events

FILE-OFFICE Microsoft Office Excel remote exploit attempt 1:33362 Drop and generate

events

FILE-OFFICE Microsoft Office Excel security descriptor out of bou nds read attempt 1:40957 Drop and generate

events

FILE-OFFICE Microsoft Office Excel shared strings memory corruption attempt 1:41979 Drop and generate

events

FILE-OFFICE Microsoft Office Excel shared strings memory corruption attempt 1:41976 Drop and generate

events

FILE-OFFICE Microsoft Office Excel sheet object use after free at tempt 1:38471 Drop and generate

events

FILE-OFFICE Microsoft Office Excel slicer style use-after-free at tempt 1:36714 Drop and generate

events

FILE-OFFICE Microsoft Office Excel SST record use after free atte mpt 1:40719 Drop and generate

events

FILE-OFFICE Microsoft Office Excel StyleXF invalid icvXF out of b ounds read attempt 1:36958 Drop and generate

events

FILE-OFFICE Microsoft Office Excel SXLI record integer overrun at tempt 1:41730 Drop and generate

FILE-OFFICE Microsoft Office Excel use after free attempt 1:47496 Drop and generate

events

FILE-OFFICE Microsoft Office Excel Viewer remote code execution attempt 1:40723 Drop and generate

events

FILE-OFFICE Microsoft Office Excel xlsb use-after-free attempt 1: 40102 Drop and generate

events

FILE-OFFICE Microsoft Office Excel xlsb use-after-free attempt 1: 40104 Drop and generate

events

FILE-OFFICE Microsoft Office Excel xlsb use-after-free attempt 1: 40116 Drop and generate

events

FILE-OFFICE Microsoft Office Excel xlsb use-after-free attempt 1: 41565 Drop and generate

events

FILE-OFFICE Microsoft Office Excel xlsb use-after-free attempt 1: 40106 Drop and generate

events

FILE-OFFICE Microsoft Office Excel xlsb use-after-free attempt 1: 40121 Drop and generate

events

FILE-OFFICE Microsoft Office GDI library TIFF handling integer ov erflow attempt 1:28464 Drop and generate

events

FILE-OFFICE Microsoft Office GDI library TIFF handling integer ov erflow attempt 1:28466 Drop and generate

events

FILE-OFFICE Microsoft Office GDI library TIFF handling integer ov erflow attempt 1:28525 Drop and generate

events

FILE-OFFICE Microsoft Office GDI library TIFF handling integer ov erflow attempt 1:28472 Drop and generate

events

FILE-OFFICE Microsoft Office GDI library TIFF handling integer ov erflow attempt 1:28468 Drop and generate

events

FILE-OFFICE Microsoft Office GDI library TIFF handling integer ov erflow attempt 1:28470 Drop and generate

events

FILE-OFFICE Microsoft Office malformed odttf integer overflow att empt 1:36707 Drop and generate

events

FILE-OFFICE Microsoft Office metafile conversion out of bounds re ad attempt 1:37265 Drop and generate

events

FILE-OFFICE Microsoft Office metafile conversion out of bounds re ad attempt 1:37266 Drop and generate

events

FILE-OFFICE Microsoft Office mfplat.dll dll-load exploit attempt 1:37262 Drop and generate

events

FILE-OFFICE Microsoft Office mqrt.dll dll-load exploit attempt 1: 42863 Drop and generate

events

FILE-OFFICE Microsoft Office mqrt.dll dll-load exploit attempt 1: 42864 Drop and generate

events

FILE-OFFICE Microsoft Office mqrt.dll dll-load exploit attempt 1: 42198 Drop and generate

events

FILE-OFFICE Microsoft Office mqrt.dll dll-load exploit attempt 1: 43802 Drop and generate

events

FILE-OFFICE Microsoft Office mqrt.dll dll-load exploit attempt 1: 43803 Drop and generate

events

FILE-OFFICE Microsoft Office mqrt.dll dll-load exploit attempt 1: 36994 Drop and generate

events

FILE-OFFICE Microsoft Office MSCOMCTL ActiveX control tabstrip me thod attempt 1:23844 Drop and generate

events

FILE-OFFICE Microsoft Office msdaora.dll dll-load exploit attempt 1:37555 Drop and generate

events

FILE-OFFICE Microsoft Office mso.dll out of bounds memory access attempt 1:39837 Drop and generate

events

FILE-OFFICE Microsoft Office None type objclass RTF evasion attempt 1:45467 Drop and generate

events

FILE-OFFICE Microsoft Office nwdblib.dll dll-load exploit attempt 1:37000 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37700 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37701 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37702 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37703 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37704 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37705 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37706 Drop and generate

events

FILE-OFFICE Microsoft Office ole object external file loading att empt 1:37707 Drop and generate

events

FILE-OFFICE Microsoft Office phoneinfo.dll dll-load exploit attempt 1:37556 Drop and generate FILE-OFFICE Microsoft Office PowerPoint OpenType font overly larg e instructionLength out of bounds read attempt 1:40938 Drop and generate FILE-OFFICE Microsoft Office PowerPoint ppcore invalid pointer re ference attempt 1:40147 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office PowerPoint WMF conversion informatio n disclosure attempt 1:40967 Drop and generate

events

FILE-OFFICE Microsoft Office Publisher out of bounds read attempt 1:40965 Drop and generate

events

FILE-OFFICE Microsoft Office remote code execution attempt 1:4565 4 Drop and generate

events

FILE-OFFICE Microsoft Office remote code execution attempt 1:4565 5 Drop and generate FILE-OFFICE Microsoft Office request for api-ms-win-core-winrt-l1 -1-0.dll over SMB attempt 1:37263 Drop and generate FILE-OFFICE Microsoft Office request for elsext.dll over SMB atte mpt 1:37001 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office request for mfplat.dll over SMB atte mpt 1:37261 Drop and generate

events

FILE-OFFICE Microsoft Office request for mqrt.dll over SMB attemp t 1:36993 Drop and generate

events

FILE-OFFICE Microsoft Office request for msdaora.dll over SMB att empt 1:37557 Drop and generate

events

FILE-OFFICE Microsoft Office request for nwdblib.dll over SMB att empt 1:37002 Drop and generate

events

FILE-OFFICE Microsoft Office request for phoneinfo.dll over SMB attempt 1:37558 Drop and generate

events

FILE-OFFICE Microsoft Office request for spframe.dll over SMB att empt 1:36995 Drop and generate

events

FILE-OFFICE Microsoft Office request for wuaext.dll over SMB atte mpt 1:36930 Drop and generate

events

FILE-OFFICE Microsoft Office RTF double-free remote code executio n attempt 1:34086 Drop and generate

events

FILE-OFFICE Microsoft Office RTF embedded ole file out of bounds write attempt 1:46561 Drop and generate

events

FILE-OFFICE Microsoft Office RTF footnote format use after free attempt 1:41577 Drop and generate FILE-OFFICE Microsoft Office RTF out-of-bounds array access remot e code execution attempt 1:34093 Drop and generate FILE-OFFICE Microsoft Office RTF parser heap overflow attempt 1:3 7273 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office RTF WRAssembly ASLR bypass download attempt 1:39528 Drop and generate

events

FILE-OFFICE Microsoft Office SDTI signed integer underflow attemp t 1:27850 Generate events

FILE-OFFICE Microsoft Office spframe.dll dll-load exploit attempt 1:36996 Drop and generate

events

FILE-OFFICE Microsoft Office Visio request for visdlgu.dll over S MB attempt 1:40080 Drop and generate

events

FILE-OFFICE Microsoft Office Visio TAG\_xxxSheet code execution at tempt 1:26163 Drop and generate

events

FILE-OFFICE Microsoft Office Visio visdlgu.dll dll-load exploit attempt 1:40079 Drop and generate FILE-OFFICE Microsoft Office Word 2003 macro byte opcode large da ta structure arbitrary code execution attempt 1:28205 Drop and generate FILE-OFFICE Microsoft Office Word 2010 Sepx memory corruption att empt 1:42755 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office Word 2016 use after free attempt 1:4 3159 Drop and generate

events

FILE-OFFICE Microsoft Office Word ActiveX object uninitialized me mory access attempt 1:34743 Drop and generate

events

FILE-OFFICE Microsoft Office Word ActiveX object uninitialized me mory access attempt 1:37409 Drop and generate

events

FILE-OFFICE Microsoft Office Word array index out-of-bounds attempt 1:32711 Drop and generate

events

FILE-OFFICE Microsoft Office Word BCSRuntime.dll dll-load exploit attempt 1:37588 Drop and generate

events

FILE-OFFICE Microsoft Office Word bitmap stream parsing remote co de execution attempt 1:38110 Drop and generate

events

FILE-OFFICE Microsoft Office Word bitmap stream parsing remote co de execution attempt 1:38111 Drop and generate FILE-OFFICE Microsoft Office Word document invalid cell count mem ory corruption attempt 1:27854 Drop and generate FILE-OFFICE Microsoft Office Word document invalid cell count mem ory corruption attempt 1:27856 Drop and generate FILE-OFFICE Microsoft Office Word Document invalid directory entr y use after free attempt 1:35497 Drop and generate FILE-OFFICE Microsoft Office Word document memory corruption atte mpt 1:34062 Drop and generate

events

events

events

events

events

FILE-OFFICE Microsoft Office Word docx subDocument file include attempt 1:45370 Drop and generate

events

FILE-OFFICE Microsoft Office Word EPS filter PostScript object us e after free attempt 1:36026 Drop and generate

events

FILE-OFFICE Microsoft Office Word external document access use-af ter-free attempt 1:37598 Drop and generate

events

FILE-OFFICE Microsoft Office Word FGetCpFlowDr memory corruption attempt 1:36740 Drop and generate

events

FILE-OFFICE Microsoft Office Word gdiplus integer overflow attemp t 1:36965 Drop and generate

events

FILE-OFFICE Microsoft Office Word incomplete ActiveX control use- after-free attempt 1:35503 Drop and generate

events

FILE-OFFICE Microsoft Office Word incorrect ptCount element denia l of service attempt 1:34428 Drop and generate FILE-OFFICE Microsoft Office Word incorrect schema property remot e code execution attempt 1:33715 Drop and generate FILE-OFFICE Microsoft Office Word invalid number of cells memory corruption attempt 1:27852 Drop and generate

events

events

events

FILE-OFFICE Microsoft Office Word ipdesign.dll ActiveX object acc ess attempt 1:38126 Drop and generate

events

FILE-OFFICE Microsoft Office Word ipdesign.dll ActiveX object acc ess attempt 1:38127 Drop and generate

events

FILE-OFFICE Microsoft Office Word malformed document file use aft er free attempt 1:35521 Drop and generate

events

FILE-OFFICE Microsoft Office Word malformed jpeg memory corruptio n attempt 1:39835 Drop and generate

events

FILE-OFFICE Microsoft Office Word malformed OCXINFO element EoP attempt 1:27858 Drop and generate

events

FILE-OFFICE Microsoft Office Word mso.dll subcomponent use after free attempt 1:39221 Drop and generate

events

FILE-OFFICE Microsoft Office Word mso.dll use-after-free attempt 1:35505 Drop and generate

events

FILE-OFFICE Microsoft Office Word msptls.dll integer underflow at tempt 1:35511 Drop and generate

events

FILE-OFFICE Microsoft Office Word nested tblStylePr element use a fter free attempt 1:35018 Drop and generate

events

FILE-OFFICE Microsoft Office Word nested tblStylePr element use a fter free attempt 1:35020 Drop and generate

events

FILE-OFFICE Microsoft Office Word OCX use after free attempt 1:35 201 Drop and generate

events

FILE-OFFICE Microsoft Office Word OGL module out of bounds read attempt 1:36966 Drop and generate

events

FILE-OFFICE Microsoft Office Word OGL module out of bounds read attempt 1:36967 Drop and generate

events

FILE-OFFICE Microsoft Office Word OLMAPI32.dll dll-load exploit attempt 1:37589 Drop and generate

events

FILE-OFFICE Microsoft Office Word out of bounds memory read attempt 1:40701 Drop and generate

events

FILE-OFFICE Microsoft Office Word Out-of-Bounds Write attempt 1:4 1140 Drop and generate

events

FILE-OFFICE Microsoft Office Word PmwdFromDoc use after free atte mpt 1:36716 Drop and generate

events

FILE-OFFICE Microsoft Office Word pointer release validation use after free attempt 1:36934 Drop and generate

events

FILE-OFFICE Microsoft Office Word PrcData out of bounds read atte mpt 1:40667 Drop and generate

events

FILE-OFFICE Microsoft Office Word request for BCSRuntime.dll over SMB attempt 1:37590 Drop and generate

events

FILE-OFFICE Microsoft Office Word request for OLMAPI32.dll over S MB attempt 1:37591 Drop and generate FILE-OFFICE Microsoft Office Word RTF Control.TaskSymbol.1 heap c orruption attempt - Win.Trojan.Sofacy 1:35325 Drop and generate

events

events

FILE-OFFICE Microsoft Office Word rtf file ffdefres integer under flow attempt 1:37559 Drop and generate

events

FILE-OFFICE Microsoft Office Word RTF file parsing buffer overflo w attempt 1:40368 Drop and generate

events

FILE-OFFICE Microsoft Office Word rtf invalid listoverridecount v alue attempt 1:24974 Drop and generate

events

FILE-OFFICE Microsoft Office Word styleWithEffects use-after-free attempt 1:32147 Drop and generate

events

FILE-OFFICE Microsoft Office Word template remote code execution attempt 1:41962 Drop and generate

events

FILE-OFFICE Microsoft Office Word TTF out-of-bounds memory access attempt 1:38782 Drop and generate

events

FILE-OFFICE Microsoft Office Word unsupported XML schema out of b ounds read attempt 1:39520 Drop and generate

events

FILE-OFFICE Microsoft Office Word with embedded Flash file transf er 1:18546 Drop and generate FILE-OFFICE Microsoft Office Word WordPerfect converter EnumFontF amProc use after free attempt 1:34739 Drop and generate FILE-OFFICE Microsoft Office Word WordPerfect converter ForeignTo Rtf32 use after free attempt 1:34737 Drop and generate FILE-OFFICE Microsoft Office Word wwlib out of bounds memory acce ss attempt 1:39518 Drop and generate

events

events

events

events

FILE-OFFICE Microsoft Office Word wwlib out of bounds read attemp t 1:40673 Drop and generate

events

FILE-OFFICE Microsoft Office Word wwlib out of bounds read attemp t 1:40679 Drop and generate

events

FILE-OFFICE Microsoft Office Word wwlib out of bounds read attemp t 1:39831 Drop and generate

events

FILE-OFFICE Microsoft Office Word wwlib out-of-bounds memory acce ss attempt 1:39503 Drop and generate

events

FILE-OFFICE Microsoft Office Word wwlib use after free attempt 1: 33350 Drop and generate FILE-OFFICE Microsoft Office Word wwlib.dll corrupt fcPlcfFldMom out of bounds read attempt 1:35501 Drop and generate FILE-OFFICE Microsoft Office Word wwlib.dll corrupt fcPlcfFldMom uninitialized memory access attempt 1:36203 Drop and generate FILE-OFFICE Microsoft Office Word wwlib.dll invalid pointer read attempt 1:38100 Drop and generate

events

events

events

events

FILE-OFFICE Microsoft Office Word wwlib.dll out of bounds read at tempt 1:35509 Drop and generate

events

FILE-OFFICE Microsoft Office Word XML parsing use after free atte mpt 1:36960 Drop and generate

events

FILE-OFFICE Microsoft Office Word XST structure out of bounds rea d attempt 1:40951 Drop and generate

events

FILE-OFFICE Microsoft Office wuaext.dll dll-load exploit attempt 1:36931 Drop and generate

events

FILE-OFFICE Microsoft Office XML nested num tag double-free attempt 1:36244 Drop and generate

events

FILE-OFFICE Microsoft Office XML nested num tag double-free attempt 1:34066 Drop and generate

events

FILE-OFFICE Microsoft Outlook email rules file memory corruption attempt 1:48403 Drop and generate

FILE-OFFICE Microsoft Outlook rwz file memory corruption attempt 1:48406 Drop and generate

events

FILE-OFFICE Microsoft Outlook rwz file memory corruption attempt 1:48407 Drop and generate

events

FILE-OFFICE Microsoft Outlook rwz file memory corruption attempt 1:48408 Drop and generate

events

FILE-OFFICE Microsoft Outlook use-after-free vulnerability attemp t 1:46601 Drop and generate

events

FILE-OFFICE Microsoft Outlook use-after-free vulnerability attemp t 1:46602 Drop and generate

events

FILE-OFFICE Microsoft PowerPoint ntdll out of bounds read attempt 1:40681 Drop and generate

events

FILE-OFFICE Microsoft Powerpoint shape object null pointer derefe rence attempt 1:37579 Drop and generate FILE-OFFICE Microsoft Powerpoint shape objects null pointer deref erence memory corruption attempt 1:37600 Drop and generate FILE-OFFICE Microsoft Visio lmetaclasscount buffer overflow attempt 1:36427 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:31926 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21937 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:23305 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21896 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21897 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21898 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21899 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21900 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21901 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21902 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21903 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21904 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21905 Drop and generate FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt 1:21906 Drop and generate FILE-OFFICE Microsoft Windows common controls stack buffer overfl ow via malicious MSComctlLib object attempt 1:30161 Drop and generate FILE-OFFICE Microsoft Windows common controls stack buffer overfl ow via malicious toolbar and author attempt 1:30165 Drop and generate FILE-OFFICE Microsoft Windows common controls stack buffer overfl ow via MIME HTML document attempt 1:30153 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

FILE-OFFICE Microsoft Windows common controls stack buffer overfl ow via MIME HTML document attempt 1:30159 Drop and generate

events

FILE-OFFICE Microsoft Windows OLE Packer Remote Code Execution at tempt 1:36147 Drop and generate

events

FILE-OFFICE Microsoft Windows OLE Packer Remote Code Execution at tempt 1:36148 Drop and generate

events

FILE-OFFICE Microsoft Word document malicious iframe code injecti on attempt 1:48423 Drop and generate

events

FILE-OFFICE Microsoft Word document malicious iframe code injecti on attempt 1:48424 Drop and generate

events

FILE-OFFICE Microsoft Word malformed RTF memory corruption attemp t 1:46940 Drop and generate

events

FILE-OFFICE Microsoft Word malformed RTF memory corruption attemp t 1:46941 Drop and generate FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary co de execution attempt 1:21797 Drop and generate FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary co de execution attempt 1:21798 Drop and generate FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary co de execution attempt 1:21799 Drop and generate FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary co de execution attempt 1:21800 Drop and generate FILE-OFFICE MSCOMCTL ActiveX control deserialization arbitrary co de execution attempt 1:21801 Drop and generate FILE-OFFICE OpenOffice Word document table parsing multiple heap based buffer overflow attempt 3:17665 Drop and generate FILE-OFFICE Powerpoint mouseover powershell malware download atte mpt 1:43179 Drop and generate

events

events

events

events

events

events

events

events

FILE-OFFICE RFT document malformed header 1:38580 Drop and generate

events

FILE-OFFICE RTF Composite Moniker object creation attempt 1:45415 Drop and generate

events

FILE-OFFICE RTF document incorrect file magic attempt 1:39526 Drop and generate

events

FILE-OFFICE Symantec multiple product Dec2SS PowerPoint file buff er overflow attempt 1:39417 Drop and generate

events

FILE-OFFICE Symantec multiple product Dec2SS PowerPoint file buff er overflow attempt 1:39418 Drop and generate

events

FILE-OFFICE Symantec multiple product Dec2SS PowerPoint file buff er overflow attempt 1:39419 Drop and generate

events

FILE-OFFICE Symantec multiple product Dec2SS PowerPoint file buff er overflow attempt 1:39420 Drop and generate

events

FILE-OFFICE Symantec multiple product Dec2SS PowerPoint file buff er overflow attempt 1:39421 Drop and generate

events

FILE-OFFICE Symantec multiple product Dec2SS PowerPoint file buff er overflow attempt 1:39422 Drop and generate

events

FILE-OTHER Acrobat Adobe Pro XPS out-of-bounds read attempt 1:479 93 Drop and generate

events

FILE-OTHER Acrobat Adobe Pro XPS out-of-bounds read attempt 1:479 94 Drop and generate

events

FILE-OTHER Adobe Acrobat DC invalid TIFF tagtype out of bounds re ad attempt 1:38954 Drop and generate

FILE-OTHER Adobe Acrobat EMF embedded DIB out of bound read attempt 1:46699 Drop and generate

events

FILE-OTHER Adobe Acrobat EMF embedded GIF LZW compression out of bound read attempt 1:46727 Drop and generate FILE-OTHER Adobe Acrobat EMF embedded GIF LZW compression out of bound read attempt 1:46728 Drop and generate FILE-OTHER Adobe Acrobat EMF file GIF LZW coding table memory cor ruption attempt 1:43893 Drop and generate

events

events

events

FILE-OTHER Adobe Acrobat EMF file GIF sub-block memory corruption attempt 1:43916 Drop and generate

events

FILE-OTHER Adobe Acrobat EMF file kerning data memory corruption attempt 1:43963 Drop and generate

events

FILE-OTHER Adobe Acrobat EMF line segments memory corruption atte mpt 1:44086 Drop and generate FILE-OTHER Adobe Acrobat EMF malformed EmfPlusPointF object buffe r overflow attempt 1:46707 Drop and generate FILE-OTHER Adobe Acrobat EMF malformed EmfPlusPointF object buffe r overflow attempt 1:46708 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF Alphablend memory corruption att empt 1:47131 Drop and generate

events

events

events

events

FILE-OTHER Adobe Acrobat Pro EMF Alphablend memory corruption att empt 1:47132 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF embedded GIF memory corruption attempt 1:46694 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF embedded GIF memory corruption attempt 1:46695 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawPath out of bounds re ad attempt 1:47354 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawPath out of bounds re ad attempt 1:47355 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawRects record out of b ounds read attempt 1:45819 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawRects record out of b ounds read attempt 1:45820 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawRects record out of b ounds read attempt 1:45821 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawRects record out of b ounds read attempt 1:45822 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF EMR\_STRETCHDIBITS size out of bo unds read attempt 1:46703 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF EMR\_STRETCHDIBITS size out of bo unds read attempt 1:46704 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF file out-of-bounds read attempt 1:48074 Drop and generate

events

events

events

events

events

events

events

events

FILE-OTHER Adobe Acrobat Pro EMF file out-of-bounds read attempt 1:48075 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF file out-of-bounds write attempt 1:47959 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF file out-of-bounds write attempt 1:47960 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF file out-of-bounds write attempt 1:48107 Drop and generate

FILE-OTHER Adobe Acrobat Pro EMF file use-after-free attempt 1:48 034 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF ImageConversion out-of-bounds wr ite attempt 1:48124 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF ImageConversion out-of-bounds wr ite attempt 1:48125 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF ImageConversion out-of-bounds wr ite attempt 1:47926 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF ImageConversion out-of-bounds wr ite attempt 1:47927 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF malformed bitmap rectangle desti nation out of bounds read attempt 1:45849 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF malformed bitmap rectangle desti nation out of bounds read attempt 1:45850 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF malformed bitmap rectangle desti nation out of bounds read attempt 1:45851 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF malformed bitmap rectangle desti nation out of bounds read attempt 1:45852 Drop and generate FILE-OTHER Adobe Acrobat Pro EMF memory corruption attempt 1:4797 5 Drop and generate

events

events

events

events

events

events

FILE-OTHER Adobe Acrobat Pro EMF memory corruption attempt 1:4797 6 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF out of bounds read attempt 1:468 12 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF out of bounds read attempt 1:468 13 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF out of bounds read attempt 1:467 33 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF out of bounds read attempt 1:467 34 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF out-of-bounds read attempt 1:479 83 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF out-of-bounds read attempt 1:479 84 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF RegionNodeCount out-of-bounds wr ite attempt 1:47308 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF RegionNodeCount out-of-bounds wr ite attempt 1:47309 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF use-after-free attempt 1:47193 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro EMF use-after-free attempt 1:47194 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro malformed EMF out of bounds read att empt 1:48242 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro malformed EMF out of bounds read att empt 1:48243 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro nested IFD out of bounds read attemp t 1:45793 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro nested IFD out of bounds read attemp t 1:45794 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro path element out of bounds memory ac cess attempt 1:45989 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro path element out of bounds memory ac cess attempt 1:45990 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro path rendertransform out of bound wr ite attempt 1:46691 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro PDX malformed index out of bounds me mory read attempt 1:46651 Drop and generate FILE-OTHER Adobe Acrobat Pro PDX malformed index out of bounds me mory read attempt 1:46652 Drop and generate FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:44984 Drop and generate

events

events

events

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45786 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45787 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45665 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45666 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45667 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt 1:45668 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro untrusted pointer dereference attemp t 1:47630 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro untrusted pointer dereference attemp t 1:47631 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro WebCapture out of bounds read attemp t 1:44927 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS file out-of-bounds read attempt 1:47987 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS file out-of-bounds read attempt 1:47988 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS heap overflow attempt 1:47217 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS heap overflow attempt 1:47218 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS malformed TIFF data out of bound s access attempt 1:45860 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS malformed TIFF data out of bound s access attempt 1:45861 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS out-of-bounds read attempt 1:472 37 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS out-of-bounds read attempt 1:472 38 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS out-of-bounds read attempt 1:472 08 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS out-of-bounds read attempt 1:472 09 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS out-of-bounds write attempt 1:47 985 Drop and generate

events

FILE-OTHER Adobe Acrobat Pro XPS out-of-bounds write attempt 1:47 986 Drop and generate FILE-OTHER Adobe Acrobat Professional EMF file JPEG Huffman table memory corrupt attempt 1:44033 Drop and generate FILE-OTHER Adobe Acrobat Professional XPS2PDF memory corruption attempt 1:43900 Drop and generate

events

events

events

FILE-OTHER Adobe Acrobat Reader FDF submitForm cross-site scripti ng attempt 1:28575 Generate events

FILE-OTHER Adobe Acrobat Reader jp2 double free attempt 1:46659 Drop and generate

events

FILE-OTHER Adobe Acrobat Reader jp2 double free attempt 1:46660 Drop and generate

events

FILE-OTHER Adobe Acrobat Reader U3D engine memory corruption atte mpt 1:48217 Drop and generate

events

FILE-OTHER Adobe Acrobat Reader U3D engine memory corruption atte mpt 1:48218 Drop and generate

events

FILE-OTHER Adobe Acrobat request for updaternotifications.dll ove r SMB attempt 1:38171 Drop and generate

events

FILE-OTHER Adobe AcrobatDC EMF buffer underflow attempt 1:41635 Drop and generate

events

FILE-OTHER Adobe Flash Player ATF image file out of bounds read attempt 1:46264 Drop and generate

events

FILE-OTHER Adobe Flash Player ATF image file out of bounds read attempt 1:46265 Drop and generate

events

FILE-OTHER Adobe Flash Player h264 decoder heap overflow attempt 1:41613 Drop and generate

events

FILE-OTHER Adobe Flash Player h264 decoder heap overflow attempt 1:41615 Drop and generate

events

FILE-OTHER Adobe Flash Player h264 decoder heap overflow attempt 1:41617 Drop and generate FILE-OTHER Adobe Flash Player h264 decoder luminance adjustment o ut of bounds memory access attempt 1:41611 Drop and generate FILE-OTHER Adobe Flash Player invalid mpd memory corruption attempt 1:34518 Drop and generate

events

events

events

FILE-OTHER Adobe Flash Player javascript parsing cross site scrip ting attempt 1:37441 Drop and generate

events

FILE-OTHER Adobe Flash Player malformed JPEG XR heap overflow att empt 1:39277 Drop and generate

events

FILE-OTHER Adobe Flash Player mp4 avcC atom memory corruption att empt 1:34510 Drop and generate

events

FILE-OTHER Adobe Flash Player mp4 avcC atom memory corruption att empt 1:34511 Drop and generate FILE-OTHER Adobe Flash Player mp4 h264 decompression routine out of bounds read attempt 1:41631 Drop and generate FILE-OTHER Adobe Flash Player unsupported video encoding remote c ode execution attempt 1:37778 Drop and generate FILE-OTHER Adobe Professional EMF embedded image heap overflow at tempt 1:46709 Drop and generate

events

events

events

events

FILE-OTHER Adobe Professional EMF embedded image heap overflow at tempt 1:46710 Drop and generate

events

FILE-OTHER Adobe Professional EMF embedded image heap overflow at tempt 1:47628 Drop and generate

events

FILE-OTHER Adobe Professional EMF embedded image heap overflow at tempt 1:47629 Drop and generate

events

FILE-OTHER Adobe Reader CoolType.DLL out-of-bounds memory access attempt 1:33454 Drop and generate

events

FILE-OTHER AfterMidnight post exploitation tool aftermidnight.dll dll-load exploit attempt 1:42890 Drop and generate FILE-OTHER AfterMidnight post exploitation tool request for after midnight.dll over SMB attempt 1:42891 Drop and generate

events

events

FILE-OTHER ATMFD Adobe font driver reserved command denial of ser vice attempt 1:30240 Drop and generate

events

FILE-OTHER ATMFD Adobe font driver reserved command denial of ser vice attempt 1:30241 Drop and generate

events

FILE-OTHER ATMFD Adobe font driver reserved command denial of ser vice attempt 1:28202 Drop and generate

events

FILE-OTHER ATMFD Adobe font driver reserved command denial of ser vice attempt 1:28203 Drop and generate

events

FILE-OTHER Cisco IOS-XE update directory traversal attempt 3:4076 7 Drop and generate

events

FILE-OTHER Cisco IOS-XE update directory traversal attempt 3:4076 9 Drop and generate FILE-OTHER Cisco Webex ARF Player LZW decompress memory corruptio n denial of service attempt 3:30942 Drop and generate FILE-OTHER Cisco WebEx Network Recording Player for ARF files dll -load exploit attempt 3:45524 Drop and generate

events

events

events

FILE-OTHER Cisco WebEx Network Recording Player for ARF files dll -load exploit attempt 3:45525 Drop and generate

events

FILE-OTHER Cisco WebEx Network Recording Player out of bounds wri te attempt 3:47394 Drop and generate

events

FILE-OTHER Cisco WebEx Network Recording Player out of bounds wri te attempt 3:47395 Drop and generate

events

FILE-OTHER Cisco WebEx Network Recording Player out of bounds wri te attempt 3:47363 Drop and generate

events

FILE-OTHER Cisco WebEx Network Recording Player out of bounds wri te attempt 3:47364 Drop and generate

events

FILE-OTHER Cisco WebEx Network Recording Player stack buffer over flow attempt 3:47878 Drop and generate

events

FILE-OTHER Cisco WebEx Network Recording Player stack buffer over flow attempt 3:47879 Drop and generate

events

FILE-OTHER Cisco WebEx Player atas32.dll memory overread attempt 3:30921 Drop and generate

events

FILE-OTHER Cisco Webex WRF heap corruption attempt 3:30912 Drop and generate

events

FILE-OTHER Cisco Webex WRF heap corruption attempt 3:30902 Drop and generate

events

FILE-OTHER CorelDRAW X8 EMF invalid ihBrush field value out of bo unds read attempt 1:41344 Drop and generate

events

FILE-OTHER EMF embedded image out of bound read attempt 1:45811 Drop and generate

events

FILE-OTHER EMF embedded image out of bound read attempt 1:45812 Drop and generate

events

FILE-OTHER EMF EmrText object out of bounds read attempt 1:45782 Drop and generate

events

FILE-OTHER EMF EmrText object out of bounds read attempt 1:45783 Drop and generate

events

FILE-OTHER GDCM DICOM image integer overflow attempt 1:38623 Drop and generate

events

FILE-OTHER GE Cimplicity bcl file loading external file attempt 1 :32256 Drop and generate

events

FILE-OTHER GE Cimplicity CimView load remote file attempt 1:32254 Drop and generate

events

FILE-OTHER GE Cimplicity CimView load remote file attempt 1:32255 Drop and generate

events

FILE-OTHER HDF5 H5O\_dtype\_decode\_helper heap buffer overflow atte mpt 1:40803 Drop and generate

events

FILE-OTHER InPage reader remote code execution attemptt 1:47440 Drop and generate

events

FILE-OTHER InPage reader remote code execution attemptt 1:47441 Drop and generate

events

FILE-OTHER IrfanView JPEG2000 reference tile width value buffer o verflow attempt 1:42177 Drop and generate

events

FILE-OTHER Java JRE sandbox breach attempt 1:21869 Generate events

FILE-OTHER Kingsoft Writer long font name buffer overflow attempt 1:37799 Drop and generate

events

FILE-OTHER Kingsoft Writer long font name buffer overflow attempt 1:30533 Drop and generate

events

FILE-OTHER Known malicious jar archive download attempt 1:26030 Drop and generate

events

FILE-OTHER Libgraphite empty feature list denial of service attempt 1:36225 Drop and generate

events

FILE-OTHER Libgraphite empty feature list denial of service attempt 1:36227 Drop and generate

events

FILE-OTHER Libgraphite LocaLookup out-of-bounds read attempt 1:36 212 Drop and generate

events

FILE-OTHER Microsoft .NET Resources file remote code execution at tempt 1:48122 Drop and generate

events

FILE-OTHER Microsoft .NET Resources file remote code execution at tempt 1:48123 Drop and generate

events

FILE-OTHER Microsoft Edge Chakra JavaScript engine out of bounds read attempt 1:38317 Drop and generate

events

FILE-OTHER Microsoft Graphics remote code execution attempt 1:475 19 Drop and generate

events

FILE-OTHER Microsoft Graphics remote code execution attempt 1:475 20 Drop and generate

events

FILE-OTHER Microsoft Internet Explorer malformed ico integer over flow attempt 1:40982 Drop and generate

events

FILE-OTHER Microsoft Internet Explorer malformed ico integer over flow attempt 1:40983 Drop and generate

events

FILE-OTHER Microsoft Internet Explorer SVG heap corruption attemp t 1:32166 Drop and generate

events

FILE-OTHER Microsoft Journal file exploitation attempt 1:34399 Drop and generate

events

FILE-OTHER Microsoft Journal file exploitation attempt 1:34400 Drop and generate

events

FILE-OTHER Microsoft Journal file parsing remote code execution attempt 1:35961 Drop and generate

events

FILE-OTHER Microsoft Journal file parsing remote code execution attempt 1:35962 Drop and generate

events

FILE-OTHER Microsoft Journal memory corruption attempt 1:34371 Drop and generate

events

FILE-OTHER Microsoft Journal memory corruption attempt 1:34372 Drop and generate

events

FILE-OTHER Microsoft Journal memory corruption attempt 1:34385 Drop and generate

events

FILE-OTHER Microsoft Journal memory corruption attempt 1:34386 Drop and generate

events

FILE-OTHER Microsoft Journal out of bounds read attempt 1:34390 Drop and generate

events

FILE-OTHER Microsoft Journal out of bounds read attempt 1:34403 Drop and generate

events

FILE-OTHER Microsoft Journal out of bounds read attempt 1:34404 Drop and generate

events

FILE-OTHER Microsoft Journal out of bounds write attempt 1:34387 Drop and generate

events

FILE-OTHER Microsoft Journal out of bounds write attempt 1:34388 Drop and generate

events

FILE-OTHER Microsoft LNK remote code execution attempt 1:47476 Drop and generate

events

FILE-OTHER Microsoft LNK remote code execution attempt 1:47477 Drop and generate

events

FILE-OTHER Microsoft Office OLE DLL side load attempt 1:40962 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:32313 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:32314 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:32315 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:32316 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:32186 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:32187 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:37726 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:37727 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:37824 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:37825 Drop and generate

events

FILE-OTHER Microsoft Office ole object external file loading atte mpt 1:38742 Drop and generate

events

FILE-OTHER Microsoft Office RTF out-of-bounds memory access attempt 1:40727 Drop and generate

events

FILE-OTHER Microsoft Office RTF out-of-bounds memory access attempt 1:41792 Drop and generate

events

FILE-OTHER Microsoft Office RTF out-of-bounds memory access attempt 1:33705 Drop and generate

events

FILE-OTHER Microsoft Windows .lnk shortcut file executing system3 2 executable attempt 1:46942 Drop and generate

events

FILE-OTHER Microsoft Windows .lnk shortcut file executing system3 2 executable attempt 1:46943 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file out-of-bounds memory access attempt 1:39260 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file out-of-bounds memory access attempt 1:39261 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file out-of-bounds memory access attempt 1:42148 Drop and generate

events

events

events

events

FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file out-of-bounds memory access attempt 1:42150 Drop and generate

events

FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file out-of-bounds memory access attempt 1:42151 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file remote code execution attempt 1:35495 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file remote code execution attempt 1:35496 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file remote code execution attempt 1:35483 Drop and generate FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file remote code execution attempt 1:35484 Drop and generate FILE-OTHER Microsoft Windows ATMFD kernel pool overflow attempt 1 :35304 Drop and generate

events

events

events

events

events

events

FILE-OTHER Microsoft Windows ATMFD kernel pool overflow attempt 1 :35305 Drop and generate FILE-OTHER Microsoft Windows atmfd.dll font driver malformed OTF file remote code execution attempt 1:38063 Drop and generate FILE-OTHER Microsoft Windows atmfd.dll font driver malformed OTF file remote code execution attempt 1:38064 Drop and generate FILE-OTHER Microsoft Windows atmfd.dll font driver malformed OTF file remote code execution attempt 1:35485 Drop and generate FILE-OTHER Microsoft Windows atmfd.dll font driver malformed OTF file remote code execution attempt 1:35486 Drop and generate FILE-OTHER Microsoft Windows BLF file local privilege escalation attempt 1:40689 Drop and generate

events

events

events

events

events

events

FILE-OTHER Microsoft Windows BLF file local privilege escalation attempt 1:40690 Drop and generate

events

FILE-OTHER Microsoft Windows BLF file local privilege escalation attempt 1:40691 Drop and generate

events

FILE-OTHER Microsoft Windows BLF file local privilege escalation attempt 1:40692 Drop and generate

events

FILE-OTHER Microsoft Windows Defender malformed RAR memory corrup tion attempt 1:46163 Drop and generate

events

FILE-OTHER Microsoft Windows Defender malformed RAR memory corrup tion attempt 1:46164 Drop and generate

events

FILE-OTHER Microsoft Windows Device Guard bypass via compiled hel p file attempt 1:43851 Drop and generate

events

FILE-OTHER Microsoft Windows Font Viewer cmap offset integer unde rflow attempt 1:36952 Drop and generate

events

FILE-OTHER Microsoft Windows Font Viewer cmap offset integer unde rflow attempt 1:36953 Drop and generate FILE-OTHER Microsoft Windows FontView OpenType Font atmfd.dll inv alid memory reference attempt 1:35517 Drop and generate FILE-OTHER Microsoft Windows FontView OpenType Font atmfd.dll inv alid memory reference attempt 1:35518 Drop and generate

events

events

events

FILE-OTHER Microsoft Windows GDI DrvQueryFontData function uninit ialized glyph data remote code execution attempt 1:35491

FILE-OTHER Microsoft Windows GDI DrvQueryFontData function uninit ialized glyph data remote code execution attempt 1:35492

Drop and generate events

Drop and generate events

FILE-OTHER Microsoft Windows GDI32.dll cmap numUVSMappings overfl ow attempt 1:40942 Drop and generate

FILE-OTHER Microsoft Windows Journal CWispTiss use after free att empt 1:37577 Drop and generate

events

FILE-OTHER Microsoft Windows Journal CWispTiss use after free att empt 1:37578 Drop and generate

events

FILE-OTHER Microsoft Windows Journal integer overflow attempt 1:3 6697 Drop and generate

events

FILE-OTHER Microsoft Windows Journal integer overflow attempt 1:3 6698 Drop and generate FILE-OTHER Microsoft Windows kernel-mode driver TTF file glyf tab le out of bounds attempt 1:35519 Drop and generate FILE-OTHER Microsoft Windows kernel-mode driver TTF file glyf tab le out of bounds attempt 1:35520 Drop and generate FILE-OTHER Microsoft Windows malformed TrueType file RCVT out of bounds read attempt 1:40408 Drop and generate FILE-OTHER Microsoft Windows malformed TrueType file RCVT out of bounds read attempt 1:40409 Drop and generate FILE-OTHER Microsoft Windows malformed TrueType file remote code execution attempt 1:36736 Drop and generate

events

events

events

events

events

events

FILE-OTHER Microsoft Windows malformed TrueType file remote code execution attempt 1:36737 Drop and generate

events

FILE-OTHER Microsoft Windows malformed TTF integer overflow attempt 1:46188 Drop and generate

events

FILE-OTHER Microsoft Windows malformed TTF integer overflow attempt 1:46189 Drop and generate

events

FILE-OTHER Microsoft Windows Media Center link file code executio n attempt 1:35983 Drop and generate

events

FILE-OTHER Microsoft Windows Media Center link file code executio n attempt 1:38778 Drop and generate

events

FILE-OTHER Microsoft Windows Media Center link file code executio n attempt 1:38779 Drop and generate

events

FILE-OTHER Microsoft Windows OTF cmap table parsing integer overf low attempt 1:40705 Drop and generate

events

FILE-OTHER Microsoft Windows OTF cmap table parsing integer overf low attempt 1:40706 Drop and generate

events

FILE-OTHER Microsoft Windows OTF file parsing error exploitation attempt 1:35489 Drop and generate

events

FILE-OTHER Microsoft Windows OTF file parsing error exploitation attempt 1:35490 Drop and generate

events

FILE-OTHER Microsoft Windows TTF file out of bounds access attemp t 1:41991 Drop and generate FILE-OTHER Microsoft Windows Type 1 font blend operator negative operand code execution attempt 1:33724 Drop and generate FILE-OTHER Microsoft Windows Type 1 font blend operator negative operand code execution attempt 1:33725 Drop and generate FILE-OTHER Microsoft Windows Uniscribe privilege escalation attempt 1:41934 Drop and generate

events

events

events

events

FILE-OTHER Microsoft Windows Uniscribe privilege escalation attempt 1:41932 Drop and generate FILE-OTHER Microsoft Windows win32k.sys glyph bitmap boundary out of bounds memory access attempt 1:38493 Drop and generate FILE-OTHER Microsoft Windows win32k.sys glyph bitmap boundary out of bounds memory access attempt 1:38494 Drop and generate

events

events

FILE-OTHER Microsoft Word WordPerfect CSTYL border element stack overflow attempt 1:28502 Drop and generate

events

FILE-OTHER Microsoft Word WordPerfect CSTYL border element stack overflow attempt 1:36498 Drop and generate

events

FILE-OTHER Microsoft Word WordPerfect CSTYL border element stack overflow attempt 1:36501 Drop and generate

events

FILE-OTHER Microsoft XML invalid priority in xsl template 1:32501 Drop and generate

events

FILE-OTHER Microsoft XML invalid priority in xsl template 1:32502 Drop and generate

events

FILE-OTHER MSXML dynamic pointer casting arbitrary code execution attempt 1:25275 Drop and generate FILE-OTHER National Instruments LabVIEW LvVarientUnflatten remote code execution attempt 1:41370 Drop and generate FILE-OTHER Oniguruma expression parser out of bounds write attemp t 1:43181 Drop and generate

events

events

events

FILE-OTHER Oracle Java awt\_setPixels out-of-bounds read attempt 1 :32562 Drop and generate

events

FILE-OTHER Oracle Java SE GSUB FeatureCount Buffer Overflow attempt 1:32508 Drop and generate

events

FILE-OTHER Oracle OIT ContentAccess libvs\_mwkd out of bounds writ e attempt 1:38860 Drop and generate

events

FILE-OTHER overly large XML file MSXML heap overflow attempt 1:28 286 Drop and generate

events

FILE-OTHER overly large XML file MSXML heap overflow attempt 1:25 270 Drop and generate

events

FILE-OTHER RealNetworks RealPlayer RMP file heap buffer overflow attempt 1:29207 Drop and generate

events

FILE-OTHER RealNetworks RealPlayer RMP file heap buffer overflow attempt 1:29208 Drop and generate

events

FILE-OTHER RealNetworks RealPlayer RMP file heap buffer overflow attempt 1:29209 Drop and generate

events

FILE-OTHER RealNetworks RealPlayer RMP stack buffer overflow atte mpt 1:29182 Drop and generate

events

FILE-OTHER RealNetworks RealPlayer RMP stack buffer overflow atte mpt 1:29183 Drop and generate

events

FILE-OTHER SIL LibGraphite BracketPairStack out of bounds access exploit attempt 1:36385 Drop and generate FILE-OTHER Symantec Antivirus ALPkOldFormatDecompressor out of bo unds read attempt 1:39402 Drop and generate FILE-OTHER Symantec Norton Antivirus ccScanw.dll Unpack ShortLZ m emory corruption attempt 1:39385 Drop and generate FILE-OTHER Symantec TNEF decoder integer overflow attempt 1:39431 Drop and generate

events

events

events

events

FILE-OTHER Tablib yaml.load code execution attempt 1:42195 Drop and generate

events

FILE-OTHER TrueType Font Windows EOT font engine remote code exec ution attempt 1:46186 Drop and generate

events

FILE-OTHER TrueType Font Windows EOT font engine remote code exec ution attempt 1:46187 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46003 Drop and generate

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46006 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46007 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46008 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46009 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46010 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46011 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46012 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46013 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46014 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46015 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46016 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46017 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46018 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46019 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46020 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46021 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER SFVRT-1035 attack attempt 3:46022 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER TALOS-2015-0002 attack attempt 3:36210 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER TALOS-2015-0011 attack attempt 3:35727 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER TALOS-2016-0195 attack attempt 3:40299 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER TALOS-2018-0670 attack attempt 3:47721 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER TALOS-2018-0670 attack attempt 3:47722 Drop and generate

events

FILE-OTHER TRUFFLEHUNTER TALOS-CAN-0053 attack attempt 3:36214 Drop and generate

events

FILE-OTHER Type 1 font memory out-of-bounds read attempt 1:33722 Drop and generate

events

FILE-OTHER Type 1 font memory out-of-bounds read attempt 1:33723 Drop and generate

events

FILE-OTHER Visual Basic scripting engine Filter argument mishandl ing attempt 1:36441 Drop and generate

FILE-PDF Acrobat malformed html tag out of bounds read attempt 1: 44967 Drop and generate

events

FILE-PDF Acrobat Reader FontDescriptor object type confusion atte mpt 1:43883 Drop and generate

events

FILE-PDF Acrobat Reader Open Cascade Library memory corruption at tempt 1:40778 Drop and generate FILE-PDF Acrobat Reader PDFDocEncoding object WinAnsiEncoding mem ory corruption attempt 1:43877 Drop and generate FILE-PDF Acrobat Reader TIFF malformed IFD tag heap overflow atte mpt 1:42910 Drop and generate

events

events

events

FILE-PDF Acrobat Reader TIFF malformed IFD tag heap overflow atte mpt 1:42912 Drop and generate

events

FILE-PDF Acrobat Reader TIFF malformed IFD tag heap overflow atte mpt 1:42914 Drop and generate

events

FILE-PDF Acrobat TrueTypeFont file out of bounds read attempt 1:4 4949 Drop and generate

events

FILE-PDF Adobe Acrobat addAnnot object untrusted pointer derefere nce attempt 1:44873 Drop and generate FILE-PDF Adobe Acrobat and Adobe Acrobat Reader field dictionary null pointer dereference attempt 1:28597 Drop and generate FILE-PDF Adobe Acrobat animateSyncButton use after free attempt 1 :41142 Drop and generate FILE-PDF Adobe Acrobat CoolType font representation decoding memo ry corruption attempt 1:37458 Drop and generate FILE-PDF Adobe Acrobat CoolType malformed font memory corruption attempt 1:37454 Drop and generate FILE-PDF Adobe Acrobat embedded JPEG2000 invalid header out of bo unds memory access attempt 1:42309 Drop and generate FILE-PDF Adobe Acrobat field dictionary value Unicode buffer over flow attempt 1:44940 Drop and generate

events

events

events

events

events

events

events

FILE-PDF Adobe Acrobat FileAttachment use-after-free attempt 1:38 799 Drop and generate

events

FILE-PDF Adobe Acrobat PDF font character encoding out of bounds write attempt 1:44987 Drop and generate

events

FILE-PDF Adobe Acrobat Pro malformed embedded TTF file memory cor ruption attempt 1:47774 Drop and generate

events

FILE-PDF Adobe Acrobat Pro malformed embedded TTF file memory cor ruption attempt 1:47775 Drop and generate

events

FILE-PDF Adobe Acrobat Pro malformed embedded TTF file memory cor ruption attempt 1:47776 Drop and generate

events

FILE-PDF Adobe Acrobat Pro malformed embedded TTF file memory cor ruption attempt 1:47777 Drop and generate

events

FILE-PDF Adobe Acrobat Reader 11.0.09 keystroke combobox use afte r free attempt 1:34548 Drop and generate

events

FILE-PDF Adobe Acrobat Reader Acroform engine memory corruption attempt 1:39131 Drop and generate

events

FILE-PDF Adobe Acrobat Reader addAnnot invalid type conversion at tempt 1:34514 Drop and generate

events

FILE-PDF Adobe Acrobat Reader addAnnot invalid type conversion at tempt 1:34516 Drop and generate

events

FILE-PDF Adobe Acrobat Reader annotation oversized array memory c orruption attempt 1:38223 Drop and generate

FILE-PDF Adobe Acrobat Reader api call handling arbitrary executi on attempt 1:31021 Drop and generate

events

FILE-PDF Adobe Acrobat Reader APP13 heap overflow attempt 1:41329 Drop and generate

events

FILE-PDF Adobe Acrobat Reader badly formatted type 0 font attempt 1:28600 Drop and generate

events

FILE-PDF Adobe Acrobat Reader badly formatted type 0 font attempt 1:28601 Drop and generate

events

FILE-PDF Adobe Acrobat Reader bookmarkRoot memory corruption atte mpt 1:45862 Drop and generate

events

FILE-PDF Adobe Acrobat Reader bookmarkRoot memory corruption atte mpt 1:45863 Drop and generate

events

FILE-PDF Adobe Acrobat Reader bookmarkRoot memory corruption atte mpt 1:45864 Drop and generate

events

FILE-PDF Adobe Acrobat Reader bookmarkRoot memory corruption atte mpt 1:45865 Drop and generate

events

FILE-PDF Adobe Acrobat Reader ComboBox field Format action use-af ter-free attempt 1:35323 Drop and generate

events

FILE-PDF Adobe Acrobat Reader CoolType blend memory corruption at tempt 1:34524 Drop and generate

events

FILE-PDF Adobe Acrobat Reader Cooltype callother memory corruptio n attempt 1:34526 Drop and generate

events

FILE-PDF Adobe Acrobat Reader cross reference table memory corrup tion attempt 1:41320 Drop and generate

events

FILE-PDF Adobe Acrobat Reader CTJPEGWriter null pointer dereferen ce attempt 1:42896 Drop and generate

events

FILE-PDF Adobe Acrobat Reader custom string length function memor y corruption attempt 1:37399 Drop and generate

events

FILE-PDF Adobe Acrobat Reader DC OCG setIntent memory corruption attempt 1:46638 Drop and generate

events

FILE-PDF Adobe Acrobat Reader DC OCG setIntent memory corruption attempt 1:46639 Drop and generate

events

FILE-PDF Adobe Acrobat Reader DCT encoded stream null pointer der eference attempt 1:31011 Drop and generate

events

FILE-PDF Adobe Acrobat Reader duplicate U3D header memory corrupt ion attempt 1:43924 Drop and generate FILE-PDF Adobe Acrobat Reader embedded font type max subroutine b uffer overflow attempt 1:32834 Drop and generate FILE-PDF Adobe Acrobat Reader embedded font type max subroutine b uffer overflow attempt 1:32835 Drop and generate FILE-PDF Adobe Acrobat Reader embedded JavaScript remote code execution attempt 1:34557 Drop and generate

events

events

events

events

FILE-PDF Adobe Acrobat Reader embedded JPEG 2000 flst heap overfl ow attempt 1:42212 Drop and generate FILE-PDF Adobe Acrobat Reader embedded PRC stream NULL dereferenc e denial of service attempt 1:31612 Drop and generate FILE-PDF Adobe Acrobat Reader embedded TTF name record out of bou nds read attempt 1:39534 Drop and generate

events

events

events

FILE-PDF Adobe Acrobat Reader exportAsXFAStr use after free attempt 1:44013 Drop and generate

events

FILE-PDF Adobe Acrobat Reader font enumeration use after free att empt 1:46809 Drop and generate

FILE-PDF Adobe Acrobat Reader Forms Data Format embedded javascri pt attempt 1:43961 Drop and generate

events

FILE-PDF Adobe Acrobat Reader getAnnotsRichMedia return type conf usion attempt 1:45868 Drop and generate

events

FILE-PDF Adobe Acrobat Reader getAnnotsRichMedia return type conf usion attempt 1:45869 Drop and generate

events

FILE-PDF Adobe Acrobat Reader go-to action NTLM credential disclosure attempt 1:46675 Drop and generate

events

FILE-PDF Adobe Acrobat Reader go-to action NTLM credential disclosure attempt 1:46676 Drop and generate

events

FILE-PDF Adobe Acrobat Reader go-to action NTLM credential disclosure attempt 1:46677 Drop and generate

events

FILE-PDF Adobe Acrobat Reader go-to action NTLM credential disclosure attempt 1:46678 Drop and generate

events

FILE-PDF Adobe Acrobat Reader graphics engine memory corruption attempt 1:43977 Drop and generate

events

FILE-PDF Adobe Acrobat Reader graphics engine memory corruption attempt 1:43979 Drop and generate

events

FILE-PDF Adobe Acrobat Reader graphics engine memory corruption attempt 1:43991 Drop and generate

events

FILE-PDF Adobe Acrobat Reader graphics engine memory corruption attempt 1:43993 Drop and generate

events

FILE-PDF Adobe Acrobat Reader heap buffer overflow attempt 1:3465 0 Drop and generate

events

FILE-PDF Adobe Acrobat Reader heap-based buffer overflow attempt 1:25563 Drop and generate

events

FILE-PDF Adobe Acrobat Reader integer overflow attempt 1:31015 Drop and generate

events

FILE-PDF Adobe Acrobat Reader invalid JPEG stream double free att empt 1:29902 Drop and generate

events

FILE-PDF Adobe Acrobat Reader invalid JPEG stream double free att empt 1:29904 Drop and generate

events

FILE-PDF Adobe Acrobat Reader invalid trailer memory corruption attempt 1:45866 Drop and generate

events

FILE-PDF Adobe Acrobat Reader invalid trailer memory corruption attempt 1:45867 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JavaScript annotation use after fre e attempt 1:46721 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JavaScript annotation use after fre e attempt 1:46722 Drop and generate FILE-PDF Adobe Acrobat Reader JavaScript API trustPropagatorFunct ion execution bypass attempt 1:34550 Drop and generate FILE-PDF Adobe Acrobat Reader JavaScript data structure use after free attempt 1:46653 Drop and generate

events

events

events

FILE-PDF Adobe Acrobat Reader JavaScript data structure use after free attempt 1:46654 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JavaScript infinite recursion heap overflow attempt 1:44956 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JavaScript model privileged API byp ass attempt 1:37464 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JavaScript navigation pane use afte r free attempt 1:41150 Drop and generate

FILE-PDF Adobe Acrobat Reader javascript toolbar button use after free attempt 1:28843 Drop and generate

events

FILE-PDF Adobe Acrobat Reader javascript toolbar button use after free attempt 1:28845 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG malformed data out-of-bounds r ead attempt 1:47699 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG malformed data out-of-bounds r ead attempt 1:47700 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG parsing out of bounds read att empt 1:47438 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG parsing out of bounds read att empt 1:47439 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG2 row out of bounds memory corruption attempt 1:32819 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG2 symbol header out of bounds r ead attempt 1:47647 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JBIG2 symbol header out of bounds r ead attempt 1:47648 Drop and generate FILE-PDF Adobe Acrobat Reader JPEG engine spurious object referen ce use after free attempt 1:40455 Drop and generate FILE-PDF Adobe Acrobat Reader JPEG handling memory corruption att empt 1:39536 Drop and generate

events

events

events

FILE-PDF Adobe Acrobat Reader JPEG Huffman table memory corruptio n attempt 1:48100 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JPEG Huffman table memory corruptio n attempt 1:48101 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JPEG Huffman table memory corruptio n attempt 1:48102 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JPEG Huffman table memory corruptio n attempt 1:48103 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JPEG parsing out of bounds read att empt 1:39569 Drop and generate

events

FILE-PDF Adobe Acrobat Reader JS notification object double free attempt 1:34652 Drop and generate

events

FILE-PDF Adobe Acrobat Reader known malicious variable exploit at tempt 1:25818 Drop and generate

events

FILE-PDF Adobe Acrobat Reader length-compute UTF-16 string buffer overflow attempt 1:31008 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed AES key memory corruption attempt 1:42802 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed embeded TTF file memory c orruption attempt 1:39687 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed embeded TTF file memory c orruption attempt 1:39699 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed FlateDecode stream use af ter free attempt 1:38981 Drop and generate FILE-PDF Adobe Acrobat Reader malformed JBIG2 decode segment null pointer crash attempt 1:29062 Drop and generate FILE-PDF Adobe Acrobat Reader malformed object stream memory corruption attempt 1:40557 Drop and generate

events

events

events

FILE-PDF Adobe Acrobat Reader malformed PRC file out of bounds re ad attempt 1:42296 Drop and generate

FILE-PDF Adobe Acrobat Reader malformed shading modifier heap cor ruption attempt 1:20659 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed TrueType font memory corruption attempt 1:43998 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed U3D object use after free attempt 1:32813 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed unicode font name code ex ecution attempt 1:40515 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed URI information disclosur e attempt 1:42813 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed UTF-16 string memory corruption attempt 1:37397 Drop and generate

events

FILE-PDF Adobe Acrobat Reader malformed UTF-16 string memory corruption attempt 1:43886 Drop and generate

events

FILE-PDF Adobe Acrobat Reader memory disclosure attempt 1:28577 Drop and generate

events

FILE-PDF Adobe Acrobat Reader mishandling of invalid triangle edg e access attempt 1:35239 Drop and generate

events

FILE-PDF Adobe Acrobat Reader mishandling of invalid triangle edg e access attempt 1:35240 Drop and generate

events

FILE-PDF Adobe Acrobat Reader null pointer dereference attempt 1: 37469 Drop and generate

events

FILE-PDF Adobe Acrobat Reader openDoc dangling pointer attempt 1: 34559 Drop and generate

events

FILE-PDF Adobe Acrobat Reader OTF font head table size overflow attempt 1:28585 Drop and generate

events

FILE-PDF Adobe Acrobat Reader pattern object memory corruption at tempt 1:29669 Drop and generate

events

FILE-PDF Adobe Acrobat Reader PCR null pointer dereference attemp t 1:34546 Drop and generate FILE-PDF Adobe Acrobat Reader pdfshell preview mode - possible de nial of service attempt 1:37530 Drop and generate FILE-PDF Adobe Acrobat Reader pdfshell preview mode - possible de nial of service attempt 1:37531 Drop and generate FILE-PDF Adobe Acrobat Reader pointer dereference attempt 1:46723 Drop and generate

events

events

events

events

FILE-PDF Adobe Acrobat Reader pointer dereference attempt 1:46724 Drop and generate

events

FILE-PDF Adobe Acrobat Reader PostScript font parsing memory corruption attempt 1:39556 Drop and generate

events

FILE-PDF Adobe Acrobat Reader raster image memory corruption atte mpt 1:32815 Drop and generate

events

FILE-PDF Adobe Acrobat Reader raster image memory corruption atte mpt 1:39798 Drop and generate

events

FILE-PDF Adobe Acrobat Reader SaveAs use-after-free attempt 1:405 85 Drop and generate

events

FILE-PDF Adobe Acrobat Reader security bypass attempt 1:46680 Drop and generate

events

FILE-PDF Adobe Acrobat Reader security bypass attempt 1:46681 Drop and generate

events

FILE-PDF Adobe Acrobat Reader setPageAction use after free attemp t 1:34845 Drop and generate

FILE-PDF Adobe Acrobat Reader stateModel use-after-free attempt 1 :34592 Drop and generate

events

FILE-PDF Adobe Acrobat Reader string replacement heap overflow at tempt 1:32170 Drop and generate FILE-PDF Adobe Acrobat Reader structtreeroot children recursive c all denial of service attempt 1:25466 Drop and generate FILE-PDF Adobe Acrobat Reader structtreeroot children recursive c all denial of service attempt 1:25467 Drop and generate FILE-PDF Adobe Acrobat Reader TTF parsing bad cmap format attempt 1:25536 Drop and generate

events

events

events

events

FILE-PDF Adobe Acrobat Reader TTF remote code execution attempt 1 :28591 Drop and generate

events

FILE-PDF Adobe Acrobat Reader U3D CLODMeshDeceleration code execu tion attempt 1:20429 Drop and generate FILE-PDF Adobe Acrobat Reader U3D e3\_bone object out of bounds me mory access attempt 1:39454 Drop and generate FILE-PDF Adobe Acrobat Reader U3D format Line Set Continuation ou t-of-bounds memory access attempt 1:32021 Drop and generate FILE-PDF Adobe Acrobat Reader use-after-free attempt 1:47297 Drop and generate

events

events

events

events

FILE-PDF Adobe Acrobat Reader use-after-free attempt 1:47298 Drop and generate

events

FILE-PDF Adobe Acrobat Reader WillSave action use after free atte mpt 1:34473 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:26927 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:28252 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:28621 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:31686 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:37828 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:26651 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:31103 Drop and generate FILE-PDF Adobe Acrobat Reader X XML forms specially crafted RLE8 format BMP integer overflow attempt 1:31104 Drop and generate FILE-PDF Adobe Acrobat Reader XFA addInstance use after free atte mpt 1:40639 Drop and generate

events

events

events

events

events

events

events

events

events

events

FILE-PDF Adobe Acrobat Reader XFA app.setTimeOut memory corruptio n attempt 1:26021 Drop and generate FILE-PDF Adobe Acrobat Reader XFA engine memory leak - possible c ode instrumentation detected 1:38818 Drop and generate FILE-PDF Adobe Acrobat Reader XFA engine memory leak ASLR bypass attempt 1:38819 Drop and generate

events

events

events

FILE-PDF Adobe Acrobat Reader XFA excelGroup memory corruption at tempt 1:40575 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XFA form use after free attempt 1:4 6649 Drop and generate

FILE-PDF Adobe Acrobat Reader XFA relayoutPageArea memory corrupt ion attempt 1:40569 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XFA resolveNode memory corruption attempt 1:40573 Drop and generate

events

FILE-PDF Adobe Acrobat Reader xfa subform use after free attempt 1:41399 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XFA use after free attempt 1:46696 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XFA use after free attempt 1:46697 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XI JavaScript annotation use after free attempt 1:44857 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XLST parsing engine use after free attempt 1:48042 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XML Java used in app.setTimeOut 1:2 8658 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XObject image object use after free attempt 1:39153 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XRef object integer overflow attemp t 1:32793 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XSL multi-dimensional array memory corruption attempt 1:39532 Drop and generate

events

FILE-PDF Adobe Acrobat Reader XSLT substring memory corruption at tempt 1:40436 Drop and generate

events

FILE-PDF Adobe Acrobat thermometer object untrusted pointer deref erence attempt 1:44925 Drop and generate

events

FILE-PDF Adobe Acrobat U3D Bone Weight Modifier memory corruption attempt 1:37448 Drop and generate

events

FILE-PDF Adobe Acrobat XFA engine heap memory corruption attempt 1:43948 Drop and generate

events

FILE-PDF Adobe Acrobat XFA engine stack buffer overflow attempt 1 :41193 Drop and generate

events

FILE-PDF Adobe Acrobat XFA Engine use after free attempt 1:41325 Drop and generate

events

FILE-PDF Adobe Acrobat XFA field initialization memory corruption attempt 1:44083 Drop and generate

events

FILE-PDF ADOBE ActiveX Browser Plugin client side request injecti on attempt 1:46856 Drop and generate

events

FILE-PDF ADOBE ActiveX Browser Plugin client side request injecti on attempt 1:46857 Drop and generate

events

FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt 1:46490 Drop and generate

events

FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt 1:46491 Drop and generate

events

FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt 1:39703 Drop and generate

events

FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt 1:47223 Drop and generate

events

FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt 1:47224 Drop and generate

events

FILE-PDF Adobe Reader AcroForm dictionary object use after free attempt 1:39015 Drop and generate

FILE-PDF Adobe Reader compareDocuments JavaScript function use-af ter-free attempt 1:38923 Drop and generate

events

FILE-PDF Adobe Reader CoolType engine FlateDecode use-after-free attempt 1:39864 Drop and generate

events

FILE-PDF Adobe Reader corrupt bookmark use after free attempt 1:4 0571 Drop and generate

events

FILE-PDF Adobe Reader createAVView JavaScript use-after-free atte mpt 1:38918 Drop and generate

events

FILE-PDF Adobe Reader CTJPEGDecoderReadNextTile out of bounds rea d attempt 1:39013 Drop and generate FILE-PDF Adobe Reader DisablePermEnforcement JavaScript function use-after-free attempt 1:38911 Drop and generate FILE-PDF Adobe Reader double memory free call remote code executi on attempt 1:39098 Drop and generate

events

events

events

FILE-PDF Adobe Reader embedded font out of bounds memory access attempt 1:40236 Drop and generate

events

FILE-PDF Adobe Reader embedded TTF heap overflow attempt 1:39546 Drop and generate

events

FILE-PDF Adobe Reader execAVDialog JavaScript function use-after- free attempt 1:38991 Drop and generate

events

FILE-PDF Adobe Reader execMenuItem buffer overflow attempt 1:4390 5 Drop and generate

events

FILE-PDF Adobe Reader Graphic State Parameter Dictionaries use af ter free attempt 1:37460 Drop and generate

events

FILE-PDF Adobe Reader invalid object reference use after free att empt 1:42790 Drop and generate FILE-PDF Adobe Reader Javascript API ANSendForReview - possible p rivilege escalation attempt 1:35809 Drop and generate FILE-PDF Adobe Reader Javascript API ANStartApproval - possible p rivilege escalation attempt 1:35811 Drop and generate FILE-PDF Adobe Reader JavaScript API documentToStream use after f ree attempt 1:42175 Drop and generate

events

events

events

events

FILE-PDF Adobe Reader JavaScript recursive calls memory corruptio n attempt 1:40825 Drop and generate

events

FILE-PDF Adobe Reader javascript setExportValues field object use after free attempt 1:35380 Drop and generate

events

FILE-PDF Adobe Reader javascript setExportValues field object use after free attempt 1:35382 Drop and generate

events

FILE-PDF Adobe Reader JavaScript string from stream memory corrup tion attempt 1:42202 Drop and generate

events

FILE-PDF Adobe Reader JavaScript use after free attempt 1:40707 Drop and generate FILE-PDF Adobe Reader JPEG 2000 chrominance subsampling memory co rruption attempt 1:38211 Drop and generate FILE-PDF Adobe Reader JPEG 2000 memory corruption attempt 1:39028 Drop and generate

events

events

events

FILE-PDF Adobe Reader JPEG2000 chroma sub-pattern memory corruption attempt 1:37450 Drop and generate

events

FILE-PDF Adobe Reader JPEG2000 pclr tag out of bounds read attemp t 1:42275 Drop and generate

events

FILE-PDF Adobe Reader MakeMeasurement buffer overflow attempt 1:3 5308 Drop and generate

FILE-PDF Adobe Reader malformed ICC profile memory corruption att empt 1:39752 Drop and generate

events

FILE-PDF Adobe Reader malformed JPEG2000 image invalid colr size out of bounds read attempt 1:46731 Drop and generate FILE-PDF Adobe Reader malformed JPEG2000 image invalid colr size out of bounds read attempt 1:46732 Drop and generate FILE-PDF Adobe Reader malformed JPEG2000 image invalid NumberComp onents out of bounds read attempt 1:38966 Drop and generate FILE-PDF Adobe Reader malformed Universal 3D stream memory corrup tion attempt 1:38959 Drop and generate

events

events

events

events

FILE-PDF Adobe Reader nested events use-after-free attempt 1:3543 0 Drop and generate

events

FILE-PDF Adobe Reader parser object use-after-free attempt 1:4069 5 Drop and generate

events

FILE-PDF Adobe Reader PDF defineGetter execMenuItem use after fre e attempt 1:38899 Drop and generate

events

FILE-PDF Adobe Reader PDF embedded javascript events use after free attempt 1:44900 Drop and generate

events

FILE-PDF Adobe Reader PDF embedded JPEG memory corruption attempt 1:39102 Drop and generate

events

FILE-PDF Adobe Reader PDF execMenuItem use after free attempt 1:3 8907 Drop and generate

events

FILE-PDF Adobe Reader PDF memory corruption attempt 1:42859 Drop and generate

events

FILE-PDF Adobe Reader PDF onEvent execMenuItem use after free att empt 1:38900 Drop and generate

events

FILE-PDF Adobe Reader PDF setAction execMenuItem use after free attempt 1:38901 Drop and generate

events

FILE-PDF Adobe Reader PDF setPageAction execMenuItem use after free attempt 1:38902 Drop and generate

events

FILE-PDF Adobe Reader setItems use-after-free attempt 1:35408 Drop and generate

events

FILE-PDF Adobe Reader setItems use-after-free attempt 1:35410 Drop and generate

events

FILE-PDF Adobe Reader setTimeOut app.launchURL privilege escalati on attempt 1:35321 Drop and generate

events

FILE-PDF Adobe Reader submitForm read out of bounds attempt 1:389 31 Drop and generate

events

FILE-PDF Adobe Reader ToolEventHandler use-after-free attempt 1:3 5319 Drop and generate

events

FILE-PDF Adobe Reader TrueType font file numberofmetrics out of b ounds read attempt 1:40440 Drop and generate

events

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt 1:38909 Drop and generate

events

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt 1:38937 Drop and generate

events

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt 1:38914 Drop and generate

events

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt 1:38920 Drop and generate

events

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt 1:38935 Drop and generate

events

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt 1:38877 Drop and generate

events

FILE-PDF Adobe Reader XFA API preOpen use after free attempt 1:39 061 Drop and generate

events

FILE-PDF Adobe Reader XFA event use after free attempt 1:44144 Drop and generate FILE-PDF Adobe Reader XFA exclGroup JavaScript out of bounds memo ry access attempt 1:40602 Drop and generate FILE-PDF Adobe Reader XFA form use-after-free attempt 1:39007 Drop and generate

events

events

events

FILE-PDF Adobe Reader XFA FormInstanceManager use after free atte mpt 1:39017 Drop and generate

events

FILE-PDF Adobe Reader XFA javascript out of bound memory corruption attempt 1:38943 Drop and generate

events

FILE-PDF Adobe Reader XFA javascript use after free attempt 1:387 94 Drop and generate

events

FILE-PDF Adobe Reader XFA large array use after free attempt 1:42 943 Drop and generate

events

FILE-PDF Adobe Reader XFA loadXML use after free attempt 1:43906 Drop and generate

events

FILE-PDF Adobe Reader XFA prePrint use after free attempt 1:38895 Drop and generate

events

FILE-PDF Adobe Reader XFA remerge JavaScript use after free attempt 1:40577 Drop and generate

events

FILE-PDF Adobe Reader XLST parsing engine use after free attempt 1:40587 Drop and generate

events

FILE-PDF Adobe Reader XML Metadata memory corruption attempt 1:40 618 Drop and generate

events

FILE-PDF Adobe Reader XML XSL transform exploitation attempt 1:35 779 Drop and generate

events

FILE-PDF Adobe Reader XSLT Transform use after free attempt 1:405 13 Drop and generate

events

FILE-PDF Adobe Reader XSLT Transform use after free attempt 1:405 09 Drop and generate

events

FILE-PDF Adobe Reader XSLT Transform use after free attempt 1:405 05 Drop and generate

events

FILE-PDF Adobe Reader XSLT Transform use after free attempt 1:405 11 Drop and generate

events

FILE-PDF Adobe Reader XSLT Transform use after free attempt 1:405 07 Drop and generate

events

FILE-PDF Artifex MuPDF JBIG2 negative width value out of bounds r ead attempt 1:41224 Drop and generate FILE-PDF Google Chrome PDFium jpeg2000 SIZ segment check failure heap buffer overflow attempt 1:39161 Drop and generate FILE-PDF Iceni Argus PDF uninitialized WordStyle color length cod e overflow attempt 1:40917 Drop and generate

events

events

events

FILE-PDF Javascript openDoc UNC network request attempt 1:25449 Drop and generate

events

FILE-PDF Microsoft Edge PDF Builder out of bounds read attempt 1: 41601 Drop and generate

events

FILE-PDF Microsoft Edge PDF Builder out of bounds read attempt 1: 41602 Drop and generate

events

FILE-PDF Microsoft Edge pdf parsing information disclosure attemp t 1:46226 Drop and generate

events

FILE-PDF Microsoft Edge pdf parsing information disclosure attemp t 1:46227 Drop and generate

events

FILE-PDF Microsoft Reader dynamic object stream uninitialized mem ory corruption attempt 1:37566 Drop and generate

events

FILE-PDF Microsoft Windows PDF Library invalid JPX image heap cor ruption attempt 1:37594 Drop and generate

events

FILE-PDF Microsoft Windows PDF Library invalid JPX image heap cor ruption attempt 1:37595 Drop and generate

events

FILE-PDF Nitro Pro out of bounds memory write attempt 1:40776 Drop and generate

events

FILE-PDF Nitro Pro PDF Reader out of bounds write attempt 1:41196 Drop and generate

events

FILE-PDF obfuscated header in PDF 3:16343 Drop and generate

events

FILE-PDF OpenType parsing buffer overflow attempt 1:25461 Drop and generate

events

FILE-PDF OpenType parsing buffer overflow attempt 1:25462 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2017-0270 attack attempt 3:41360 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2017-0270 attack attempt 3:41362 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2017-0322 attack attempt 3:42313 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0518 attack attempt 3:45521 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0518 attack attempt 3:45522 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0532 attack attempt 3:45715 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0532 attack attempt 3:45716 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0569 attack attempt 3:46292 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0569 attack attempt 3:46293 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0590 attack attempt 3:46550 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0590 attack attempt 3:46551 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0639 attack attempt 3:47340 Drop and generate

events

FILE-PDF TRUFFLEHUNTER TALOS-2018-0639 attack attempt 3:47341 Drop and generate

events

HI\_ANOM\_SERVER\_ALERT 120:1 Generate events

HI\_CLIENT\_APACHE\_WS 119:12 Generate events

HI\_CLIENT\_ASCII 119:1 Generate events

HI\_CLIENT\_BARE\_BYTE 119:4 Generate events

HI\_CLIENT\_DIR\_TRAV 119:11 Generate events

HI\_CLIENT\_DOUBLE\_DECODE 119:2 Generate events

HI\_CLIENT\_IIS\_BACKSLASH 119:9 Generate events

HI\_CLIENT\_IIS\_DELIMITER 119:13 Generate events

HI\_CLIENT\_IIS\_UNICODE 119:7 Generate events

HI\_CLIENT\_LARGE\_CHUNK 119:16 Generate events

HI\_CLIENT\_LONG\_HEADER 119:19 Generate events

HI\_CLIENT\_MULTI\_SLASH 119:8 Generate events

HI\_CLIENT\_NON\_RFC\_CHAR 119:14 Generate events

HI\_CLIENT\_OVERSIZE\_DIR 119:15 Generate events

HI\_CLIENT\_PROXY\_USE 119:17 Generate events

HI\_CLIENT\_SELF\_DIR\_TRAV 119:10 Generate events

HI\_CLIENT\_U\_ENCODE 119:3 Generate events

HI\_CLIENT\_UTF\_8 119:6 Generate events

HI\_CLIENT\_WEBROOT\_DIR 119:18 Generate events

HI\_SERVER\_PDF\_FILE\_CASCADE\_COMP 120:16 Generate events

HI\_SERVER\_PDF\_FILE\_DEFLATE\_DECOM\_FAIL 120:14 Generate events

HI\_SERVER\_PDF\_FILE\_PARSE\_FAIL 120:17 Generate events

HI\_SERVER\_PDF\_FILE\_UNSUP\_COMP\_TYPE 120:15 Generate events

HI\_SERVER\_SWF\_FILE\_LZMA\_DECOM\_FAIL 120:13 Generate events

HI\_SERVER\_SWF\_FILE\_ZLIB\_DECOM\_FAIL 120:12 Generate events

INDICATOR-COMPROMISE Connection to malware sinkhole - CERT.PL 1:3 9851 Drop and generate

events

INDICATOR-COMPROMISE connection to zeus malware sinkhole 1:31214 Drop and generate

events

INDICATOR-COMPROMISE DNS request for known malware sinkhole domai n iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

- WannaCry 1:4403 7

Generate events

INDICATOR-COMPROMISE Java user-agent request to svchost.jpg 1:260 25 Drop and generate

events

INDICATOR-COMPROMISE known malicious SSL certificate - Win.Trojan .Dridex 1:35222 Drop and generate

events

INDICATOR-COMPROMISE Liz0ziM php shell command and control attemp t 1:31501 Drop and generate

events

INDICATOR-COMPROMISE Liz0ziM php shell command and control attemp t 1:31502 Drop and generate

events

INDICATOR-COMPROMISE Liz0ziM php shell download attempt 1:31499 Drop and generate

events

INDICATOR-COMPROMISE Liz0ziM php shell upload attempt 1:31500 Drop and generate

events

INDICATOR-COMPROMISE Malicious VBA script detected 1:44875 Drop and generate

events

INDICATOR-COMPROMISE Metasploit PowerShell CLI Download and Run attempt 1:45136 Drop and generate

events

INDICATOR-COMPROMISE Metasploit run hidden powershell attempt 1:4 5137 Drop and generate

events

INDICATOR-COMPROMISE Microsoft Word internal object auto update attempt 1:45519 Drop and generate

events

INDICATOR-COMPROMISE Microsoft Word internal object auto update attempt 1:45520 Drop and generate

events

INDICATOR-COMPROMISE MinerDeploy monitor request attempt 1:31531 Drop and generate

events

INDICATOR-COMPROMISE Potential Redirect from Compromised WordPres s site to Fedex - Spammed Malware Download attempt 1:32888

Drop and generate events

INDICATOR-COMPROMISE potential Squiblydoo application whitelistin g bypass attempt 1:40829 Drop and generate

events

INDICATOR-COMPROMISE SettingContent-ms file type download attempt 1:47651 Drop and generate

events

INDICATOR-COMPROMISE SettingContent-ms file type download attempt 1:47652 Drop and generate

events

INDICATOR-COMPROMISE SettingContent-ms file type download attempt 1:47653 Drop and generate

events

INDICATOR-COMPROMISE SettingContent-ms file type download attempt 1:47654 Drop and generate

events

INDICATOR-COMPROMISE suspicious test for public IP - www.dawhois. com 1:30230 Drop and generate

events

INDICATOR-COMPROMISE Wild Neutron potential exploit attempt 1:357 45 Drop and generate

events

INDICATOR-COMPROMISE Win.Trojan.Bedep variant outbound connection 1:33188 Drop and generate INDICATOR-COMPROMISE Windows Internet Explorer EMET check and gar bage collection 1:29821 Drop and generate INDICATOR-COMPROMISE ZenCart compromise attempt detected 1:30065 Drop and generate

events

events

events

INDICATOR-COMPROMISE ZenCart malicious redirect attempt detected 1:30066 Drop and generate

events

INDICATOR-OBFUSCATION Coinhive cryptocurrency miner obfuscated de tected 1:45810 Drop and generate

events

INDICATOR-OBFUSCATION DOC header followed by PDF header 1:25454 Drop and generate INDICATOR-OBFUSCATION Dridex String.prototype function definition obfuscation attempt 1:42947 Drop and generate INDICATOR-OBFUSCATION FOPO obfuscated PHP file upload attempt 1:4 4235 Drop and generate

events

events

events

INDICATOR-OBFUSCATION fromCharCode seen in exploit kit landing pa ges 1:26092 Drop and generate

events

INDICATOR-OBFUSCATION GIF header followed by PDF header 1:25451 Drop and generate INDICATOR-OBFUSCATION Javascript obfuscation - createElement - se en in IFRAMEr Tool attack 1:28420 Drop and generate INDICATOR-OBFUSCATION Javascript obfuscation - document - seen in IFRAMEr Tool attack 1:28023 Drop and generate INDICATOR-OBFUSCATION Javascript obfuscation - document - seen in IFRAMEr Tool usage 1:27735 Drop and generate INDICATOR-OBFUSCATION Javascript obfuscation - fromCharCode - see n in IFRAMEr Tool attack 1:28421 Drop and generate INDICATOR-OBFUSCATION Javascript obfuscation - fromCharCode 1:272 72 Drop and generate

events

events

events

events

events

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr To ol attack 1:28941 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr To ol attack 1:28811 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr To ol attack 1:28812 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr To ol attack 1:28024 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr To ol attack 1:28346 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr To ol attack 1:28422 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - seen in Nuclear ex ploit kit 1:29190 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - split - seen in IF RAMEr Tool attack 1:27736 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - split - seen in IF RAMEr Tool attack 1:27920 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - split - seen in IF RAMEr Tool attack 1:28345 Drop and generate

events

INDICATOR-OBFUSCATION Javascript obfuscation - split - seen in IF RAMEr Tool attack 1:27592 Drop and generate

events

INDICATOR-OBFUSCATION JPEG header followed by PDF header 1:25453 Drop and generate INDICATOR-OBFUSCATION obfuscated document command - used in IFRAM Er tool injection 1:25592 Drop and generate INDICATOR-OBFUSCATION obfuscated getElementsByTagName string - se en in exploit kits 1:27073 Drop and generate INDICATOR-OBFUSCATION obfuscated getElementsByTagName string - se en in exploit kits 1:27074 Drop and generate INDICATOR-OBFUSCATION Obfuscated javascript/html generated by myo bfuscate.com detected 1:26441 Drop and generate INDICATOR-OBFUSCATION obfuscated portable executable - seen in ex ploit kits 1:26352 Drop and generate

events

events

events

events

events

events

INDICATOR-OBFUSCATION PNG header followed by PDF header 1:25452 Drop and generate

events

INDICATOR-OBFUSCATION potential math library debugging 1:29213 Drop and generate INDICATOR-OBFUSCATION Rig EK fromCharCode offset 33 obfuscated ge tElementsByTagName call 1:43256 Drop and generate INDICATOR-OBFUSCATION RTF file objdata hex-escape obfuscation att empt 1:48303 Drop and generate

events

events

events

INDICATOR-OBFUSCATION RTF file objdata hex-escape obfuscation att empt 1:48304 Drop and generate

events

INDICATOR-OBFUSCATION RTF file objdata hlsrc obfuscation attempt 1:48305 Drop and generate

events

INDICATOR-OBFUSCATION RTF file objdata hlsrc obfuscation attempt 1:48306 Drop and generate

events

INDICATOR-OBFUSCATION String.fromCharCode concatenation 1:26101 Drop and generate

events

INDICATOR-SCAN User-Agent known malicious user-agent The Mole 1:2 9462 Drop and generate

events

INDICATOR-SHELLCODE Cisco ASA alloc\_ch connection string 3:45597 Drop and generate

events

MALWARE-BACKDOOR CobaltStrike inbound beacon download 1:45904 Drop and generate

events

MALWARE-BACKDOOR CobaltStrike inbound beacon download 1:45905 Drop and generate

events

MALWARE-BACKDOOR DarkSeoul related wiper 1:26326 Drop and generate

events

MALWARE-BACKDOOR Jokra dropper download 1:26332 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38683 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38684 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38685 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38686 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38689 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38690 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38691 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38692 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38693 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38694 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38695 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38696 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38697 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38698 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38699 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38700 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38701 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38702 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38703 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38704 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38705 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38706 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38707 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38708 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38709 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38710 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38711 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38712 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38713 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38717 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38718 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:38719 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:39058 Drop and generate

events

MALWARE-BACKDOOR JSP webshell backdoor detected 1:39059 Drop and generate

events

MALWARE-BACKDOOR PHP IRCBot command execution attempt 1:32247 Drop and generate

events

MALWARE-BACKDOOR PHP IRCBot file edit attempt 1:32248 Drop and generate

events

MALWARE-BACKDOOR PHP IRCBot port bind attempt 1:32249 Drop and generate

events

MALWARE-BACKDOOR phpMyAdmin server\_sync.php backdoor access attempt 1:24256 Drop and generate

events

MALWARE-BACKDOOR ReGeorg proxy read attempt 1:38327 Drop and generate

events

MALWARE-BACKDOOR ReGeorg socks proxy connection attempt 1:38328 Drop and generate

events

MALWARE-BACKDOOR ReGeorg socks proxy initial connection attempt 1 :38329 Drop and generate

events

MALWARE-BACKDOOR ToolsPack PHP Backdoor access 1:21550 Drop and generate

events

MALWARE-BACKDOOR Unix.Malware.Chaos backdoor trigger attempt 1:45 975 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Agent variant outbound connection 1 :22095 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Andromeda variant outbound connecti on 1:31558 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Andromeda variant outbound connecti on 1:31559 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Blohi variant outbound connection 1 :32055 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Boda Malware Checkin 1:26842 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Demtranc variant outbound connectio n 1:24115 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Demtranc variant outbound connectio n 1:24116 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Demtranc variant outbound connectio n 1:24117 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Demtranc variant outbound connectio n 1:24118 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Demtranc variant outbound connectio n 1:24119 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Demtranc variant outbound connectio n 1:24120 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Dulevco.A runtime detection 1:26610 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Hikit outbound banner response 1:30 948 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Nicabown variant outbound connectio n 1:35384 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.PCRat data upload 1:26655 Drop and generate

events

MALWARE-BACKDOOR Win.Backdoor.Speccom variant outbound connection 1:33823 Drop and generate

events

MALWARE-BACKDOOR Win.Trojan.GGDoor.22 variant outbound connection 1:19747 Drop and generate

events

MALWARE-BACKDOOR Win.Trojan.Ransomlock runtime detection 1:24530 Drop and generate

events

MALWARE-BACKDOOR Windows vernot download 1:26328 Drop and generate

events

MALWARE-CNC AbbadonPOS variant outbound connection 1:36890 Drop and generate

events

MALWARE-CNC Aldi bot variant outbound connection user-agent 1:219 12 Drop and generate

events

MALWARE-CNC Aldi variant outbound connection C&C checkin 1:21911 Drop and generate

events

MALWARE-CNC Andr.Adware.Judy malicious dex file download attempt 1:43292 Drop and generate

events

MALWARE-CNC Andr.Adware.Judy malicious java file download attempt 1:43293 Drop and generate

events

MALWARE-CNC Andr.Tool.Snowfox Androidbauts/snowfox outbound conne ction 1:40500 Drop and generate

events

MALWARE-CNC Andr.Tool.Snowfox Androidbauts/snowfox outbound conne ction 1:40501 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant file download attempt 1:420 28 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant file download attempt 1:420 29 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant file download attempt 1:420 30 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:38668 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42021 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42022 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42023 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42024 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42025 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42026 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42027 Drop and generate

events

MALWARE-CNC Andr.Trojan.Agent variant outbound connection 1:42031 Drop and generate

events

MALWARE-CNC Andr.Trojan.AnubisCrypt variant outbound post detecte d 1:47877 Drop and generate

events

MALWARE-CNC Andr.Trojan.Bazuc initial outbound connection 1:29922 Drop and generate

events

MALWARE-CNC Andr.Trojan.Bazuc jobs check outbound connection 1:29 923 Drop and generate

events

MALWARE-CNC Andr.Trojan.Congur variant outbound connection detect ed 1:44554 Drop and generate

events

MALWARE-CNC ANDR.Trojan.FakeApp outbound connection 1:29978 Drop and generate

events

MALWARE-CNC Andr.Trojan.Femas variant outbound connection 1:43981 Drop and generate

events

MALWARE-CNC Andr.Trojan.Femas variant outbound connection 1:43982 Drop and generate

events

MALWARE-CNC Andr.Trojan.Kemoge outbound connection 1:36471 Drop and generate

events

MALWARE-CNC Andr.Trojan.MysteryBot outbound connection 1:47723 Drop and generate

events

MALWARE-CNC Andr.Trojan.Oldboot variant outbound connection 1:308 15 Drop and generate

events

MALWARE-CNC Andr.Trojan.Scarelocker outbound connection 1:31644 Drop and generate

events

MALWARE-CNC Andr.Trojan.SMSSend outbound connection 1:31593 Drop and generate

events

MALWARE-CNC Andr.Trojan.Sysch variant outbound connection 1:41336 Drop and generate

events

MALWARE-CNC Andr.Trojan.Sysch variant outbound connection 1:41337 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46356 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46357 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46358 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46359 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46360 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46361 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46362 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46363 Drop and generate

events

MALWARE-CNC Andr.Trojan.Wroba outbound connection 1:46364 Drop and generate

events

MALWARE-CNC Andr.Trojan.Xamaria variant outbound connection 1:478 60 Drop and generate

events

MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt 1:467 87 Drop and generate

events

MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt 1:467 88 Drop and generate

events

MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt 1:467 89 Drop and generate

events

MALWARE-CNC Android Red Alert Trojan outbound connection 1:44619 Drop and generate

events

MALWARE-CNC Android Red Alert Trojan outbound connection 1:44620 Drop and generate

events

MALWARE-CNC Android Red Alert Trojan outbound connection 1:44621 Drop and generate

events

MALWARE-CNC Android Red Alert Trojan outbound connection 1:44622 Drop and generate

events

MALWARE-CNC Android.CoolReaper.Trojan outbound connection 1:32956 Drop and generate

events

MALWARE-CNC Apple OSX Flashback malware user-agent 1:21910 Drop and generate

events

MALWARE-CNC Apple OSX Flashback malware variant outbound connecti on 1:22033 Drop and generate

events

MALWARE-CNC Apple OSX Flashback malware variant outbound connecti on 1:22034 Drop and generate

events

MALWARE-CNC Apple OSX.Flashback variant outbound connection 1:217 55 Drop and generate

events

MALWARE-CNC Apple OSX.Flashback variant outbound connection 1:217 56 Drop and generate

events

MALWARE-CNC Apple OSX.Flashback variant outbound connection 1:217 57 Drop and generate

events

MALWARE-CNC Apple OSX.Flashback variant outbound connection 1:217 58 Drop and generate

events

MALWARE-CNC Apple OSX.Revir-1 variant outbound connection 1:20202 Drop and generate

events

MALWARE-CNC Apple OSX.Sabpub variant outbound connection 1:21877 Drop and generate

events

MALWARE-CNC ATSEngine credit card number sent via URL parameter 1 :37051 Drop and generate

events

MALWARE-CNC ATSEngine initial beacon 1:37050 Drop and generate

events

MALWARE-CNC BabaYaga inbound connection 1:48025 Drop and generate

events

MALWARE-CNC BabaYaga outbound connection 1:48026 Drop and generate

events

MALWARE-CNC BabaYaga outbound connection 1:48027 Drop and generate

events

MALWARE-CNC Backdoor.MSIL.Kazybot.A botnet server connection atte mpt 1:40308 Drop and generate

events

MALWARE-CNC bagle.a http notification detection 1:9418 Generate events

MALWARE-CNC Bancos fake JPG encrypted config file download 1:2672 2 Drop and generate

events

MALWARE-CNC Bancos variant outbound connection SQL query POST dat a 1:26075 Drop and generate

events

MALWARE-CNC binary download while video expected 1:38517 Drop and generate

events

MALWARE-CNC BitBot Idle C2 response 1:26837 Drop and generate

events

MALWARE-CNC Bitvote miner kernel driver outbound request attempt 1:46406 Drop and generate

events

MALWARE-CNC Bitvote miner kernel driver payload download attempt 1:46407 Drop and generate

events

MALWARE-CNC BLYPT installer createproc outbound traffic 1:28011 Drop and generate

events

MALWARE-CNC BLYPT installer reuse outbound traffic 1:28008 Drop and generate

events

MALWARE-CNC BLYPT installer startupkey outbound traffic 1:28007 Drop and generate

events

MALWARE-CNC BLYPT installer tserror outbound traffic 1:28010 Drop and generate

events

MALWARE-CNC Bobax botnet variant outbound connection 1:16489 Drop and generate

events

MALWARE-CNC Boot.Bootroot Variant data upload 1:28230 Drop and generate

events

MALWARE-CNC Brazilian Banking Trojan data theft 1:27649 Drop and generate

events

MALWARE-CNC Bredolab bot variant outbound connection 1:16144 Drop and generate

events

MALWARE-CNC Briewots.A runtime traffic detected 1:20011 Drop and generate

events

MALWARE-CNC Brontok Worm variant outbound connection 1:26288 Drop and generate

events

MALWARE-CNC Catch-All malicious Chrome extension dropper outbound connection 1:45114 Drop and generate MALWARE-CNC Cbeplay Ransomware variant outbound connection - Abno rmal HTTP Headers 1:26696 Generate events MALWARE-CNC Cbeplay Ransomware variant outbound connection - POST Body 1:26697 Drop and generate

events

events

MALWARE-CNC Clob bot traffic 1:16289 Drop and generate

events

MALWARE-CNC CNC Dirtjumper variant outbound connection 1:26010 Drop and generate

events

MALWARE-CNC CNC Dirtjumper variant outbound connection 1:26011 Drop and generate

events

MALWARE-CNC Cobalt Strike DNS beacon inbound TXT record 1:45908 Drop and generate

events

MALWARE-CNC Cobalt Strike DNS beacon outbound TXT record 1:45907 Drop and generate

events

MALWARE-CNC CobaltStrike DNS Beacon outbound A record 1:45906 Drop and generate

events

MALWARE-CNC CobaltStrike trial version inbound beacon response 1: 45909 Drop and generate

events

MALWARE-CNC Coldroot RAT outbound connection 1:46156 Drop and generate

events

MALWARE-CNC cridex HTTP Response - default0.js 1:26780 Drop and generate

events

MALWARE-CNC Cryptofortress Decryption Software Purchase Tor Websi te 1:33912 Drop and generate

events

MALWARE-CNC CTFMONv4 beacon attempt 3:38746 Drop and generate

events

MALWARE-CNC Cutwail landing page connection 1:21548 Drop and generate

events

MALWARE-CNC Dapato banking Trojan variant outbound connection 1:2 6264 Drop and generate

events

MALWARE-CNC Deputy Dog implant outbound connection 1:42880 Drop and generate

events

MALWARE-CNC DeputyDog diskless method outbound connection 1:28493 Drop and generate

events

MALWARE-CNC Dharma ransomware dropper initial outbound connection 1:46795 Drop and generate

events

MALWARE-CNC Dharma ransomware dropper outbound connection 1:46796 Drop and generate

events

MALWARE-CNC DNS suspicious .bit dns query 1:41083 Drop and generate

events

MALWARE-CNC DNS suspicious .bit tcp dns query 1:42841 Drop and generate

events

MALWARE-CNC Doc.Downloader.Agent file download attempt 1:40450 Drop and generate

events

MALWARE-CNC Doc.Downloader.Dridex outbound connection 1:33411 Drop and generate

events

MALWARE-CNC Doc.Downloader.Dridex outbound connection 1:33342 Drop and generate

events

MALWARE-CNC Doc.Downloader.Dridex outbound connection 1:33456 Drop and generate

events

MALWARE-CNC Doc.Dropper.Agent variant outbound connection 1:40444 Drop and generate

events

MALWARE-CNC Doc.Dropper.Agent variant outbound connection 1:40445 Drop and generate

events

MALWARE-CNC Doc.Dropper.Lazarus initial download 1:45647 Drop and generate

events

MALWARE-CNC Doc.Dropper.Lazarus initial download 1:45648 Drop and generate

events

MALWARE-CNC Dofoil file download attempt 1:46236 Drop and generate

events

MALWARE-CNC Dofoil outbound connection attempt 1:46235 Drop and generate

events

MALWARE-CNC Fake PDFEscape font pack cryptominer 1:47593 Drop and generate

events

MALWARE-CNC Fake PDFEscape font pack cryptominer 1:47594 Drop and generate

events

MALWARE-CNC FBI Ransom Trojan variant outbound connection 1:26335 Drop and generate

events

MALWARE-CNC FIN4 VBA Macro credentials upload attempt 1:32776 Drop and generate

events

MALWARE-CNC Flame malware connection - /view.php 1:23057 Drop and generate

events

MALWARE-CNC Fort Disco Registration variant outbound connection 1 :27599 Drop and generate

events

MALWARE-CNC Gauss malware check-in 1:23824 Drop and generate

events

MALWARE-CNC Gozi trojan checkin 1:23635 Drop and generate

events

MALWARE-CNC Gozi Win.Trojan.connection to C&C 1:16391 Drop and generate

events

MALWARE-CNC GPON botnet outbound communication 1:46842 Drop and generate

events

MALWARE-CNC Harakit botnet traffic 1:26563 Drop and generate

events

MALWARE-CNC HILIGHT outbound connection attempt 3:38752 Drop and generate

events

MALWARE-CNC Installation Keylogger Osx.Trojan.Mokes data exfiltra tion 1:46482 Drop and generate

events

MALWARE-CNC Installation Win.Trojan.Umberial variant outbound con nection 1:29057 Drop and generate

events

MALWARE-CNC Ios.Backdoor.SYNful inbound connection 1:36054 Drop and generate

events

MALWARE-CNC IoT Reaper botnet CNC 1:44654 Drop and generate

events

MALWARE-CNC IoT Reaper botnet CNC 1:44656 Drop and generate

events

MALWARE-CNC IoT Reaper botnet 1:44653 Drop and generate

events

MALWARE-CNC Jaff ransomware outbound connection 1:42899 Drop and generate

events

MALWARE-CNC Java.Trojan.Adwind variant outbound connection 1:4784 3 Drop and generate

events

MALWARE-CNC JAVAFOG Java malware backdoor connection to cnc serve r 1:29408 Drop and generate

events

MALWARE-CNC Jimini outbound connection attempt 3:38751 Drop and generate

events

MALWARE-CNC Js.Downloader.Cryptojacking miner download attempt 1: 46946 Drop and generate

events

MALWARE-CNC Js.Keylogger.Scanbox outbound connection 1:42925 Drop and generate

events

MALWARE-CNC Js.Keylogger.Scanbox outbound connection 1:42926 Drop and generate

events

MALWARE-CNC Js.Trojan.Agent JS Sniffer beacon connection 1:47320 Drop and generate

events

MALWARE-CNC Js.Trojan.Agent JS Sniffer compromised website 1:4732 4 Drop and generate

events

MALWARE-CNC Js.Trojan.Agent JS Sniffer compromised website 1:4732 5 Drop and generate

events

MALWARE-CNC Js.Trojan.Agent JS Sniffer outbound connection 1:4732 1 Drop and generate

events

MALWARE-CNC Js.Trojan.Agent JS Sniffer outbound connection 1:4732 2 Drop and generate

events

MALWARE-CNC Js.Trojan.Agent JS Sniffer outbound connection 1:4732 3 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic malicious file download 1:48151 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic malicious file download 1:48152 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic variant outbound connection 1:48153 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic variant outbound connection 1:48154 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic variant outbound connection 1:48155 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic variant outbound connection 1:48156 Drop and generate

events

MALWARE-CNC JS.Trojan.Generic variant outbound connection 1:48157 Drop and generate

events

MALWARE-CNC Kegis.A outbound connection 1:31424 Drop and generate

events

MALWARE-CNC known command and control channel traffic -- Corefloo d 1:18934 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16828 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16833 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16822 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16812 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16824 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16826 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16811 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16832 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16817 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16810 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:18939 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16816 Drop and generate

events

MALWARE-CNC known command and control channel traffic 1:16827 Drop and generate

events

MALWARE-CNC known command and control traffic - Pushbot 1:23261 Drop and generate

events

MALWARE-CNC known malicious SSL certificate - Sykipot C&C 1:21047 Drop and generate

events

MALWARE-CNC known malicious SSL certificate - Troldesh C&C 1:3502 7 Drop and generate

events

MALWARE-CNC known malicious SSL certificate - Win.Trojan.Adwind 1 :38134 Drop and generate

events

MALWARE-CNC Koobface request for captcha 1:16485 Drop and generate

events

MALWARE-CNC Koobface variant outbound connection 1:16484 Drop and generate

events

MALWARE-CNC Koobface worm executable download 1:16670 Drop and generate

events

MALWARE-CNC Linux.Backdoor.Tsunami outbound connection 1:29493 Drop and generate

events

MALWARE-CNC Linux.Backdoor.Tsunami outbound connection 1:29494 Drop and generate

events

MALWARE-CNC Linux.DDoS.D93 outbound connection 1:40991 Drop and generate

events

MALWARE-CNC Linux.Downloader.Mumblehard variant outbound connecti on 1:34462 Drop and generate

events

MALWARE-CNC Linux.Trojan.Bifrose outbound connection 1:38333 Drop and generate

events

MALWARE-CNC Linux.Trojan.Jynxkit outbound connection 1:31925 Drop and generate

events

MALWARE-CNC Linux.Trojan.Mumblehard variant outbound connection 1 :34461 Drop and generate

events

MALWARE-CNC Linux.Trojan.Roopre outbound connection 1:30938 Drop and generate

events

MALWARE-CNC Linux.Trojan.Torte variant outbound connection 1:3781 7 Drop and generate

events

MALWARE-CNC Linux.Trojan.XORDDoS outbound connection 1:33646 Drop and generate

events

MALWARE-CNC Linux.Trojan.XORDDoS outbound connection 1:33647 Drop and generate

events

MALWARE-CNC Linux.Trojan.XORDDoS outbound connection 1:33648 Drop and generate

events

MALWARE-CNC Linux.Trojan.XORDDoS outbound connection 1:34261 Drop and generate

events

MALWARE-CNC Linux.Trojan.XORDDoS outbound connection 1:34262 Drop and generate

events

MALWARE-CNC Linux.Trojan.XORDDoS outbound connection 1:34263 Drop and generate

events

MALWARE-CNC Linux.Worm.Darlloz variant outbound connection 1:3201 3 Drop and generate

events

MALWARE-CNC MacBack Win.Trojan.variant outbound connection 1:1901 8 Drop and generate

events

MALWARE-CNC MacBack Win.Trojan.variant outbound connection 1:1901 9 Drop and generate

events

MALWARE-CNC MacBack Win.Trojan.variant outbound connection 1:1901 6 Drop and generate

events

MALWARE-CNC MacBack Win.Trojan.variant outbound connection 1:1901 7 Drop and generate

events

MALWARE-CNC MacOS.Backdoor.Xslcmd outbound connection 1:34155 Drop and generate

events

MALWARE-CNC MacOS.Flashback.A variant outbound connection 1:20762 Drop and generate

events

MALWARE-CNC MacOS.Trojan.MacVX outbound connection 1:34567 Drop and generate

events

MALWARE-CNC MacOS.Trojan.Wirelurker variant outbound connection 1 :34115 Drop and generate

events

MALWARE-CNC MacOS.Trojan.Wirelurker variant outbound connection 1 :34116 Drop and generate

events

MALWARE-CNC Malicious BitCoiner Miner download - Win.Trojan.Miner d 1:30551 Drop and generate

events

MALWARE-CNC Malicious BitCoiner Miner download - Win.Trojan.Syste ma 1:30552 Drop and generate

events

MALWARE-CNC Medfos Trojan variant outbound connection 1:26613 Drop and generate

events

MALWARE-CNC Milkoad.A First Request 1:36916 Drop and generate

events

MALWARE-CNC Miniduke server contact 1:26690 Drop and generate

events

MALWARE-CNC MultiOS.Trojan.OSCelestial variant inbound connection 1:45980 Drop and generate

events

MALWARE-CNC Necurs Rootkit op.cgi 1:25504 Drop and generate

events

MALWARE-CNC Necurs Rootkit sba.cgi 1:25503 Drop and generate

events

MALWARE-CNC Night Dragon initial beacon 1:18458 Drop and generate

events

MALWARE-CNC Night Dragon keepalive message 1:18459 Drop and generate

events

MALWARE-CNC Obfuscated Javascript Attack runtime detection 1:3853 0 Drop and generate

events

MALWARE-CNC OnionDuke variant outbound connection 1:33081 Drop and generate

events

MALWARE-CNC Orbit Downloader denial of service update 1:27726 Drop and generate

events

MALWARE-CNC Orbit Downloader denial of service update 1:27727 Drop and generate

events

MALWARE-CNC Orbit Downloader denial of service update 1:27728 Drop and generate

events

MALWARE-CNC Osx.Backdoor.iWorm variant outbound connection 1:3217 5 Drop and generate

events

MALWARE-CNC Osx.Downloader.Crossrider outbound download request 1 :46700 Drop and generate

events

MALWARE-CNC Osx.Downloader.MacDownloader variant outbound connect ion 1:41661 Drop and generate

events

MALWARE-CNC Osx.Downloader.MacDownloader variant outbound connect ion 1:41662 Drop and generate

events

MALWARE-CNC Osx.Downloader.MacDownloader variant outbound connect ion 1:41663 Drop and generate

events

MALWARE-CNC Osx.Keylogger.Elite variant outbound connection 1:414 58 Drop and generate

events

MALWARE-CNC Osx.Keylogger.Elite variant outbound connection 1:414 59 Drop and generate

events

MALWARE-CNC Osx.Keylogger.Elite variant outbound connection 1:414 60 Drop and generate

events

MALWARE-CNC Osx.Keylogger.Elite variant outbound connection 1:414 61 Drop and generate

events

MALWARE-CNC Osx.Trojan.Calisto outbound connection 1:47414 Drop and generate

events

MALWARE-CNC Osx.Trojan.Calisto outbound connection 1:47415 Drop and generate

events

MALWARE-CNC OSX.Trojan.HackBack variant outbound connection 1:270 58 Drop and generate

events

MALWARE-CNC Osx.Trojan.Janicab outbound connection 1:27545 Drop and generate

events

MALWARE-CNC Osx.Trojan.Janicab outbound connection 1:27546 Drop and generate

events

MALWARE-CNC Osx.Trojan.Janicab outbound connection 1:27547 Drop and generate

events

MALWARE-CNC Osx.Trojan.Janicab runtime traffic detected 1:27544 Drop and generate

events

MALWARE-CNC Osx.Trojan.Keranger outbound connection 1:38116 Drop and generate

events

MALWARE-CNC Osx.Trojan.Keydnap variant backdoor detected 1:40258 Drop and generate

events

MALWARE-CNC Osx.Trojan.Keydnap variant dropper detected 1:40310 Drop and generate

events

MALWARE-CNC Osx.Trojan.Keydnap variant initial backdoor download attempt 1:40260 Drop and generate

events

MALWARE-CNC OSX.Trojan.KitM variant outbound connection user-agen t 1:26815 Drop and generate

events

MALWARE-CNC OSX.Trojan.KitM variant outbound connection 1:26816 Drop and generate

events

MALWARE-CNC Osx.Trojan.Komplex outbound connection 1:40709 Drop and generate

events

MALWARE-CNC Osx.Trojan.Komplex outbound connection 1:40710 Drop and generate

events

MALWARE-CNC OSX.Trojan.Mabouia outbound connection 1:36810 Drop and generate

events

MALWARE-CNC OSX.Trojan.Morcut file download 1:26998 Generate events

MALWARE-CNC OSX.Trojan.Morcut variant outbound connection 1:26997 Generate events

MALWARE-CNC Osx.Trojan.OceanLotus outbound connection attempt 1:4 5400 Drop and generate

events

MALWARE-CNC Osx.Trojan.Yinli outbound connection 1:33328 Drop and generate

events

MALWARE-CNC Osx.Trojan.Yinli outbound connection 1:33329 Drop and generate

events

MALWARE-CNC Osx.Trojan.Yinli outbound connection 1:33330 Drop and generate

events

MALWARE-CNC Outbound malicious vbscript attempt 1:46792 Drop and generate

events

MALWARE-CNC Pdf.Phishing.Agent variant outbound connection detect ed 1:45483 Drop and generate

events

MALWARE-CNC Phoenix exploit kit post-compromise behavior 1:21860 Drop and generate

events

MALWARE-CNC Php.Dropper.Mayhem variant outbound connection 1:4497 5 Drop and generate MALWARE-CNC Php.Malware.SoakSoakRedirect Malware traffic containi ng WordPress Administrator credentials 1:32891 Drop and generate MALWARE-CNC PlugX outbound communication attempt 3:38756 Drop and generate

events

events

events

MALWARE-CNC PlugX outbound communication attempt 3:38757 Drop and generate

events

MALWARE-CNC PlugX outbound connection attempt 3:38755 Drop and generate

events

MALWARE-CNC PointGuide variant outbound connection 1:19328 Drop and generate

events

MALWARE-CNC Potential Banking Trojan Config File Download 1:24885 Drop and generate

events

MALWARE-CNC Potential Gozi Trojan HTTP Header Structure 1:26924 Drop and generate MALWARE-CNC Potential hostile executable served from compromised or malicious WordPress site 1:36914 Drop and generate MALWARE-CNC Potential Win.Trojan.Kraziomel Download - 000.jpg 1:2 7533 Drop and generate

events

events

events

MALWARE-CNC PowerShell Empire HTTP listener response 1:45352 Drop and generate

events

MALWARE-CNC PowerShell Empire variant outbound connection 1:44561

MALWARE-CNC PowerShell Empire variant outbound connection 1:44562 Drop and generate

events

MALWARE-CNC PowerShell Empire variant outbound connection 1:44564 Drop and generate

events

MALWARE-CNC PowerShell Empire variant outbound connection 1:38259 Drop and generate

events

MALWARE-CNC PowerShell Empire variant outbound connection 1:38260 Drop and generate

events

MALWARE-CNC PowerShell Empire variant outbound connection 1:38261 Drop and generate

events

MALWARE-CNC Powershell PRB backdoor initial outbound communicatio n attempt 1:47076 Drop and generate

events

MALWARE-CNC Pushdo client communication 1:15165 Drop and generate

events

MALWARE-CNC Pushdo Spiral Traffic 1:26721 Drop and generate

events

MALWARE-CNC Pushdo Spiral Traffic 1:25471 Drop and generate

events

MALWARE-CNC Py.Malware.EvilOSX 404 Error Page Payload/Command Del ivery 1:47505 Drop and generate

events

MALWARE-CNC RDN Banker Data Exfiltration 1:27774 Drop and generate

events

MALWARE-CNC RemoteSpy connection to CNC server 1:31073 Drop and generate

events

MALWARE-CNC Rogue AV download/update 1:16695 Drop and generate

events

MALWARE-CNC RSPlug Win.Trojan.file download 1:15564 Drop and generate

events

MALWARE-CNC RSPlug Win.Trojan.file download 1:15565 Drop and generate

events

MALWARE-CNC RSPlug Win.Trojan.server connection 1:15563 Drop and generate

events

MALWARE-CNC Rtf.Trojan.Felixroot variant download attempt 1:48279 Drop and generate

events

MALWARE-CNC Rtf.Trojan.Felixroot variant download attempt 1:48280 Drop and generate

events

MALWARE-CNC Rtf.Trojan.Mauris outbound download attempt 1:40812 Drop and generate

events

MALWARE-CNC Rubella Macro Builder generated payload 1:46628 Drop and generate

events

MALWARE-CNC Rubella Macro Builder generated payload 1:46629 Drop and generate

events

MALWARE-CNC Rubella Macro Builder generated payload 1:46630 Drop and generate

events

MALWARE-CNC Rubella Macro Builder generated payload 1:46631 Drop and generate

events

MALWARE-CNC Russian Bank scam malware GET request to server 1:301 67 Drop and generate

events

MALWARE-CNC Russian Bank scam malware POST to server 1:30168 Drop and generate

events

MALWARE-CNC Sality virus HTTP GET request 1:15553 Drop and generate

events

MALWARE-CNC SambaCry ransomware download attempt 1:45468 Drop and generate

events

MALWARE-CNC SambaCry ransomware download attempt 1:45470 Drop and generate

events

MALWARE-CNC SambaCry ransomware download attempt 1:45471 Drop and generate

events

MALWARE-CNC SambaCry ransomware download attempt 1:45472 Drop and generate

events

MALWARE-CNC SambaCry ransomware download attempt 1:45473 Drop and generate

events

MALWARE-CNC Security Cleaner Pro Install Confirmation 1:28250 Drop and generate

events

MALWARE-CNC Shiqiang Gang malicious XLS targeted attack detection 1:30990 Drop and generate

events

MALWARE-CNC Spyeye bot variant outbound connection 1:16669 Drop and generate

events

MALWARE-CNC SpyForms malware call home 1:16362 Drop and generate

events

MALWARE-CNC SubSeven client connection to server 1:15938 Drop and generate

events

MALWARE-CNC Suspected Unix.Malware.GoScanSSH outbound beacon atte mpt 1:45974 Drop and generate

events

MALWARE-CNC Thinkpoint fake antivirus - credit card submission 1: 17816 Drop and generate

events

MALWARE-CNC Thinkpoint fake antivirus - user display 1:17815 Drop and generate

events

MALWARE-CNC TinyDropper variant outbound connection 1:36889 Drop and generate

events

MALWARE-CNC Torpig bot sinkhole server DNS lookup 1:16693 Drop and generate

events

MALWARE-CNC Trojan Agent YEH variant outbound connection 1:25765 Drop and generate

events

MALWARE-CNC Trojan Banker FTC variant outbound connection 1:25829 Drop and generate

events

MALWARE-CNC Trojan Downloader7 1:26723 Drop and generate

events

MALWARE-CNC Trojan.NitLove variant outbound connection 1:34609 Drop and generate

events

MALWARE-CNC Trojan.Win32.Cigamve request 1:35306 Drop and generate

events

MALWARE-CNC Trojan.Win32.Ralminey POST request 1:35348 Drop and generate

events

MALWARE-CNC TT-bot botnet variant outbound connection 1:16493 Drop and generate

events

MALWARE-CNC Unix.Trojan.Chalubo downloader connection 1:48281 Drop and generate

events

MALWARE-CNC Unix.Trojan.Chalubo outbound connection 1:48282 Drop and generate

events

MALWARE-CNC Unix.Trojan.Chalubo outbound connection 1:48283 Drop and generate

events

MALWARE-CNC Unix.Trojan.Chalubo outbound connection 1:48284 Drop and generate

events

MALWARE-CNC Unix.Trojan.Chalubo outbound connection 1:48285 Drop and generate

events

MALWARE-CNC Unix.Trojan.Chalubo outbound connection 1:48286 Drop and generate

events

MALWARE-CNC Unix.Trojan.Erebus variant outbound connection 1:4335 1 Generate events

MALWARE-CNC Unix.Trojan.Gafgyt variant new bot registered 1:48275 Drop and generate

events

MALWARE-CNC Unix.Trojan.Hanthie variant outbound connection 1:277 46 Drop and generate

events

MALWARE-CNC Unix.Trojan.Mirai variant post compromise download at tempt 1:40612 Drop and generate

events

MALWARE-CNC Unix.Trojan.Mirai variant post compromise download 1: 42113 Drop and generate

events

MALWARE-CNC Unix.Trojan.Prowli variant outbound connection 1:4723 6 Drop and generate

events

MALWARE-CNC Unix.Trojan.PyCryptoMiner outbound connection 1:45956 Drop and generate

events

MALWARE-CNC Unix.Trojan.Vpnfilter plugin variant connection attempt 1:47377 Drop and generate

events

MALWARE-CNC Unix.Trojan.Vpnfilter variant connection attempt 1:47 084 Drop and generate

events

MALWARE-CNC Unix.Trojan.Vpnfilter variant outbound connection att empt 1:45563 Drop and generate

events

MALWARE-CNC Unix.Trojan.Vpnfilter variant outbound connection att empt 1:45564 Drop and generate

events

MALWARE-CNC Unix.Trojan.Vpnfilter variant SSL connection attempt 1:46782 Drop and generate

events

MALWARE-CNC Unix.Trojan.Vpnfilter variant SSL connection attempt 1:46783 Drop and generate

events

MALWARE-CNC Unix.Worm.Hakai outbound connection 1:48192 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/dllhost/ac 1:25396 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/ms/check 1:25397 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/ms/flush 1:25398 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/nt/sk 1:25395 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/nt/th 1:25394 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/win/cab 1:25400 Drop and generate

events

MALWARE-CNC URI request for /cgi-bin/win/wcx 1:25399 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - .sys.php?getexe = 1:19625 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /160.rar - Win3 2/Morto.A 1:19882 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /1cup/script.ph p 1:19628 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /app/?prj= 1:19 635 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /blog/images/35 21.jpg?v 1:19636 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /botnet/adduser .php?uid= 1:27980 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /games/java\_tru st.php?f= 1:19778 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /inst.php?fff= 1:16924 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /install.asp?ma c= 1:19637 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /kx4.txt 1:1963 8 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /r\_autoidcnt.as p?mer\_seq= 1:19627 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /setup\_b.asp?pr j= 1:19626 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /VertexNet/addu ser.php?uid= 1:19632 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - /VertexNet/task s.php?uid= 1:19633 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - AnSSip= 1:19631 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - optima/index.ph p 1:19913 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - pte.aspx?ver= 1 :19622 Drop and generate

events

MALWARE-CNC URI request for known malicious URI - vic.aspx?ver= 1 :19623 Drop and generate

events

MALWARE-CNC URI request for known malicious uri config.ini on 332 2.org domain 1:19493 Drop and generate

events

MALWARE-CNC URI request for runforestrun - JS.Runfore 1:23473 Drop and generate

events

MALWARE-CNC User-Agent ASafaWeb Scan 1:21327 Generate events

MALWARE-CNC User-Agent known Adware user agent Gamevance tl\_v 1:2 1591 Drop and generate

events

MALWARE-CNC User-Agent known Adware user agent gbot 1:21636 Drop and generate

events

MALWARE-CNC User-Agent known Adware user agent mus - TDSS related 1:21639 Drop and generate

events

MALWARE-CNC User-Agent known Adware user-agent string - Win.Adwar e.Prepscram 1:39886 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - 04/XP 1:25243 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Alerter COM 1 :24442 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Alina 1:26686 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - ALIZER 1:3351 9 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Async HTTP Ag ent 1:5900 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - dt12012 1:278 68 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - EMERY - Win.T rojan.W97M 1:34843 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - extra IE vers ion 1:32978 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Flame malware 1:23019 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Google Omaha - Win.Trojan.ExtenBro 1:33649 Drop and generate MALWARE-CNC User-Agent known malicious user agent - Lizard/1.0 1: 24631 Drop and generate

events

events

MALWARE-CNC User-Agent known malicious user agent - logogo.exe 1: 30250 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - malware 1:165 51 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - me0hoi 1:2524 5 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - micro 1:42831 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - msctls\_progre ss32 1:26751 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - multi-browser 1:32980 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - NewBrandTest 1:25119 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Opera/9.61 1: 24575 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - PoisonIvy RAT 1:23627 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - SAH Agent 1:5 808 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - SessionI 1:42 832 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - spam\_bot 1:25 659 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Tear Applicat ion 1:16497 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - test\_hInterne t 1:24633 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Testing 1:244 41 Drop and generate MALWARE-CNC User-Agent known malicious user agent - TixDll - Win. Trojan.Adload.dyhq 1:29824 Drop and generate MALWARE-CNC User-Agent known malicious user agent - User-Agent he llo crazyk 1:31090 Drop and generate

events

events

events

MALWARE-CNC User-Agent known malicious user agent - User-Agent sv chost 1:31122 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - User-Agent Us er-Agent Mozilla 1:30918 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - User-Agent Us er-Agent 1:25009 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - User-Agent Us er-Agent 1:25476 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - vaccinepc 1:2 4634 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Win 1:26702 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - Win.Backdoor. Jolob 1:30308 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - yahoonews 1:2 7263 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent - you 1:23903 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent BloodguyBrowser -\_- 1:32294 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent BOT/0.1 1:21925 Drop and generate

events

MALWARE-CNC User-Agent known Malicious user agent Brutus AET 1:26 558 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent cibabam 1:26248 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent DownloadMR - So limba 1:33831 Drop and generate MALWARE-CNC User-Agent known malicious user agent globalupdate - Osx.Trojan.Wirelurker 1:32402 Drop and generate MALWARE-CNC User-Agent known malicious user agent InetAll - Win.T rojan.Pennonec 1:30301 Drop and generate

events

events

events

MALWARE-CNC User-Agent known malicious user agent NOKIAN95/WEB 1: 26522 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent Opera 10 1:2657 7 Drop and generate

events

MALWARE-CNC User-Agent known malicious user agent RAbcLib 1:22939 Drop and generate MALWARE-CNC User-Agent known malicious user agent string - httpte stman - Win.Backdoor.Rabasheeta 1:32060 Drop and generate MALWARE-CNC User-Agent known malicious user agent TCYWinHTTPDownl oad 1:21526 Drop and generate MALWARE-CNC User-Agent known malicious user agent VUPHTTP - Win.T rojan.Puvespia 1:32455 Drop and generate MALWARE-CNC User-Agent known malicious user agent YZF 1:21476 Drop and generate

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent - ace4956e-736e -11e6-9584-d7165ca591df - Win.Trojan.Tarayt 1:44213

Drop and generate events

MALWARE-CNC User-Agent known malicious user-agent - DNS Changer 1 :33522 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent - Downing - Win .Trojan.Otwycal 1:33633 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent - Google page 1 :24792 Drop and generate MALWARE-CNC User-Agent known malicious user-agent - KAIIOOOO871 - Win.Trojan.Dridex 1:33907 Drop and generate MALWARE-CNC User-Agent known malicious user-agent - Version/100 - Win.Trojan.Tarayt 1:44317 Drop and generate MALWARE-CNC User-Agent known malicious user-agent - Win.Trojan.Ba rys 1:33914 Drop and generate

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent - Win.Trojan.Mi munita 1:29645 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent - Win.Trojan.Mo wfote 1:29358 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent - Win.Trojan.Ni tedrem 1:28860 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent - Win.Trojan.Ti rips 1:29431 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent blacksun - Win. Trojan.Blacksun 1:31417 Drop and generate

events

MALWARE-CNC User-Agent known malicious User-Agent Browser - Win.T rojan.Bruterdep 1:30290 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent DefaultBotPassw ord - Win.Trojan.Tirabot 1:31150 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent ebot - Win.Troj an.Modulog 1:30331 Drop and generate

events

events

events

MALWARE-CNC User-Agent known malicious User-Agent ErrCode - W32/F ujacks.htm 1:18247 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent EyeS\_Client\_1.0 - Win.Trojan.Seey 1:30344 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent getcmd - Win.Tr ojan.Burnwoo 1:30314 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent getcmdw23 - Win .Trojan.Burnwoo 1:30315 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent Neutrino/2.1 - Win.Trojan.Necurs 1:30518 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent rome0321 - Win. Trojan.Soraya 1:31225 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - 2508In st - Win.Backdoor.Upatre 1:33234 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - 2608cw -1 - Win.Backdoor.Upatre 1:33233 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - 2608cw -2 - Win.Backdoor.Upatre 1:33235 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - 2808in st - Win.Backdoor.Upatre 1:33236 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Andr.T rojan.Agent 1:42019 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Andr.T rojan.Agent 1:42020 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - AppUpd ate - Win.Backdoor.Upatre 1:33232 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - bbbbbb bbbb - Win.Backdoor.Upatre 1:33253 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - connec t - Win.Backdoor.Upatre 1:32383 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Crypto n 1:40800 Drop and generate

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - darkne ss 1:20106 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Downlo ader 1.8 - Win.Trojan.Graftor 1:31688 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Elite Keylogger 1:41456 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Explor er - Win.Backdoor.Upatre 1:33242 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - F.5.E. C 1:40217 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Firefo x - Win.Backdoor.Upatre 1:33230 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Firefo x/5.0 - Win.Backdoor.Upatre 1:33231 Drop and generate

events

events

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Fretho g 1:42454 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - fsrhrs rg - Win.Trojan.Nemucod 1:38961 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - hi - W in.Backdoor.Upatre 1:33254 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Hotbar 1:43220 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - HttpCa ll - Win.Trojan.Rukypee 1:31947 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - iMacro s - Win.Backdoor.Upatre 1:33255 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - InfoBo t 1:20104 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Instal l - Win.Backdoor.Upatre 1:31990 Drop and generate

events

events

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Instal ler/1.0 - Win.Backdoor.Upatre 1:33239 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - IPHONE 1:20105 Generate events

events

MALWARE-CNC User-Agent known malicious user-agent string - JexBos s 1:38304 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Linux. Trojan.Zollard 1:35710 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Linux. Trojan.Zollard 1:28852 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - macrot est - Win.Backdoor.Upatre 1:33256 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Mazill a/5.0 - Win.Backdoor.Upatre 1:33207 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - meterp reter 1:20201 Drop and generate

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Mozila 1:36833 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Mozill a - Win.Backdoor.Upatre 1:33243 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Mozill a/5.0 - Win.Trojan.Upatre 1:31557 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - MSIE 7 .0 na - Win.Trojan.Koobface 1:31543 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - MSIE 9 .0 in version 10 format 1:29999 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - MyIE 3 .01 1:36131 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - MyProg ramm - Win.Trojan.Rukypee 1:31948 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - myupda te - Win.Backdoor.Upatre 1:32384 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - onlyma cros - Win.Backdoor.Upatre 1:33257 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - onlyup date - Win.Backdoor.Upatre 1:33260 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Opera - Win.Backdoor.Upatre 1:33244 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - OperaM ini - Win.Backdoor.Upatre 1:33246 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Peers1 2 - Win.Backdoor.Upatre 1:33248 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Player - Win.Backdoor.Upatre 1:33237 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Poison 1:44440 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - realup date - Win.Backdoor.Upatre 1:33047 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Sality 1:40733 Drop and generate

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Sality 1:44362 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Skypee - Win.Trojan.Rukypee 1:31949 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - SLSSoa pClient - Win.Backdoor.Upatre 1:33249 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - SocSte aler 1:45229 Drop and generate

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - SocSte aler 1:45230 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Sublin k 1:42830 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - testup date - Win.Backdoor.Upatre 1:33259 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Tintin - Win.Backdoor.Upatre 1:33250 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Treck - Win.Backdoor.Upatre 1:31991 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - uguogo - Win.Trojan.Nemucod 1:38962 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - update - Win.Backdoor.Upatre 1:32125 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Update s downloader - Win.Backdoor.Upatre 1:33258 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - USER\_C HECK - Win.Backdoor.Upatre 1:33251 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Venik 1:40782 Drop and generate

events

events

events

events

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Virut 1:40869 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Virut 1:40870 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Visbot 1:41318 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - WATCli ent - Win.Backdoor.Upatre 1:33252 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Win.Ba ckdoor.Chopper 1:42838 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Win.Do wnloader.Powload 1:47695 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Win.Do wnloader.Powload 1:47696 Drop and generate

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Ma lware.DistTrack 1:41539 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Ra nsomware.Thanatos 1:45816 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Win.To ol.SMSBomber 1:45051 Drop and generate

events

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Darkcpn 1:34834 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Darkshell 1:40212 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Datper 1:44772 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Datper 1:44773 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Dluca 1:29371 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Fareit 1:40066 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.FighterPOS 1:38234 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Graftor 1:44214 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.MagicHound 1:41656 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Perseus 1:40251 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Punkey 1:34607 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Simda 1:41403 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.TrickBot 1:40643 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.TrickBot 1:40644 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.VBInject 1:40216 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string - Win.Tr ojan.Volgmer 1:44886 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - Wurst - Win.Backdoor.Upatre 1:33238 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - X-Mas 1:41441 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string - XAgent - Operation Pawn Storm 1:33513 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string 0pera 10 1:20230 Drop and generate

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string 12345678 90 1:21469 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string Aldi Bot 1:21206 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string API Guid e test program 1:21188 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent string Baby Rem ote - Win32/Babmote.A 1:20009 Drop and generate

events

events

MALWARE-CNC User-Agent known malicious user-agent string crackim 1:34291 Drop and generate

events

MALWARE-CNC User-Agent known malicious User-Agent string CustomSp y - Win.Trojan.Etek 1:29341 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string Decibal - Win.Trojan.Decibal 1:32030 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string dolit 1: 33884 Drop and generate

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string EI Plugi n updater 1:35316 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string ErrorFix 1:19482 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string fast uax 1:32333 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string feranet/ 0.4 - Win32/Ferabsa.A 1:20012 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string Flag 1:2 1225 Drop and generate

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string fortis 1 :29174 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string getURLdo wn 1:28558 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string Google B ot 1:21278 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string http - W in.Trojan.Waski 1:32295 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent string HTTP 1.1 - Win.Trojan.Tapslix 1:29139 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string IExplore 1:27710 Drop and generate

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string Instally 1:40528 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string J13A 1:2 6685 Drop and generate

events

MALWARE-CNC User-Agent known malicious User-Agent string MacProte ctor 1:19589 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string MBVDFRES CT 1:20293 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string Mozilla/ /4.0 1:20231 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string mozilla/ 2.0 1:39710 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string MSIE 4.0 1 - Win.Trojan.Careto 1:29760 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string Opera/8. 89 - P2P-Worm.Win32.Palevo.ddm 1:19756 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string psi 1:21 455 Drop and generate

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent string RookIE/1 .0 1:18388 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string RUpdate 1:32645 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string STORMDDO S - Backdoor.Win32.Inject.ctt 1:19480 Drop and generate

events

events

MALWARE-CNC User-Agent known malicious user-agent string umbra 1: 27709 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agent string update - Win.Trojan.Waski 1:32296 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string Updates downloader - Win.Trojan.Upatre 1:29887 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string Uploador - Win.Trojan.CrossRAT 1:46052 Drop and generate MALWARE-CNC User-Agent known malicious user-agent string Win32 Am ti 1:21175 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent Update1.0 - Win .Trojan.Downbini 1:29180 Drop and generate MALWARE-CNC User-Agent known malicious User-Agent wget 3.0 1:1917 5 Drop and generate

events

events

events

events

events

events

MALWARE-CNC User-Agent known malicious user-agent z00sAgent - Win .Trojan.Zbot 1:28859 Drop and generate

events

MALWARE-CNC User-Agent known malicious user-agnet string Win.Troj an.ZeusVM 1:30210 Drop and generate

events

MALWARE-CNC User-Agent request for known PUA user agent - SelectR ebates 1:18353 Drop and generate

events

MALWARE-CNC User-Agent suspicious user-agent WarpHTTP - Win.Troja n.Yohakest 1:29150 Generate events

MALWARE-CNC User-Agent Win.Trojan.Agent malicious user agent 1:42 886 Drop and generate

events

MALWARE-CNC User-Agent Xsser mRAT user-agent 1:32052 Drop and generate

events

MALWARE-CNC VBMania mass mailing worm activity 1:17234 Drop and generate

events

MALWARE-CNC VBMania mass mailing worm download 1:17235 Drop and generate

events

MALWARE-CNC Vbs.Downloader.Agent inbound connection 1:46436 Drop and generate

events

MALWARE-CNC Vbs.Downloader.Agent inbound connection 1:46437 Drop and generate

events

MALWARE-CNC Vbs.Downloader.Agent inbound connection 1:46438 Drop and generate

events

MALWARE-CNC Vbs.Downloader.Agent inbound delivery attempt 1:46439 Drop and generate

events

MALWARE-CNC Vbs.Downloader.Kryptik known malicious user-agent str ing 1:46435 Drop and generate

events

MALWARE-CNC Vbs.Trojan.Agent inbound payload download 1:45643 Drop and generate

events

MALWARE-CNC Vbs.Trojan.Agent inbound payload download 1:45644 Drop and generate

events

MALWARE-CNC Vbs.Trojan.Agent inbound payload download 1:45645 Drop and generate

events

MALWARE-CNC Vbs.Trojan.Agent outbound connection 1:45642 Drop and generate

events

MALWARE-CNC Vbs.Trojan.Agent outbound system information disclosu re 1:45646 Drop and generate

events

MALWARE-CNC Vbs.Worm.SysinfY2X outbound beacon 1:46894 Drop and generate MALWARE-CNC Vicepass outbound connection initial request to the C NC sending system information 1:33930 Drop and generate

events

events

MALWARE-CNC WashingTon ssl certificate negotiation attempt 1:4288 5 Drop and generate

events

MALWARE-CNC Win-Linux.Trojan.Derusbi variant outbound connection 1:38255 Drop and generate

events

MALWARE-CNC Win-Linux.Trojan.Derusbi variant outbound connection 1:38256 Drop and generate

events

MALWARE-CNC Win-Linux.Trojan.Derusbi variant outbound connection 1:38257 Drop and generate

events

MALWARE-CNC Win.Adware.Doyo client outbound connection 1:46434 Drop and generate

events

MALWARE-CNC Win.Adware.Doyo initial connection 1:46433 Drop and generate

events

MALWARE-CNC Win.Adware.Taplika toolbar download attempt 1:46963 Drop and generate

events

MALWARE-CNC Win.Adware.Xiazai outbound connection 1:39730 Drop and generate

events

MALWARE-CNC Win.Agent.BHHK variant outbound connection 1:33227 Drop and generate

events

MALWARE-CNC Win.Backdoor.Aumlib variant outbound connection 1:276 29 Drop and generate

events

MALWARE-CNC Win.Backdoor.Aumlib variant outbound connection 1:276 30 Drop and generate

events

MALWARE-CNC Win.Backdoor.Aumlib variant outbound connection 1:276 31 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:27966 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:27968 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:28323 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:42834 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:42835 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:42836 Drop and generate

events

MALWARE-CNC Win.Backdoor.Chopper web shell connection 1:42837 Drop and generate

events

MALWARE-CNC Win.Backdoor.Comdinter variant outbound connection 1: 30310 Drop and generate

events

MALWARE-CNC Win.Backdoor.Comdinter variant outbound connection 1: 30311 Drop and generate

events

MALWARE-CNC Win.Backdoor.Corkow variant outbound connection 1:320 86 Drop and generate

events

MALWARE-CNC Win.Backdoor.DFSCook variant JS dropper outbound conn ection 1:38584 Drop and generate

events

MALWARE-CNC Win.Backdoor.DFSCook variant outbound connection 1:38 585 Drop and generate

events

MALWARE-CNC Win.Backdoor.DFSCook variant outbound connection 1:38 586 Drop and generate

events

MALWARE-CNC Win.Backdoor.DFSCook variant outbound connection 1:38 588 Drop and generate

events

MALWARE-CNC Win.Backdoor.DFSCook variant temporary redirect attempt 1:38587 Drop and generate

events

MALWARE-CNC Win.Backdoor.Effseart variant outbound connection 1:3 2456 Drop and generate

events

MALWARE-CNC Win.Backdoor.Erotimpact variant outbound connection 1 :34132 Drop and generate

events

MALWARE-CNC Win.Backdoor.Eskaetee outbound connection 1:32780 Drop and generate

events

MALWARE-CNC Win.Backdoor.Eskaetee outbound connection 1:32781 Drop and generate

events

MALWARE-CNC Win.Backdoor.EvilBunny variant outbound connection 1: 34049 Drop and generate

events

MALWARE-CNC Win.Backdoor.Evilgrab outbound connection 1:37447 Drop and generate

events

MALWARE-CNC Win.Backdoor.Exadog outbound connection 1:32486 Drop and generate

events

MALWARE-CNC Win.Backdoor.Exadog variant outbound connection 1:324 87 Drop and generate

events

MALWARE-CNC Win.Backdoor.Havex outbound connection 1:32513 Drop and generate

events

MALWARE-CNC Win.Backdoor.Igliveforg variant initial outbound conn ection 1:34041 Drop and generate

events

MALWARE-CNC Win.Backdoor.Igliveforg variant outbound connection 1 :34042 Drop and generate

events

MALWARE-CNC Win.Backdoor.Iniduoh variant outbound connection 1:47 701 Drop and generate

events

MALWARE-CNC Win.Backdoor.Iniduoh variant outbound connection 1:28 817 Drop and generate

events

MALWARE-CNC Win.Backdoor.IsSpace initial outbound connection 1:35 750 Drop and generate

events

MALWARE-CNC Win.Backdoor.IsSpace outbound connection 1:35749 Drop and generate

events

MALWARE-CNC Win.Backdoor.JRat inbound self-signed SSL certificate 1:39159 Drop and generate

events

MALWARE-CNC Win.Backdoor.JRat inbound self-signed SSL certificate 1:39160 Drop and generate

events

MALWARE-CNC Win.Backdoor.Lesirt variant outbound connection 1:285 99 Drop and generate

events

MALWARE-CNC Win.Backdoor.Medusa variant inbound connection 1:3305 8 Drop and generate

events

MALWARE-CNC Win.Backdoor.Medusa variant outbound connection 1:330 59 Drop and generate

events

MALWARE-CNC Win.Backdoor.Medusa variant outbound connection 1:330 60 Drop and generate

events

MALWARE-CNC Win.Backdoor.MSIL.Liroospu variant outbound connectio n 1:32222 Drop and generate

events

MALWARE-CNC Win.Backdoor.MSIL.Torct variant outbound connection 1 :31957 Drop and generate

events

MALWARE-CNC Win.Backdoor.Mysayad file wipe attempt 1:32598 Drop and generate

events

MALWARE-CNC Win.Backdoor.Mysayad file wipe attempt 1:32600 Drop and generate

events

MALWARE-CNC Win.Backdoor.Mysayad outbound connection 1:32599 Drop and generate

events

MALWARE-CNC Win.Backdoor.Nirunte variant outbound connection 1:34 470 Drop and generate

events

MALWARE-CNC Win.Backdoor.Nisinul variant outbound connection 1:36 294 Drop and generate

events

MALWARE-CNC Win.Backdoor.Plez outbound connection 1:34289 Drop and generate

events

MALWARE-CNC Win.Backdoor.Plez outbound connection 1:34290 Drop and generate

events

MALWARE-CNC Win.Backdoor.Poison variant outbound connection detec ted 1:44438 Drop and generate

events

MALWARE-CNC Win.Backdoor.Poison variant outbound connection detec ted 1:44439 Drop and generate

events

MALWARE-CNC Win.Backdoor.Ptiger variant outbound connection 1:288 08 Drop and generate

events

MALWARE-CNC Win.Backdoor.StoneDrill get commands outbound connect ion 1:45092 Drop and generate

events

MALWARE-CNC Win.Backdoor.StoneDrill login outbound connection 1:4 5091 Drop and generate

events

MALWARE-CNC Win.Backdoor.StoneDrill server selection outbound con nection 1:45090 Drop and generate

events

MALWARE-CNC Win.Backdoor.Talsab variant outbound connection 1:269 54 Drop and generate

events

MALWARE-CNC Win.Backdoor.Triton Triton ICS malware transfer attempt 1:45477 Drop and generate

events

MALWARE-CNC Win.Backdoor.Triton Triton ICS malware transfer attempt 1:45478 Drop and generate

events

MALWARE-CNC Win.Backdoor.Typideg variant outbound connection 1:32 734 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31992 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31993 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31994 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31995 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31996 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31997 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31998 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:31999 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:32000 Drop and generate

events

MALWARE-CNC Win.Backdoor.Upatre SSL Cert inbound 1:32001 Drop and generate

events

MALWARE-CNC Win.Backdoor.Venik outbound connection 1:37065 Drop and generate

events

MALWARE-CNC Win.Backdoor.Venik variant outbound connection 1:2836 6 Drop and generate

events

MALWARE-CNC Win.Backdoor.Zeus variant outbound connection 1:32015 Drop and generate

events

MALWARE-CNC Win.Backdoor.Zupdax variant outbound connection 1:341 17 Drop and generate

events

MALWARE-CNC Win.Backdoor.Zuza variant outbound connection 1:28325 Drop and generate

events

MALWARE-CNC Win.Backdoor.Zuza variant outbound connection 1:28326 Drop and generate

events

MALWARE-CNC Win.Banker.Delf variant outbound connection 1:31820 Drop and generate

events

MALWARE-CNC Win.Coinminer.PyroMineIoT outbound connection 1:47373 Drop and generate

events

MALWARE-CNC Win.Coinminer.PyroMineIoT outbound connection 1:47374 Drop and generate

events

MALWARE-CNC Win.Coinminer.PyroMineIoT outbound connection 1:47375 Drop and generate

events

MALWARE-CNC Win.Coinminer.PyroMineIoT outbound connection 1:47376 Drop and generate

events

MALWARE-CNC Win.Doc.GrayEnergy malicious document download attemp t 1:48307 Drop and generate

events

MALWARE-CNC Win.Doc.GrayEnergy malicious document download attemp t 1:48308 Drop and generate

events

MALWARE-CNC Win.Downloader.Agent variant certificate negotiation 1:42172 Drop and generate

events

MALWARE-CNC Win.Downloader.Agent variant outbound connection 1:42 171 Drop and generate

events

MALWARE-CNC Win.Downloader.Beshida outbound connection 1:33994 Drop and generate

events

MALWARE-CNC Win.Downloader.Bladabindi variant outbound download r equest 1:31288 Drop and generate

events

MALWARE-CNC Win.Downloader.Boltolog variant outbound connection d ownload request 1:35034 Drop and generate

events

MALWARE-CNC Win.Downloader.Dimnie file download attempt 1:42242 Drop and generate

events

MALWARE-CNC Win.Downloader.Jadowndec attempted outbound connectio n 1:32613 Drop and generate

events

MALWARE-CNC Win.Downloader.Jadowndec attempted outbound connectio n 1:32614 Drop and generate

events

MALWARE-CNC Win.Downloader.Jrml variant outbound connection 1:354 37 Drop and generate

events

MALWARE-CNC Win.Downloader.Netkrypt inbound response 1:34138 Drop and generate

events

MALWARE-CNC Win.Downloader.Ogimant outbound connection detected 1 :40214 Drop and generate

events

MALWARE-CNC Win.Downloader.Ogimant outbound connection detected 1 :40215 Drop and generate

events

MALWARE-CNC Win.Downloader.QuantLoader external connection attemp t 1:40249 Drop and generate

events

MALWARE-CNC Win.Downloader.QuantLoader variant outbound connectio n attempt 1:46820 Drop and generate

events

MALWARE-CNC Win.Downloader.Razy variant outbound connection 1:443 07 Drop and generate

events

MALWARE-CNC Win.Downloader.Sanny URI request for known malicious URI 1:46270 Drop and generate

events

MALWARE-CNC Win.Downloader.Siromost variant outbound connection 1 :34324 Drop and generate

events

MALWARE-CNC Win.Downloader.SnatchLoader variant inbound connectio n 1:45097 Drop and generate

events

MALWARE-CNC Win.Downloader.SnatchLoader variant outbound connecti on 1:45098 Drop and generate

events

MALWARE-CNC Win.Downloader.Wannamine malicious Powershell downloa d attempt 1:46203 Drop and generate

events

MALWARE-CNC Win.Downloader.Wannaminer malicious Powershell downlo ad attempt 1:46202 Drop and generate

events

MALWARE-CNC Win.Downloader.XAgent variant outbound connection 1:4 8140 Drop and generate

events

MALWARE-CNC Win.Downloader.Zebrocy initial outbound request 1:467 86 Drop and generate

events

MALWARE-CNC Win.Downloader.Zebrocy known malicious user-agent str ing 1:46785 Drop and generate

events

MALWARE-CNC Win.Dropper.Agent inbound connection 1:35221 Drop and generate MALWARE-CNC Win.Dropper.Agent ransomware downloader outbound conn ection detected 1:43475 Drop and generate MALWARE-CNC Win.Dropper.Agent ransomware downloader outbound conn ection detected 1:43476 Drop and generate MALWARE-CNC Win.Dropper.Agent ransomware downloader outbound conn ection detected 1:43477 Drop and generate MALWARE-CNC Win.Dropper.Ch variant outbound connection 1:32670 Drop and generate

events

events

events

events

events

MALWARE-CNC Win.Dropper.IcedID outbound connection 1:47436 Drop and generate

events

MALWARE-CNC Win.Dropper.IcedID payload download 1:47435 Drop and generate

events

MALWARE-CNC Win.Dropper.NavRat payload download 1:46871 Drop and generate

events

MALWARE-CNC Win.Dropper.Vega variant outbound connection detected 1:46836 Drop and generate

events

MALWARE-CNC Win.Dropper.Vega variant outbound connection detected 1:46837 Drop and generate

events

MALWARE-CNC Win.Fudu outbound variant connection 1:34876 Drop and generate

events

MALWARE-CNC Win.Keylogger.AgentTesla variant outbound connection 1:40238 Drop and generate

events

MALWARE-CNC Win.Malware.Disttrack variant outbound connection 1:4 1540 Drop and generate

events

MALWARE-CNC Win.Malware.Disttrack variant outbound connection 1:4 0906 Drop and generate

events

MALWARE-CNC Win.Malware.Emotet variant outbound connection 1:4389 0 Drop and generate

events

MALWARE-CNC Win.Malware.Freenki variant outbound connection 1:452 39 Drop and generate

events

MALWARE-CNC Win.Malware.Furtim variant outbound connection 1:3943 0 Drop and generate

events

MALWARE-CNC Win.Malware.Ramnit outbound REGISTER\_BOT beacon 1:472 44 Drop and generate

events

MALWARE-CNC Win.Perseus variant outbound connection 1:40252 Drop and generate

events

MALWARE-CNC Win.Ransomware.Alfa outbound connection 1:39767 Drop and generate

events

MALWARE-CNC Win.Ransomware.Bandarchor variant outbound connection 1:46138 Drop and generate

events

MALWARE-CNC Win.Ransomware.Bandarchor variant outbound connection 1:46139 Drop and generate

events

MALWARE-CNC Win.Ransomware.Bandarchor variant outbound connection 1:46140 Drop and generate

events

MALWARE-CNC Win.Ransomware.Bandarchor variant outbound connection 1:46141 Drop and generate

events

MALWARE-CNC Win.Ransomware.BlackShades Crypter outbound connectio n 1:39173 Drop and generate

events

MALWARE-CNC Win.Ransomware.CryptoLocker binary download response attempt 1:41498 Drop and generate

events

MALWARE-CNC Win.Ransomware.Fantom outbound connection 1:40043 Drop and generate

events

MALWARE-CNC Win.Ransomware.Fantom post encryption outbound connec tion 1:40044 Drop and generate

events

MALWARE-CNC Win.Ransomware.Fantom post encryption outbound connec tion 1:40045 Drop and generate

events

MALWARE-CNC Win.Ransomware.FlatChestWare varint outbound connecti on 1:44279 Drop and generate

events

MALWARE-CNC Win.Ransomware.GandCrab outbound connection 1:45694 Drop and generate

events

MALWARE-CNC Win.Ransomware.GandCrab outbound connection 1:47766 Drop and generate

events

MALWARE-CNC Win.Ransomware.Gandcrab variant outbound connection 1 :46636 Drop and generate

events

MALWARE-CNC Win.Ransomware.Gibon variant inbound connection 1:450 96 Drop and generate

events

MALWARE-CNC Win.Ransomware.Gibon variant outbound connection 1:45 095 Drop and generate

events

MALWARE-CNC Win.Ransomware.LeChiffre outbound connection 1:37844 Drop and generate

events

MALWARE-CNC Win.Ransomware.Matrix outbound connection 1:46339 Drop and generate

events

MALWARE-CNC Win.Ransomware.Princess variant outbound connection attempt 1:47621 Drop and generate

events

MALWARE-CNC Win.Ransomware.Ranscam request.html response 1:39636 Drop and generate

events

MALWARE-CNC Win.Ransomware.Sage variant outbound connection 1:420 59 Drop and generate

events

MALWARE-CNC Win.Ransomware.Satan outbound connection 1:46818 Drop and generate

events

MALWARE-CNC Win.Ransomware.Shrug2 outbound connection 1:47692 Drop and generate

events

MALWARE-CNC Win.Ransomware.Sigma outbound connection 1:46065 Drop and generate

events

MALWARE-CNC Win.Ransomware.SyncCrypt variant initial outbound con nection 1:44220 Drop and generate

events

MALWARE-CNC Win.Ransomware.SyncCrypt variant initial outbound con nection 1:44221 Drop and generate

events

MALWARE-CNC Win.Ransomware.SyncCrypt variant initial outbound con nection 1:44222 Drop and generate

events

MALWARE-CNC Win.Ransomware.Urausy variant outbound connection 1:2 8033 Drop and generate

events

MALWARE-CNC Win.Ransomware.Viro variant outbound connection 1:480 22 Drop and generate

events

MALWARE-CNC Win.Ransomware.X-Mas outbound connection 1:41442 Drop and generate

events

MALWARE-CNC Win.Ransomware.X-Mas variant keylogger outbound conne ction 1:41443 Drop and generate

events

MALWARE-CNC Win.Ransomware.X-Mas variant keylogger outbound conne ction 1:41444 Drop and generate

events

MALWARE-CNC Win.Rootkit.Necurs outbound connection 1:31070 Drop and generate

events

MALWARE-CNC Win.Rootkit.Necurs possible URI with encrypted POST 1 :25577 Drop and generate

events

MALWARE-CNC Win.Rootkit.Sednit variant outbound connection 1:4091 1 Drop and generate

events

MALWARE-CNC Win.Spyware.Autoit outbound connection 1:46416 Drop and generate

events

MALWARE-CNC Win.Spyware.Invisimole CnC outbound connection 1:4701 6 Drop and generate

events

MALWARE-CNC Win.Spyware.Rombertik outbound connection 1:33161 Drop and generate

events

MALWARE-CNC Win.Tinybanker variant outbound connection 1:31641 Drop and generate

events

MALWARE-CNC Win.Tinybanker variant outbound connection 1:31642 Drop and generate

events

MALWARE-CNC Win.Trojan-Downloader.Becontr variant outbound connec tion 1:31928 Drop and generate

events

MALWARE-CNC Win.Trojan-Downloader.Bipamid variant outbound connec tion 1:32012 Drop and generate

events

MALWARE-CNC Win.Trojan-Downloader.Delorado variant outbound conne ction 1:31834 Drop and generate

events

MALWARE-CNC Win.Trojan-Downloader.Nekill variant outbound connect ion 1:32061 Drop and generate

events

MALWARE-CNC Win.Trojan-Downloader.Pedrp variant outbound connecti on 1:31941 Drop and generate

events

MALWARE-CNC Win.Trojan.12percent ransomware generator download 1: 48437 Drop and generate

events

MALWARE-CNC Win.Trojan.12percent ransomware generator download 1: 48438 Drop and generate

events

MALWARE-CNC Win.Trojan.7ev3n variant outbound connection 1:39053 Drop and generate

events

MALWARE-CNC Win.Trojan.Acanas variant outbound connection 1:32293 Drop and generate

events

MALWARE-CNC Win.Trojan.AcridRain outbound connection 1:48035 Drop and generate

events

MALWARE-CNC Win.Trojan.Adelinoq outbound connection 1:34844 Drop and generate

events

MALWARE-CNC Win.Trojan.Adialer variant outbound connection 1:3905 2 Drop and generate

events

MALWARE-CNC Win.Trojan.ADKR connection 1:28074 Drop and generate

events

MALWARE-CNC Win.Trojan.Adload.dyhq variant outbound connection 1: 29828 Drop and generate

events

MALWARE-CNC Win.Trojan.Adnel outbound connection detected 1:39909 Drop and generate

events

MALWARE-CNC Win.Trojan.Adylkuzz variant initial outbound connecti on 1:42945 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent beacon reply attempt 1:34113 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent download attempt 1:48082 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent outbound connection 1:45658 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent outbound POST attempt 1:37686 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent outbound request 1:46501 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent outbound request 1:46502 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant compromise download attempt 1:41133 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant compromise download attempt 1:41134 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant compromise download attempt 1:41135 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant connection 1:28300 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection detected 1:47026 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection detected 1:47027 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:35104 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:26119 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:36048 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:28415 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:35313 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:27120 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent variant outbound connection 1:23342 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent-ALPW variant outbound connection 1:3 4996 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent.DF - Data Exfiltration 1:28976 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent.DF - User-Agent Missing Bracket 1:28 977 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent.evf variant connection 1:27670 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent.grdm variant outbound connection 1:1 9704 Drop and generate

events

MALWARE-CNC Win.Trojan.Agent.grdm variant outbound connection 1:1 9705 Drop and generate

events

MALWARE-CNC Win.Trojan.Ajtonj variant outbound connection 1:31346 Drop and generate

events

MALWARE-CNC Win.Trojan.Akaza variant outbound connection 1:32357 Drop and generate

events

MALWARE-CNC Win.Trojan.Alina variant outbound connection 1:36331 Drop and generate

events

MALWARE-CNC Win.Trojan.Alina variant outbound connection 1:37027 Drop and generate

events

MALWARE-CNC Win.Trojan.Aluereon TDSS infection variant outbound c onnection 1:21638 Drop and generate

events

MALWARE-CNC Win.Trojan.Alurewo outbound connection 1:31079 Drop and generate

events

MALWARE-CNC Win.Trojan.Alurewo outbound connection 1:31080 Drop and generate

events

MALWARE-CNC Win.Trojan.Alurewo outbound connection 1:28960 Drop and generate

events

MALWARE-CNC Win.Trojan.Alusins variant outbound connection 1:2938 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Amasages variant outbound connection 1:338 91 Drop and generate

events

MALWARE-CNC Win.Trojan.Ammy download attempt 1:46488 Drop and generate

events

MALWARE-CNC Win.Trojan.Ammy heartbeat 1:46487 Drop and generate

events

MALWARE-CNC Win.Trojan.Ammyy RAT outbound connection 1:46964 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm Click Fraud Request 1:31465 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm Click Fraud Request 1:31466 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm variant outbound connection 1:30196 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm variant outbound connection 1:34958 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm variant outbound connection 1:32770 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm variant outbound connection 1:32374 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm variant outbound connection 1:31467 Drop and generate

events

MALWARE-CNC Win.Trojan.Androm variant outbound connection 1:29216 Drop and generate

events

MALWARE-CNC Win.Trojan.Andromeda initial outbound connection 1:35 387 Drop and generate

events

MALWARE-CNC Win.Trojan.Andromeda variant outbound connection 1:33 496 Drop and generate

events

MALWARE-CNC Win.Trojan.Anony variant connection 1:28914 Drop and generate

events

MALWARE-CNC Win.Trojan.Arfadinf variant outbound connection 1:370 37 Drop and generate

events

MALWARE-CNC Win.Trojan.AridViper variant outbound connection 1:36 468 Drop and generate

events

MALWARE-CNC Win.Trojan.AridViper variant outbound connection 1:36 469 Drop and generate

events

MALWARE-CNC Win.Trojan.ARS VBS loader outbound connection 1:47338 Drop and generate

events

MALWARE-CNC Win.Trojan.Asprox inbound connection 1:32065 Drop and generate

events

MALWARE-CNC Win.Trojan.Asprox outbound connection 1:32066 Drop and generate

events

MALWARE-CNC Win.Trojan.Asprox outbound connection 1:32067 Drop and generate

events

MALWARE-CNC Win.Trojan.Atezag variant outbound connection 1:27169 Drop and generate

events

MALWARE-CNC Win.Trojan.Athena variant outbound connection 1:33674 Drop and generate

events

MALWARE-CNC Win.Trojan.Athena variant outbound connection 1:33675 Drop and generate

events

MALWARE-CNC Win.Trojan.Athena variant outbound connection 1:41031 Drop and generate

events

MALWARE-CNC Win.Trojan.Atrax variant outbound connection 1:34596 Drop and generate

events

MALWARE-CNC Win.Trojan.Atrax variant outbound connection 1:34597 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant outbound connection 1:41173 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant outbound connection 1:41174 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant outbound connection 1:41175 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant outbound connection 1:41176 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant outbound connection 1:41177 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant outbound connection 1:41178 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant post compromise download at tempt 1:41179 Drop and generate

events

MALWARE-CNC Win.Trojan.August variant post compromise download at tempt 1:41180 Drop and generate

events

MALWARE-CNC Win.Trojan.Autoit-73 configuration file download atte mpt 1:40751 Drop and generate

events

MALWARE-CNC Win.Trojan.Autoit-73 configuration file download atte mpt 1:40752 Drop and generate

events

MALWARE-CNC Win.Trojan.AzoRult variant outbound connection detec ted 1:47602 Drop and generate

events

MALWARE-CNC Win.Trojan.AZORult variant outbound connection 1:4733 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Babar outbound connection 1:33677 Drop and generate

events

MALWARE-CNC Win.Trojan.Backdoor file download 1:23946 Drop and generate

events

MALWARE-CNC Win.Trojan.Backdoor Remote Shell Server download 1:28 994 Drop and generate

events

MALWARE-CNC Win.Trojan.Backdoor variant outbound connection 1:239 45 Drop and generate

events

MALWARE-CNC Win.Trojan.Backdoor.Tomvode variant outbound connecti on 1:26809 Drop and generate

events

MALWARE-CNC Win.Trojan.Backoff initial outbound connection 1:3158 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Backoff initial outbound connection 1:3245 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Backspace outbound connection 1:34346 Drop and generate

events

MALWARE-CNC Win.Trojan.Backswap self-signed certificate exchange 1:46965 Drop and generate

events

MALWARE-CNC Win.Trojan.Badur download attempt 1:31681 Drop and generate

events

MALWARE-CNC Win.Trojan.Badur variant outbound connection 1:31683 Drop and generate

events

MALWARE-CNC Win.Trojan.Bagsu variant outbound connection 1:36066 Drop and generate

events

MALWARE-CNC Win.Trojan.Bagsu variant outbound connection 1:36064 Drop and generate

events

MALWARE-CNC Win.Trojan.Bagsu variant outbound connection 1:36065 Drop and generate

events

MALWARE-CNC Win.Trojan.Baisogu outbound connection 1:35471 Drop and generate

events

MALWARE-CNC Win.Trojan.BamCompiled variant inbound updates 1:2198 4 Drop and generate

events

MALWARE-CNC Win.Trojan.BamCompiled variant outbound connection 1: 21983 Drop and generate

events

MALWARE-CNC Win.Trojan.Banbra HTTP Header Structure 1:34995 Drop and generate

events

MALWARE-CNC Win.Trojan.Banbra variant connection 1:28125 Drop and generate

events

MALWARE-CNC Win.Trojan.Banbra variant outbound connection 1:34994 Drop and generate

events

MALWARE-CNC Win.Trojan.Banbra variant outbound connection 1:24534 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos outbound connection 1:28802 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos password stealing attempt 1:31112 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection - ksa.t xt 1:26370 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:25626 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:31113 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:25766 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:31020 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:32130 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:29895 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:34931 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:30919 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:31916 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:31649 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:28012 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:34452 Drop and generate

events

MALWARE-CNC Win.Trojan.Bancos variant outbound connection 1:34453 Drop and generate

events

MALWARE-CNC Win.Trojan.BancosBanload variant outbound connection 1:25259 Drop and generate

events

MALWARE-CNC Win.Trojan.Bandios inbound delivery attempt 1:46285 Drop and generate

events

MALWARE-CNC Win.Trojan.Bandios inbound delivery attempt 1:46286 Drop and generate

events

MALWARE-CNC Win.Trojan.Bandios user agent outbound communication attempt 1:46284 Drop and generate

events

MALWARE-CNC Win.Trojan.Bandook/Anbacas outbound connection attemp t 1:46051 Drop and generate

events

MALWARE-CNC Win.Trojan.Banechant outbound variant connection 1:27 747 Drop and generate

events

MALWARE-CNC Win.Trojan.Bankeiya outbound connection 1:32469 Drop and generate

events

MALWARE-CNC Win.Trojan.Bankeiya outbound connection 1:31183 Drop and generate

events

MALWARE-CNC Win.Trojan.banker outbound connection 1:28141 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:19765 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:25074 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:25609 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:29337 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:40775 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:28547 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:32093 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:31964 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:24533 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker variant outbound connection 1:23262 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker.bkhu variant outbound connection 1: 19353 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker.boxg connect to cnc server 1:23242 Drop and generate

events

MALWARE-CNC Win.Trojan.Banker.NWT variant outbound connection 1:3 6522 Drop and generate

events

MALWARE-CNC Win.Trojan.Banking download attempt initiated 1:48355 Drop and generate

events

MALWARE-CNC Win.Trojan.Banking download attempt initiated 1:48356 Drop and generate

events

MALWARE-CNC Win.Trojan.Banklaed variant outbound connection 1:340 39 Drop and generate

events

MALWARE-CNC Win.Trojan.Bankshot variant outbound connection 1:472 35 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload download 1:28107 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload information upload 1:28106 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46574 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46575 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46576 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46577 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46580 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46581 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46582 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46583 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46584 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46585 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46586 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46589 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46590 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious file download 1:46591 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious system information discl osure 1:46578 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload malicious system information discl osure 1:46579 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload outbound connection 1:36834 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant inbound connection 1:29031 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:3413 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:3105 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:3436 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:3436 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:2421 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:2810 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload variant outbound connection 1:3190 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload 1:37066 Drop and generate

events

MALWARE-CNC Win.Trojan.Banload.awt variant outbound connection 1: 32037 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection detected 1:4 0338 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection 1:34181 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection 1:34182 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection 1:34183 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection 1:34281 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection 1:34282 Drop and generate

events

MALWARE-CNC Win.Trojan.Bartallex outbound connection 1:34283 Drop and generate

events

MALWARE-CNC Win.Trojan.Basostab variant outbound connection 1:319 09 Drop and generate

events

MALWARE-CNC Win.Trojan.Batec outbound connection 1:37127 Drop and generate

events

MALWARE-CNC Win.Trojan.Batlopma variant outbound connection 1:424 47 Drop and generate

events

MALWARE-CNC Win.Trojan.Bedep initial outbound connection 1:35386 Drop and generate

events

MALWARE-CNC Win.Trojan.Bedep.variant CNC server response 1:38367 Drop and generate

events

MALWARE-CNC Win.Trojan.Bedepshel variant outbound connection 1:34 327 Drop and generate

events

MALWARE-CNC Win.Trojan.BeeOne runtime traffic detected 1:21430 Drop and generate

events

MALWARE-CNC Win.Trojan.Berbew variant outbound connection 1:40596 Drop and generate

events

MALWARE-CNC Win.Trojan.Bergard outbound connection 1:35472 Drop and generate

events

MALWARE-CNC Win.Trojan.Betabot variant connection 1:27643 Drop and generate

events

MALWARE-CNC Win.Trojan.Betabot variant outbound connection detect ed 1:47601 Drop and generate

events

MALWARE-CNC Win.Trojan.Betad variant outbound connection 1:21230 Drop and generate

events

MALWARE-CNC Win.Trojan.Bicolo variant outbound connection 1:29985 Drop and generate

events

MALWARE-CNC Win.Trojan.Bicololo outbound connection 1:31355 Drop and generate

events

MALWARE-CNC Win.Trojan.Bicololo variant outbound connection 1:294 96 Drop and generate

events

MALWARE-CNC Win.Trojan.Biloky variant outbound connection 1:24216 Drop and generate

events

MALWARE-CNC Win.Trojan.Binjo variant outbound connection 1:27645 Drop and generate

events

MALWARE-CNC Win.Trojan.Bisonal RAT beacon 1:26945 Drop and generate

events

MALWARE-CNC Win.Trojan.Bisonha variant outbound connection 1:2780 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Bitsto variant connection 1:28212 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackCoffee outbound connection 1:35436 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackCoffee outbound connection 1:35551 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackEnergy DropBear SSH public key 1:3735 6 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackEnergy DropBear SSH server password a uthentication 1:37357 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackEnergy INF file download attempt 1:32 259 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackEnergy2 outbound connection 1:32189 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackEnergy3 outbound connection 1:32188 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackIce variant outbound connection 1:466 09 Drop and generate

events

MALWARE-CNC Win.Trojan.Blackmoon outbound connection 1:37466 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc connect command 1:26739 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc data command 1:26735 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc dataget command 1:26738 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc datapost command 1:26731 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc die command 1:26727 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc dns command 1:26740 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc download command 1:26746 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc exec command 1:26741 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc fastddos command 1:26747 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc ftp command 1:26745 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc full command 1:26750 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc http command 1:26725 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc icmp command 1:26736 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc loginpost command 1:26730 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc range command 1:26744 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc resolve command 1:26742 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc simple command 1:26729 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc sleep command 1:26728 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc slowhttp command 1:26748 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc stop command 1:26726 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc syn command 1:26732 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc tcpdata command 1:26737 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc udp command 1:26733 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev cnc udpdata command 1:26734 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev rev 1 outbound traffic 1:26713 Drop and generate

events

MALWARE-CNC Win.Trojan.BlackRev rev 2 outbound traffic 1:26714 Drop and generate

events

MALWARE-CNC Win.Trojan.Blackshades variant outbound communication 1:46608 Drop and generate

events

MALWARE-CNC Win.Trojan.Bledoor TCP tunnel in UDP 1:24087 Drop and generate

events

MALWARE-CNC Win.Trojan.Blobrsa variant outbound connection 1:2956 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Blocker variant outbound connection HTTP H eader Structure 1:26775 Drop and generate

events

MALWARE-CNC Win.Trojan.Blocker variant outbound connection POST 1 :26776 Drop and generate

events

MALWARE-CNC Win.Trojan.Boato variant outbound connection 1:29367 Drop and generate

events

MALWARE-CNC Win.Trojan.Boaxxe variant outbound connection 1:38509 Drop and generate

events

MALWARE-CNC Win.Trojan.Boda variant outbound connection 1:29294 Drop and generate

events

MALWARE-CNC Win.Trojan.Boleteiro variant outbound connection 1:32 035 Drop and generate

events

MALWARE-CNC Win.Trojan.Bondupdater outbound cnc connection 1:4842 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Boolflot variant outbound connection 1:259 73 Drop and generate

events

MALWARE-CNC Win.Trojan.Brabat variant outbound connection 1:29861 Drop and generate

events

MALWARE-CNC Win.Trojan.Bredo variant outbound connection 1:26019 Drop and generate

events

MALWARE-CNC Win.Trojan.Bredolab variant outbound connection 1:215 62 Drop and generate

events

MALWARE-CNC Win.Trojan.Brolux variant outbound connection 1:36540 Drop and generate

events

MALWARE-CNC Win.Trojan.Broonject variant outbound connection 1:32 373 Drop and generate

events

MALWARE-CNC Win.Trojan.Bruecimig variant outbound connection 1:34 028 Drop and generate

events

MALWARE-CNC Win.Trojan.Bspire variant connection 1:28439 Drop and generate

events

MALWARE-CNC Win.Trojan.Bublik variant outbound connection 1:23103 Drop and generate

events

MALWARE-CNC Win.Trojan.Bublik variant outbound connection 1:23778 Drop and generate

events

MALWARE-CNC Win.Trojan.Budir initial variant outbound connection 1:29081 Drop and generate

events

MALWARE-CNC Win.Trojan.Bulilit variant outbound connection 1:2935 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Bulta external connection attempt 1:40209 Drop and generate

events

MALWARE-CNC Win.Trojan.Buterat variant outbound connection 1:2526 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Buterat variant outbount connection detect ed 1:44450 Drop and generate

events

MALWARE-CNC Win.Trojan.Buzus variant outbound connection 1:25661 Drop and generate

events

MALWARE-CNC Win.Trojan.CactusTorch download attempt detected 1:45 232 Drop and generate

events

MALWARE-CNC Win.Trojan.Cahecon outbound connection 1:31121 Drop and generate

events

MALWARE-CNC Win.Trojan.CannibalRAT initial outbound connection 1: 45771 Drop and generate

events

MALWARE-CNC Win.Trojan.CannibalRAT outbound reporting attempt 1:4 5772 Drop and generate

events

MALWARE-CNC Win.Trojan.CannibalRAT outbound upload attempt 1:4577 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Cannon outbound connection 1:48429 Drop and generate

events

MALWARE-CNC Win.Trojan.Cannon outbound connection 1:48430 Drop and generate

events

MALWARE-CNC Win.Trojan.Caphaw outbound connection 1:29670 Drop and generate

events

MALWARE-CNC Win.Trojan.Caphaw variant outbound connection 1:28042 Drop and generate

events

MALWARE-CNC Win.Trojan.Capimac variant outbound connection 1:3421 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Careto outbound connection 1:29788 Drop and generate

events

MALWARE-CNC Win.Trojan.Careto plugin download 1:29789 Drop and generate

events

MALWARE-CNC Win.Trojan.Careto plugin download 1:29790 Drop and generate

events

MALWARE-CNC Win.Trojan.Careto plugin download 1:29791 Drop and generate

events

MALWARE-CNC Win.Trojan.Castov variant connection 1:27664 Drop and generate

events

MALWARE-CNC Win.Trojan.Castov variant connection 1:27665 Drop and generate

events

MALWARE-CNC Win.Trojan.Castov variant connection 1:28559 Drop and generate

events

MALWARE-CNC Win.Trojan.CeeInject external connection 1:40232 Drop and generate

events

MALWARE-CNC Win.Trojan.Cendode system information disclosure atte mpt 1:33218 Drop and generate

events

MALWARE-CNC Win.Trojan.CenterPos outbound connection 1:36460 Drop and generate

events

MALWARE-CNC Win.Trojan.Cerber outbound connection 1:41424 Drop and generate

events

MALWARE-CNC Win.Trojan.Cerber variant inbound connection attempt 1:42421 Drop and generate

events

MALWARE-CNC Win.Trojan.Cerber variant outbound connection 1:44177 Drop and generate

events

MALWARE-CNC Win.Trojan.Cetsiol outbound connection 1:37117 Drop and generate

events

MALWARE-CNC Win.Trojan.Chabava outbound connection 1:30743 Drop and generate

events

MALWARE-CNC Win.Trojan.Chafer malicious communication attempt 1:4 5972 Drop and generate

events

MALWARE-CNC Win.Trojan.Chafer malicious communication attempt 1:4 5973 Drop and generate

events

MALWARE-CNC Win.Trojan.Chebri variant outbound connection 1:31973 Drop and generate

events

MALWARE-CNC Win.Trojan.Chekafe variant connection 1:27640 Drop and generate

events

MALWARE-CNC Win.Trojan.Cheprobnk variant outbound connection 1:34 347 Drop and generate

events

MALWARE-CNC Win.Trojan.Chewbacca outbound connection 1:29440 Drop and generate

events

MALWARE-CNC Win.Trojan.chfx variant outbound connection 1:28548 Drop and generate

events

MALWARE-CNC Win.Trojan.Chif variant outbound connection 1:24482 Drop and generate

events

MALWARE-CNC Win.Trojan.Chinoxy variant outbound connection 1:2699 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Chinoxy variant outbound connection 1:2700 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Chiviper variant outbound connection 1:244 40 Drop and generate

events

MALWARE-CNC Win.Trojan.Chkbot outbound connection 1:31833 Drop and generate

events

MALWARE-CNC Win.Trojan.Chopstick variant outbound request 1:32665 Drop and generate

events

MALWARE-CNC Win.Trojan.Chopstick variant outbound request 1:32667 Drop and generate

events

MALWARE-CNC Win.Trojan.Chowspy variant outbound connection 1:2566 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Choxy variant outbound connection 1:29091 Drop and generate

events

MALWARE-CNC Win.Trojan.Chrozil variant outbound connection 1:3411 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Chthonic outbound file download attempt 1: 44276 Drop and generate

events

MALWARE-CNC Win.Trojan.Chthonic outbound file download attempt 1: 44277 Drop and generate

events

MALWARE-CNC Win.Trojan.Chulastran variant initial version check o utbound connection 1:29293 Drop and generate

events

MALWARE-CNC Win.Trojan.Chulastran variant outbound connection 1:2 9292 Drop and generate

events

MALWARE-CNC Win.Trojan.Cidox variant outbound connection attempt 1:46137 Drop and generate

events

MALWARE-CNC Win.Trojan.Cidox variant outbound connection 1:29356 Drop and generate

events

MALWARE-CNC WIN.Trojan.Clemint variant outbound connection 1:3224 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Clicker Win.Trojan.Hatigh.C variant outbou nd connection 1:19351 Drop and generate

events

MALWARE-CNC Win.Trojan.CobInt outbound connection 1:47901 Drop and generate

events

MALWARE-CNC Win.Trojan.CobInt outbound connection 1:47902 Drop and generate

events

MALWARE-CNC Win.Trojan.CobInt outbound connection 1:47903 Drop and generate

events

MALWARE-CNC Win.Trojan.CobInt outbound connection 1:47904 Drop and generate

events

MALWARE-CNC Win.Trojan.CobInt outbound connection 1:47906 Drop and generate

events

MALWARE-CNC Win.Trojan.Codiltak variant outbound connection 1:284 86 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner inbound connection detected 1:44 895 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner inbound connection detected 1:44 899 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner outbound connection 1:44896 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner outbound connection 1:44897 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner outbound connection 1:44898 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner variant outbound connection 1:28 410 Drop and generate

events

MALWARE-CNC Win.Trojan.CoinMiner variant outbound connection 1:28 411 Drop and generate

events

MALWARE-CNC Win.Trojan.Collicky variant inbound command attempt 1 :37141 Drop and generate

events

MALWARE-CNC Win.Trojan.Comisproc outbound connection detected 1:4 0205 Drop and generate

events

MALWARE-CNC Win.Trojan.Comisproc outbound connection detected 1:4 0206 Drop and generate

events

MALWARE-CNC Win.Trojan.Comisproc outbound connection detected 1:4 0207 Drop and generate

events

MALWARE-CNC Win.Trojan.command and control communication 1:16459 Drop and generate

events

MALWARE-CNC Win.Trojan.Comowba variant outbound connection 1:2990 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Compfolder variant outbound connection 1:3 4872 Drop and generate

events

MALWARE-CNC Win.Trojan.Concbak outbound connection 1:33913 Drop and generate

events

MALWARE-CNC Win.Trojan.Conficker variant outbound connection 1:28 543 Drop and generate

events

MALWARE-CNC Win.Trojan.Conficker variant outbound connection 1:28 542 Drop and generate

events

MALWARE-CNC Win.Trojan.Conrec variant outbound connection 1:29113 Generate events

MALWARE-CNC Win.Trojan.Cordmix variant outbound connection 1:2901 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Corebot variant outbound connection 1:3627 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Corebot variant outbound connection 1:3627 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Coresh outbound identification request 1:3 0060 Drop and generate

events

MALWARE-CNC Win.Trojan.Coreshell variant outbound connection 1:32 551 Drop and generate

events

MALWARE-CNC Win.Trojan.CosmicDuke HTTP data exfiltration attempt 1:31556 Drop and generate

events

MALWARE-CNC Win.Trojan.Coswid.klk variant outbound connection 1:2 2103 Drop and generate

events

MALWARE-CNC Win.Trojan.CowerSnail command and control response de tected 1:46872 Drop and generate

events

MALWARE-CNC Win.Trojan.CowerSnail initial outbound connection att empt 1:46873 Drop and generate

events

MALWARE-CNC Win.Trojan.Cozybear variant outbound connection 1:348 31 Drop and generate

events

MALWARE-CNC Win.Trojan.Cozybear variant outbound connection 1:348 32 Drop and generate

events

MALWARE-CNC Win.Trojan.Cridex encrypted POST check-in 1:26779 Drop and generate

events

MALWARE-CNC Win.Trojan.Cridex variant outbound connection 1:32368 Drop and generate

events

MALWARE-CNC Win.Trojan.Cript outbound connection 1:39084 Drop and generate

events

MALWARE-CNC Win.Trojan.Cript outbound connection 1:39085 Drop and generate

events

MALWARE-CNC Win.Trojan.Cript outbound connection 1:39086 Drop and generate

events

MALWARE-CNC Win.Trojan.Crisis variant outbound connection 1:23968 Drop and generate

events

MALWARE-CNC Win.Trojan.Critroni certificate exchange 1:34917 Drop and generate

events

MALWARE-CNC Win.Trojan.Critroni outbound connection 1:31718 Drop and generate

events

MALWARE-CNC Win.Trojan.CrossRAT outbound connection attempt 1:460 50 Drop and generate

events

MALWARE-CNC Win.Trojan.Crowti variant outbound connection 1:30047 Drop and generate

events

MALWARE-CNC Win.Trojan.Cry variant outbound connection 1:40339 Drop and generate

events

MALWARE-CNC Win.Trojan.Cry variant outbound connection 1:40340 Drop and generate

events

MALWARE-CNC Win.Trojan.Crypaura variant outbound connection 1:346 24 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptolocker download detected 1:32289 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptolocker download detected 1:32290 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoLocker outbound connection 1:28416 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptolocker outbound connection 1:34965 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoLocker variant connection 1:28044 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoLocker.B connection test 1:29376 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoPHP variant outbound connection 1:32 735 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoPHP variant outbound connection 1:32 736 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptor outbound connection 1:31224 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoRoger outbound POST attempt 1:39327 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall 3.0 variant outbound connection 1:33431 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall 3.0 variant outbound connection 1:33432 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall 3.0 variant outbound connection 1:33433 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall 3.0 variant outbound connection 1:33434 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall 3.0 variant outbound connection 1:33435 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall click fraud response 1:35344 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoWall downloader attempt 1:31449 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoWall outbound connection 1:31450 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection 1:3 1223 Drop and generate

events

MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection 1:3 4318 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection 1:3 2225 Drop and generate

events

MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection 1:3 1014 Drop and generate

events

MALWARE-CNC Win.Trojan.Crypvault outbound connection 1:34143 Drop and generate

events

MALWARE-CNC Win.Trojan.CryPy ransomware variant outbound connecti on 1:40549 Drop and generate

events

MALWARE-CNC Win.Trojan.CrystalAttack outbound file download attempt 1:44278 Drop and generate

events

MALWARE-CNC Win.Trojan.Cycbot variant outbound connection 1:21269 Drop and generate

events

MALWARE-CNC Win.Trojan.Cycbot variant outbound connection 1:20232 Drop and generate

events

MALWARE-CNC Win.Trojan.Cyvadextr variant outbound connection 1:34 966 Drop and generate

events

MALWARE-CNC Win.Trojan.Cyvadextr variant outbound connection 1:26 987 Drop and generate

events

MALWARE-CNC Win.Trojan.Daikou variant outbound connection 1:31314 Drop and generate

events

MALWARE-CNC Win.Trojan.Dalexis variant outbound connection 1:3454 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Dalexis variant outbound connection 1:3454 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Danabot outbound connection 1:46966 Drop and generate

events

MALWARE-CNC Win.Trojan.Danabot outbound connection 1:46967 Drop and generate

events

MALWARE-CNC Win.Trojan.Danabot outbound connection 1:46968 Drop and generate

events

MALWARE-CNC Win.Trojan.Dapato CMS spambot check-in 1:26813 Drop and generate

events

MALWARE-CNC Win.Trojan.Darkhotel outbound connection 1:32825 Drop and generate

events

MALWARE-CNC Win.Trojan.Darkhotel response connection attempt 1:32 827 Drop and generate

events

MALWARE-CNC Win.Trojan.Darkhotel variant outbound connection 1:32 824 Drop and generate

events

MALWARE-CNC Win.Trojan.DarkSeoul variant payload download 1:46959 Drop and generate

events

MALWARE-CNC Win.Trojan.DarkShell external connection attempt 1:40 213 Drop and generate

events

MALWARE-CNC Win.Trojan.DarkSky variant outbound connection 1:4594 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Darkwebot variant outbound connection 1:19 731 Drop and generate

events

MALWARE-CNC Win.Trojan.Dashikut outbound connection 1:37100 Drop and generate

events

MALWARE-CNC Win.Trojan.Datper variant outbound request detected 1 :48197 Drop and generate

events

MALWARE-CNC Win.Trojan.Datper variant outbound request detected 1 :48198 Drop and generate

events

MALWARE-CNC Win.Trojan.Daws variant outbound connection 1:25625 Drop and generate

events

MALWARE-CNC Win.Trojan.DDEDownloader variant outbound connection detected 1:45231 Drop and generate

events

MALWARE-CNC Win.Trojan.Decibal variant outbound connection 1:3203 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Deedevil variant outbound connection 1:311 35 Drop and generate

events

MALWARE-CNC Win.Trojan.Delf variant HTTP Response 1:31826 Drop and generate

events

MALWARE-CNC Win.Trojan.Delf variant outbound connection 1:21441 Drop and generate

events

MALWARE-CNC Win.Trojan.Delf variant outbound connection 1:21427 Drop and generate

events

MALWARE-CNC Win.Trojan.Delf variant outbound connection 1:15730 Drop and generate

events

MALWARE-CNC Win.Trojan.Delf variant outbound connection 1:31827 Drop and generate

events

MALWARE-CNC Win.Trojan.Delf.CL variant outbound connection 1:2325 4 Drop and generate

events

MALWARE-CNC Win.Trojan.DelfInject.gen!X variant outbound connecti on 1:19912 Drop and generate

events

MALWARE-CNC Win.Trojan.Derkziel variant outbound connection 1:373 74 Drop and generate

events

MALWARE-CNC Win.Trojan.Derusbi outbound connection 1:37534 Drop and generate

events

MALWARE-CNC Win.Trojan.Descrantol variant outbound connection 1:2 9056 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34307 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34308 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34311 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34312 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34313 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34314 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34315 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34316 Drop and generate

events

MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection 1 :34317 Drop and generate

events

MALWARE-CNC Win.Trojan.Deshacop variant outbound connection 1:404 61 Drop and generate

events

MALWARE-CNC Win.Trojan.Destoplug variant outbound connection 1:31 258 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter Banker variant second stage downloa d attempt 1:40550 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter Banker variant successful installat ion report attempt 1:40551 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter CasinoLoader SQL injection 1:29878 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter CasinoLoader SQL injection 1:29879 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter CasinoLoader SQL injection 1:29880 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter CasinoLoader SQL injection 1:29881 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter variant outbound connection 1:31669 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter variant outbound connection 1:25553 Drop and generate

events

MALWARE-CNC Win.Trojan.Dexter variant outbound connection 1:31897 Drop and generate

events

MALWARE-CNC Win.Trojan.Dilavtor variant outbound connection 1:256 00 Drop and generate

events

MALWARE-CNC Win.Trojan.Dimnie outbound connection 1:42243 Drop and generate

events

MALWARE-CNC Win.Trojan.Dino variant outbound connection 1:35069 Drop and generate

events

MALWARE-CNC Win.Trojan.Dipverdle variant outbound connection 1:28 853 Drop and generate

events

MALWARE-CNC Win.Trojan.Directate outbound connection 1:35317 Drop and generate

events

MALWARE-CNC Win.Trojan.Direvex variant outbound connection 1:3732 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Dishigy variant outbound connection 1:2333 2 Drop and generate

events

MALWARE-CNC Win.Trojan.DistTrack command and control traffic 1:23 893 Drop and generate

events

MALWARE-CNC Win.Trojan.DMALocker variant outbound connection 1:39 116 Drop and generate

events

MALWARE-CNC Win.Trojan.DNSChanger variant outbound connection 1:3 3523 Drop and generate

events

MALWARE-CNC Win.Trojan.DNSChanger variant outbound connection 1:3 3524 Drop and generate

events

MALWARE-CNC Win.Trojan.DNSMessenger outbound connection 1:44595 Drop and generate

events

MALWARE-CNC Win.Trojan.DocumentCrypt variant outbound connection 1:42228 Drop and generate

events

MALWARE-CNC Win.Trojan.Dofoil inbound connection 1:28809 Drop and generate

events

MALWARE-CNC Win.Trojan.Dofoil variant outbound connection 1:21311 Drop and generate

events

MALWARE-CNC Win.Trojan.Dofoil variant outbound connection 1:21313 Drop and generate

events

MALWARE-CNC Win.Trojan.Dofoil variant outbound connection 1:28040 Drop and generate

events

MALWARE-CNC Win.Trojan.Dofoil variant outbound payload request 1: 21538 Drop and generate

events

MALWARE-CNC Win.Trojan.DomaIQ variant outbound connection 1:29664 Drop and generate

events

MALWARE-CNC Win.Trojan.Dondat variant outbound connection 1:29344 Drop and generate

events

MALWARE-CNC Win.Trojan.Dondat variant outbound connection 1:29345 Drop and generate

events

MALWARE-CNC Win.Trojan.Doneste variant outbound connection 1:2955 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Donoff outbound connection detected 1:3996 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Donoff outbound connection detected 1:3996 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Donvibs variant outbound connection 1:4352 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Donvibs variant outbound connection 1:4352 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Dorkbot variant outbound connection 1:2488 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Dosoloid variant outbound connection 1:312 40 Drop and generate

events

MALWARE-CNC Win.Trojan.Doublepulsar variant process injection com mand 1:42331 Drop and generate

events

MALWARE-CNC Win.Trojan.Doublepulsar variant successful injection response 1:42330 Drop and generate

events

MALWARE-CNC Win.Trojan.Doublepulsar variant successful ping respo nse 1:42329 Drop and generate

events

MALWARE-CNC Win.Trojan.Doublepulsar variant successful ping respo nse 1:43459 Drop and generate

events

MALWARE-CNC Win.Trojan.Downbot variant connection 1:27642 Drop and generate

events

MALWARE-CNC Win.Trojan.Downeks variant initial outbound connectio n 1:42083 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader variant outbound connection 1:3 2129 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader variant outbound connection 1:2 3245 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader variant outbound connection 1:1 9712 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader variant outbound connection 1:2 5465 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader variant outbound connection 1:2 2059 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader variant outbound connection 1:2 1525 Drop and generate MALWARE-CNC Win.Trojan.Downloader Win.Trojan.FraudLoad.emq varian t outbound connection 1:19348 Drop and generate MALWARE-CNC Win.Trojan.Downloader.Agent variant outbound connecti on 1:26995 Drop and generate

events

events

events

MALWARE-CNC Win.Trojan.Downloader.Agent variant outbound connecti on 1:26996 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader.Dtcontx outbound connection 1:2 8418 Drop and generate

events

MALWARE-CNC Win.Trojan.Downloader.Win32.Yakes.cbi variant outboun d connection 1:20081 Drop and generate

events

MALWARE-CNC Win.Trojan.DownloadGuide variant outbound traffic 1:4 7835 Drop and generate

events

MALWARE-CNC Win.Trojan.DownloadGuide variant outbound traffic 1:4 7836 Drop and generate

events

MALWARE-CNC Win.Trojan.DownloadGuide variant outbound traffic 1:4 7837 Drop and generate

events

MALWARE-CNC Win.Trojan.Drafukey variant outbound connection 1:291 09 Drop and generate

events

MALWARE-CNC Win.Trojan.Drafukey variant outbound connection 1:291 12 Drop and generate

events

MALWARE-CNC Win.Trojan.DragonOK variant outbound connection 1:413 15 Drop and generate

events

MALWARE-CNC Win.Trojan.DragonOK variant outbound connection 1:413 16 Drop and generate

events

MALWARE-CNC Win.Trojan.DragonOK variant outbound connection 1:413 17 Drop and generate

events

MALWARE-CNC Win.Trojan.Drawnetz variant outbound connection 1:303 23 Drop and generate

events

MALWARE-CNC Win.Trojan.Drepitt variant outbound connection 1:3237 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex certificate exchange 1:38620 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex certificate exchange 1:38621 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex certificate exchange 1:38378 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex download attempt 1:38916 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex dropper variant outbound connection 1:37733 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial file download 1:45930 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial file download 1:45931 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial file download 1:45932 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33745 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33746 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33747 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33748 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33749 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33750 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33751 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33752 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33753 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33754 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33755 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33704 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex initial outbound connection 1:33145 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex Microsoft Word document dropper dow nload attempt 1:35102 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex outbound connection 1:38018 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex self-signed certificate exchange 1: 39163 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex self-signed certificate exchange 1: 39164 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex variant CNC traffic 1:38917 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex variant outbound connection 1:32677 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex variant outbound connection 1:32678 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3385 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex3 initial outbound connection 1:3386 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Dridex4 initial outbound connection 1:3403 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Drolnux variant outbound connection 1:4020 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Droot outbound connection 1:37067 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper connect to server 1:23307 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper initial outbound connection attemp t 1:46743 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper malicious executable download atte mpt 1:46744 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper malicious script download attempt 1:46742 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper outbound connection 1:27867 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper outbound connection 1:46936 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper variant outbound connection 1:2926 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper variant outbound connection 1:2159 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper variant outbound connection 1:4637 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Dropper Win.Trojan.Agent.alda variant outb ound connection 1:19339 Drop and generate

events

MALWARE-CNC Win.Trojan.Dujfudg outbound connection 1:34611 Drop and generate

events

MALWARE-CNC Win.Trojan.Dulom variant outbound connection 1:25072 Drop and generate

events

MALWARE-CNC Win.Trojan.Dunihi outbound connection 1:46827 Drop and generate

events

MALWARE-CNC Win.Trojan.Duntek Checkin GET Request 1:10403 Drop and generate

events

MALWARE-CNC Win.Trojan.DustySky variant outbound connection 1:363 96 Drop and generate

events

MALWARE-CNC Win.Trojan.Dynamer variant outbound connection 1:3346 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Ecsudown outbound connection 1:31768 Drop and generate

events

MALWARE-CNC Win.Trojan.Egamipload variant outbound connection 1:3 3818 Drop and generate

events

MALWARE-CNC Win.Trojan.Egamipload variant outbound connection 1:3 3819 Drop and generate

events

MALWARE-CNC Win.Trojan.Egamipload variant outbound connection 1:3 3820 Drop and generate

events

MALWARE-CNC Win.Trojan.Egamipload variant outbound connection 1:3 3821 Drop and generate

events

MALWARE-CNC Win.Trojan.Egamipload variant outbound connection 1:3 3822 Drop and generate

events

MALWARE-CNC Win.Trojan.Egamipload variant outbound connection 1:2 8820 Drop and generate

events

MALWARE-CNC Win.Trojan.Egobot variant outbound connection 1:28989 Drop and generate

events

MALWARE-CNC Win.Trojan.Eitenckay initial outbound connection 1:34 045 Drop and generate

events

MALWARE-CNC Win.Trojan.Eldorado variant outbound connection 1:262 11 Drop and generate

events

MALWARE-CNC Win.Trojan.Elise variant outbound connection 1:35050 Drop and generate

events

MALWARE-CNC Win.Trojan.Elise.B variant outbound connection 1:3535 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Ellell variant outbound connection 1:44316 Drop and generate

events

MALWARE-CNC Win.Trojan.Elpapok outbound connection 1:31753 Drop and generate

events

MALWARE-CNC Win.Trojan.Emdivi outbound connection 1:34818 Drop and generate

events

MALWARE-CNC Win.Trojan.Emdivi variant outbound request detected 1 :48199 Drop and generate

events

MALWARE-CNC Win.Trojan.Emotet variant download 1:47616 Drop and generate

events

MALWARE-CNC Win.Trojan.Emotet variant download 1:47617 Drop and generate

events

MALWARE-CNC Win.Trojan.Emotet variant outbound connection attempt 1:48402 Drop and generate

events

MALWARE-CNC Win.Trojan.Enchanim variant connection 1:27655 Drop and generate

events

MALWARE-CNC Win.Trojan.Endstar variant outbound connection 1:3402 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Endstar variant outbound connection 1:3402 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Engr variant outbound connection 1:37552 Drop and generate

events

MALWARE-CNC Win.Trojan.Eorezo variant outbound connection 1:43457 Drop and generate

events

MALWARE-CNC Win.Trojan.Epipenwa variant connection 1:27639 Drop and generate

events

MALWARE-CNC Win.Trojan.Epipenwa variant outbound connection 1:270 14 Drop and generate

events

MALWARE-CNC Win.Trojan.Epixed variant outbound connection 1:29076 Drop and generate

events

MALWARE-CNC Win.Trojan.Equation outbound connection 1:33543 Drop and generate

events

MALWARE-CNC Win.Trojan.Equation outbound connection 1:33545 Drop and generate

events

MALWARE-CNC Win.Trojan.Equation outbound connection 1:33546 Drop and generate

events

MALWARE-CNC Win.Trojan.Eupuds variant connection 1:27965 Drop and generate

events

MALWARE-CNC Win.Trojan.Exacrytion variant outbound connection 1:3 4044 Drop and generate

events

MALWARE-CNC Win.Trojan.Expiro outbound connection 1:31813 Drop and generate

events

MALWARE-CNC Win.Trojan.ExplorerHijack variant outbound connection 1:30257 Drop and generate

events

MALWARE-CNC Win.Trojan.ExplorerHijack variant outbound connection 1:29897 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 004 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 005 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 006 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 007 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 008 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 009 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 010 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 011 Drop and generate

events

MALWARE-CNC Win.Trojan.Explosive variant outbound connection 1:34 012 Drop and generate

events

MALWARE-CNC Win.Trojan.Expone variant outbound connection 1:31062 Drop and generate

events

MALWARE-CNC Win.Trojan.Extant variant outbound connection 1:32550 Drop and generate

events

MALWARE-CNC Win.Trojan.Ezbro variant outbound connection 1:31955 Drop and generate

events

MALWARE-CNC Win.Trojan.FakeAV TDSS/PurpleHaze variant outbound co nnection - base64 encoded 1:21318 Drop and generate MALWARE-CNC Win.Trojan.FakeAV variant outbound connection 1:27711 Drop and generate

events

events

MALWARE-CNC Win.Trojan.FakeAV variant outbound connection 1:36107 Drop and generate

events

MALWARE-CNC Win.Trojan.Fakeav variant outbound data connection 1: 28930 Drop and generate

events

MALWARE-CNC Win.Trojan.FakeAV variant traffic 1:19657 Drop and generate

events

MALWARE-CNC Win.Trojan.Fakeavlock variant outbound connection 1:2 5675 Drop and generate

events

MALWARE-CNC Win.Trojan.FallChill variant outbound connection 1:44 943 Drop and generate

events

MALWARE-CNC Win.Trojan.FallChill variant outbound connection 1:44 944 Drop and generate

events

MALWARE-CNC Win.Trojan.FallChill variant outbound connection 1:44 945 Drop and generate

events

MALWARE-CNC Win.Trojan.FallChill variant outbound connection 1:44 946 Drop and generate

events

MALWARE-CNC Win.Trojan.Fallchill variant outbound connection 1:47 708 Drop and generate

events

MALWARE-CNC Win.Trojan.Fanny outbound connection 1:34857 Drop and generate

events

MALWARE-CNC Win.Trojan.FannyWorm outbound connection 1:33678 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit outbound connection 1:40067 Drop and generate

events

MALWARE-CNC Win.Trojan.FareIt variant outbound connection 1:21418 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:46922 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:27775 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:43129 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:44569 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:44570 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:28607 Drop and generate

events

MALWARE-CNC Win.Trojan.Fareit variant outbound connection 1:43972 Drop and generate

events

MALWARE-CNC Win.Trojan.Farfli outbound connection 1:29924 Drop and generate

events

MALWARE-CNC Win.Trojan.Farfli outbound connection 1:34322 Drop and generate

events

MALWARE-CNC Win.Trojan.Farfli variant outbound connection 1:32310 Drop and generate

events

MALWARE-CNC Win.Trojan.FastPOS keylog exfiltration 1:39343 Drop and generate

events

MALWARE-CNC Win.Trojan.FastPOS status update 1:39344 Drop and generate

events

MALWARE-CNC Win.Trojan.FastPOS update request 1:39345 Drop and generate

events

MALWARE-CNC Win.Trojan.Felixroot variant download attempt 1:48277 Drop and generate

events

MALWARE-CNC Win.Trojan.Felixroot variant download attempt 1:48278 Drop and generate

events

MALWARE-CNC Win.Trojan.Fepgul variant outbound connection 1:22060 Drop and generate

events

MALWARE-CNC Win.Trojan.FighterPOS variant outbound connection 1:3 8235 Drop and generate

events

MALWARE-CNC Win.Trojan.FighterPOS variant outbound connection 1:3 4216 Drop and generate

events

MALWARE-CNC Win.Trojan.FileEncoder IP geolocation checkin attempt 1:33449 Drop and generate

events

MALWARE-CNC Win.Trojan.FileEncoder variant outbound connection 1: 33450 Drop and generate

events

MALWARE-CNC Win.Trojan.Finforst outbound connection 1:32893 Drop and generate

events

MALWARE-CNC Win.Trojan.Fireball variant outbound connection 1:434 67 Drop and generate

events

MALWARE-CNC Win.Trojan.Fireball variant outbound connection 1:434 68 Drop and generate

events

MALWARE-CNC Win.Trojan.Firefly outbound communcation 1:29075 Drop and generate

events

MALWARE-CNC Win.Trojan.Flactionbot outbound connection 1:34636 Drop and generate

events

MALWARE-CNC Win.Trojan.Flactionbot outbound connection 1:34637 Drop and generate

events

MALWARE-CNC Win.Trojan.Flusihoc variant outbound connection 1:370 68 Drop and generate

events

MALWARE-CNC Win.Trojan.FlyStudio known command and control channe l traffic 1:16823 Drop and generate

events

MALWARE-CNC Win.Trojan.Folyris outbound connection detected 1:399 58 Drop and generate

events

MALWARE-CNC Win.Trojan.FormBook variant outbound request detected 1:48287 Drop and generate

events

MALWARE-CNC Win.Trojan.FormBook variant outbound request detected 1:48288 Drop and generate

events

MALWARE-CNC Win.Trojan.Fosniw variant connection attempt 1:46049 Drop and generate

events

MALWARE-CNC Win.Trojan.Foxy variant outbound connection 1:33299 Drop and generate

events

MALWARE-CNC Win.Trojan.FraudPack variant outbound connection 1:16 809 Drop and generate

events

MALWARE-CNC Win.Trojan.Frethog variant inbound connection attempt 1:42453 Drop and generate

events

MALWARE-CNC Win.Trojan.Frethog variant outbound connection 1:4245 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Fulairo variant outbound connection 1:3432 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Gaertob variant outbound connection 1:2948 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Galfun variant outbound connection 1:27662 Drop and generate

events

MALWARE-CNC Win.Trojan.Galock variant connection 1:27939 Drop and generate

events

MALWARE-CNC Win.Trojan.Gamarue - Mozi1la User-Agent 1:27248 Drop and generate

events

MALWARE-CNC Win.Trojan.Gamarue outbound connection 1:23600 Drop and generate

events

MALWARE-CNC Win.Trojan.Gamarue variant outbound connection 1:3321 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Gamut configuration download 1:30087 Drop and generate

events

MALWARE-CNC Win.Trojan.Gapz variant connection 1:27659 Drop and generate

events

MALWARE-CNC Win.Trojan.Garsuni variant outbound connection 1:3111 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Gasonen variant outbound connection 1:4304 9 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger fake 404 response 1:38563 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger initial exfiltration attempt 1:38562 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger keylog exfiltration attempt 1:38564 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger outbound connection - keysto rkes 1:38559 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger outbound connection - screen shot 1:38560 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger outbound connection 1:38557 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger outbound connection 1:38558 Drop and generate

events

MALWARE-CNC Win.Trojan.GateKeylogger plugins download attempt 1:3 8561 Drop and generate

events

MALWARE-CNC Win.Trojan.Gbot.oce variant outbound connection 1:207 59 Drop and generate

events

MALWARE-CNC Win.Trojan.Gefetroe variant outbound connection 1:334 39 Drop and generate

events

MALWARE-CNC Win.Trojan.Gen variant outbound communication 1:46048 Drop and generate

events

MALWARE-CNC Win.Trojan.Gen variant outbound connection 1:44689 Drop and generate

events

MALWARE-CNC Win.Trojan.Gendwndrop variant outbound connection 1:4 0823 Drop and generate

events

MALWARE-CNC Win.Trojan.Generic-24 variant outbound connection 1:2 1428 Drop and generate

events

MALWARE-CNC Win.Trojan.Geodo variant outbound connection 1:32604 Drop and generate

events

MALWARE-CNC Win.Trojan.Gh0st variant outbound connection 1:37020 Drop and generate

events

MALWARE-CNC Win.Trojan.GhostPuppet malicious document download at tempt 1:48175 Drop and generate

events

MALWARE-CNC Win.Trojan.GhostPuppet malicious document download at tempt 1:48176 Drop and generate

events

MALWARE-CNC Win.Trojan.Gisetik information disclosure attempt 1:3 0979 Drop and generate

events

MALWARE-CNC Win.Trojan.Globeimposter outbound connection 1:43950 Drop and generate

events

MALWARE-CNC Win.Trojan.Glupteba payload download request 1:31606 Drop and generate

events

MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection 1:3 0288 Drop and generate

events

MALWARE-CNC Win.Trojan.Gnutler variant outbound connection 1:2487 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Godzilla outbound connection 1:44787 Drop and generate

events

MALWARE-CNC Win.Trojan.Gokawa variant outbound connection 1:36781 Drop and generate

events

MALWARE-CNC Win.Trojan.Goobraz variant outbound connection 1:2913 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Goolelo variant connection 1:27678 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47444 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47445 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47446 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47447 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47448 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47449 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47450 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47451 Drop and generate

events

MALWARE-CNC Win.Trojan.Gorgon outbound connection 1:47452 Drop and generate

events

MALWARE-CNC Win.Trojan.Gosik.A registration 1:19055 Drop and generate

events

MALWARE-CNC Win.Trojan.Gozi.Prinimalka variant outbound connectio n 1:24361 Drop and generate

events

MALWARE-CNC Win.Trojan.Gozi/Neverquest variant outbound connectio n 1:28814 Drop and generate

events

MALWARE-CNC Win.Trojan.Gozi/Neverquest variant outbound connectio n 1:28815 Drop and generate

events

MALWARE-CNC Win.Trojan.GozNym variant outbound connection 1:38638 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor outbound connection 1:37637 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor outbound connection 1:32987 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor outbound connection 1:32988 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor outbound connection 1:32989 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant HTTP Response 1:34997 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant inbound connection 1:29300 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:2925 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:2926 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:2949 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:3182 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:3219 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:2966 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:3168 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Graftor variant outbound connection 1:3023 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Grobios outbound connection 1:47525 Drop and generate

events

MALWARE-CNC Win.Trojan.Gupd variant outbound connection 1:26203 Drop and generate

events

MALWARE-CNC Win.Trojan.gzfw connection 1:28075 Drop and generate

events

MALWARE-CNC Win.Trojan.Hacktool variant outbound connection 1:250 93 Drop and generate

events

MALWARE-CNC Win.Trojan.hacktool variant outbound connection 1:164 96 Drop and generate

events

MALWARE-CNC Win.Trojan.Hadeki variant outbound connection 1:31303 Drop and generate

events

MALWARE-CNC Win.Trojan.Hades outbound connection 1:40467 Drop and generate

events

MALWARE-CNC Win.Trojan.Hadsruda outbound connection detected 1:40 059 Drop and generate

events

MALWARE-CNC Win.Trojan.Hadsruda outbound connection detected 1:40 060 Drop and generate

events

MALWARE-CNC Win.Trojan.Hancitor variant outbound connection 1:398 00 Drop and generate

events

MALWARE-CNC Win.Trojan.Hancitor variant outbound connection 1:323 32 Drop and generate

events

MALWARE-CNC Win.Trojan.Hangman.A outbound connection 1:36497 Drop and generate

events

MALWARE-CNC Win.Trojan.HAVEX-RAT variant outbound connection 1:31 255 Drop and generate

events

MALWARE-CNC Win.Trojan.hdog connectivity check-in version 2 1:282 85 Drop and generate

events

MALWARE-CNC Win.Trojan.Helauto variant connection 1:27905 Drop and generate

events

MALWARE-CNC Win.Trojan.Helminth variant outbound connection 1:391 76 Drop and generate

events

MALWARE-CNC WIN.Trojan.Hesechca variant outbound connection 1:322 72 Drop and generate

events

MALWARE-CNC Win.Trojan.Hesperbot variant outbound connection 1:31 051 Drop and generate

events

MALWARE-CNC Win.Trojan.Heur outbound connection 1:35426 Drop and generate

events

MALWARE-CNC Win.Trojan.Heur variant outbound connection 1:33153 Drop and generate

events

MALWARE-CNC Win.Trojan.Hippo variant outbound connection 1:44011 Drop and generate

events

MALWARE-CNC Win.Trojan.Hodoor APT variant outbound connection 1:3 6106 Drop and generate

events

MALWARE-CNC Win.Trojan.Hodoor APT variant 1:36105 Drop and generate

events

MALWARE-CNC Win.Trojan.Houdini backdoor file download request 1:4 1712 Drop and generate

events

MALWARE-CNC Win.Trojan.Httneilc variant outbound connection 1:313 59 Drop and generate

events

MALWARE-CNC Win.Trojan.Httpbot.qdc variant outbound connection 1: 19052 Drop and generate

events

MALWARE-CNC Win.Trojan.Hufysk variant outbound connection 1:24062 Drop and generate

events

MALWARE-CNC Win.Trojan.Hupigon Connection attempt 1:44042 Drop and generate

events

MALWARE-CNC Win.Trojan.Hupigon variant outbound connection 1:2022 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Huxerox variant outbound connection 1:2914 8 Drop and generate

events

MALWARE-CNC Win.Trojan.HW32 variant outbound connection 1:46129 Drop and generate

events

MALWARE-CNC Win.Trojan.Hydraq variant outbound connection 1:16368 Drop and generate

events

MALWARE-CNC Win.Trojan.Hydraq.variant outbound detected 1:32250 Drop and generate

events

MALWARE-CNC Win.Trojan.IcedId outbound connection 1:45050 Drop and generate

events

MALWARE-CNC Win.Trojan.ICLoader outbound connection 1:47264 Drop and generate

events

MALWARE-CNC Win.Trojan.ICLoader outbound connection 1:47265 Drop and generate

events

MALWARE-CNC Win.Trojan.ICLoader outbound connection 1:47051 Drop and generate

events

MALWARE-CNC Win.Trojan.Inexsmar variant outbound connection 1:354 00 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector external connection attempt 1:402 23 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector inbound connection 1:28803 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector Info Stealer Trojan variant outbo und connection 1:26984 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector outbound connection 1:28804 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector variant outbound connection 1:314 42 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector variant outbound connection 1:250 70 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector variant outbound connection 1:288 07 Drop and generate

events

MALWARE-CNC Win.Trojan.Injector variant outbound connection 1:202 21 Drop and generate

events

MALWARE-CNC Win.Trojan.Insidious outbound connection 1:33992 Drop and generate

events

MALWARE-CNC Win.Trojan.Insidious outbound connection 1:33993 Drop and generate

events

MALWARE-CNC Win.Trojan.Iplorko.A runtime detection 1:31007 Drop and generate

events

MALWARE-CNC Win.Trojan.Ismdoor variant outbound connection 1:4212 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Ismdoor variant outbound connection 1:4212 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Isniffer outbound connection 1:37225 Drop and generate

events

MALWARE-CNC Win.Trojan.Isniffer outbound connection 1:37226 Drop and generate

events

MALWARE-CNC Win.Trojan.Isniffer outbound connection 1:37227 Drop and generate

events

MALWARE-CNC Win.Trojan.Isniffer outbound connection 1:37228 Drop and generate

events

MALWARE-CNC Win.Trojan.iSpy variant outbound connection 1:40559 Drop and generate

events

MALWARE-CNC Win.Trojan.iSpy variant outbound connection 1:40242 Drop and generate

events

MALWARE-CNC Win.Trojan.iSpySoft variant exfiltration attempt 1:38 510 Drop and generate

events

MALWARE-CNC Win.Trojan.iSpySoft variant outbound connection 1:375 21 Drop and generate

events

MALWARE-CNC Win.Trojan.iSpySoft variant outbound connection 1:375 22 Drop and generate

events

MALWARE-CNC Win.Trojan.iSpySoft variant outbound connection 1:375 23 Drop and generate

events

MALWARE-CNC Win.Trojan.ITranslator variant outbound connection 1: 48115 Drop and generate

events

MALWARE-CNC Win.Trojan.ITranslator variant outbound connection 1: 48116 Drop and generate

events

MALWARE-CNC Win.Trojan.ITranslator variant outbound connection 1: 48117 Drop and generate

events

MALWARE-CNC Win.Trojan.ITranslator variant outbound connection 1: 48120 Drop and generate

events

MALWARE-CNC Win.Trojan.Jackpos outbound connection 1:29816 Drop and generate

events

MALWARE-CNC Win.Trojan.Jackpos outbound connection 1:29817 Drop and generate

events

MALWARE-CNC Win.Trojan.Jadowndec outbound connection 1:38643 Drop and generate

events

MALWARE-CNC Win.Trojan.Jadowndec outbound connection 1:38644 Drop and generate

events

MALWARE-CNC Win.Trojan.Jadowndec outbound connection 1:38645 Drop and generate

events

MALWARE-CNC Win.Trojan.Jadowndec outbound connection 1:38646 Drop and generate

events

MALWARE-CNC Win.Trojan.Jadowndec outbound connection 1:38647 Drop and generate

events

MALWARE-CNC Win.Trojan.Jadtre variant outbound connection 1:33883 Drop and generate

events

MALWARE-CNC Win.Trojan.Jaik variant outbound connection 1:30977 Drop and generate

events

MALWARE-CNC Win.Trojan.Janicab outbound connection 1:29149 Drop and generate

events

MALWARE-CNC Win.Trojan.Jemerr outbound connection 1:35318 Drop and generate

events

MALWARE-CNC Win.Trojan.Jemerr variant outbound connection 1:34877 Drop and generate

events

MALWARE-CNC Win.Trojan.Jinchodz variant outbound connection 1:202 29 Drop and generate

events

MALWARE-CNC Win.Trojan.Joanap variant outbound connection 1:46885 Drop and generate

events

MALWARE-CNC Win.Trojan.Jorik variant outbound connection 1:19711 Drop and generate

events

MALWARE-CNC Win.Trojan.Jorik variant outbound connection 1:24566 Drop and generate

events

MALWARE-CNC Win.Trojan.Jorik variant outbound connection 1:20756 Drop and generate

events

MALWARE-CNC Win.Trojan.Jorik.Kolilks variant outbound connection 1:25049 Drop and generate

events

MALWARE-CNC Win.Trojan.Kabob outbound connection 1:43063 Drop and generate

events

MALWARE-CNC Win.Trojan.Kahn variant outbound connection 1:21551 Drop and generate

events

MALWARE-CNC Win.Trojan.Kahn variant outbound connection 1:21552 Drop and generate

events

MALWARE-CNC Win.Trojan.Kanav variant outbound connection 1:31929 Drop and generate

events

MALWARE-CNC Win.Trojan.Kanav variant outbound connection 1:31930 Drop and generate

events

MALWARE-CNC Win.Trojan.KanKan variant connection 1:28242 Drop and generate

events

MALWARE-CNC Win.Trojan.Kapahyku variant outbound connection 1:404 65 Drop and generate

events

MALWARE-CNC Win.Trojan.Kapento variant outbound connection 1:3623 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Karnos variant outbound connection 1:30982 Drop and generate

events

MALWARE-CNC Win.Trojan.Karnos variant outbound connection 1:30983 Drop and generate

events

MALWARE-CNC Win.Trojan.Kasnam variant connection 1:28604 Drop and generate

events

MALWARE-CNC Win.Trojan.Kasnam variant connection 1:28605 Drop and generate

events

MALWARE-CNC Win.Trojan.Kayfcbk outbound connection 1:34610 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy download detected 1:32220 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy outbound connection 1:35462 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy variant outbound connection 1:20280 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy variant outbound connection 1:20281 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy variant outbound connection 1:21547 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy variant outbound connection 1:28405 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy variant outbound connection 1:37816 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy variant outbound connection 1:21239 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy/FakeAV Checkin with IE6 User-Agent 1: 26578 Drop and generate

events

MALWARE-CNC Win.Trojan.Kazy/FakeAV Checkin with IE6 User-Agent 1: 26579 Drop and generate

events

MALWARE-CNC Win.Trojan.Kbot variant outbound connection 1:22058 Drop and generate

events

MALWARE-CNC Win.Trojan.Kbot variant outbound connection 1:26719 Drop and generate

events

MALWARE-CNC Win.Trojan.Kbot variant outbound connection 1:26720 Drop and generate

events

MALWARE-CNC Win.Trojan.KediRAT outbound connection 1:44396 Drop and generate

events

MALWARE-CNC Win.Trojan.Kegotip variant report to cnc-server 1:236 33 Drop and generate

events

MALWARE-CNC Win.Trojan.Kelihos variant outbound connection 1:2156 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Kelihos variant outbound connection 1:2156 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Kelihos variant outbound connection 1:2156 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Keylogger inbound connection 1:29616 Drop and generate

events

MALWARE-CNC Win.Trojan.Keylogger outbound connection 1:29615 Drop and generate

events

MALWARE-CNC Win.Trojan.Keywsec variant outbound request for malic ious dll exe and js detected 1:47548 Drop and generate

events

MALWARE-CNC Win.Trojan.Keywsec variant post-compromise outbound r equest detected 1:47547 Drop and generate MALWARE-CNC Win.Trojan.Khalog variant outbound connection 1:28485 Drop and generate

events

events

MALWARE-CNC Win.Trojan.Kimsuky variant outbound connection 1:3100 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Kirts exfiltration attempt 1:38890 Drop and generate

events

MALWARE-CNC Win.Trojan.Kishlog variant outbound connection 1:2894 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Kishlog variant outbound connection 1:2894 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Kishop variant initial runtime outbound co nnection 1:29339 Drop and generate

events

MALWARE-CNC Win.Trojan.Kjdoom outbound connection 1:34598 Drop and generate

events

MALWARE-CNC Win.Trojan.Kjdoom outbound connection 1:34599 Drop and generate

events

MALWARE-CNC Win.Trojan.Kjdoom outbound connection 1:34600 Drop and generate

events

MALWARE-CNC Win.Trojan.Klovbot variant outbound connection 1:2463 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Kmnokay outbound connection 1:29289 Drop and generate

events

MALWARE-CNC Win.Trojan.Koceg.B variant outbound connection 1:1949 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Kolok variant connection 1:27720 Drop and generate

events

MALWARE-CNC Win.Trojan.Konus outbound connection 1:35031 Drop and generate

events

MALWARE-CNC Win.Trojan.Konus variant outbound connection detected 1:44391 Drop and generate

events

MALWARE-CNC Win.Trojan.Konus variant outbound connection detected 1:44392 Drop and generate

events

MALWARE-CNC Win.Trojan.Konus variant outbound connection detected 1:44393 Drop and generate

events

MALWARE-CNC Win.Trojan.Konus variant outbound connection detected 1:43190 Drop and generate

events

MALWARE-CNC Win.Trojan.Koobface variant outbound connection 1:315 44 Drop and generate

events

MALWARE-CNC Win.Trojan.Koobface variant outbound connection 1:315 45 Drop and generate

events

MALWARE-CNC Win.Trojan.Kopdel variant outbound connection 1:29495 Drop and generate

events

MALWARE-CNC Win.Trojan.KopiLuwak variant outbound request detecte d 1:44762 Drop and generate

events

MALWARE-CNC Win.Trojan.KopiLuwak variant outbound request detecte d 1:44763 Drop and generate

events

MALWARE-CNC Win.Trojan.Korgapam outbound connection 1:31706 Drop and generate

events

MALWARE-CNC Win.Trojan.Kovter outbound connection 1:37045 Drop and generate

events

MALWARE-CNC Win.Trojan.Kovter variant outbound connection 1:33453 Drop and generate

events

MALWARE-CNC Win.Trojan.Kovter variant outbound connection 1:38145 Drop and generate

events

MALWARE-CNC Win.Trojan.Kovter variant outbound connection 1:33228 Drop and generate

events

MALWARE-CNC Win.Trojan.Kradod connection attempt 1:43969 Drop and generate

events

MALWARE-CNC Win.Trojan.Kraens delivery attempt 1:46421 Drop and generate

events

MALWARE-CNC Win.Trojan.Kraens delivery attempt 1:46422 Drop and generate

events

MALWARE-CNC Win.Trojan.Kraens initial outbound request 1:46423 Drop and generate

events

MALWARE-CNC Win.Trojan.Kraken outbound connection 1:34292 Drop and generate

events

MALWARE-CNC Win.Trojan.Krap variant outbound connection 1:20755 Drop and generate

events

MALWARE-CNC Win.Trojan.Kriptovor variant outbound connection 1:34 476 Drop and generate

events

MALWARE-CNC Win.Trojan.Krodown variant connection attempt 1:46134 Drop and generate

events

MALWARE-CNC Win.Trojan.Krodown variant connection attempt 1:46135 Drop and generate

events

MALWARE-CNC Win.Trojan.Kronos variant outbound connection 1:31691 Drop and generate MALWARE-CNC Win.Trojan.Kryptic 7-byte URI Invalid Firefox Headers - no Accept-Language 1:27257 Drop and generate MALWARE-CNC Win.Trojan.Kryptic variant outbound connection 1:2565 2 Drop and generate

events

events

events

MALWARE-CNC Win.Trojan.Kryptik variant outbound connection 1:1682 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Kryptik variant outbound connection 1:3212 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Kryptik.Kazy variant outbound connection 1 :23987 Drop and generate

events

MALWARE-CNC Win.Trojan.Ksypypro outbound connection 1:32882 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuaibu inbound server configuration respon se 1:42301 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuaibu outbound connection 1:42302 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuaibu outbound file download attempt 1:42 303 Drop and generate

events

MALWARE-CNC Win.Trojan.KukuBot variant outbound connection 1:1973 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluos variant outbound connection 1:32976 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluos variant outbound connection 1:32977 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz Potential phishing URL 1:28255 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant download request 1:30773 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant inbound run command from cn c 1:26677 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant inbound run command from cn c 1:26678 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant inbound run command from cn c 1:26679 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant inbound run command from cn c 1:26680 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant inbound run command from cn c 1:26681 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant outbound connection 1:23244 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant outbound connection 1:26967 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant outbound connection 1:30073 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuluoz variant outbound connection 1:32706 Drop and generate

events

MALWARE-CNC Win.Trojan.Kuping variant outbound connection 1:47420 Drop and generate

events

MALWARE-CNC Win.Trojan.Lagulon.A outbound connection 1:33061 Drop and generate

events

MALWARE-CNC Win.Trojan.Larefervt variant outbound connection 1:32 034 Drop and generate

events

MALWARE-CNC Win.Trojan.Larosden variant outbound connection 1:320 33 Drop and generate

events

MALWARE-CNC Win.Trojan.Latentbot variant outbound connection 1:37 618 Drop and generate

events

MALWARE-CNC Win.Trojan.Ldmon variant outbound connection 1:29082 Drop and generate

events

MALWARE-CNC Win.Trojan.Lechiket variant outbound connection 1:295 61 Drop and generate

events

MALWARE-CNC Win.Trojan.Lecpetex variant outbound connection 1:320 48 Drop and generate

events

MALWARE-CNC Win.Trojan.Leralogs variant outbound connection 1:368 41 Drop and generate

events

MALWARE-CNC Win.Trojan.Levyatan variant outbound connection 1:313 44 Drop and generate

events

MALWARE-CNC Win.Trojan.Lientchtp variant outbound connection 1:39 785 Drop and generate

events

MALWARE-CNC Win.Trojan.Likseput variant connection 1:27636 Drop and generate

events

MALWARE-CNC Win.Trojan.Limlspy variant outbound connection 1:2902 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Linkup outbound connection 1:29666 Drop and generate

events

MALWARE-CNC Win.Trojan.Liteol variant connection 1:28094 Drop and generate

events

MALWARE-CNC Win.Trojan.Litmpuca.A variant outbound connection 1:2 1946 Drop and generate

events

MALWARE-CNC Win.Trojan.Lizarbot outbound connection 1:32126 Drop and generate

events

MALWARE-CNC Win.Trojan.Locati variant outbound connection 1:26072 Drop and generate

events

MALWARE-CNC Win.Trojan.LockPoS outbound connection attempt 1:4556 0 Drop and generate

events

MALWARE-CNC Win.Trojan.LockPoS outbound connection attempt 1:4556 1 Drop and generate

events

MALWARE-CNC Win.Trojan.LockPoS outbound connection attempt 1:4556 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky dropper variant outbound request det ected 1:44610 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky dropper variant outbound request det ected 1:44611 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky dropper variant outbound request det ected 1:44027 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky dropper variant outbound request det ected 1:44028 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky JS dropper outbound connection 1:388 87 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky outbound callout 1:44780 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky outbound callout 1:44781 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky outbound callout 1:44782 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky payload download - 987t67g 1:41476 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky payload download - result 1:41478 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:38888 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:40910 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:37834 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:37835 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:40816 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:40011 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:41334 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:41335 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:38331 Drop and generate

events

MALWARE-CNC Win.Trojan.Locky variant outbound connection 1:40527 Drop and generate

events

MALWARE-CNC Win.Trojan.LogPOS variant outbound connection 1:33854 Drop and generate

events

MALWARE-CNC Win.Trojan.Logreaz variant outbound connection 1:3487 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Loodir outbound connection 1:32854 Drop and generate

events

MALWARE-CNC Win.Trojan.Lorapu variant outbound connection 1:27551 Drop and generate

events

MALWARE-CNC Win.Trojan.Lorask variant outbound connection 1:29044 Drop and generate

events

MALWARE-CNC Win.Trojan.Lorask variant outbound connection 1:29045 Drop and generate

events

MALWARE-CNC Win.Trojan.Lorozoad variant outbound connection 1:393 69 Drop and generate

events

MALWARE-CNC Win.Trojan.Loxes variant outbound connection 1:29556 Drop and generate

events

MALWARE-CNC Win.Trojan.Lpdsuite GET request 1:35300 Drop and generate

events

MALWARE-CNC Win.Trojan.Lpdsuite POST request 1:35301 Drop and generate

events

MALWARE-CNC Win.Trojan.Lucuis variant outbound connection 1:24514 Drop and generate

events

MALWARE-CNC Win.Trojan.Lumbko variant initial outbound connection 1:29638 Drop and generate

events

MALWARE-CNC Win.Trojan.Lumbko variant outbound connection 1:29637 Drop and generate

events

MALWARE-CNC Win.Trojan.Luoxk malicious payload download attempt 1 :47327 Drop and generate

events

MALWARE-CNC Win.Trojan.Macnsed variant outbound connection 1:2507 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Madeba outbound connection detected 1:4001 6 Drop and generate

events

MALWARE-CNC Win.Trojan.MadMax implant outbound connection attempt 1:42883 Drop and generate

events

MALWARE-CNC Win.Trojan.MadMax implant outbound connection 1:42884 Drop and generate

events

MALWARE-CNC Win.Trojan.Madnedos outbound system information discl osure 1:29907 Drop and generate

events

MALWARE-CNC Win.Trojan.MadnessPro outbound connection 1:31053 Drop and generate

events

MALWARE-CNC Win.Trojan.Maener variant download request 1:32328 Drop and generate

events

MALWARE-CNC Win.Trojan.Maener variant outbound connection 1:32329 Drop and generate

events

MALWARE-CNC Win.Trojan.Maener variant outbound connection 1:32330 Drop and generate

events

MALWARE-CNC Win.Trojan.Maener variant outbound connection 1:32331 Drop and generate

events

MALWARE-CNC Win.Trojan.Maetdik variant initial outbound connectio n 1:29073 Drop and generate

events

MALWARE-CNC Win.Trojan.Maetdik variant outbound connection 1:2907 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Magania variant outbound connection 1:2401 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Malear variant outbound connection 1:41682 Drop and generate

events

MALWARE-CNC Win.Trojan.Malear variant outbound connection 1:41683 Drop and generate

events

MALWARE-CNC Win.Trojan.Malear variant outbound connection 1:41684 Drop and generate

events

MALWARE-CNC Win.Trojan.Malear variant outbound connection 1:41685 Drop and generate

events

MALWARE-CNC Win.Trojan.Malear variant outbound connection 1:41686 Drop and generate

events

MALWARE-CNC Win.Trojan.Malear variant outbound connection 1:41687 Drop and generate

events

MALWARE-CNC Win.Trojan.Malex variant outbound connection 1:40183 Drop and generate

events

MALWARE-CNC Win.Trojan.Malex variant outbound connection 1:26204 Drop and generate

events

MALWARE-CNC Win.Trojan.Mangit initial outbound connection 1:39653 Drop and generate

events

MALWARE-CNC Win.Trojan.Mantal variant outbound connection 1:34362 Drop and generate

events

MALWARE-CNC Win.Trojan.Maozhi variant outbound connection 1:31913 Drop and generate

events

MALWARE-CNC Win.Trojan.Mapoyun variant outbound connection attemp t 1:47427 Drop and generate

events

MALWARE-CNC Win.Trojan.Marap outbound beacon detected 1:47650 Drop and generate

events

MALWARE-CNC Win.Trojan.Marmoolak variant outbound connection 1:31 119 Drop and generate

events

MALWARE-CNC Win.Trojan.Marsjoke variant post infection beacon 1:4 0432 Drop and generate

events

MALWARE-CNC Win.Trojan.Marsjoke variant post infection beacon 1:4 0433 Drop and generate

events

MALWARE-CNC Win.Trojan.Marten variant outbound connection 1:29557 Drop and generate

events

MALWARE-CNC Win.Trojan.Mathanuc outbound connection 1:34581 Drop and generate

events

MALWARE-CNC Win.Trojan.Matsnu system information disclosure 1:299 16 Drop and generate

events

MALWARE-CNC Win.Trojan.Matsnu variant outbound conection 1:43183 Drop and generate

events

MALWARE-CNC Win.Trojan.Matsnu variant outbound conection 1:43184 Drop and generate

events

MALWARE-CNC Win.Trojan.Matsnu variant outbound connection 1:31316 Drop and generate

events

MALWARE-CNC Win.Trojan.Matsune variant outbound connection 1:3235 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Mazben file download 1:23467 Drop and generate

events

MALWARE-CNC Win.Trojan.Mcdravsm variant outbound connection 1:313 45 Drop and generate

events

MALWARE-CNC Win.Trojan.MCnovogic.A variant outbound connection 1: 19658 Drop and generate MALWARE-CNC Win.Trojan.Mecklow variant outbound connection system information disclosure 1:31343 Drop and generate

events

events

MALWARE-CNC Win.Trojan.Mecklow.C runtime traffic detected 1:20837 Generate events

MALWARE-CNC Win.Trojan.Medfos outbound connection 1:28143 Drop and generate

events

MALWARE-CNC Win.Trojan.Medfos variant outbound connection 1:27093 Drop and generate

events

MALWARE-CNC Win.Trojan.Medfos variant outbound connection 1:25660 Drop and generate

events

MALWARE-CNC Win.Trojan.Medialabs variant outbound connection 1:25 570 Drop and generate

events

MALWARE-CNC Win.Trojan.Medialabs variant outbound connection 1:25 571 Drop and generate

events

MALWARE-CNC Win.Trojan.Meilat variant connection 1:27641 Drop and generate

events

MALWARE-CNC Win.Trojan.Memlog SMB file transfer 1:32017 Drop and generate

events

MALWARE-CNC Win.Trojan.Mentor inbound connection - post infection 1:21435 Drop and generate

events

MALWARE-CNC Win.Trojan.Meowner runtime detection 1:33876 Drop and generate

events

MALWARE-CNC Win.Trojan.Meowner runtime detection 1:33877 Drop and generate

events

MALWARE-CNC Win.Trojan.Meowner runtime detection 1:33878 Drop and generate

events

MALWARE-CNC Win.Trojan.Meowner runtime detection 1:33879 Drop and generate

events

MALWARE-CNC Win.Trojan.Merong variant connection 1:27644 Drop and generate

events

MALWARE-CNC Win.Trojan.Mevade variant outbound connection 1:27955 Drop and generate

events

MALWARE-CNC Win.Trojan.Mevade variant outbound connection 1:28148 Drop and generate

events

MALWARE-CNC Win.Trojan.Micropsia outbound connection 1:43222 Drop and generate

events

MALWARE-CNC Win.Trojan.Micropsia outbound connection 1:43223 Drop and generate

events

MALWARE-CNC Win.Trojan.Micropsia outbound connection 1:43224 Drop and generate

events

MALWARE-CNC Win.Trojan.Midhos variant outbound connection 1:22100 Drop and generate

events

MALWARE-CNC Win.Trojan.Mikcer variant outbound connection 1:42386 Drop and generate

events

MALWARE-CNC Win.Trojan.Mikcer variant outbound connection 1:42233 Drop and generate

events

MALWARE-CNC Win.Trojan.Mindweq variant connection 1:27811 Drop and generate

events

MALWARE-CNC Win.Trojan.MiniFlame variant outbound connection 1:24 406 Generate events

MALWARE-CNC Win.Trojan.MiniFlame variant outbound connection 1:24 407 Generate events

MALWARE-CNC Win.Trojan.Mirage variant outbound connection 1:24437 Drop and generate

events

MALWARE-CNC Win.Trojan.Mirage variant outbound connection 1:24438 Drop and generate

events

MALWARE-CNC Win.Trojan.MirageFox variant outbound connection 1:48 092 Drop and generate

events

MALWARE-CNC Win.Trojan.MirageFox variant outbound connection 1:48 093 Drop and generate

events

MALWARE-CNC Win.Trojan.Miras variant outbound connection 1:31755 Drop and generate

events

MALWARE-CNC Win.Trojan.Miuref variant outbound connection 1:40771 Drop and generate

events

MALWARE-CNC Win.Trojan.Mivast outbound connection 1:35416 Drop and generate

events

MALWARE-CNC Win.Trojan.Mizzmo variant outbound connection 1:29301 Drop and generate

events

MALWARE-CNC Win.Trojan.MnuBot variant outbound SQL connection 1:4 6998 Drop and generate

events

MALWARE-CNC Win.Trojan.Moarider variant outbound connection 1:423 90 Drop and generate

events

MALWARE-CNC Win.Trojan.Moarider variant outbound connection 1:423 91 Drop and generate

events

MALWARE-CNC Win.Trojan.Mobef variant outbound connection attempt 1:46047 Drop and generate

events

MALWARE-CNC Win.Trojan.Modimer Trojanized MediaGet outbound conne ction 1:46099 Drop and generate

events

MALWARE-CNC Win.Trojan.ModPOS outbound connection 1:37036 Drop and generate

events

MALWARE-CNC Win.Trojan.Mojap variant outbound connection 1:29138 Drop and generate

events

MALWARE-CNC Win.Trojan.Mowfote variant initial outbound connectio n 1:29359 Drop and generate

events

MALWARE-CNC Win.Trojan.MrWhite out bound communication attempt 1: 41088 Drop and generate

events

MALWARE-CNC Win.Trojan.MSDownloader variant download 1:47935 Drop and generate

events

MALWARE-CNC Win.Trojan.MSDownloader variant download 1:47936 Drop and generate

events

MALWARE-CNC Win.Trojan.MSDownloader variant outbound connection 1 :47934 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL variant outbound connection 1:31315 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL-Pwsfcbk SQL connection 1:35385 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Honerep variant outbound connection 1 :31907 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Larosden variant outbound connection 1:32050 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Menteni variant outbound connection 1 :32016 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Misnt variant outbound connection 1:3 6526 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Misnt variant outbound connection 1:3 6325 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Misnt variant outbound connection 1:3 6326 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Misnt variant outbound connection 1:3 6327 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Misnt variant outbound connection 1:3 6328 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Misnt variant outbound connection 1:3 6329 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Seribe variant outbound connection 1: 31836 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Stimilik outbound variant connection 1:36577 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Stimilik outbound variant connection 1:36578 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Troloscup outbound variant connection 1:36566 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Troloscup outbound variant connection 1:36567 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Troloscup outbound variant connection 1:36568 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Troloscup outbound variant connection 1:36569 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Troloscup outbound variant connection 1:36570 Drop and generate

events

MALWARE-CNC Win.Trojan.MSIL.Troloscup outbound variant connection 1:36571 Drop and generate

events

MALWARE-CNC Win.Trojan.Msnmm variant outbound connection 1:34982 Drop and generate

events

MALWARE-CNC Win.Trojan.MsUpdater initial variant outbound connect ion 1:21241 Drop and generate

events

MALWARE-CNC Win.Trojan.MsUpdater variant outbound connection 1:21 240 Drop and generate

events

MALWARE-CNC Win.Trojan.MsUpdater variant outbound connection 1:21 242 Drop and generate

events

MALWARE-CNC Win.Trojan.Mudrop variant outbound connection 1:34286 Drop and generate

events

MALWARE-CNC Win.Trojan.Mumawow outbound connection 1:30251 Drop and generate

events

MALWARE-CNC Win.Trojan.Murofet variant outbound connection 1:2144 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Mutopy variant outbound connection 1:28373 Drop and generate

events

MALWARE-CNC Win.Trojan.Mylobot additional payload download 1:4724 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Mylobot additional payload download 1:4724 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Mylobot inbound connection 1:47243 Drop and generate

events

MALWARE-CNC Win.Trojan.N40 variant outbound connection 1:46821 Drop and generate

events

MALWARE-CNC Win.Trojan.Naberkalara variant outbound connection 1: 35732 Drop and generate

events

MALWARE-CNC Win.Trojan.Nalodew variant outbound connection 1:3448 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Name variant outbound connection 1:30239 Drop and generate

events

MALWARE-CNC Win.Trojan.Namihno variant outbound request 1:26695 Generate events

MALWARE-CNC Win.Trojan.Namospu variant outbound connection 1:3584 2 Drop and generate

events

MALWARE-CNC Win.Trojan.NanHaiShu variant outbound connection 1:39 861 Drop and generate

events

MALWARE-CNC Win.Trojan.Napolar phishing attack 1:29869 Drop and generate

events

MALWARE-CNC Win.Trojan.Napolar variant outbound connection 1:2807 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Nautilus outbound call 1:45221 Drop and generate

events

MALWARE-CNC Win.Trojan.Necurs variant outbound connection 1:30091 Drop and generate

events

MALWARE-CNC Win.Trojan.Necurs variant outbound connection 1:30519 Drop and generate

events

MALWARE-CNC Win.Trojan.Nelaja variant outbound connection 1:27647 Drop and generate

events

MALWARE-CNC Win.Trojan.Nemim outbound connection detected 1:40007 Drop and generate

events

MALWARE-CNC Win.Trojan.Nemim variant outbound connection 1:30074 Drop and generate

events

MALWARE-CNC Win.Trojan.Nemucod outbound connection 1:44677 Drop and generate

events

MALWARE-CNC Win.Trojan.Nessfi outbound connection 1:37101 Drop and generate

events

MALWARE-CNC Win.Trojan.Nessfi outbound connection 1:37102 Drop and generate

events

MALWARE-CNC Win.Trojan.NetEagle variant outbound connection 1:355 70 Drop and generate

events

MALWARE-CNC Win.Trojan.Nethief information disclosure attempt 1:3 1004 Drop and generate

events

MALWARE-CNC Win.Trojan.Nethief information disclosure attempt 1:3 1005 Drop and generate

events

MALWARE-CNC Win.Trojan.Nethief initial outbound connection 1:3100 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Neurevt variant outbound connection 1:2720 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Neuron variant inbound service request det ected 1:45062 Drop and generate

events

MALWARE-CNC Win.Trojan.Neuron variant inbound service request det ected 1:45063 Drop and generate

events

MALWARE-CNC Win.Trojan.Neuron variant inbound service request det ected 1:45064 Drop and generate

events

MALWARE-CNC Win.Trojan.Neuron variant inbound service request det ected 1:45065 Drop and generate

events

MALWARE-CNC Win.Trojan.NewPos outbound connection 1:34052 Drop and generate

events

MALWARE-CNC Win.Trojan.Nflog variant outbound connection 1:25667 Drop and generate

events

MALWARE-CNC Win.Trojan.Nflog variant outbound connection 1:25668 Drop and generate

events

MALWARE-CNC Win.Trojan.Nibagem outbound variant connection 1:3559 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Nibagem outbound variant connection 1:3559 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Nimisi variant outbound connection 1:36108 Drop and generate

events

MALWARE-CNC Win.Trojan.Nineblog variant outbound connection 1:292 99 Drop and generate

events

MALWARE-CNC Win.Trojan.Nivdort variant outbound connection 1:2678 4 Drop and generate

events

MALWARE-CNC Win.Trojan.njrat njRAT trojan outbound attempt 1:4782 2 Drop and generate

events

MALWARE-CNC Win.Trojan.njrat njRAT trojan variant download 1:4782 3 Drop and generate

events

MALWARE-CNC Win.Trojan.njrat njRAT trojan variant download 1:4782 4 Drop and generate

events

MALWARE-CNC Win.Trojan.njrat njRAT trojan variant download 1:4782 5 Drop and generate

events

MALWARE-CNC Win.Trojan.njrat njRAT trojan variant download 1:4782 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Nocpos information disclosure attempt 1:33 083 Drop and generate

events

MALWARE-CNC Win.Trojan.Nocpos initial outbound connection 1:33082 Drop and generate

events

MALWARE-CNC Win.Trojan.Noctabor variant outbound connection 1:303 04 Drop and generate

events

MALWARE-CNC Win.Trojan.Nocturnal outbound connection 1:46895 Drop and generate

events

MALWARE-CNC Win.Trojan.Nodslit variant outbound connection 1:3680 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Norekab variant outbound connection 1:2946 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Nurjax.A outbound connection 1:33152 Drop and generate

events

MALWARE-CNC Win.Trojan.Nursteal variant outbound connection 1:296 35 Drop and generate

events

MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection 1:1986 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Nymaim variant outbound connection 1:44788 Drop and generate

events

MALWARE-CNC Win.Trojan.Nymaim variant outbound connection 1:44789 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48083 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48084 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48085 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48086 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48087 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48088 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48089 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48090 Drop and generate

events

MALWARE-CNC Win.Trojan.Occamy variant outbound connection 1:48091 Drop and generate

MALWARE-CNC Win.Trojan.Octopus outbound connection attempt 1:4826 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Oddjob outbound connection 1:42395 Drop and generate

events

MALWARE-CNC Win.Trojan.Odlanor information exfiltration attempt 1 :34446 Drop and generate

events

MALWARE-CNC Win.Trojan.Ohlat variant connection 1:28097 Drop and generate

events

MALWARE-CNC Win.Trojan.OilRig variant outbound connection attempt 1:45946 Drop and generate

events

MALWARE-CNC Win.Trojan.OilRig variant outbound connection attempt 1:45947 Drop and generate

events

MALWARE-CNC Win.Trojan.OilRig variant outbound connection attempt 1:45948 Drop and generate

events

MALWARE-CNC Win.Trojan.OilRig variant outbound connection 1:47898 Drop and generate

events

MALWARE-CNC Win.Trojan.OilRig variant outbound connection 1:47899 Drop and generate

events

MALWARE-CNC Win.Trojan.OilRig variant outbound connection 1:47900 Drop and generate

events

MALWARE-CNC Win.Trojan.Oilrig variant outbound connection 1:41434 Drop and generate

events

MALWARE-CNC Win.Trojan.Oilrig variant outbound connection 1:41435 Drop and generate

events

MALWARE-CNC Win.Trojan.Oilrig variant outbound connection 1:41436 Drop and generate

events

MALWARE-CNC Win.Trojan.Oilrig variant outbound connection 1:41437 Drop and generate

events

MALWARE-CNC Win.Trojan.Oilrig variant outbound connection 1:41438 Drop and generate

events

MALWARE-CNC Win.Trojan.OlympicDestroyer variant outbound connecti on 1:48435 Drop and generate

events

MALWARE-CNC Win.Trojan.OlympicDestroyer variant outbound connecti on 1:48436 Drop and generate

events

MALWARE-CNC Win.Trojan.Omexo outbound connection 1:28072 Drop and generate

events

MALWARE-CNC Win.Trojan.OnlineGameHack variant outbound connection 1:27039 Drop and generate

events

MALWARE-CNC Win.Trojan.OnLineGames variant outbound connection 1: 33284 Drop and generate

events

MALWARE-CNC Win.Trojan.Orbot variant outbound connection 1:31317 Drop and generate

events

MALWARE-CNC Win.Trojan.Orcarat variant outbound connection 1:3239 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Orcarat variant outbound connection 1:3239 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Orcarat variant outbound connection 1:3239 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Orcarat variant outbound connection 1:3239 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Orcim variant outbound connection 1:26952 Drop and generate

MALWARE-CNC Win.Trojan.Oshidor variant outbound connection 1:2998 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Ostap out bound communication attempt 1:41 089 Drop and generate

events

MALWARE-CNC Win.Trojan.Otupsys variant outbound connection 1:3171 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Ovnavart variant outbound connection 1:300 36 Drop and generate

events

MALWARE-CNC Win.Trojan.Palebot variant outbound connection 1:3219 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Paligenpo outbound connection 1:37063 Drop and generate

events

MALWARE-CNC Win.Trojan.PandaZeus malicious certificate exchange 1 :44591 Drop and generate

events

MALWARE-CNC Win.Trojan.PandaZeus self-signed certificate exchange 1:44592 Drop and generate

events

MALWARE-CNC Win.Trojan.Papras variant outbound connection 1:31468 Drop and generate

events

MALWARE-CNC Win.Trojan.Paradise ransomware inbound executable 1:4 4366 Drop and generate

events

MALWARE-CNC Win.Trojan.Paradise ransomware outbound post 1:44365 Drop and generate

events

MALWARE-CNC Win.Trojan.Penget variant outbound connection 1:33933 Drop and generate

events

MALWARE-CNC Win.Trojan.Pfinet outbound connection 1:31832 Drop and generate

events

MALWARE-CNC Win.Trojan.Pherbot variant outbound connection 1:1972 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Philadelphia variant initial outbound conn ection 1:40289 Drop and generate

events

MALWARE-CNC Win.Trojan.Philadelphia variant status update outboun d connection 1:40290 Drop and generate

events

MALWARE-CNC Win.Trojan.Phoenot variant inbound connection 1:27013 Drop and generate

events

MALWARE-CNC Win.Trojan.Phoenot variant outbound connection 1:2701 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Phrovon outbound connection 1:28244 Drop and generate

events

MALWARE-CNC Win.Trojan.Picommex outbound connection 1:34001 Drop and generate

events

MALWARE-CNC Win.Trojan.Picommex outbound connection 1:34002 Drop and generate

events

MALWARE-CNC Win.Trojan.Picommex outbound connection 1:34003 Drop and generate

events

MALWARE-CNC Win.Trojan.Pincav variant outbound connection 1:23628 Drop and generate

events

MALWARE-CNC Win.Trojan.PipCreat RAT beacon 1:26942 Drop and generate

events

MALWARE-CNC Win.Trojan.PipCreat RAT dropper download 1:26941 Drop and generate

events

MALWARE-CNC Win.Trojan.Pirminay variant outbout connection 1:2986 2 Drop and generate

MALWARE-CNC Win.Trojan.PLEAD downloader outbound connection 1:475 56 Drop and generate

events

MALWARE-CNC Win.Trojan.PLEAD downloader outbound connection 1:475 57 Drop and generate

events

MALWARE-CNC Win.Trojan.Plugx outbound connection 1:28561 Drop and generate

events

MALWARE-CNC WIN.Trojan.Plugx variant outbound connection 1:32179 Drop and generate

events

MALWARE-CNC Win.Trojan.Plusau outbound connection 1:29340 Drop and generate

events

MALWARE-CNC Win.Trojan.Pmabot outbound connection 1:37212 Drop and generate

events

MALWARE-CNC Win.Trojan.Pmabot outbound connection 1:37213 Drop and generate

events

MALWARE-CNC Win.Trojan.Pmabot outbound connection 1:37214 Drop and generate

events

MALWARE-CNC Win.Trojan.Pmabot outbound connection 1:37215 Drop and generate

events

MALWARE-CNC Win.Trojan.Pmkype variant outbound connection 1:29899 Drop and generate

events

MALWARE-CNC Win.Trojan.Pony HTTP response connection 1:29870 Drop and generate

events

MALWARE-CNC Win.Trojan.Poogetad Variant connection attempt 1:4392 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Poolfiend variant outbound connection 1:32 852 Drop and generate

events

MALWARE-CNC Win.Trojan.Poolfiend variant outbound connection 1:32 853 Drop and generate

events

MALWARE-CNC Win.Trojan.Popureb variant outbound connection detect ed 1:44443 Drop and generate

events

MALWARE-CNC Win.Trojan.Popyerd variant outbound connection 1:2930 6 Drop and generate

events

MALWARE-CNC Win.Trojan.POSCardStealer variant outbound connection 1:29484 Drop and generate

events

MALWARE-CNC Win.Trojan.Poseidon outbound connection 1:33851 Drop and generate

events

MALWARE-CNC Win.Trojan.Poseidon outbound connection 1:33852 Drop and generate

events

MALWARE-CNC Win.Trojan.Poshtroper variant outbound connection 1:1 9722 Drop and generate

events

MALWARE-CNC Win.Trojan.Post\_Show RAT beacon 1:26943 Drop and generate

events

MALWARE-CNC Win.Trojan.Post\_Show RAT beacon 1:26944 Drop and generate

events

MALWARE-CNC Win.Trojan.Potao outbound connection 1:35733 Drop and generate

events

MALWARE-CNC Win.Trojan.Potao.A variant outbound connection 1:1957 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Poweliks outbound connection 1:33165 Drop and generate

events

MALWARE-CNC Win.Trojan.PowerMacro DNS query response 1:41788 Drop and generate

MALWARE-CNC Win.Trojan.Poxters external connection 1:40288 Drop and generate

events

MALWARE-CNC Win.Trojan.Printlove variant outbound connection 1:25 545 Drop and generate

events

MALWARE-CNC Win.Trojan.PRISM variant outbound connection 1:27802 Drop and generate

events

MALWARE-CNC Win.Trojan.PRISM variant outbound connection 1:27803 Drop and generate

events

MALWARE-CNC Win.Trojan.ProjectHook configuration file download at tempt 1:30332 Drop and generate

events

MALWARE-CNC Win.Trojan.ProjectHook information disclosure attempt 1:30333 Drop and generate

events

MALWARE-CNC Win.Trojan.ProjectHook initial outbound connection 1: 30334 Drop and generate

events

MALWARE-CNC Win.Trojan.Projecthook variant outbound connection 1: 30299 Drop and generate

events

MALWARE-CNC Win.Trojan.Projecthook variant outbound connection 1: 30300 Drop and generate

events

MALWARE-CNC Win.Trojan.Prok variant outbound connection 1:34950 Drop and generate

events

MALWARE-CNC Win.Trojan.Prorat variant outbound connection 1:22054 Drop and generate

events

MALWARE-CNC Win.Trojan.Proteus outbound connection 1:41033 Drop and generate

events

MALWARE-CNC Win.Trojan.Proxy Win.Trojan.Dosenjo.C variant outboun d connection 1:19429 Drop and generate

events

MALWARE-CNC Win.Trojan.ProxyChange 1:35303 Drop and generate

events

MALWARE-CNC Win.Trojan.Proxydown variant connection 1:29313 Drop and generate

events

MALWARE-CNC Win.Trojan.Proxyier variant outbound connection 1:229 37 Drop and generate

events

MALWARE-CNC Win.Trojan.Punkey outbound connection 1:34161 Drop and generate

events

MALWARE-CNC Win.Trojan.Punkey variant outbound connection 1:34608 Drop and generate

events

MALWARE-CNC Win.Trojan.Puver variant outbound connection 1:32096 Drop and generate

events

MALWARE-CNC Win.Trojan.Pvzin variant outbound connection 1:34459 Drop and generate

events

MALWARE-CNC Win.Trojan.Pwexes variant outbound connection 1:33996 Drop and generate

events

MALWARE-CNC Win.Trojan.Pwexes variant outbound connection 1:33997 Drop and generate

events

MALWARE-CNC Win.Trojan.PyLocky outbound connection attempt 1:4802 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Pyrtomsop outbound connection 1:31124 Drop and generate

events

MALWARE-CNC Win.Trojan.Pyteconte variant outbound connection 1:29 893 Drop and generate

events

MALWARE-CNC Win.Trojan.Qadars variant outbound connection 1:28528 Drop and generate

MALWARE-CNC Win.Trojan.Qakbot connection to cnc server 1:28990 Drop and generate

events

MALWARE-CNC Win.Trojan.Qakbot outbound POST attempt 1:39063 Drop and generate

events

MALWARE-CNC Win.Trojan.Qakbot variant network speed test 1:38606 Drop and generate

events

MALWARE-CNC Win.Trojan.Qarallax initial outbound connection 1:397 74 Drop and generate

events

MALWARE-CNC Win.Trojan.Qarallax outbound connection 1:46747 Drop and generate

events

MALWARE-CNC Win.Trojan.Qarallax outbound connection 1:46748 Drop and generate

events

MALWARE-CNC Win.Trojan.Qbot variant outbound connection 1:39411 Drop and generate

events

MALWARE-CNC Win.Trojan.Qiwmonk outbound connection detected 1:402 04 Drop and generate

events

MALWARE-CNC Win.Trojan.QQFish variant outbound connection 1:19056 Drop and generate

events

MALWARE-CNC Win.Trojan.QQPass variant outbound connection 1:42348 Drop and generate

events

MALWARE-CNC Win.Trojan.Quarian variant outbound connection - prox y connection 1:24858 Drop and generate

events

MALWARE-CNC Win.Trojan.Quimonk variant outbound connection detect ed 1:44639 Drop and generate

events

MALWARE-CNC Win.Trojan.Qulkonwi outbound connection 1:31748 Drop and generate

events

MALWARE-CNC Win.Trojan.Qytags variant outbound connection 1:36186 Drop and generate

events

MALWARE-CNC Win.Trojan.Radamant inbound connection 1:37317 Drop and generate

events

MALWARE-CNC Win.Trojan.Ragua variant outbound connection 1:31712 Drop and generate

events

MALWARE-CNC Win.Trojan.Ragua variant outbound connection 1:31713 Drop and generate

events

MALWARE-CNC Win.Trojan.Ragua variant outbound connection 1:31714 Drop and generate

events

MALWARE-CNC Win.Trojan.Ramnit variant outbound connection 1:44972 Drop and generate

events

MALWARE-CNC Win.Trojan.Ramnit variant outbound connection 1:44973 Drop and generate

events

MALWARE-CNC Win.Trojan.Ramnit variant outbound connection 1:48079 Drop and generate

events

MALWARE-CNC Win.Trojan.Ramnit variant outbound connection 1:48080 Drop and generate

events

MALWARE-CNC Win.Trojan.Ramnit variant outbound connection 1:48081 Drop and generate

events

MALWARE-CNC Win.Trojan.Ramnit variant outbound detected 1:33600 Drop and generate

events

MALWARE-CNC Win.Trojan.Randrew variant outbound connection 1:4030 9 Drop and generate

events

MALWARE-CNC Win.Trojan.Ransom variant outbound connection 1:38733 Drop and generate

MALWARE-CNC Win.Trojan.Rarog outbound communication attempt 1:462 38 Drop and generate

events

MALWARE-CNC Win.Trojan.Rarog outbound communication attempt 1:462 39 Drop and generate

events

MALWARE-CNC Win.Trojan.Rarog user-agent outbound communication at tempt 1:46240 Drop and generate

events

MALWARE-CNC Win.Trojan.Ratankba variant outbound connection 1:417 80 Drop and generate

events

MALWARE-CNC Win.Trojan.Rbrute inbound connection 1:30883 Drop and generate

events

MALWARE-CNC Win.Trojan.Reabfrus variant connection 1:27660 Drop and generate

events

MALWARE-CNC Win.Trojan.Reabfrus variant connection 1:27661 Drop and generate

events

MALWARE-CNC Win.Trojan.Recub variant outbound connection 1:30284 Drop and generate

events

MALWARE-CNC Win.Trojan.Redcontrole variant outbound connection 1: 36770 Drop and generate

events

MALWARE-CNC Win.Trojan.Redosdru variant outbound connection 1:405 48 Drop and generate

events

MALWARE-CNC Win.Trojan.Redyms variant outbound connection 1:27596 Drop and generate

events

MALWARE-CNC Win.Trojan.Regiskazi outbound connection 1:35083 Drop and generate

events

MALWARE-CNC Win.Trojan.Rehacker outbound connection 1:30753 Drop and generate

events

MALWARE-CNC Win.Trojan.Rehtesyk outbound connection 1:32311 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant inbound payload download 1: 47300 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant outbound connection 1:47299 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant outbound connection 1:47301 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant outbound connection 1:47302 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant outbound connection 1:47303 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant outbound connection 1:47304 Drop and generate

events

MALWARE-CNC Win.Trojan.Remcos variant outbound connection 1:47305 Drop and generate

events

MALWARE-CNC Win.Trojan.Renegin outbound GET attempt 1:38724 Drop and generate

events

MALWARE-CNC Win.Trojan.Renos variant outbound connection 1:39448 Drop and generate

events

MALWARE-CNC Win.Trojan.Reswor variant outbound connection 1:25996 Drop and generate

events

MALWARE-CNC Win.Trojan.Retadup variant outbound connection 1:4479 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Retgate variant outbound connection 1:3183 7 Drop and generate

MALWARE-CNC Win.Trojan.Revenge RAT inbound heartbeat check 1:4596 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Revenge RAT initial outbound connection 1: 45961 Drop and generate

events

MALWARE-CNC Win.Trojan.Reventon variant outbound connection 1:256 27 Drop and generate

events

MALWARE-CNC Win.Trojan.Reyptson ransomware download 1:44760 Drop and generate

events

MALWARE-CNC Win.Trojan.Rhubot variant outbound connection 1:29422 Drop and generate

events

MALWARE-CNC Win.Trojan.Rimod variant outbound connection 1:25663 Drop and generate

events

MALWARE-CNC Win.Trojan.RockLoader variant outbound connection 1:3 8608 Drop and generate

events

MALWARE-CNC Win.Trojan.Rocra variant outbound connection 1:26608 Drop and generate

events

MALWARE-CNC Win.Trojan.Rofin variant outbound connection 1:31328 Drop and generate

events

MALWARE-CNC Win.Trojan.Rofin variant outbound connection 1:39056 Drop and generate

events

MALWARE-CNC Win.Trojan.Rokrat file upload attempt 1:45510 Drop and generate

events

MALWARE-CNC Win.Trojan.Rokrat variant outbound connection detecte d 1:45607 Drop and generate

events

MALWARE-CNC Win.Trojan.Rombrast Trojan outbound connection 1:2691 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Rombrast Trojan outbound connection 1:2691 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Rombrast variant outbound connection 1:252 58 Drop and generate

events

MALWARE-CNC Win.Trojan.Ropest variant outbound connection 1:32338 Drop and generate

events

MALWARE-CNC Win.Trojan.Rortiem outbound connection 1:43985 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix file upload attempt 1:46253 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix malicious download request 1:27567 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix malicious download 1:28940 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix outbound connection attempt 1:46249 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix outbound connection attempt 1:46250 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix outbound connection attempt 1:46251 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix outbound connection attempt 1:46252 Drop and generate

events

MALWARE-CNC Win.Trojan.Rovnix variant outbound connection 1:34868 Drop and generate

events

MALWARE-CNC Win.Trojan.Roxfora variant outbound connection 1:2886 1 Drop and generate

MALWARE-CNC Win.Trojan.Ruinmail outbound connection 1:36800 Drop and generate

events

MALWARE-CNC Win.Trojan.Ruskill variant outbound connection 1:2537 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Rusrushel variant outbound connection 1:36 267 Drop and generate

events

MALWARE-CNC Win.Trojan.Rusrushel variant outbound connection 1:36 268 Drop and generate

events

MALWARE-CNC Win.Trojan.Rusrushel variant outbound connection 1:36 269 Drop and generate

events

MALWARE-CNC Win.Trojan.Saaglup variant outbound connection 1:3209 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Saibipoc outbound connection 1:34865 Drop and generate

events

MALWARE-CNC Win.Trojan.Saibipoc outbound connection 1:34866 Drop and generate

events

MALWARE-CNC Win.Trojan.Sakurel outbound connection 1:35415 Drop and generate

events

MALWARE-CNC Win.Trojan.Sakurel variant outbound connection 1:3732 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Sality variant outbound connection 1:41034 Drop and generate

events

MALWARE-CNC Win.Trojan.Sality variant outbound connection 1:40605 Drop and generate

events

MALWARE-CNC Win.Trojan.Sality variant outbound connection 1:40606 Drop and generate

events

MALWARE-CNC Win.Trojan.Sality variant outbound connection 1:19964 Drop and generate

events

MALWARE-CNC Win.Trojan.Sality variant outbound connection 1:37516 Drop and generate

events

MALWARE-CNC Win.Trojan.Sality variant outbound connection 1:40334 Drop and generate

events

MALWARE-CNC Win.Trojan.Sanny malware variant FTP login 1:46271 Drop and generate

events

MALWARE-CNC Win.Trojan.Sanny malware variant FTP login 1:46272 Drop and generate

events

MALWARE-CNC Win.Trojan.Sapart variant outbound connection 1:31174 Drop and generate

events

MALWARE-CNC Win.Trojan.Sapertilz variant outbound connection 1:32 287 Drop and generate

events

MALWARE-CNC Win.Trojan.Satana ransomware outbound connection 1:40 541 Drop and generate

events

MALWARE-CNC Win.Trojan.Sathurbot outbound connection 1:36670 Drop and generate

events

MALWARE-CNC Win.Trojan.Saturn initial download 1:45754 Drop and generate

events

MALWARE-CNC Win.Trojan.Saturn initial download 1:45755 Drop and generate

events

MALWARE-CNC Win.Trojan.Savnut.B variant outbound connection 1:195 90 Drop and generate

events

MALWARE-CNC Win.Trojan.Scar variant outbound connection 1:35047 Drop and generate

MALWARE-CNC Win.Trojan.Scar variant outbound connection 1:28886 Drop and generate

events

MALWARE-CNC Win.Trojan.Scar variant outbound connection 1:26325 Drop and generate

events

MALWARE-CNC Win.Trojan.Scarpnex variant outbound connection 1:311 71 Drop and generate

events

MALWARE-CNC Win.Trojan.Scarpnex variant outbound connection 1:311 72 Drop and generate

events

MALWARE-CNC Win.Trojan.Scarpnex variant outbound connection 1:311 73 Drop and generate

events

MALWARE-CNC Win.Trojan.Scarsi variant outbound connection 1:34108 Drop and generate

events

MALWARE-CNC Win.Trojan.Scudy outbound connection 1:41331 Drop and generate

events

MALWARE-CNC Win.Trojan.SDBot variant outbound connection 1:31458 Drop and generate

events

MALWARE-CNC Win.Trojan.Sdconsent outbound connection 1:29644 Drop and generate

events

MALWARE-CNC Win.trojan.Seaduke outbound connection 1:35254 Drop and generate

events

MALWARE-CNC Win.Trojan.Secdeskinf outbound connection 1:32506 Drop and generate

events

MALWARE-CNC Win.Trojan.Sefnit outbound connection 1:30923 Drop and generate

events

MALWARE-CNC Win.Trojan.Sefnit variant outbound connection 1:36732 Drop and generate

events

MALWARE-CNC Win.Trojan.Selasloot variant outbound connection 1:25 669 Drop and generate

events

MALWARE-CNC Win.Trojan.Sesramot variant outbound connection 1:372 96 Drop and generate

events

MALWARE-CNC Win.Trojan.Sesramot variant outbound connection 1:372 97 Drop and generate

events

MALWARE-CNC Win.Trojan.Seveto variant outbound connection 1:24214 Drop and generate

events

MALWARE-CNC Win.Trojan.Seyelifon variant outbound connection 1:35 804 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44797 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44798 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44799 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44800 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44801 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44802 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44803 Drop and generate

events

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44804 Drop and generate

MALWARE-CNC Win.Trojan.Shadowpad DNS TXT encrypted outbound conne ction 1:44807 Drop and generate

events

MALWARE-CNC Win.Trojan.ShadyRAT variant outbound connection 1:302 16 Drop and generate

events

MALWARE-CNC Win.Trojan.Shakti variant outbound connection 1:40027 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant connectivity check 1:39852 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant connectivity check 1:39853 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant connectivity check 1:39854 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant connectivity check 1:39855 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant executable download 1:39856 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant executable download 1:39857 Drop and generate

events

MALWARE-CNC Win.Trojan.Sharik variant outbound connection 1:30214 Drop and generate

events

MALWARE-CNC Win.Trojan.Shiz variant initial outbound connection 1 :29038 Drop and generate

events

MALWARE-CNC Win.Trojan.Shiz variant outbound connection 1:29039 Drop and generate

events

MALWARE-CNC Win.Trojan.Shiz variant outbound connection 1:26657 Drop and generate

events

MALWARE-CNC Win.Trojan.Sidopa variant outbound connection 1:28562 Drop and generate

events

MALWARE-CNC Win.Trojan.Sigly variant outbound connection 1:25541 Drop and generate

events

MALWARE-CNC Win.Trojan.Silence cnc module download 1:44770 Drop and generate

events

MALWARE-CNC Win.Trojan.Silence inbound download 1:44769 Drop and generate

events

MALWARE-CNC Win.Trojan.Silence monitoring module download 1:44771 Drop and generate

events

MALWARE-CNC Win.Trojan.Silence outbound request 1:44768 Drop and generate

events

MALWARE-CNC Win.Trojan.Silverstar outbound connection 1:45960 Drop and generate

events

MALWARE-CNC Win.Trojan.Simda variant outbound connection 1:34296 Drop and generate

events

MALWARE-CNC Win.Trojan.Simda variant outbound connection 1:34297 Drop and generate

events

MALWARE-CNC Win.Trojan.Sinowal javascript delivery method 1:21631 Drop and generate

events

MALWARE-CNC Win.Trojan.Sinowal variant connection 1:27864 Drop and generate

events

MALWARE-CNC Win.Trojan.Sinpid variant outbound connection 1:32023 Drop and generate

events

MALWARE-CNC Win.Trojan.Sinrin initial JS dropper outbound connect ion 1:39064 Drop and generate

MALWARE-CNC Win.Trojan.SixMuch variant outbound connection 1:2910 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Skintrim variant outbound connection 1:252 57 Drop and generate

events

MALWARE-CNC Win.Trojan.Sloft variant outbound connection 1:31142 Drop and generate

events

MALWARE-CNC Win.Trojan.Sloth variant command and control traffic 1:30276 Drop and generate

events

MALWARE-CNC Win.Trojan.Sloth variant command and control traffic 1:30277 Drop and generate

events

MALWARE-CNC Win.Trojan.Sloth variant command and control traffic 1:30278 Drop and generate

events

MALWARE-CNC Win.Trojan.Sloth variant command and control traffic 1:30279 Drop and generate

events

MALWARE-CNC Win.Trojan.Sluegot variant connection 1:28565 Drop and generate

events

MALWARE-CNC Win.Trojan.Small variant outbound connection 1:32075 Drop and generate

events

MALWARE-CNC Win.Trojan.Smokeloader outbound response 1:47073 Drop and generate

events

MALWARE-CNC Win.Trojan.Smominru outbound call 1:45826 Drop and generate

events

MALWARE-CNC Win.Trojan.Smominru outbound call 1:45827 Drop and generate

events

MALWARE-CNC Win.Trojan.SniperSpy variant outbound connection 1:29 464 Drop and generate

events

MALWARE-CNC Win.Trojan.Soaphrish variant outbound connection 1:32 202 Drop and generate

events

MALWARE-CNC Win.Trojan.SocketPlayer outbound connection 1:47005 Drop and generate

events

MALWARE-CNC Win.Trojan.SocketPlayer outbound connection 1:47006 Drop and generate

events

MALWARE-CNC Win.Trojan.Sodebral HTTP Response attempt 1:32607 Drop and generate

events

MALWARE-CNC Win.Trojan.Sodebral HTTP Response attempt 1:32608 Drop and generate

events

MALWARE-CNC Win.Trojan.Sodebral variant outbound connection 1:326 06 Drop and generate

events

MALWARE-CNC Win.Trojan.Sofacy outbound connection 1:37024 Drop and generate

events

MALWARE-CNC Win.Trojan.SoftPulse variant outbound connection 1:31 717 Drop and generate

events

MALWARE-CNC Win.Trojan.Sojax variant outbound connection 1:34887 Drop and generate

events

MALWARE-CNC Win.Trojan.Sojax variant outbound connection 1:34888 Drop and generate

events

MALWARE-CNC Win.Trojan.Solimba download attempt 1:29417 Drop and generate

events

MALWARE-CNC Win.Trojan.Somoca vaniant outbound connection 1:32036 Drop and generate

events

MALWARE-CNC Win.Trojan.Soraya variant initial outbound connection 1:31228 Drop and generate

MALWARE-CNC Win.Trojan.Sovfo variant outbound connection 1:37457 Drop and generate

events

MALWARE-CNC Win.Trojan.Spesseo variant outbound connection 1:4299 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Spesseo variant outbound connection 1:4299 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Spy variant outbound connection 1:24217 Drop and generate

events

MALWARE-CNC Win.Trojan.Spy.Agent variant outbound connection 1:26 840 Drop and generate

events

MALWARE-CNC Win.Trojan.Spy.Agent variant outbound connection 1:26 841 Drop and generate

events

MALWARE-CNC Win.Trojan.SpyBanker variant outbound connection 1:34 959 Drop and generate

events

MALWARE-CNC Win.Trojan.SpyBanker variant outbound connection 1:33 444 Drop and generate

events

MALWARE-CNC Win.Trojan.SpyBanker.ZSL variant outbound connection 1:27648 Drop and generate

events

MALWARE-CNC Win.Trojan.SpyEye variant outbound connection 1:23382 Drop and generate

events

MALWARE-CNC Win.Trojan.SpyEye variant outbound connection 1:19164 Drop and generate

events

MALWARE-CNC Win.Trojan.Spyeye variant outbound connectivity check 1:21306 Drop and generate

events

MALWARE-CNC Win.Trojan.Spyeye-206 variant outbound connection 1:2 0763 Drop and generate

events

MALWARE-CNC Win.Trojan.Spyeye-207 variant outbound connection 1:2 0927 Drop and generate

events

MALWARE-CNC Win.Trojan.SpySmall variant outbound connection 1:309 14 Drop and generate

events

MALWARE-CNC Win.Trojan.SpySmall variant outbound connection 1:309 15 Drop and generate

events

MALWARE-CNC Win.Trojan.SquirtDanger get module list outbound requ est 1:46475 Drop and generate

events

MALWARE-CNC Win.Trojan.SquirtDanger inbound delivery attempt 1:46 476 Drop and generate

events

MALWARE-CNC Win.Trojan.SquirtDanger inbound delivery attempt 1:46 477 Drop and generate

events

MALWARE-CNC Win.Trojan.SquirtDanger inbound delivery attempt 1:46 478 Drop and generate

events

MALWARE-CNC Win.Trojan.SquirtDanger inbound delivery attempt 1:46 479 Drop and generate

events

MALWARE-CNC Win.Trojan.Stantinko variant outbound connection 1:32 334 Drop and generate

events

MALWARE-CNC Win.Trojan.Startpage variant outbound connection 1:21 436 Drop and generate

events

MALWARE-CNC Win.Trojan.Steckt IRCbot executable download 1:28983 Drop and generate

events

MALWARE-CNC Win.Trojan.Stimilina variant outbound connection dete cted 1:44753 Drop and generate

events

MALWARE-CNC Win.Trojan.Stitur variant outbound connection 1:29291 Drop and generate

MALWARE-CNC Win.Trojan.Strictor variant outbound connection 1:292 20 Drop and generate

events

MALWARE-CNC Win.Trojan.Stupeval variant outbound connection 1:367 65 Drop and generate

events

MALWARE-CNC Win.Trojan.Subla variant outbound connection 1:31418 Drop and generate

events

MALWARE-CNC Win.Trojan.Svekifc outbound persistent connection 1:2 9976 Drop and generate

events

MALWARE-CNC Win.Trojan.Svekifc system information disclosure 1:29 975 Drop and generate

events

MALWARE-CNC Win.Trojan.Swaylib outbound variant connection 1:349 36 Drop and generate

events

MALWARE-CNC Win.Trojan.Sweeper variant dropper download attempt 1 :38566 Drop and generate

events

MALWARE-CNC Win.Trojan.Sweeper variant dropper initial download attempt 1:38565 Drop and generate

events

MALWARE-CNC Win.Trojan.Swisyn variant outbound connection 1:25670 Drop and generate

events

MALWARE-CNC Win.Trojan.Swisyn variant outbound connection 1:23335 Drop and generate

events

MALWARE-CNC Win.Trojan.Swisyn variant outbound connection 1:20213 Drop and generate

events

MALWARE-CNC Win.Trojan.Swisyn variant outbound connection 1:21760 Drop and generate

events

MALWARE-CNC Win.Trojan.Swisyn variant outbound connection 1:21761 Drop and generate

events

MALWARE-CNC Win.Trojan.Sydigu variant outbound connection 1:29559 Drop and generate

events

MALWARE-CNC Win.Trojan.Syhcmd variant connection 1:27637 Drop and generate

events

MALWARE-CNC Win.Trojan.Sylonif variant outbound connection 1:3003 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant dropper download connection 1:37646 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant HTTP response attempt 1:3192 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:37647 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:33443 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:30262 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:25511 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:32583 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:33457 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:31452 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:30198 Drop and generate

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:31530 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:32584 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:30953 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:30954 Drop and generate

events

MALWARE-CNC Win.Trojan.Symmi variant outbound connection 1:30955 Drop and generate

events

MALWARE-CNC Win.Trojan.Syndicasec variant outbound connection 1:4 7025 Drop and generate

events

MALWARE-CNC Win.Trojan.Syscan outbound connection 1:40761 Drop and generate

events

MALWARE-CNC Win.Trojan.Sysmain outbound connection 1:34957 Drop and generate

events

MALWARE-CNC Win.Trojan.Taidoor variant outbound connection 1:2020 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Tanmar outbound connection 1:36627 Drop and generate

events

MALWARE-CNC Win.Trojan.Tapaoux variant connection 1:28947 Drop and generate

events

MALWARE-CNC Win.Trojan.Tarayt outbound connection 1:44211 Drop and generate

events

MALWARE-CNC Win.Trojan.Tarayt outbound connection 1:44212 Drop and generate

events

MALWARE-CNC Win.Trojan.Targnik variant outbound connection 1:3077 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Tartober variant connection 1:27699 Drop and generate

events

MALWARE-CNC Win.Trojan.Tavex outbound connection 1:36639 Drop and generate

events

MALWARE-CNC Win.Trojan.Tdrop2 variant dropper download attempt 1: 37053 Drop and generate

events

MALWARE-CNC Win.Trojan.TDSS variant outbound connection 1:30203 Drop and generate

events

MALWARE-CNC Win.Trojan.TDSS variant outbound connection 1:30204 Drop and generate

events

MALWARE-CNC Win.Trojan.tdss.1.gen install-time detection - findzp roportal1.com 1:16269 Drop and generate

events

MALWARE-CNC Win.Trojan.tdss.1.gen install-time detection - yourne wsblog.net 1:16268 Drop and generate

events

MALWARE-CNC Win.Trojan.Teabevil variant outbound connection 1:366 29 Drop and generate

events

MALWARE-CNC Win.Trojan.Teabevil variant outbound connection 1:366 30 Drop and generate

events

MALWARE-CNC Win.Trojan.Tearspear variant outbound connection 1:29 140 Drop and generate

events

MALWARE-CNC Win.Trojan.TechSupportScam installed binary outbound connection 1:47067 Drop and generate

events

MALWARE-CNC Win.Trojan.TechSupportScam installed binary outbound connection 1:47068 Drop and generate

MALWARE-CNC Win.Trojan.Telebot variant outbound connection 1:4830 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Telebot variant outbound connection 1:4830 1 Drop and generate

events

MALWARE-CNC Win.Trojan.Telebot variant outbound connection 1:4830 2 Drop and generate

events

MALWARE-CNC Win.Trojan.Telehot outbound connection 1:37064 Drop and generate

events

MALWARE-CNC Win.Trojan.Tempedreve Samba probe 1:33932 Drop and generate

events

MALWARE-CNC Win.Trojan.Tenad variant outbound connection 1:29179 Drop and generate

events

MALWARE-CNC Win.Trojan.Tenavt connection 1:27817 Drop and generate

events

MALWARE-CNC Win.Trojan.Tendrit variant outbound connection 1:3445 8 Drop and generate

events

MALWARE-CNC Win.Trojan.Tenexmed inbound shell command attempt 1:3 0986 Drop and generate

events

MALWARE-CNC Win.Trojan.Tenexmed outbound connection 1:30985 Drop and generate

events

MALWARE-CNC Win.Trojan.Tentobr outbound connection 1:36666 Drop and generate

events

MALWARE-CNC Win.Trojan.Tepoyx outbound connection detection 1:338 73 Drop and generate

events

MALWARE-CNC Win.Trojan.Teqimp outbound connection 1:34601 Drop and generate

events

MALWARE-CNC Win.Trojan.Terminator RAT variant outbound connection 1:28482 Drop and generate

events

MALWARE-CNC Win.Trojan.Tesch variant outbound connection 1:28419 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt outbound connection 1:33893 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt outbound connection 1:34280 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt outbound connection 1:35794 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt outbound connection 1:37052 Drop and generate

events

MALWARE-CNC Win.Trojan.Teslacrypt outbound POST attempt 1:37717 Drop and generate

events

MALWARE-CNC Win.Trojan.Teslacrypt outbound POST attempt 1:37718 Drop and generate

events

MALWARE-CNC Win.Trojan.Teslacrypt outbound POST attempt 1:37719 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt server reply 1:38017 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt variant outbound connection 1:3 8150 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt variant outbound connection 1:3 9040 Drop and generate

events

MALWARE-CNC Win.Trojan.TeslaCrypt variant outbound connection 1:3 8949 Drop and generate

MALWARE-CNC Win.Trojan.Tinba outbound connection 1:33650 Drop and generate

events

MALWARE-CNC Win.Trojan.Tinba variant outbound connection 1:32270 Drop and generate

events

MALWARE-CNC Win.Trojan.Tinba variant outbound connection 1:39685 Drop and generate

events

MALWARE-CNC Win.Trojan.Tiny variant outbound connection 1:29981 Drop and generate

events

MALWARE-CNC Win.Trojan.TinyZBot outbound SOAP connection attempt 1:32957 Drop and generate

events

MALWARE-CNC Win.Trojan.TinyZBot response connection attempt 1:329 58 Drop and generate

events

MALWARE-CNC Win.Trojan.Tirabot variant outbound connection 1:3168 0 Drop and generate

events

MALWARE-CNC Win.Trojan.Tobinload variant outbound connection 1:31 066 Drop and generate

events

MALWARE-CNC Win.Trojan.Tofsee variant outbound connection 1:28864 Drop and generate

events

MALWARE-CNC Win.Trojan.Toga variant outbound connection 1:39887 Drop and generate

events

MALWARE-CNC Win.Trojan.Tohwen variant outbound connection 1:29883 Drop and generate

events

MALWARE-CNC Win.Trojan.Tooka GET attempt 1:38680 Drop and generate

events

MALWARE-CNC Win.Trojan.Toopu dll embedded in png download attempt 1:32986 Drop and generate

events

MALWARE-CNC Win.Trojan.Toopu outbound connection 1:32990 Drop and generate

events

MALWARE-CNC Win.Trojan.TorLocker variant outbound connection 1:32 892 Drop and generate

events

MALWARE-CNC Win.Trojan.Torpplar variant outbound connection 1:476 78 Drop and generate

events

MALWARE-CNC Win.Trojan.TorrentLocker variant outbound connection 1:32464 Drop and generate

events

MALWARE-CNC Win.Trojan.TorrentLocker/Teerac payment page request 1:35394 Drop and generate

events

MALWARE-CNC Win.Trojan.Totbrick variant inbound connection attemp t 1:44314 Drop and generate

events

MALWARE-CNC Win.Trojan.Totbrick variant outbound connection 1:443 13 Drop and generate

events

MALWARE-CNC Win.Trojan.Toumlec variant outbound connection 1:3130 6 Drop and generate

events

MALWARE-CNC Win.Trojan.Toumlec variant outbound connection 1:3130 7 Drop and generate

events

MALWARE-CNC Win.Trojan.Toupi variant outbound connection 1:31895 Drop and generate

events

MALWARE-CNC Win.Trojan.Tracur variant outbound connection 1:19801 Drop and generate

events

MALWARE-CNC Win.Trojan.Trans variant outbound connection 1:39738 Drop and generate

events

MALWARE-CNC Win.Trojan.Travnet Botnet data upload 1:26656 Drop and generate

MALWARE-CNC Win.Trojan.Treizt variant connection 1:27759 Drop and generate

events

MALWARE-CNC Win.Trojan.Trfijan outbound connection 1:36893 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44403 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44404 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44405 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44406 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44407 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44408 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44409 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44410 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44411 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44412 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44413 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44414 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot malicious communication attempt 1 :44415 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange 1:44399 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange 1:44400 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange 1:44401 Drop and generate

events

MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange 1:44402 Drop and generate

events

MALWARE-CNC Win.Trojan.Trioptid outbound connection 1:33989 Drop and generate

events

MALWARE-CNC Win.Trojan.Trioptid outbound connection 1:33990 Drop and generate

events

MALWARE-CNC Win.Trojan.TripleNine RAT beacon 1:26940 Drop and generate

events

MALWARE-CNC Win.Trojan.Turla outbound connection 1:48028 Drop and generate

events

MALWARE-CNC Win.Trojan.Turla outbound connection 1:33547 Drop and generate

events

MALWARE-CNC Win.Trojan.Twerket variant outbound connection 1:3297 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Tyaui variant outbound connection 1:29117 Drop and generate

MALWARE-CNC Win.Trojan.TYPEFRAME malware download attempt 1:47086 Drop and generate

events

MALWARE-CNC Win.Trojan.TYPEFRAME malware download attempt 1:47087 Drop and generate

events

MALWARE-CNC Win.Trojan.TYPEFRAME malware download attempt 1:47088 Drop and generate

events

MALWARE-CNC Win.Trojan.TYPEFRAME malware download attempt 1:47089 Drop and generate

events

MALWARE-CNC Win.Trojan.TYPEFRAME malware download attempt 1:47090 Drop and generate

events

MALWARE-CNC Win.Trojan.UDPOS outbound command and control IP addr ess check 1:45963 Drop and generate

events

MALWARE-CNC Win.Trojan.UDPOS outbound data exfiltration 1:45967 Drop and generate

events

MALWARE-CNC Win.Trojan.UDPOS outbound data exfiltration 1:45968 Drop and generate

events

MALWARE-CNC Win.Trojan.UDPOS outbound heartbeat 1:45966 Drop and generate

events

MALWARE-CNC Win.Trojan.UDPOS outbound system information disclous re 1:45964 Drop and generate

events

MALWARE-CNC Win.Trojan.Ufraie variant outbound connection 1:28813 Drop and generate

events

MALWARE-CNC Win.Trojan.UFRStealer variant outbound connection 1:2 6691 Drop and generate

events

MALWARE-CNC Win.Trojan.Unlock92 outbound connection 1:39465 Drop and generate

events

MALWARE-CNC Win.Trojan.Unruy outbound callout 1:46612 Drop and generate

events

MALWARE-CNC Win.Trojan.UP007 variant outbound connection 1:38603 Drop and generate

events

MALWARE-CNC Win.Trojan.Upatre variant outbound connection 1:33594 Drop and generate

events

MALWARE-CNC Win.Trojan.Upatre variant outbound connection 1:33211 Drop and generate

events

MALWARE-CNC Win.Trojan.Upatre variant outbound connection 1:33282 Drop and generate

events

MALWARE-CNC Win.Trojan.Upero variant outbound connection 1:26703 Drop and generate

events

MALWARE-CNC Win.Trojan.Uptime RAT beacon 1:26946 Drop and generate

events

MALWARE-CNC Win.Trojan.Urausy Botnet variant outbound connection 1:25807 Drop and generate

events

MALWARE-CNC Win.Trojan.Uroburos inbound command 1:30192 Drop and generate

events

MALWARE-CNC Win.Trojan.Uroburos inbound encrypted data 1:30193 Drop and generate

events

MALWARE-CNC Win.Trojan.Uroburos usermode-centric client request 1 :30191 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif malicious file download 1:47147 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif malicious file download 1:47148 Drop and generate

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45566 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45567 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45331 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45333 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45334 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45335 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45336 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45337 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45338 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45339 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45340 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45341 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45342 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45343 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45344 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt 1:45345 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection 1:44616 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection 1:44617 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection 1:44618 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection 1:39686 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection 1:42894 Drop and generate

events

MALWARE-CNC Win.Trojan.Ursnif variant outbound connection 1:42895 Drop and generate

events

MALWARE-CNC Win.Trojan.Utishaf variant outbound connection 1:3124 2 Drop and generate

events

MALWARE-CNC Win.Trojan.VaccinePC variant outbound connection 1:24 632 Drop and generate

events

MALWARE-CNC Win.Trojan.Valden variant outbound connection 1:29125 Drop and generate

events

MALWARE-CNC Win.Trojan.Vawtrak variant outbound connection 1:3746 7 Drop and generate

MALWARE-CNC Win.Trojan.VBKrypt variant connection 1:28045 Drop and generate

events

MALWARE-CNC Win.Trojan.VBPasswordStealer variant outbound connect ion 1:34047 Drop and generate

events

MALWARE-CNC Win.Trojan.Vbula variant initial CNC contact 1:26793 Drop and generate

events

MALWARE-CNC Win.Trojan.Vbula variant outbound connection 1:26792 Drop and generate

events

MALWARE-CNC Win.Trojan.Vbvoleur.a variant outbound connection 1:2 3394 Drop and generate

events

MALWARE-CNC Win.Trojan.Vcaredrix variant outbound connection 1:35 005 Drop and generate

events

MALWARE-CNC Win.Trojan.Vectecoin coin mining program download att empt 1:31273 Drop and generate

events

MALWARE-CNC Win.Trojan.Vectecoin information disclosure attempt 1 :31271 Drop and generate

events

MALWARE-CNC Win.Trojan.Vectecoin outbound command request attempt 1:31272 Drop and generate

events

MALWARE-CNC Win.Trojan.Vega variant outbound connection detected 1:46838 Drop and generate

events

MALWARE-CNC Win.Trojan.Veli variant outbound connection 1:24563 Drop and generate

events

MALWARE-CNC Win.Trojan.Velso ransomware download 1:45551 Drop and generate

events

MALWARE-CNC Win.Trojan.Velso ransomware download 1:45552 Drop and generate

events

MALWARE-CNC Win.Trojan.Verbscut variant outbound connection 1:293 04 Drop and generate

events

MALWARE-CNC Win.Trojan.Vermin outbound connection attempt 1:45651 Drop and generate

events

MALWARE-CNC Win.Trojan.Vextstl outbound connection 1:31290 Drop and generate

events

MALWARE-CNC Win.Trojan.VEye2 remote access tool download 1:45208 Drop and generate

events

MALWARE-CNC Win.Trojan.Vibrio file download - 4g3vg334 1:41477 Drop and generate

events

MALWARE-CNC Win.Trojan.Vibro outbound connection detected 1:39882 Drop and generate

events

MALWARE-CNC Win.Trojan.Virut variant outbound connection 1:25572 Drop and generate

events

MALWARE-CNC Win.Trojan.Virut-3 variant outbound connection 1:2075 4 Drop and generate

events

MALWARE-CNC Win.Trojan.Vivia variant outbound connection 1:29324 Drop and generate

events

MALWARE-CNC Win.Trojan.Vondola configuration file download attemp t 1:30987 Drop and generate

events

MALWARE-CNC Win.Trojan.Vondola information disclosure attempt 1:3 0988 Drop and generate

events

MALWARE-CNC Win.Trojan.Vonterra outbound connection 1:37047 Drop and generate

events

MALWARE-CNC Win.Trojan.vSkimmer outbound connection 1:29416 Drop and generate

MALWARE-CNC Win.Trojan.Vundo variant outbound connection 1:24493 Drop and generate

events

MALWARE-CNC Win.Trojan.Vundo variant outbound connection 1:24494 Drop and generate

events

MALWARE-CNC Win.Trojan.Vundo variant outbound connection 1:24495 Drop and generate

events

MALWARE-CNC Win.Trojan.Vundo variant outbound connection 1:24496 Drop and generate

events

MALWARE-CNC Win.Trojan.Vundo variant outbound connection 1:24497 Drop and generate

events

MALWARE-CNC Win.Trojan.Waldek variant initial outbound connection detected 1:47600 Drop and generate

events

MALWARE-CNC Win.Trojan.Wallex variant outbound connection 1:38613 Drop and generate

events

MALWARE-CNC Win.Trojan.Waski variant outbound connection 1:31722 Drop and generate

events

MALWARE-CNC Win.Trojan.Waterspout outbound connection 1:31883 Drop and generate

events

MALWARE-CNC Win.Trojan.Wcvalep variant outbound connection 1:2907 1 Drop and generate

events

MALWARE-CNC Win.Trojan.WEC variant outbound connection 1:29882 Drop and generate

events

MALWARE-CNC Win.Trojan.Wecod variant outbound connection 1:26024 Drop and generate

events

MALWARE-CNC Win.Trojan.Wedots outbound variant connection 1:36622 Drop and generate

events

MALWARE-CNC Win.Trojan.Wedots outbound variant connection 1:36623 Drop and generate

events

MALWARE-CNC Win.Trojan.Wedots outbound variant connection 1:36624 Drop and generate

events

MALWARE-CNC Win.Trojan.Werdlod variant outbound connection 1:3483 3 Drop and generate

events

MALWARE-CNC Win.Trojan.Wheelsof variant outbound connection 1:348 62 Drop and generate

events

MALWARE-CNC Win.Trojan.Wheelsof variant outbound connection 1:348 63 Drop and generate

events

MALWARE-CNC Win.Trojan.Win32 Facebook Secure Cryptor C2 1:26965 Drop and generate

events

MALWARE-CNC Win.Trojan.Win32.Kimsuky variant file stealing 1:2807 3 Drop and generate

events

MALWARE-CNC Win.Trojan.WinPlock variant outbound connection 1:363 04 Drop and generate

events

MALWARE-CNC Win.Trojan.Winpud encoded payload download attempt 1: 42098 Drop and generate

events

MALWARE-CNC Win.Trojan.WIntruder outbound connection 1:34128 Drop and generate

events

MALWARE-CNC Win.Trojan.WOWCheckC Attempted CNC 1:32769 Drop and generate

events

MALWARE-CNC Win.Trojan.Wraut variant outbound connection 1:44659 Drop and generate

events

MALWARE-CNC Win.Trojan.Wuwo initial infection variant outbound co nnection 1:24235 Drop and generate

MALWARE-CNC Win.Trojan.XBlocker outbound connection 1:24381 Drop and generate

events

MALWARE-CNC Win.Trojan.XBlocker outbound connection 1:24382 Drop and generate

events

MALWARE-CNC Win.Trojan.Xerq outbound connection 1:33892 Drop and generate

events

MALWARE-CNC Win.Trojan.Xobtide outbound connection 1:34867 Drop and generate

events

MALWARE-CNC Win.Trojan.XTalker outbound connection 1:34869 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm second stage configuration download attempt 1:45574 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm variant initial outbound connection d etected 1:44774 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm variant initial outbound connection d etected 1:44775 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm variant initial outbound connection d etected 1:44776 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm variant initial outbound connection d etected 1:44777 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm variant initial outbound connection d etected 1:44778 Drop and generate

events

MALWARE-CNC Win.Trojan.xxmm variant initial outbound connection d etected 1:44779 Drop and generate

events

MALWARE-CNC Win.Trojan.Yakes variant certificate 1:36198 Drop and generate

events

MALWARE-CNC Win.Trojan.Yakes variant dropper 1:36202 Drop and generate

events

MALWARE-CNC Win.Trojan.Yakes variant outbound connection 1:36199 Drop and generate

events

MALWARE-CNC Win.Trojan.Yakes variant outbound connection 1:27054 Drop and generate

events

MALWARE-CNC Win.Trojan.Yesudac variant outbound connection 1:3183 5 Drop and generate

events

MALWARE-CNC Win.Trojan.Yoban RAT outbound connection 1:46984 Drop and generate

events

MALWARE-CNC Win.Trojan.Yoban RAT outbound connection 1:46985 Drop and generate

events

MALWARE-CNC Win.Trojan.Yohakest variant file upload outbound conn ection 1:29153 Drop and generate

events

MALWARE-CNC Win.Trojan.Yohakest variant followup outbound connect ion 1:29154 Drop and generate

events

MALWARE-CNC Win.Trojan.Yohakest variant initial runtime outbound connection 1:29152 Drop and generate

events

MALWARE-CNC Win.Trojan.yty file exfiltration outbound request 1:4 6070 Drop and generate

events

MALWARE-CNC Win.Trojan.yty module download request 1:46068 Drop and generate

events

MALWARE-CNC Win.Trojan.yty module request 1:46069 Drop and generate

events

MALWARE-CNC Win.Trojan.yty plugin downloader initial outbound con nection 1:46067 Drop and generate

MALWARE-CNC Win.Trojan.Zbot configuration file download 1:30270 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot drop zone file upload 1:30271 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot fake PNG config file download without User-Agent 1:26480 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot outbound connection 1:30063 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot outbound connection 1:30064 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot payment .scr download 1:27010 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection 1: 26023 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:32123 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:29566 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:24169 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:31084 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:27007 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:27008 Drop and generate

events

MALWARE-CNC Win.Trojan.Zbot variant outbound connection 1:23972 Drop and generate

events

MALWARE-CNC Win.Trojan.Zboter.E variant outbound connection 1:197 02 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeagle outbound connection 1:29353 Drop and generate

events

MALWARE-CNC Win.Trojan.Zebrocy outbound connection 1:48431 Drop and generate

events

MALWARE-CNC Win.Trojan.Zebrocy outbound connection 1:48432 Drop and generate

events

MALWARE-CNC Win.Trojan.Zebrocy outbound connection 1:48395 Drop and generate

events

MALWARE-CNC Win.Trojan.Zebrocy outbound connection 1:48396 Drop and generate

events

MALWARE-CNC Win.Trojan.Zebrocy outbound data connection 1:25949 Drop and generate

events

MALWARE-CNC Win.Trojan.Zebrocy TLS server hello attempt 1:48397 Drop and generate

events

MALWARE-CNC Win.Trojan.Zediv outbound connection 1:31319 Drop and generate

events

MALWARE-CNC Win.Trojan.Zegost variant outbound connection 1:47567 Drop and generate

events

MALWARE-CNC Win.Trojan.Zemot configuration download attempt 1:320 72 Drop and generate

events

MALWARE-CNC Win.Trojan.Zemot outbound connection 1:32073 Drop and generate

MALWARE-CNC Win.Trojan.ZeroAccess URI and Referer 1:25224 Drop and generate

events

MALWARE-CNC Win.Trojan.ZeroAccess variant outbound connection 1:2 7680 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeroaccess variant outbound connection 1:2 4224 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeroaccess variant outbound connection 1:2 6930 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeroaccess variant outbound connection 1:2 6931 Drop and generate

events

MALWARE-CNC Win.Trojan.Zerolocker variant outbound connection 1:3 2197 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus config file download 1:38994 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus dropper variant connection 1:27970 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration 1:27 919 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus outbound connection 1:37838 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus outbound connection 1:28800 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant download attempt 1:40611 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant inbound connection 1:39705 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:30258 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:29127 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:35030 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:30548 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:27918 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:38995 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:31218 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:32585 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:32586 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:29884 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:35746 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:26923 Drop and generate

events

MALWARE-CNC Win.Trojan.Zeus variant outbound connection 1:35549 Drop and generate

events

MALWARE-CNC Win.Trojan.ZeusVM embedded image config file download 1:30211 Drop and generate

events

MALWARE-CNC Win.Trojan.Zimwervi variant outbound connection 1:367 77 Drop and generate

events

MALWARE-CNC Win.Trojan.Zinnemls variant outbound connection 1:345 72 Drop and generate

events

MALWARE-CNC Win.Trojan.Zoxpng variant outbound connection 1:32285 Drop and generate

events

MALWARE-CNC Win.Trojan.Zurgop variant outbound beaconing connecti on 1:44171 Drop and generate

events

MALWARE-CNC Win.Trojan.Zusy inbound CNC response 1:33520 Drop and generate

events

MALWARE-CNC Win.Trojan.Zusy variant outbound connection 1:29349 Drop and generate

events

MALWARE-CNC Win.Trojan.Zusy variant outbound connection 1:33521 Drop and generate

events

MALWARE-CNC Win.Trojan.Zusy variant outbound connection 1:31295 Drop and generate

events

MALWARE-CNC Win.Work.Rokiwobi inbound command from C&C 1:24185 Drop and generate

events

MALWARE-CNC Win.Worm.Brontok user-agent outbound connection 1:200 21 Drop and generate

events

MALWARE-CNC Win.Worm.Brontok user-agent outbound connection 1:466 42 Drop and generate

events

MALWARE-CNC Win.Worm.Dusta.br outbound connnection 1:19703 Drop and generate

events

MALWARE-CNC Win.Worm.Enosch variant outbound connection 1:33482 Drop and generate

events

MALWARE-CNC Win.Worm.Gamarue variant outbound connection 1:25256 Drop and generate

events

MALWARE-CNC Win.Worm.Goldrv variant outbound connection 1:33931 Drop and generate

events

MALWARE-CNC Win.Worm.IRCbot outbound connection 1:28209 Drop and generate

events

MALWARE-CNC Win.Worm.Jenxcus variant outbound connection 1:32605 Drop and generate

events

MALWARE-CNC Win.Worm.Klogwjds variant outbound connection 1:34319 Drop and generate

events

MALWARE-CNC Win.Worm.Luder variant outbound connection 1:26774 Drop and generate

events

MALWARE-CNC Win.Worm.Mafusc variant outbound connection 1:33966 Drop and generate

events

MALWARE-CNC Win.Worm.Mozibe variant outbound connection 1:34460 Drop and generate

events

MALWARE-CNC Win.Worm.Phelshap variant outbound connection 1:30917 Drop and generate

events

MALWARE-CNC Win.Worm.Redhip variant outbound connection 1:48147 Drop and generate

events

MALWARE-CNC Win.Worm.Redhip variant outbound connection 1:48148 Drop and generate

events

MALWARE-CNC Win.Worm.Redhip variant outbound connection 1:48149 Drop and generate

events

MALWARE-CNC Win.Worm.Redhip variant outbound connection 1:48150 Drop and generate

events

MALWARE-CNC Win.Worm.Sohanad.ila variant outbound connection 1:19 357 Drop and generate

events

MALWARE-CNC Win.Worm.Tuscas variant outbound connection 1:34029 Drop and generate

events

MALWARE-CNC Win.Worm.VBNA variant outbound connection 1:31262 Drop and generate

events

MALWARE-CNC Win.Zusy variant outbound connection 1:44652 Drop and generate

events

MALWARE-CNC Win.Zusy variant outbound connection 1:35076 Drop and generate

events

MALWARE-CNC Win/Linux.Trojan.Derusbi variant outbound connection 1:38258 Drop and generate

events

MALWARE-CNC Win32.Backdoor.Ropindo variant outbound post detected 1:47511 Drop and generate

events

MALWARE-CNC Win32.Backdoor.Turla variant outbound connection 1:47 773 Drop and generate

events

MALWARE-CNC Win32.Trojan.NeutrinoPOS connection attempt 1:43575 Drop and generate

events

MALWARE-CNC Win32/Autorun.JN variant outbound connection 1:26966 Drop and generate

events

MALWARE-CNC Word.Trojan.Emotet obfuscated powershell 1:44559 Drop and generate

events

MALWARE-CNC Worm.Silly variant outbound connection 1:27633 Drop and generate

events

MALWARE-CNC Worm.Win32.Faketube update request 1:19058 Drop and generate

events

MALWARE-CNC Worm.Win32.Nusump.A variant outbound connection 1:190 53 Drop and generate

events

MALWARE-CNC XDOT outbound connection attempt 3:38754 Drop and generate

events

MALWARE-CNC XP Fake Antivirus Check-in 1:26812 Drop and generate

events

MALWARE-CNC XP Fake Antivirus Payment Page Request 1:26811 Drop and generate

events

MALWARE-CNC Xsser mRAT GPS data upload 1:32053 Drop and generate

events

MALWARE-CNC y3k 1.2 variant outbound connection icq notification 1:7116 Drop and generate

events

MALWARE-CNC Zbot malware config file download request 1:16528 Drop and generate

events

MALWARE-CNC Zbot malware config file download request 1:16527 Drop and generate

events

MALWARE-CNC ZeroAccess Clickserver callback 1:25054 Drop and generate

events

MALWARE-CNC Zeus/Zbot malware config file download request 1:1548 1 Drop and generate

events

MALWARE-CNC ZoxPNG initial outbound connection 1:42882 Drop and generate

events

MALWARE-OTHER Adobe Flash exploit download attempt - Group 6 1:34 990 Drop and generate

events

MALWARE-OTHER Alureon - Malicious IFRAME load attempt 1:22061 Generate events

MALWARE-OTHER ANDR.Trojan.iBanking outbound connection attempt 1: 30070 Drop and generate

events

MALWARE-OTHER ANDR.Trojan.iBanking outbound connection attempt 1: 30071 Drop and generate

events

MALWARE-OTHER Andr.Trojan.KungFu variant download 1:39974 Drop and generate

events

MALWARE-OTHER ANDR.Trojan.ZertSecurity encrypted information leak 1:26796 Drop and generate

events

MALWARE-OTHER Apple iTunes Connect HTTP response phishing attempt 1:36338 Drop and generate

events

MALWARE-OTHER Clickserver ad harvesting redirection attempt 1:269 33 Generate events

MALWARE-OTHER Clickserver ad harvesting redirection attempt 1:269 34 Generate events

MALWARE-OTHER Compromised Website response - leads to Exploit Kit 1:24899 Drop and generate

events

MALWARE-OTHER Compromised Website response - leads to Exploit Kit 1:26698 Drop and generate

events

MALWARE-OTHER Compromised website response - leads to Exploit Kit 1:26093 Drop and generate

events

MALWARE-OTHER Compromised website response - leads to Exploit Kit 1:24883 Drop and generate

events

MALWARE-OTHER Compromised website response - leads to Exploit Kit 1:24884 Drop and generate

events

MALWARE-OTHER Compromised website response - leads to Exploit Kit 1:27550 Drop and generate

events

MALWARE-OTHER connection to malware sinkhole 1:30320 Drop and generate

events

MALWARE-OTHER connection to malware sinkhole 1:25018 Drop and generate

events

MALWARE-OTHER connection to malware sinkhole 1:33306 Drop and generate

events

MALWARE-OTHER DirtJumper denial of service attack traffic 1:27115 Drop and generate

events

MALWARE-OTHER DNS data exfiltration attempt 1:26803 Drop and generate MALWARE-OTHER DNS request for known malware domain toknowall.com - Unix.Trojan.Vpnfilter 1:46807 Drop and generate MALWARE-OTHER Dorifel/Quervar/XDocCrypt download 1:24144 Drop and generate

events

events

events

MALWARE-OTHER Double HTTP Server declared 1:26369 Drop and generate

events

MALWARE-OTHER Fake Adobe Flash Player malware binary requested 1: 27595 Drop and generate MALWARE-OTHER Fake Adobe Flash Player update warning enticing cli cks to malware payload 1:27594 Drop and generate MALWARE-OTHER Fake bookingdetails HTTP Response phishing attack 1 :25580 Drop and generate

events

events

events

MALWARE-OTHER Fake bookinginfo HTTP Response phishing attack 1:25 579 Drop and generate

events

MALWARE-OTHER Fake delivery information phishing attack 1:26660 Drop and generate

events

MALWARE-OTHER Fake Delta Ticket HTTP Response phishing attack 1:3 2008 Drop and generate

events

MALWARE-OTHER Fake postal receipt HTTP Response phishing attack 1 :25578 Drop and generate

events

MALWARE-OTHER Fake postal receipt HTTP Response phishing attack 1 :26261 Drop and generate

events

MALWARE-OTHER Flopex outbound communication attempt 1:39357

MALWARE-OTHER Game Over Zeus executable download detected 1:31487 Drop and generate

events

MALWARE-OTHER GPON exploit download attempt 1:46840 Drop and generate

events

MALWARE-OTHER GPON exploit download attempt 1:46841 Drop and generate

events

MALWARE-OTHER Group 6 Adobe Flash exploit download attempt 1:3499 1 Drop and generate

events

MALWARE-OTHER HideMeBetter spam injection variant 1:27565 Drop and generate

events

MALWARE-OTHER HTA script hidden window execution attempt 1:47077 Drop and generate

events

MALWARE-OTHER Html.Dropper.Xbash variant obfuscated powershell in vocation 1:47866 Drop and generate

events

MALWARE-OTHER Html.Dropper.Xbash variant obfuscated powershell in vocation 1:47867 Drop and generate

events

MALWARE-OTHER HTML.Exploit.C99 suspicious file download 1:24900 Drop and generate

events

MALWARE-OTHER HTML.Exploit.C99 suspicious file download 1:25095 Drop and generate

events

MALWARE-OTHER HTML.Exploit.C99 suspicious file download 1:24727 Drop and generate

events

MALWARE-OTHER Html.Phishing.Crea outbound connection attempt 1:34 336 Drop and generate

events

MALWARE-OTHER IFRAMEr Tool code injection attack 1:27229 Drop and generate MALWARE-OTHER Img.Trojan.Xbash variant PNG file with an embedded Windows executable 1:47868 Drop and generate MALWARE-OTHER Img.Trojan.Xbash variant PNG file with an embedded Windows executable 1:47869 Drop and generate MALWARE-OTHER Java FileDialog heap buffer overflow attempt 1:2964 0 Drop and generate

events

events

events

events

MALWARE-OTHER Java FileDialog heap buffer overflow attempt 1:2964 1 Drop and generate

events

MALWARE-OTHER known malicious user-agent string - DanaBot 1:47326 Drop and generate

events

MALWARE-OTHER Lamer outbound communication attempt 1:39356 Drop and generate

events

MALWARE-OTHER Lanman2.dll download 1:24261 Drop and generate

events

MALWARE-OTHER Mac OSX FBI ransomware 1:27246 Drop and generate

events

MALWARE-OTHER malicious iframe injection redirect attempt 1:30325 Drop and generate

events

MALWARE-OTHER malicious redirection attempt 1:24225 Drop and generate

events

MALWARE-OTHER Malvertising network attempted redirect 1:23620 Drop and generate

events

MALWARE-OTHER Malvertising redirection attempt 1:24099 Drop and generate

events

MALWARE-OTHER Malvertising redirection attempt 1:23618 Drop and generate

events

MALWARE-OTHER Malvertising redirection campaign - blackmuscat 1:2 3833 Drop and generate

events

MALWARE-OTHER MKVIS outbound communication attempt 1:39713 Drop and generate

events

MALWARE-OTHER multi-hop iframe campaign client-side exploit attempt 1:29023 Drop and generate

events

MALWARE-OTHER multi-hop iframe campaign client-side exploit attempt 1:29024 Drop and generate

events

MALWARE-OTHER multi-hop iframe campaign client-side exploit attempt 1:29025 Drop and generate

events

MALWARE-OTHER mygeeksmail.dll download 1:24257 Drop and generate

events

MALWARE-OTHER NeoSploit Malvertising - URI Requested 1:23058 Drop and generate

events

MALWARE-OTHER nikjju script injection 1:21949 Generate events

MALWARE-OTHER OSX.Trojan.HackBack file download attempt 1:27059 Drop and generate

events

MALWARE-OTHER OSX.Trojan.Imuler suspicious download 1:24799 Drop and generate

events

MALWARE-OTHER OSX.Trojan.Janicab file download attempt 1:27228 Drop and generate

events

MALWARE-OTHER Osx.Trojan.Janicab file download attempt 1:27548 Drop and generate

events

MALWARE-OTHER OSX.Trojan.KitM file download 1:26670 Drop and generate

events

MALWARE-OTHER PERL.Exploit.C99 suspicious file download 1:25094 Drop and generate

events

MALWARE-OTHER PHP.Exploit.C99 suspicious file download 1:25096 Drop and generate

events

MALWARE-OTHER PHP.Exploit.C99 suspicious file download 1:25097 Drop and generate

events

MALWARE-OTHER pisloader DNS drive command response attempt 1:3992 6 Drop and generate

events

MALWARE-OTHER pisloader DNS list command response attempt 1:39927 Drop and generate

events

MALWARE-OTHER pisloader DNS open command response attempt 1:39928 Drop and generate

events

MALWARE-OTHER pisloader DNS sinfo command response attempt 1:3992 9 Drop and generate

events

MALWARE-OTHER Portable Executable containing CoinHive download at tempt 1:47020 Drop and generate

events

MALWARE-OTHER Portable Executable containing CoinHive download at tempt 1:47021 Drop and generate

events

MALWARE-OTHER Possible malicious redirect - rebots.php 1:24017 Drop and generate

events

MALWARE-OTHER Possible Win.Trojan.Zbot variant outbound connectio n 1:29012 Drop and generate

events

MALWARE-OTHER Possible Win.Trojan.Zbot variant outbound connectio n 1:29013 Drop and generate

events

MALWARE-OTHER PwDump7.exe download 1:24259 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38650 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38651 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38653 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38654 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38655 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38656 Drop and generate

events

MALWARE-OTHER PWOBot variant download attempt 1:38657 Drop and generate

events

MALWARE-OTHER Request for a non-legit postal receipt 1:25277 Drop and generate

events

MALWARE-OTHER self-signed SSL certificate transfer for EXEPROXY attempt 1:36241 Drop and generate

events

MALWARE-OTHER Trackware e2give runtime detection - check update 1 :5907 Drop and generate

events

MALWARE-OTHER Trackware e2give runtime detection - redirect affil iate site request 1 1:5908 Drop and generate

events

MALWARE-OTHER Trackware e2give runtime detection - redirect affil iate site request 2 1:5909 Drop and generate

events

MALWARE-OTHER Trackware myway speedbar runtime detection - switch engines 1:5805 Generate events

MALWARE-OTHER Unix.Backdoor.Cdorked download attempt 1:26531 Drop and generate

events

MALWARE-OTHER Unix.Miner.Xbash variant dropped bash script 1:4787 0 Drop and generate

events

MALWARE-OTHER Unix.Miner.Xbash variant dropped bash script 1:4787 1 Drop and generate

events

MALWARE-OTHER Unix.Miner.Xbash variant dropped bash script 1:4787 2 Drop and generate

events

MALWARE-OTHER Unix.Miner.Xbash variant dropped bash script 1:4787 3 Drop and generate

events

MALWARE-OTHER Unix.Trojan.Agent variant download attempt 1:47380 Drop and generate

events

MALWARE-OTHER Unix.Trojan.Agent variant download attempt 1:47381 Drop and generate

events

MALWARE-OTHER VBScript potential executable write attempt 1:28054 Drop and generate

events

MALWARE-OTHER Win.Adware.Dlhelper outbound connection detected 1: 39803 Drop and generate

events

MALWARE-OTHER Win.Adware.Dlhelper outbound connection detected 1: 39804 Drop and generate

events

MALWARE-OTHER Win.Adware.Dlhelper outbound connection detected 1: 39805 Drop and generate

events

MALWARE-OTHER Win.Adware.Dlhelper outbound connection detected 1: 39806 Drop and generate

events

MALWARE-OTHER Win.Backdoor.Tavdig download attempt 1:28847 Drop and generate

events

MALWARE-OTHER Win.Downloader.Carp variant download attempt 1:4282 2 Drop and generate

events

MALWARE-OTHER Win.Downloader.Carp variant download attempt 1:4282 3 Drop and generate

events

MALWARE-OTHER Win.Downloader.DDECmdExec variant download 1:47844 Drop and generate

events

MALWARE-OTHER Win.Downloader.DDECmdExec variant download 1:47846 Drop and generate

events

MALWARE-OTHER Win.Downloader.DDECmdExec variant download 1:47847 Drop and generate

events

MALWARE-OTHER Win.Downloader.DDECmdExec variant download 1:47848 Drop and generate

events

MALWARE-OTHER Win.Downloader.DDECmdExec variant download 1:47849 Drop and generate

events

MALWARE-OTHER Win.Downloader.Latekonsul Runtime Detection 1:33874 Drop and generate

events

MALWARE-OTHER Win.Downloader.Ogimant outbound connection detected 1:39766 Drop and generate

events

MALWARE-OTHER Win.Downloader.Temvice outbound communication attempt 1:28381 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 13 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:245 91 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:250 86 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 21 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:245 89 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 04 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 02 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 15 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 09 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 06 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:250 88 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:250 90 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 17 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 11 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 19 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:250 84 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool suspicious file download 1:246 00 Drop and generate

events

MALWARE-OTHER Win.Exploit.Hacktool variant outbound connection 1: 25092 Drop and generate

events

MALWARE-OTHER Win.Malware.Emotet variant lateral propagation 1:43 892 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Alfa download attempt 1:39768 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Annabelle file download 1:46987 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Apocalypse download attempt 1:39746 Drop and generate

events

MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB transf er attempt 1:44648 Drop and generate

events

MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB transf er attempt 1:44650 Drop and generate

events

MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB2 trans fer attempt 1:44647 Drop and generate

events

MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SMB2 trans fer attempt 1:44649 Drop and generate MALWARE-OTHER Win.Ransomware.BadRabbit propagation via SVCCTL rem ote service attempt 1:44646 Drop and generate MALWARE-OTHER Win.Ransomware.CTB-Locker download attempt 1:33758 Drop and generate

events

events

events

MALWARE-OTHER Win.Ransomware.Gandcrab variant network share encry ption attempt 1:47278 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Kristina encryption over SMB attempt 1:44981 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Kristina encryption over SMB attempt 1:44982 Drop and generate

events

MALWARE-OTHER Win.Ransomware.MBRLock file download 1:46988 Drop and generate

events

MALWARE-OTHER Win.Ransomware.MBRLock file download 1:46989 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Ranscam initial download attempt 1:3 9637 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Samsam propagation via SMB transfer attempt 1:45484 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Samsam propagation via SMB2 transfer attempt 1:45485 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Samsam upload attempt 1:45486 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Satan payload download 1:46819 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Sorebrect download attempt 1:43442 Drop and generate

events

MALWARE-OTHER Win.Ransomware.SynAck download attempt 1:46751 Drop and generate

events

MALWARE-OTHER Win.Ransomware.SynAck download attempt 1:46752 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Thanatos ransomware inbound download attempt 1:45817 Drop and generate

events

MALWARE-OTHER Win.Ransomware.Thanatos ransomware inbound download attempt 1:45818 Drop and generate

events

MALWARE-OTHER Win.Trojan-Downloader.Jadtree GET request of RAR fi le to server 1:43221 Drop and generate

events

MALWARE-OTHER Win.Trojan.Agent E-FAX phishing attempt 1:30567 Drop and generate

events

MALWARE-OTHER Win.Trojan.Agent E-FAX phishing attempt 1:30568 Drop and generate

MALWARE-OTHER Win.Trojan.Bondupdater payload delivery attempt 1:4 8420 Drop and generate

events

MALWARE-OTHER Win.Trojan.Bondupdater payload delivery attempt 1:4 8421 Drop and generate

events

MALWARE-OTHER Win.Trojan.Dokstormac file download 1:27050 Drop and generate

events

MALWARE-OTHER Win.Trojan.Downloader download 1:24311 Drop and generate

events

MALWARE-OTHER Win.Trojan.FakeRean outbound connection detection 1 :39745 Drop and generate

events

MALWARE-OTHER Win.Trojan.Flokibot variant download attempt 1:4091 2 Drop and generate

events

MALWARE-OTHER Win.Trojan.Gauss download attempt 1:24410 Drop and generate

events

MALWARE-OTHER Win.Trojan.Gorgon attempted download 1:47453 Drop and generate

events

MALWARE-OTHER Win.Trojan.Gorgon attempted download 1:47454 Drop and generate

events

MALWARE-OTHER Win.Trojan.Hermit variant malicious dropper downloa d attempt 1:43975 Drop and generate

events

MALWARE-OTHER Win.Trojan.Injector outbound traffic 1:31510 Drop and generate

events

MALWARE-OTHER Win.Trojan.Kazy download attempt 1:26778 Drop and generate

events

MALWARE-OTHER Win.Trojan.Lethic outbound connection detected 1:39 807 Drop and generate

events

MALWARE-OTHER Win.Trojan.Lucuis malware file download 1:24515 Drop and generate

events

MALWARE-OTHER Win.Trojan.MagicHound dropper document file detecte d 1:41658 Drop and generate

events

MALWARE-OTHER Win.Trojan.Magitart outbound communication attempt 1:28483 Drop and generate

events

MALWARE-OTHER Win.Trojan.Maktub variant download attempt 1:38892 Drop and generate

events

MALWARE-OTHER Win.Trojan.Maktub variant download attempt 1:38372 Drop and generate

events

MALWARE-OTHER Win.Trojan.Maktub variant download attempt 1:38373 Drop and generate

events

MALWARE-OTHER Win.Trojan.Maktub variant download attempt 1:38374 Drop and generate

events

MALWARE-OTHER Win.Trojan.Malumpos malware download attempt 1:3500 3 Drop and generate

events

MALWARE-OTHER Win.Trojan.MiniFlame C&C command response attempt 1 :24594 Drop and generate

events

MALWARE-OTHER Win.Trojan.Miniflame download attempt 1:24408 Drop and generate

events

MALWARE-OTHER Win.Trojan.Nemucod file download 1:44078 Drop and generate

events

MALWARE-OTHER Win.Trojan.Nemucod variant file download 1:43684 Drop and generate

events

MALWARE-OTHER Win.Trojan.Nemucod variant outbound connection 1:43 685 Drop and generate

MALWARE-OTHER Win.Trojan.Petya variant download attempt 1:38442 Drop and generate

events

MALWARE-OTHER Win.Trojan.Petya variant download attempt 1:38443 Drop and generate

events

MALWARE-OTHER Win.Trojan.Petya variant download attempt 1:38444 Drop and generate

events

MALWARE-OTHER Win.Trojan.Petya variant download attempt 1:38445 Drop and generate

events

MALWARE-OTHER Win.Trojan.Petya variant download attempt 1:38446 Drop and generate

events

MALWARE-OTHER Win.Trojan.Petya variant download attempt 1:38447 Drop and generate

events

MALWARE-OTHER Win.Trojan.Retefe variant malicious certificate ins tallation page 1:39755 Drop and generate

events

MALWARE-OTHER Win.Trojan.Samas variant download attempt 1:38360 Drop and generate

events

MALWARE-OTHER Win.Trojan.Samas variant download attempt 1:38279 Drop and generate

events

MALWARE-OTHER Win.Trojan.Stoberox outbound communication attempt 1:28365 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40050 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40051 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40052 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40056 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40191 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40194 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40196 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40197 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40200 Drop and generate

events

MALWARE-OTHER Win.Trojan.Swabfex download attempt 1:40201 Drop and generate

events

MALWARE-OTHER Win.Trojan.Troll dropper document file detected 1:3 8526 Drop and generate

events

MALWARE-OTHER Win.Trojan.Ursnif variant download attempt 1:45565 Drop and generate

events

MALWARE-OTHER Win.Trojan.Wysotot variant download attempt 1:30946 Drop and generate

events

MALWARE-OTHER Win.Trojan.Xtrat outbound connection detected 1:397 34 Drop and generate

events

MALWARE-OTHER Win.Trojan.Yakes download attempt 1:27055 Drop and generate

events

MALWARE-OTHER Win.Trojan.ZBerp variant download attempt 1:31184 Drop and generate

MALWARE-OTHER Win.Worm.Pixipos Outbound Connection Attempt 1:3722 2 Drop and generate

events

MALWARE-TOOLS CKnife penetration testing tool attempt 1:39744 Drop and generate

events

MALWARE-TOOLS CKnife penetration testing tool attempt 1:39771 Drop and generate

events

MALWARE-TOOLS CKnife penetration testing tool attempt 1:39772 Drop and generate

events

MALWARE-TOOLS CKnife penetration testing tool attempt 1:39773 Drop and generate

events

MALWARE-TOOLS Havij advanced SQL injection tool user-agent string 1:21459 Drop and generate

events

MALWARE-TOOLS HOIC http denial of service attack 1:21513 Drop and generate

events

MALWARE-TOOLS JavaScript LOIC attack 1:21092 Drop and generate

events

MALWARE-TOOLS slowhttptest DoS tool 1:41771 Drop and generate

events

MALWARE-TOOLS slowhttptest DoS tool 1:21104 Drop and generate

events

MALWARE-TOOLS Win.Trojan.Downloader outbound connection attempt 1 :37651 Drop and generate

events

NETBIOS Cisco WebEx WebExService.exe remote code execution attemp t 1:48241 Drop and generate

events

OS-LINUX Linux Kernel keyring object exploit download attempt 1:3 7435 Drop and generate

events

OS-LINUX Linux Kernel keyring object exploit download attempt 1:3 7436 Drop and generate

events

OS-LINUX Linux kernel madvise race condition attempt 1:40560 Drop and generate

events

OS-LINUX Linux kernel madvise race condition attempt 1:40542 Drop and generate

events

OS-LINUX Ubuntu Apport CrashDB crash report code injection attemp t 1:41040 Drop and generate

events

OS-MOBILE Android Andr.Trojan.Waller information disclosure attempt 1:30880 Drop and generate

events

OS-MOBILE iOS lockdownd plist object buffer overflow attempt 1:35 090 Drop and generate OS-OTHER Apple OSX and iOS x509 certificate name constraints pars ing use after free attempt 1:41999 Drop and generate OS-OTHER Bash CGI environment variable injection attempt 1:31975 Drop and generate

events

events

events

OS-OTHER Bash CGI environment variable injection attempt 1:31976 Drop and generate

events

OS-OTHER Bash CGI environment variable injection attempt 1:31977 Drop and generate

events

OS-OTHER Bash CGI environment variable injection attempt 1:31978 Drop and generate

events

OS-OTHER Bash CGI nested loops word\_lineno denial of service atte mpt 1:32047 Drop and generate

events

OS-OTHER Bash redir\_stack here document handling denial of servic e attempt 1:32045 Drop and generate

OS-OTHER Intel x64 side-channel analysis information leak attempt 1:45444 Drop and generate

events

OS-OTHER Intel x64 side-channel analysis information leak attempt 1:45367 Drop and generate

events

OS-OTHER Intel x86 L1 data cache side-channel analysis informatio n leak attempt 3:47595 Drop and generate

events

OS-OTHER Intel x86 L1 data cache side-channel analysis informatio n leak attempt 3:47596 Drop and generate

events

OS-OTHER Intel x86 L1 data cache side-channel analysis informatio n leak attempt 3:47597 Drop and generate

events

OS-OTHER Intel x86 L1 data cache side-channel analysis informatio n leak attempt 3:47598 Drop and generate

events

OS-OTHER Intel x86 side-channel analysis information leak attempt 1:45362 Drop and generate

events

OS-OTHER Intel x86 side-channel analysis information leak attempt 1:45363 Drop and generate

events

OS-OTHER Intel x86 side-channel analysis information leak attempt 1:45364 Drop and generate

events

OS-OTHER Intel x86 side-channel analysis information leak attempt 1:45365 Drop and generate

events

OS-OTHER Intel x86 side-channel analysis information leak attempt 1:45366 Drop and generate

events

OS-OTHER Joyent SmartOS add entries denial of service attempt 1:4 1217 Drop and generate

events

OS-OTHER Joyent SmartOS file system name buffer overflow attempt 1:40900 Drop and generate

events

OS-OTHER Joyent SmartOS file system path buffer overflow attempt 1:40902 Drop and generate

events

OS-OTHER Joyent SmartOS ioctl integer underflow attempt 1:40898 Drop and generate

events

OS-OTHER OS X DYLD\_PRINT\_TO\_FILE privilege escalation attempt 1:3 5735 Drop and generate

events

OS-SOLARIS Solaris dtappgather local privilege escalation attempt 1:42253 Drop and generate OS-WINDOWS .NET Framework BinaryServerFormatterSink-ProcessMessag e IMessage corruption attempt 1:32474 Drop and generate OS-WINDOWS DCERPC Bind auth level packet privacy downgrade attemp t 1:38462 Drop and generate

events

events

events

OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overfl ow attempt 1:7209 Drop and generate OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt 1:14782 Drop and generate OS-WINDOWS dxgkrnl.sys privilege escalation attempt 1:46596 Drop and generate

events

events

events

OS-WINDOWS dxgkrnl.sys privilege escalation attempt 1:46597 Drop and generate

events

OS-WINDOWS Kaspersky Internet Security KLIF driver denial of serv ice attempt 1:39078 Drop and generate

events

OS-WINDOWS Kaspersky Internet Security KLIF driver denial of serv ice attempt 1:38849 Drop and generate

events

OS-WINDOWS Malicious vbscript download attempt 1:46794 Drop and generate

OS-WINDOWS Microsoft Data Sharing dssvc.dll arbitrary file deleti on attempt 1:48237 Drop and generate

events

OS-WINDOWS Microsoft Data Sharing dssvc.dll arbitrary file deleti on attempt 1:48238 Drop and generate

events

OS-WINDOWS Microsoft GDI library TIFF handling memory corruption attempt 3:28487 Drop and generate

events

OS-WINDOWS Microsoft GDI library TIFF handling memory corruption attempt 3:28488 Drop and generate

events

OS-WINDOWS Microsoft GDI PolyTextOutW out of bounds memory write attempt 1:42173 Drop and generate

events

OS-WINDOWS Microsoft Internet Explorer VerifyFile information dis closure attempt 1:38780 Drop and generate

events

OS-WINDOWS Microsoft Malware Protection Engine type confusion att empt 1:42820 Drop and generate OS-WINDOWS Microsoft OfficeHub object manager namespace privilege escalation attempt 1:46953 Drop and generate OS-WINDOWS Microsoft OfficeHub object manager namespace privilege escalation attempt 1:46954 Drop and generate OS-WINDOWS Microsoft Win32k DDI use after free attempt 1:41928 Drop and generate

events

events

events

events

OS-WINDOWS Microsoft Win32k DDI use after free attempt 1:41929 Drop and generate

events

OS-WINDOWS Microsoft Win32k DDI use after free attempt 1:41930 Drop and generate

events

OS-WINDOWS Microsoft Win32k DDI use after free attempt 1:41931 Drop and generate

events

OS-WINDOWS Microsoft Win32k kernel memory leak attempt 1:42769 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:46564 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:46565 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:42158 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:42159 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:46938 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:46939 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:46562 Drop and generate

events

OS-WINDOWS Microsoft Win32k privilege escalation attempt 1:46563 Drop and generate

events

OS-WINDOWS Microsoft Win32u NtUserThunkedMenuItemInfo use after f ree attempt 1:41926 Drop and generate

events

OS-WINDOWS Microsoft Win32u NtUserThunkedMenuItemInfo use after f ree attempt 1:41927 Drop and generate

events

OS-WINDOWS Microsoft win32u PlgBlt out of bounds memory write att empt 1:43473 Drop and generate

events

OS-WINDOWS Microsoft win32u PlgBlt out of bounds memory write att empt 1:43474 Drop and generate

OS-WINDOWS Microsoft Windows 10 and 8.1 registry key privilege es calation attempt 1:40128 Drop and generate

events

OS-WINDOWS Microsoft Windows 10 arbitrary registry key access pri velege escalation attempt 1:40400 Drop and generate OS-WINDOWS Microsoft Windows 10 arbitrary registry key access pri velege escalation attempt 1:40401 Drop and generate OS-WINDOWS Microsoft Windows 10 GDI privilege escalation attempt 1:40112 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows 10 GDI privilege escalation attempt 1:40113 Drop and generate

events

OS-WINDOWS Microsoft Windows 10 gdi32 library integer overflow at tempt 1:45881 Drop and generate

events

OS-WINDOWS Microsoft Windows 10 gdi32 library integer overflow at tempt 1:45882 Drop and generate OS-WINDOWS Microsoft Windows 10 low integrity level NTFS mount re parse point bypass attempt 1:37269 Drop and generate OS-WINDOWS Microsoft Windows 10 low integrity level NTFS mount re parse point bypass attempt 1:37270 Drop and generate OS-WINDOWS Microsoft Windows 10 low integrity level NTFS mount re parse point bypass attempt 1:37271 Drop and generate OS-WINDOWS Microsoft Windows 10 low integrity level NTFS mount re parse point bypass attempt 1:37272 Drop and generate OS-WINDOWS Microsoft Windows 10 privilege escalation attempt 1:40 114 Drop and generate

events

events

events

events

events

events

OS-WINDOWS Microsoft Windows 10 privilege escalation attempt 1:40 115 Drop and generate

events

OS-WINDOWS Microsoft Windows 10 RS2 x64 linked cursor double free attempt 1:43173 Drop and generate

events

OS-WINDOWS Microsoft Windows 7 Win32k ValidateZorder privilege es calation attempt 1:40096 Drop and generate

events

OS-WINDOWS Microsoft Windows 7 Win32k ValidateZorder privilege es calation attempt 1:40097 Drop and generate OS-WINDOWS Microsoft Windows Active Directory kerberos encryption type downgrade attempt 1:31874 Drop and generate OS-WINDOWS Microsoft Windows AFD.sys double fetch race condition attempt 1:42751 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows afd.sys memory corruption attempt 1: 36705 Drop and generate

events

OS-WINDOWS Microsoft Windows afd.sys memory corruption attempt 1: 36706 Drop and generate

events

OS-WINDOWS Microsoft Windows AHCACHE.SYS remote denial of service attempt 1:40555 Drop and generate

events

OS-WINDOWS Microsoft Windows AHCACHE.SYS remote denial of service attempt 1:40556 Drop and generate

events

OS-WINDOWS Microsoft Windows ALPC task scheduler local privilege escalation attempt 1:47702 Drop and generate

events

OS-WINDOWS Microsoft Windows ALPC task scheduler local privilege escalation attempt 1:47703 Drop and generate

events

OS-WINDOWS Microsoft Windows anonymous user token impersonation attempt 1:38475 Drop and generate

events

OS-WINDOWS Microsoft Windows anonymous user token impersonation attempt 1:38476 Drop and generate

OS-WINDOWS Microsoft Windows ATFM.DLL malformed OTF use-after-fre e attempt 1:35515 Drop and generate

events

OS-WINDOWS Microsoft Windows ATFM.DLL malformed OTF use-after-fre e attempt 1:35516 Drop and generate

events

OS-WINDOWS Microsoft Windows Calendar object heap corruption atte mpt 1:34401 Drop and generate

events

OS-WINDOWS Microsoft Windows CDD font parsing kernel memory corru ption attempt 1:35719 Drop and generate

events

OS-WINDOWS Microsoft Windows CDD font parsing kernel memory corru ption attempt 1:35720 Drop and generate

events

OS-WINDOWS Microsoft Windows clfs.sys local privilege escalation attempt 1:40657 Drop and generate

events

OS-WINDOWS Microsoft Windows clfs.sys local privilege escalation attempt 1:40658 Drop and generate

events

OS-WINDOWS Microsoft Windows clfs.sys out of bounds local privile ge escalation attempt 1:46603 Drop and generate

events

OS-WINDOWS Microsoft Windows clfs.sys out of bounds local privile ge escalation attempt 1:46604 Drop and generate

events

OS-WINDOWS Microsoft Windows ClickOnce information disclosure att empt 1:36712 Drop and generate OS-WINDOWS Microsoft Windows Clipboard Broker privilege escalatio n vulnerability attempt 1:42208 Drop and generate OS-WINDOWS Microsoft Windows Clipboard Broker privilege escalatio n vulnerability attempt 1:42209 Drop and generate OS-WINDOWS Microsoft Windows CreatePopupMenu win32k.sys use after free attempt 1:38491 Drop and generate

events

events

events

events

OS-WINDOWS Microsoft Windows CreatePopupMenu win32k.sys use after free attempt 1:38492 Drop and generate

events

OS-WINDOWS Microsoft Windows CreateWindowEx privilege escalation attempt 1:34178 Drop and generate

events

OS-WINDOWS Microsoft Windows D3D memory corruption attempt 1:4751 7 Drop and generate

events

OS-WINDOWS Microsoft Windows D3D memory corruption attempt 1:4751 8 Drop and generate

events

OS-WINDOWS Microsoft Windows D3D memory corruption attempt 1:4751 2 Drop and generate

events

OS-WINDOWS Microsoft Windows D3D memory corruption attempt 1:4751 3 Drop and generate

events

OS-WINDOWS Microsoft Windows D3D memory corruption attempt 1:4751 5 Drop and generate

events

OS-WINDOWS Microsoft Windows D3D memory corruption attempt 1:4751 6 Drop and generate OS-WINDOWS Microsoft Windows DCERPC NCACN-IP-TCP spoolss RpcSetPr interDataEx attempt 1:15528 Drop and generate OS-WINDOWS Microsoft Windows DeferWindowPos privilege escalation attempt 1:36703 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows DeferWindowPos privilege escalation attempt 1:36704 Drop and generate

events

OS-WINDOWS Microsoft Windows Desktop Bridge privilege escalation attempt 1:45900 Drop and generate

events

OS-WINDOWS Microsoft Windows Desktop Bridge privilege escalation attempt 1:45901 Drop and generate

OS-WINDOWS Microsoft Windows devenum.dll device moniker underflow attempt 1:37277 Drop and generate

events

OS-WINDOWS Microsoft Windows devenum.dll device moniker underflow attempt 1:37278 Drop and generate

events

OS-WINDOWS Microsoft Windows device content surface bitmap use af ter free attempt 1:38774 Drop and generate

events

OS-WINDOWS Microsoft Windows device content surface bitmap use af ter free attempt 1:38775 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Context bitmap use after free attempt 1:38787 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:43157 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:41567 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:41568 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:41569 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:41570 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:41571 Drop and generate

events

OS-WINDOWS Microsoft Windows Device Guard code execution attempt 1:41572 Drop and generate

events

OS-WINDOWS Microsoft Windows DeviceIoControl double fetch race co ndition attempt 1:42767 Drop and generate

events

OS-WINDOWS Microsoft Windows DFS client driver privilege escalati on attempt 1:40418 Drop and generate

events

OS-WINDOWS Microsoft Windows DFS client driver privilege escalati on attempt 1:40419 Drop and generate

events

OS-WINDOWS Microsoft Windows Diagnostics Hub dll load from stream attempt 1:40398 Drop and generate

events

OS-WINDOWS Microsoft Windows Diagnostics Hub dll load from stream attempt 1:40399 Drop and generate

events

OS-WINDOWS Microsoft Windows DirectComposition double free attemp t 1:41579 Drop and generate

events

OS-WINDOWS Microsoft Windows DirectComposition double free attemp t 1:41580 Drop and generate

events

OS-WINDOWS Microsoft Windows DNSAPI remote code execution attempt 1:46935 Drop and generate

events

OS-WINDOWS Microsoft Windows DrawMenuBarTemp memory corruption at tempt 1:38459 Drop and generate

events

OS-WINDOWS Microsoft Windows DrawMenuBarTemp memory corruption at tempt 1:38460 Drop and generate

events

OS-WINDOWS Microsoft Windows DTLSv1.0 handshake cookie buffer ove rflow attempt 1:32422 Drop and generate OS-WINDOWS Microsoft Windows DTLSv1.0 hello verify request out of bounds read attempt 1:32423 Drop and generate OS-WINDOWS Microsoft Windows dxgkrnl CreateDriverAllocations null pointer dereference attempt 1:42757 Drop and generate OS-WINDOWS Microsoft Windows dxgkrnl CreateDriverAllocations null pointer dereference attempt 1:42758 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows ECDSA certificate validation bypass attempt 1:32406 Drop and generate

events

OS-WINDOWS Microsoft Windows ECDSA certificate validation bypass attempt 1:32407 Drop and generate

events

OS-WINDOWS Microsoft Windows ECDSA certificate validation bypass attempt 1:32408 Drop and generate

events

OS-WINDOWS Microsoft Windows ECDSA certificate validation bypass attempt 1:32411 Drop and generate

events

OS-WINDOWS Microsoft Windows ECDSA certificate validation bypass attempt 1:32412 Drop and generate

events

OS-WINDOWS Microsoft Windows ECDSA certificate validation bypass attempt 1:32413 Drop and generate

events

OS-WINDOWS Microsoft Windows Edge DACL privilege escalation attempt 1:40396 Drop and generate

events

OS-WINDOWS Microsoft Windows EndDeferWindowPos null page derefere nce attempt 1:39508 Drop and generate

events

OS-WINDOWS Microsoft Windows EndDeferWindowPos null page derefere nce attempt 1:39509 Drop and generate

events

OS-WINDOWS Microsoft Windows feclient.dll dll-load exploit attemp t 1:37275 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI emf file integer overflow attemp t 1:39824 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI emf file integer overflow attemp t 1:39825 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI null pointer dereference attempt 1:42199 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI null pointer dereference attempt 1:42200 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI privilege escalation attempt 1:4 1591 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI privilege escalation attempt 1:4 1592 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI WMF out of bounds read attempt 1 :41993 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI WMF out of bounds read attempt 1 :41994 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI+ denial of service attempt 1:359 84 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI+ denial of service attempt 1:359 85 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI+ EMF buffer overread attempt 1:4 0425 Drop and generate

events

OS-WINDOWS Microsoft Windows GDI+ EMF buffer overread attempt 1:4 0426 Drop and generate

events

OS-WINDOWS Microsoft Windows GdiGradientFill null pointer derefer ence attempt 1:42771 Drop and generate

events

OS-WINDOWS Microsoft Windows GdiGradientFill null pointer derefer ence attempt 1:42772 Drop and generate

events

OS-WINDOWS Microsoft Windows gdiplus EMF EmrText out of bounds wr ite attempt 1:39843 Drop and generate

events

OS-WINDOWS Microsoft Windows gpuenergydrv.sys driver privilege es calation attempt 1:36989 Drop and generate

OS-WINDOWS Microsoft Windows GreCreateDisplayDC surface object us e after free attempt 1:38083 Drop and generate

events

OS-WINDOWS Microsoft Windows GreCreateDisplayDC surface object us e after free attempt 1:38084 Drop and generate OS-WINDOWS Microsoft Windows HIDPARSE.sys memory corruption attempt 1:45656 Drop and generate

events

events

OS-WINDOWS Microsoft Windows HIDPARSE.sys memory corruption attempt 1:45657 Drop and generate

events

OS-WINDOWS Microsoft Windows IE ETW Collector Service privilege e scalation attempt 1:42187 Drop and generate

events

OS-WINDOWS Microsoft Windows IE ETW Collector Service privilege e scalation attempt 1:42188 Drop and generate OS-WINDOWS Microsoft Windows insecure BoundaryDescriptor privileg e escalation attempt 1:40374 Drop and generate OS-WINDOWS Microsoft Windows kernel information disclosure attemp t 1:47717 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows kernel information disclosure attemp t 1:47718 Drop and generate

events

OS-WINDOWS Microsoft Windows kernel privilege escalation attempt 1:46830 Drop and generate

events

OS-WINDOWS Microsoft Windows kernel privilege escalation attempt 1:46831 Drop and generate

events

OS-WINDOWS Microsoft Windows keybd\_event type confusion code exec ution attempt 1:40665 Drop and generate

events

OS-WINDOWS Microsoft Windows keybd\_event type confusion code exec ution attempt 1:40666 Drop and generate

events

OS-WINDOWS Microsoft Windows keybd\_event type confusion code exec ution attempt 1:40886 Drop and generate

events

OS-WINDOWS Microsoft Windows keybd\_event type confusion code exec ution attempt 1:40887 Drop and generate

events

OS-WINDOWS Microsoft Windows ksecdd.sys kernel information disclosure attempt 1:40953 Drop and generate

events

OS-WINDOWS Microsoft Windows ksecdd.sys kernel information disclosure attempt 1:40954 Drop and generate

events

OS-WINDOWS Microsoft Windows ksecdd.sys kernel information disclosure attempt 1:40955 Drop and generate

events

OS-WINDOWS Microsoft Windows ksecdd.sys kernel information disclosure attempt 1:40956 Drop and generate

events

OS-WINDOWS Microsoft Windows LSARPC LsapLookupSids denial of serv ice attempt 1:38458 Drop and generate

events

OS-WINDOWS Microsoft Windows LSASS domain name buffer overflow at tempt 1:18405 Drop and generate OS-WINDOWS Microsoft Windows malformed shortcut file with comment buffer overflow attempt 1:45624 Drop and generate OS-WINDOWS Microsoft Windows malformed shortcut file with comment buffer overflow attempt 1:45625 Drop and generate OS-WINDOWS Microsoft Windows malformed TTF integer overflow attempt 1:46230 Drop and generate

events

events

events

events

OS-WINDOWS Microsoft Windows malformed TTF integer overflow attempt 1:46231 Drop and generate

events

OS-WINDOWS Microsoft Windows Media Player DataObject buffer overf low attempt 1:34731 Drop and generate

OS-WINDOWS Microsoft Windows MsMpEng custom apicall instruction u se detected 1:43381 Drop and generate

events

OS-WINDOWS Microsoft Windows MsMpEng JavaScript garbage collectio n use after free attempt 1:43056 Drop and generate OS-WINDOWS Microsoft Windows NDIS.SYS driver buffer overflow atte mpt 1:36744 Drop and generate

events

events

OS-WINDOWS Microsoft Windows NDIS.SYS driver buffer overflow atte mpt 1:36745 Drop and generate

events

OS-WINDOWS Microsoft Windows NtGdiGetEmbUFI kernel information di sclosure attempt 1:38801 Drop and generate

events

OS-WINDOWS Microsoft Windows NtGdiGetEmbUFI kernel information di sclosure attempt 1:38802 Drop and generate

events

OS-WINDOWS Microsoft Windows NtGdiSelectPen privilege escalation attempt 1:39478 Drop and generate

events

OS-WINDOWS Microsoft Windows NtGdiSelectPen privilege escalation attempt 1:39479 Drop and generate

events

OS-WINDOWS Microsoft Windows NtGdiSetBitmapAttributes privilege e scalation attempt 1:40663 Drop and generate

events

OS-WINDOWS Microsoft Windows NtGdiSetBitmapAttributes privilege e scalation attempt 1:40664 Drop and generate

events

OS-WINDOWS Microsoft Windows Ntoskrnl integer overflow privilege escalation attempt 1:40394 Drop and generate

events

OS-WINDOWS Microsoft Windows Ntoskrnl integer overflow privilege escalation attempt 1:40395 Drop and generate

events

OS-WINDOWS Microsoft Windows Ntoskrnl privilege escalation attemp t 1:40392 Drop and generate

events

OS-WINDOWS Microsoft Windows Ntoskrnl privilege escalation attemp t 1:40393 Drop and generate

events

OS-WINDOWS Microsoft Windows NtSetInformationFile hard link sandb ox bypass attempt 1:36761 Drop and generate

events

OS-WINDOWS Microsoft Windows NtSetInformationFile hard link sandb ox bypass attempt 1:36762 Drop and generate

events

OS-WINDOWS Microsoft Windows NtTraceControl information disclosur e attempt 1:42763 Drop and generate

events

OS-WINDOWS Microsoft Windows NtTraceControl information disclosur e attempt 1:42764 Drop and generate

events

OS-WINDOWS Microsoft Windows NtUserDraw privilege escalation atte mpt 1:39482 Drop and generate

events

OS-WINDOWS Microsoft Windows NtUserDraw privilege escalation atte mpt 1:39483 Drop and generate OS-WINDOWS Microsoft Windows ObReferenceObjectByHandle function p rivilege escalation attempt 1:38092 Drop and generate OS-WINDOWS Microsoft Windows operating system win32kfull heap cor ruption attempt 1:39818 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows operating system win32kfull heap cor ruption attempt 1:39819 Drop and generate

events

OS-WINDOWS Microsoft Windows RDP server PDU length heap overflow attempt 1:35151 Drop and generate

events

OS-WINDOWS Microsoft Windows registry hive privilege escalation attempt 1:40412 Drop and generate

events

OS-WINDOWS Microsoft Windows registry hive privilege escalation attempt 1:40413 Drop and generate

events

OS-WINDOWS Microsoft Windows RemoteDesktop new session flood atte mpt 1:21570 Drop and generate

events

OS-WINDOWS Microsoft Windows ROP gadget locate attempt 1:46832 Drop and generate

events

OS-WINDOWS Microsoft Windows ROP gadget locate attempt 1:46833 Drop and generate

events

OS-WINDOWS Microsoft Windows rpdesk remote code execution attempt 1:38061 Drop and generate

events

OS-WINDOWS Microsoft Windows rpdesk remote code execution attempt 1:38062 Drop and generate

events

OS-WINDOWS Microsoft Windows RRAS service arbitrary pointer deref erence attempt 1:45130 Drop and generate

events

OS-WINDOWS Microsoft Windows RRAS service arbitrary pointer deref erence attempt 1:45131 Drop and generate OS-WINDOWS Microsoft Windows sandbox ProcessFontDisablePolicy che ck bypass attempt 1:39209 Drop and generate OS-WINDOWS Microsoft Windows sandbox ProcessFontDisablePolicy che ck bypass attempt 1:39210 Drop and generate OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32409 Drop and generate

events

events

events

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32410 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32414 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32415 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32416 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32417 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:34057 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:34058 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32731 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel CertificateVerify buffer ov erflow attempt 1:32732 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel ECDH key exchange heap over flow attempt 1:32419 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel ECDH key exchange heap over flow attempt 1:32420 Drop and generate

events

OS-WINDOWS Microsoft Windows SChannel ECDH key exchange heap over flow attempt 1:32421 Drop and generate

events

OS-WINDOWS Microsoft Windows Search Service out of bounds memory access attempt 1:43175 Drop and generate

events

OS-WINDOWS Microsoft Windows Search Service out of bounds memory access attempt 1:43176 Drop and generate

events

OS-WINDOWS Microsoft Windows Server lsass.exe memory corruption attempt 1:40129 Drop and generate

events

OS-WINDOWS Microsoft Windows Server Ntoskrnl concurrent login att empt 1:40110 Drop and generate

events

OS-WINDOWS Microsoft Windows SetProcessDeviceMap arbitrary file r ead attempt 1:45873 Drop and generate

events

OS-WINDOWS Microsoft Windows SetProcessDeviceMap arbitrary file r ead attempt 1:45874 Drop and generate

events

OS-WINDOWS Microsoft Windows SMB kernel heap memory leak attempt 1:45977 Generate events

OS-WINDOWS Microsoft Windows SMB kernel heap memory leak attempt 1:45978 Generate events

OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction requ est memory leak attempt 1:42338 Drop and generate OS-WINDOWS Microsoft Windows SMB possible leak of kernel heap mem ory 1:42339 Generate events

events

OS-WINDOWS Microsoft Windows SMB remote code execution attempt 1: 42944 Drop and generate

events

OS-WINDOWS Microsoft Windows SMB remote code execution attempt 1: 41978 Drop and generate

events

OS-WINDOWS Microsoft Windows SMBv1 identical MID and FID type con fusion attempt 1:41984 Drop and generate OS-WINDOWS Microsoft Windows StripSolidHorizontal out of bounds m emory access attempt 1:40947 Drop and generate OS-WINDOWS Microsoft Windows StripSolidHorizontal out of bounds m emory access attempt 1:40948 Drop and generate OS-WINDOWS Microsoft Windows System.DirectoryServices.Protocols.U tility class memory overflow attempt 1:36014 Drop and generate OS-WINDOWS Microsoft Windows SystemCollector privilege escalation attempt 1:47850 Drop and generate

events

events

events

events

events

OS-WINDOWS Microsoft Windows SystemCollector privilege escalation attempt 1:47851 Drop and generate OS-WINDOWS Microsoft Windows Task Scheduler SystemLocal NTLM remo te path authentication challenge attempt 1:40677 Drop and generate OS-WINDOWS Microsoft Windows Task Scheduler SystemLocal NTLM remo te path authentication challenge attempt 1:40678 Drop and generate OS-WINDOWS Microsoft Windows thread lock desynchronization null p ointer dereference attempt 1:36976 Drop and generate OS-WINDOWS Microsoft Windows thread lock desynchronization null p ointer dereference attempt 1:36977 Drop and generate OS-WINDOWS Microsoft Windows TrueType font heap overflow attempt 1:46214 Drop and generate

events

events

events

events

events

events

OS-WINDOWS Microsoft Windows TrueType font heap overflow attempt 1:46215 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueType font heap overflow attempt 1:46200 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueType font heap overflow attempt 1:46201 Drop and generate OS-WINDOWS Microsoft Windows TrueType Font LookupTable out of bou nds write attempt 1:41960 Drop and generate OS-WINDOWS Microsoft Windows TrueType Font out of bounds write at tempt 1:41972 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows TrueType Font out of bounds write at tempt 1:41974 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueType font parsing integer underf low attempt 1:35525 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueType font parsing integer underf low attempt 1:35526 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueType Font parsing remote code ex ecution attempt 1:32190 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueType Font parsing remote code ex ecution attempt 1:32191 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueTypeFont GSUB table out of bound s write attempt 1:41966 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueTypeFont post table out of bound s write attempt 1:41985 Drop and generate

events

OS-WINDOWS Microsoft Windows TrueTypeFont post table out of bound s write attempt 1:41986 Drop and generate

events

OS-WINDOWS Microsoft Windows TTF invalid system memory access att empt 1:35523 Drop and generate

events

OS-WINDOWS Microsoft Windows TTF invalid system memory access att empt 1:35524 Drop and generate

events

OS-WINDOWS Microsoft Windows use after free kernel privilege esca lation attempt 1:36709 Drop and generate

events

OS-WINDOWS Microsoft Windows use after free kernel privilege esca lation attempt 1:36710 Drop and generate

events

OS-WINDOWS Microsoft Windows user hive impersonation privelege es calation attempt 1:40402 Drop and generate

events

OS-WINDOWS Microsoft Windows user hive impersonation privelege es calation attempt 1:40403 Drop and generate

events

OS-WINDOWS Microsoft Windows ValidateParentDepth out of bounds re ad attempt 1:38071 Drop and generate

events

OS-WINDOWS Microsoft Windows ValidateParentDepth out of bounds re ad attempt 1:38072 Drop and generate

events

OS-WINDOWS Microsoft Windows VHDMP generic privilege escalation attempt 1:40693 Drop and generate

events

OS-WINDOWS Microsoft Windows VHDMP generic privilege escalation attempt 1:40694 Drop and generate OS-WINDOWS Microsoft Windows WebDAV mini redirector driver privil ege escalation attempt 1:38114 Drop and generate OS-WINDOWS Microsoft Windows WebDAV mini redirector driver privil ege escalation attempt 1:38115 Drop and generate OS-WINDOWS Microsoft Windows WebDAV mini redirector driver privil ege escalation attempt 1:37586 Drop and generate OS-WINDOWS Microsoft Windows WebDAV mini redirector driver privil ege escalation attempt 1:37587 Drop and generate OS-WINDOWS Microsoft Windows WebDAV NTLM reflection attack attemp t 1:39213 Drop and generate

events

events

events

events

events

events

OS-WINDOWS Microsoft Windows WebDAV NTLM reflection attack attemp t 1:39214 Drop and generate

events

OS-WINDOWS Microsoft Windows WebDAV NTLM reflection attack attemp t 1:39215 Drop and generate

events

OS-WINDOWS Microsoft Windows WebDAV NTLM reflection attack attemp t 1:39216 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32k information disclosure attemp t 1:48393 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32k information disclosure attemp t 1:48394 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k information disclosure attemp t 1:36722 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k information disclosure attemp t 1:36723 Drop and generate OS-WINDOWS Microsoft Windows win32k NtUserSetImeInfoEx privilege escalation attempt 1:46546 Drop and generate OS-WINDOWS Microsoft Windows win32k NtUserSetImeInfoEx privilege escalation attempt 1:46547 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows Win32k TrueType Font parsing out of bounds attempt 1:34440 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32k window handle use after free attempt 1:38759 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32k window handle use after free attempt 1:38760 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys desktop switch use after free attempt 1:39495 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys desktop switch use after free attempt 1:39496 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys ExtTextOut memory corrupt ion attempt 1:40410 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys ExtTextOut memory corrupt ion attempt 1:40411 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys GetDIBits out of bounds r ead attempt 1:40687 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys GetDIBits out of bounds r ead attempt 1:40688 Drop and generate OS-WINDOWS Microsoft Windows Win32k.sys MakeWindowForegroundWithS tate null pointer dereference attempt 1:39193 Drop and generate OS-WINDOWS Microsoft Windows Win32k.sys MakeWindowForegroundWithS tate null pointer dereference attempt 1:39194 Drop and generate OS-WINDOWS Microsoft Windows Win32k.sys MakeWindowForegroundWithS tate null pointer dereference attempt 1:39195 Drop and generate OS-WINDOWS Microsoft Windows Win32k.sys MakeWindowForegroundWithS tate null pointer dereference attempt 1:39196 Drop and generate OS-WINDOWS Microsoft Windows win32k.sys memory corruption attempt 1:48362 Drop and generate

events

events

events

events

events

events

OS-WINDOWS Microsoft Windows win32k.sys memory corruption attempt 1:48363 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys memory corruption attempt 1:48364 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys memory corruption attempt 1:48365 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys palette double free attempt 1:36970 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys palette double free attempt 1:36971 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys PathToRegion buffer overf low attempt 1:38487 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys PathToRegion buffer overf low attempt 1:38488 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys privilege escalation atte mpt 1:45649 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys privilege escalation atte mpt 1:45650 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys privilege escalation atte mpt 1:48072 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys privilege escalation atte mpt 1:48073 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys privilege escalation atte mpt 1:46538 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32k.sys sbit\_Embolden use after f ree attempt 1:40428 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32k.sys TrueType font out of boun ds write attempt 1:44335 Drop and generate

events

OS-WINDOWS Microsoft Windows win32k.sys use after free attempt 1: 44833 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kbase bOutline out of bounds re ad attempt 1:39841 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kbase bOutline out of bounds re ad attempt 1:39842 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32kfull FloodFillWindow privilege escalation attempt 1:39814 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32kfull FloodFillWindow privilege escalation attempt 1:39815 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys device context use af ter free attempt 1:38808 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys device context use af ter free attempt 1:38809 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys FBitsTouch use after free attempt 1:40380 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys FBitsTouch use after free attempt 1:40381 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys font object use after free attempt 1:38761 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys font object use after free attempt 1:38762 Drop and generate OS-WINDOWS Microsoft Windows win32kfull.sys MegSetLensContextInfo rmation use after free attempt 1:40685 Drop and generate OS-WINDOWS Microsoft Windows win32kfull.sys MegSetLensContextInfo rmation use after free attempt 1:40686 Drop and generate OS-WINDOWS Microsoft Windows win32kfull.sys NtGdiExtFloodFill use after free attempt 1:39217 Drop and generate

events

events

events

events

OS-WINDOWS Microsoft Windows win32kfull.sys NtGdiExtFloodFill use after free attempt 1:39218 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys out of bounds read at tempt 1:39516 Drop and generate

events

OS-WINDOWS Microsoft Windows win32kfull.sys out of bounds read at tempt 1:39517 Drop and generate

events

OS-WINDOWS Microsoft Windows Win32kfull.sys privilege escalation attempt 1:44514 Drop and generate

events

OS-WINDOWS Microsoft Windows wind32kfull.sys out of bounds write attempt 1:37584 Drop and generate

events

OS-WINDOWS Microsoft Windows wind32kfull.sys out of bounds write attempt 1:37585 Drop and generate OS-WINDOWS Microsoft Windows WMI DCOM arbitrary .NET serializatio n code execution attempt 1:42185 Drop and generate OS-WINDOWS Microsoft Windows WmipReceiveNotifications out of boun ds write attempt 1:37567 Drop and generate

events

events

events

OS-WINDOWS Microsoft Windows WmipReceiveNotifications out of boun ds write attempt 1:37568 Drop and generate

events

OS-WINDOWS Microsoft Windows WPAD spoofing attempt 1:39227 Drop and generate

events

OS-WINDOWS TRUFFLEHUNTER TALOS-2015-0005 attack attempt 3:36222 Drop and generate

events

OS-WINDOWS TRUFFLEHUNTER TALOS-CAN-0056 attack attempt 3:36218 Drop and generate

events

OS-WINDOWS TRUFFLEHUNTER TALOS-CAN-0056 attack attempt 3:36220 Drop and generate

events

OS-WINDOWS Type one font out of bounds memory access attempt 1:33 711 Drop and generate

events

OS-WINDOWS Type one font out of bounds memory access attempt 1:33 712 Drop and generate

events

OS-WINDOWS Windows NTFS NtfsFindExistingLcb denial of service att empt 1:46466 Drop and generate

events

OS-WINDOWS Windows NTFS NtfsFindExistingLcb denial of service att empt 1:46467 Drop and generate

events

POLICY-OTHER Adobe ColdFusion admin API access attempt 1:25976 Drop and generate

events

POLICY-OTHER Adobe ColdFusion admin interface access attempt 1:25 975 Drop and generate

events

POLICY-OTHER Adobe ColdFusion component browser access attempt 1: 25977 Drop and generate

events

POLICY-OTHER CoinHive Miner client detected 1:45266 Drop and generate

events

POLICY-OTHER CoinHive Miner client detected 1:45268 Drop and generate

events

POLICY-OTHER CoinHive Miner Javascript library download detected 1:45267 Drop and generate

events

POLICY-OTHER cryptomining javascript client detected 1:47253 Drop and generate

events

POLICY-OTHER cryptomining javascript client detected 1:45265 Drop and generate

events

POLICY-OTHER Magecart js page injection attempt 1:47914 Drop and generate

events

POLICY-OTHER Magecart js page injection attempt 1:47915 Drop and generate

events

POLICY-OTHER Magecart redirect page detected 1:47913 Drop and generate

events

POLICY-OTHER McAfee Virus Scan Linux outdated version detected 1: 41515 Drop and generate

events

POLICY-OTHER TRUFFLEHUNTER TALOS-2017-0411 attack attempt 3:44012 Drop and generate

events

POLICY-SOCIAL Pidgin MSN MSNP2P message integer overflow attempt 3:14263 Drop and generate

events

PROTOCOL-DNS ISC BIND isc buffer\_add assertion failure denial of service attempt 1:40344 Drop and generate

events

PROTOCOL-OTHER MiniUPNP rootdesc.xml buffer overflow attempt 1:35 690 Drop and generate

events

PROTOCOL-OTHER TRUFFLEHUNTER SFVRT-1018 attack attempt 3:35054 Drop and generate

events

PROTOCOL-OTHER TRUFFLEHUNTER SFVRT-1018 attack attempt 3:35055 Drop and generate

events

PROTOCOL-OTHER TRUFFLEHUNTER SFVRT-1018 attack attempt 3:35056 Drop and generate

events

PROTOCOL-OTHER TRUFFLEHUNTER SFVRT-1018 attack attempt 3:35057 Drop and generate

events

PROTOCOL-TELNET Microsoft Telnet Server buffer overflow attempt 1 :33050 Drop and generate

events

PROTOCOL-VOIP Cisco Unified IP phone BVSMWeb portal attack attemp t 3:31398 Generate events

PUA-ADWARE Amonetize installer outbound connection attempt 1:2892 9 Drop and generate

events

PUA-ADWARE Apponic CIS file retrieval attempt 1:28883 Drop and generate

events

PUA-ADWARE Apponic encapsulated installer outbound connection 1:2 8884 Drop and generate

events

PUA-ADWARE Apponic encapsulated installer outbound connection 1:2 8885 Drop and generate

events

PUA-ADWARE FakeAV runtime detection 1:28324 Drop and generate

events

PUA-ADWARE IP address disclosure to advertisement sites attempt 1 :19998 Drop and generate

events

PUA-ADWARE Lucky Leap Adware outbound connection 1:30260 Drop and generate

events

PUA-ADWARE Lucky Leap Adware outbound connection 1:30261 Drop and generate

events

PUA-ADWARE Magic Downloader BHO variant outbound connection 1:475 35 Drop and generate

events

PUA-ADWARE Magic Downloader BHO variant outbound connection 1:475 36 Drop and generate

events

PUA-ADWARE Slimware Utilities variant outbound connection 1:46486 Drop and generate

events

PUA-ADWARE Slimware Utilities variant outbound connection 1:47417 Drop and generate

events

PUA-ADWARE Slimware Utilities variant outbound connection 1:47418 Drop and generate

events

PUA-ADWARE SoftPulse variant HTTP response attempt 1:33212 Drop and generate

events

PUA-ADWARE UpdateStar CIS file retrieval attempt 1:28371 Drop and generate

events

PUA-ADWARE UpdateStar encapsulated installer outbound connection 1:28372 Drop and generate

events

PUA-ADWARE Wajam outbound connection - post install 1:28279 Drop and generate

events

PUA-ADWARE Wajam outbound connection - post install 1:28280 Drop and generate

events

PUA-ADWARE Win.Adware.CloseApp variant outbound connection 1:3108 9 Drop and generate

events

PUA-ADWARE Win.Adware.Dealply outbound POST attempt 1:37642 Drop and generate

events

PUA-ADWARE Win.Adware.Gamevance variant outbound connection 1:333 04 Drop and generate PUA-ADWARE Win.Adware.Inbox/PCFixSpeed/RebateInformer variant out bound connection 1:31091 Drop and generate PUA-ADWARE Win.Adware.InstallMonster variant outbound connection 1:33483 Drop and generate

events

events

events

PUA-ADWARE Win.Adware.OpenSoftwareUpdater variant outbound connec tion attempt 1:38951 Drop and generate

events

PUA-ADWARE Win.Adware.OpenSoftwareUpdater variant outbound connec tion attempt 1:38952 Drop and generate

events

PUA-ADWARE Win.Adware.OpenSoftwareUpdater variant outbound connec tion attempt 1:38953 Drop and generate

events

PUA-ADWARE Win.Pua.Softonic installer variant outbound connection 1:46874 Drop and generate

events

PUA-OTHER Authedmine TLS client hello attempt 1:45952 Drop and generate

events

PUA-OTHER Authedmine TLS server hello attempt 1:45951 Drop and generate

events

PUA-OTHER CoinHive Miner client detected 1:46365 Drop and generate

events

PUA-OTHER Coinhive TLS client hello attempt 1:45950 Drop and generate

events

PUA-OTHER Coinhive TLS server hello attempt 1:45949 Drop and generate

events

PUA-OTHER CPUMiner-Multi cryptocurrency mining pool connection at tempt 1:45550 Drop and generate

events

PUA-OTHER Cryptocurrency Miner outbound connection attempt 1:4623 7 Drop and generate

events

PUA-OTHER CryptoNight webassembly download attempt 1:46366 Drop and generate

events

PUA-OTHER Mineralt JavaScript cryptocurrency mining attempt 1:464 13 Drop and generate

events

PUA-OTHER Mineralt JavaScript cryptocurrency mining attempt 1:464 14 Drop and generate

events

PUA-OTHER Mineralt TLS client hello attempt 1:46410 Drop and generate

events

PUA-OTHER Mineralt TLS server hello attempt 1:46411 Drop and generate

events

PUA-OTHER Moonify Miner client detected 1:46370 Drop and generate

events

PUA-OTHER Moonify TLS client hello attempt 1:46372 Drop and generate

events

PUA-OTHER Moonify TLS server hello attempt 1:46371 Drop and generate

events

PUA-OTHER obfuscated cryptomining javascript download attempt 1:4 6415 Drop and generate

events

PUA-OTHER Request for known malware domain pierrejb.agora.eu.org 1:32578 Drop and generate

events

PUA-OTHER XMR-Stak cryptocurrency mining pool connection attempt 1:45825 Drop and generate

events

PUA-OTHER XMRig cryptocurrency mining pool connection attempt 1:4 5549 Drop and generate

events

PUA-OTHER XMRMiner cryptocurrency mining pool connection attempt 1:45955 Drop and generate

events

PUA-TOOLBARS WidgiToolbar toolbar runtime detection 1:44889 Drop and generate

events

PUA-TOOLBARS Win.Toolbar.Crossrider variant outbound connection 1 :33452 Drop and generate

events

PUA-TOOLBARS Win.Toolbar.Crossrider variant outbound connection 1 :39189 Drop and generate

events

SERVER-APACHE Apache Struts allowStaticMethodAccess invocation at tempt 1:21073 Drop and generate

events

SERVER-APACHE Apache Struts allowStaticMethodAccess invocation at tempt 1:29859 Drop and generate

events

SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt 1:27575 Drop and generate

events

SERVER-APACHE Apache Struts java.net.Socket class access attempt 1:47689 Drop and generate

events

SERVER-APACHE Apache Struts OGNL getRuntime.exec static method ac cess attempt 1:47634 Drop and generate

events

SERVER-APACHE Apache Struts OGNL getRuntime.exec static method ac cess attempt 1:27574 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt - Debug gingInterceptor 1:21075 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt - GET p arameter 1:21072 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt - GET p arameter 1:21656 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt - POST parameter 1:23631 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt 1:41923 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt 1:39190 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt 1:39191 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt 1:41922 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt 1:41818 Drop and generate

events

SERVER-APACHE Apache Struts remote code execution attempt 1:41819 Drop and generate SERVER-APACHE Apache Struts wildcard matching OGNL remote code ex ecution attempt 1:27572 Drop and generate SERVER-APACHE Apache Struts wildcard matching OGNL remote code ex ecution attempt 1:27573 Drop and generate SERVER-APACHE Apache Struts xslt.location local file inclusion at tempt 1:40359 Drop and generate

events

events

events

events

SERVER-APACHE Apache Struts2 blacklisted method redirect 1:27244 Drop and generate

events

SERVER-APACHE Apache Struts2 blacklisted method redirect 1:29747 Drop and generate

events

SERVER-APACHE Apache Struts2 blacklisted method redirect 1:29748 Drop and generate

events

SERVER-APACHE Apache Struts2 blacklisted method redirectAction 1: 27243 Drop and generate

events

SERVER-APACHE Apache Struts2 remote code execution attempt 1:2724 5 Drop and generate SERVER-APACHE Apache Tomcat Java JmxRemoteLifecycleListener unaut horized serialized object attempt 1:46071 Drop and generate SERVER-APACHE Apache Tomcat remote JSP file upload attempt 1:4453 1 Drop and generate

events

events

events

SERVER-IIS Microsoft ASP.NET viewstate DoS attempt 3:15959 Drop and generate SERVER-MAIL IBM Lotus Domino Server nrouter.exe malformed GIF par sing remote exploit attempt 1:39654 Drop and generate SERVER-ORACLE Oracle WebLogic Server remote command execution att empt 1:45304 Drop and generate

events

events

events

SERVER-OTHER Advantech WebAccess DCERPC heap buffer overflow atte mpt 1:41882 Drop and generate

events

SERVER-OTHER Advantech WebAccess DCERPC stack buffer overflow att empt 1:40008 Drop and generate

events

SERVER-OTHER Advantech WebAccess DCERPC stack buffer overflow att empt 1:41846 Drop and generate

events

SERVER-OTHER Advantech WebAccess DCERPC stack buffer overflow att empt 1:41847 Drop and generate

events

SERVER-OTHER Advantech WebAccess DCERPC stack buffer overflow att empt 1:41848 Drop and generate

events

SERVER-OTHER Advantech WebAccess DCERPC stack buffer overflow att empt 1:41849 Drop and generate

events

SERVER-OTHER Apache mod\_auth\_digest out of bounds read attempt 1: 43790 Drop and generate

events

SERVER-OTHER Apache Struts allowStaticMethodAccess invocation att empt 1:26824 Drop and generate

events

SERVER-OTHER Apache Struts allowStaticMethodAccess invocation att empt 1:26825 Drop and generate

events

SERVER-OTHER Apache Struts2 skillName remote code execution attempt 1:26772 Drop and generate

events

SERVER-OTHER Apple CUPS SGI image decoding buffer overflow attemp t 1:17663 Drop and generate

events

SERVER-OTHER AuraCMS LFI attempt 1:31161 Drop and generate

events

SERVER-OTHER Cisco ASA VPN aggregateAuthDataHandler double free attempt 3:45596 Drop and generate

events

SERVER-OTHER Cisco ASA VPN aggregateAuthDataHandler double free attempt 3:45575 Drop and generate

events

SERVER-OTHER Cisco ASR1001 IKEv2 memory leak attempt 3:46110 Drop and generate SERVER-OTHER Cisco prime collaboration provisioning web framework access control bypass attempt 3:40287 Drop and generate SERVER-OTHER Cisco RV Series Router information disclosure attemp t 3:47707 Drop and generate

events

events

events

SERVER-OTHER Cisco RV180 VPN CSRF attempt 3:30929 Drop and generate

events

SERVER-OTHER Cisco RV180 VPN remote code execution attempt 3:3093 3 Drop and generate

events

SERVER-OTHER Cisco RV180W remote file inclusion attempt 3:30931 Drop and generate

events

SERVER-OTHER Cisco Small Business SPA3x/5x series denial of servi ce attempt 3:40006 Drop and generate

events

SERVER-OTHER Cisco Smart Install init discovery message stack buf fer overflow attempt 1:46096 Drop and generate SERVER-OTHER Cisco Smart Install invalid init discovery message d enial of service attempt 1:46468 Drop and generate SERVER-OTHER Cisco Tshell command injection attempt 3:30887 Drop and generate

events

events

events

SERVER-OTHER Cisco Tshell command injection attempt 3:30888 Drop and generate

events

SERVER-OTHER CMSimple remote file inclusion attempt 1:30996 Drop and generate

events

SERVER-OTHER Flexense Syncbreeze buffer overflow attempt 1:45926 Drop and generate

events

SERVER-OTHER HP AutoPass License Server CommunicationServlet dire ctory traversal attempt 1:31525 Drop and generate SERVER-OTHER HP AutoPass License Server CommunicationServlet dire ctory traversal attempt 1:31526 Drop and generate SERVER-OTHER HP Integrated Lights-Out HTTP headers processing buf fer overflow attempt 1:45682 Drop and generate SERVER-OTHER HP ProCurve Manager SNAC UpdateCertificatesServlet d irectory traversal attempt 1:27937 Drop and generate SERVER-OTHER HP ProCurve Manager SNAC UpdateDomainControllerServl et directory traversal attempt 1:27941 Drop and generate SERVER-OTHER IBM Domino LDAP server ModifyRequest stack buffer ov erflow attempt 3:36153 Drop and generate

events

events

events

events

events

events

SERVER-OTHER ISC BIND 9 DNS query overly long name denial of serv ice attempt 1:40579 Drop and generate

events

SERVER-OTHER Jackson databind deserialization remote code executi on attempt 1:45778 Drop and generate

events

SERVER-OTHER Jackson databind deserialization remote code executi on attempt 1:45779 Drop and generate

events

SERVER-OTHER Java Library CommonsCollection unauthorized serializ ed object attempt 1:36826 Drop and generate

events

SERVER-OTHER JBoss EJBInvokerServlet remote code execution attemp t 1:28851 Drop and generate

events

SERVER-OTHER JBoss JMXInvokerServlet remote code execution attemp t 1:29909 Drop and generate

events

SERVER-OTHER JBoss Richfaces expression language injection attemp t 1:47829 Drop and generate

events

SERVER-OTHER Joomla com\_maqmahelpdesk task parameter local file i nclusion attempt 1:23182 Drop and generate

events

SERVER-OTHER Magento unauthenticated arbitrary file write attempt 1:43109 Drop and generate

events

SERVER-OTHER Magento unauthenticated arbitrary file write attempt 1:39066 Drop and generate SERVER-OTHER Mediabridge Medialink MWN-WAPR300N and Tenda N3 Wire less N150 inbound admin attempt 1:38729 Drop and generate SERVER-OTHER Microsoft LDAP MaxBuffSize buffer overflow attempt 1 :42160 Drop and generate

events

events

events

SERVER-OTHER Mikrotik RouterOS directory traversal attempt 3:4768 4 Drop and generate

events

SERVER-OTHER MiniUPnPd ExecuteSoapAction buffer overflow attempt 1:25780 Drop and generate SERVER-OTHER MIT Kerberos ASN.1 asn1\_decode\_generaltime uninitial ized pointer reference attempt 3:17741 Drop and generate SERVER-OTHER Mitsubishi Electric E-Designer font field buffer ove rflow attempt 1:46925 Drop and generate

events

events

events

SERVER-OTHER Mitsubishi Electric E-Designer font field buffer ove rflow attempt 1:46926 Drop and generate

events

SERVER-OTHER Mitsubishi Electric E-Designer Status\_bit buffer ove rflow attempt 1:46923 Drop and generate

events

SERVER-OTHER Mitsubishi Electric E-Designer Status\_bit buffer ove rflow attempt 1:46924 Drop and generate

events

SERVER-OTHER Multi-Router Looking Glass remote command injection attempt 1:31741 Drop and generate

events

SERVER-OTHER NTP arbitrary pidfile and driftfile overwrite attemp t 1:37526 Drop and generate

events

SERVER-OTHER NTPD zero origin timestamp denial of service attempt 1:41367 Drop and generate

events

SERVER-OTHER ntpq flagstr buffer overflow attempt 1:42887 Drop and generate

events

SERVER-OTHER NUUO NVRMini2 stack based buffer overflow attempt 1: 48235 Drop and generate

events

SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt 1:30549 Drop and generate

events

SERVER-OTHER OpenSSL OCSP Status Request Extension denial of serv ice attempt 1:40360 Drop and generate SERVER-OTHER OpenSSL SSLv3 heartbeat read overrun attempt - vulne rable client response 1:30520 Drop and generate SERVER-OTHER OpenSSL SSLv3 heartbeat read overrun attempt 1:30510 Drop and generate SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ss l heartbleed attempt 1:30777 Drop and generate SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ss l heartbleed attempt 1:30778 Drop and generate SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ss l heartbleed attempt 1:30785 Drop and generate SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ss l heartbleed attempt 1:30514 Drop and generate SERVER-OTHER OpenSSL SSLv3 warning denial of service attempt 1:40 843 Drop and generate SERVER-OTHER OpenSSL TLSv1 heartbeat read overrun attempt - vulne rable client response 1:30521 Drop and generate SERVER-OTHER OpenSSL TLSv1 heartbeat read overrun attempt 1:30511 Drop and generate SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ss l heartbleed attempt 1:30779 Drop and generate SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ss l heartbleed attempt 1:30780 Drop and generate SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ss l heartbleed attempt 1:30786 Drop and generate SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ss l heartbleed attempt 1:30515 Drop and generate SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt - vul nerable client response 1:30522 Drop and generate SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt 1:305 24 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

events

SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt 1:305 12 Drop and generate SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt 1:30781 Drop and generate SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt 1:30782 Drop and generate SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt 1:30787 Drop and generate SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt 1:30516 Drop and generate SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt - vul nerable client response 1:30523 Drop and generate

events

events

events

events

events

events

SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt 1:305 13 Drop and generate

events

SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt 1:30783 Drop and generate SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt 1:30784 Drop and generate SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt 1:30788 Drop and generate SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt 1:30517 Drop and generate SERVER-OTHER Oracle WebLogic unsafe deserialization remote code e xecution attempt detected 1:46445 Drop and generate SERVER-OTHER Oracle Weblogic unsafe deserialization remote code e xecution attempt detected 1:46446 Drop and generate SERVER-OTHER PostgreSQL Empty Password authentication bypass atte mpt 1:46449 Drop and generate

events

events

events

events

events

events

events

SERVER-OTHER Quest Appliance NetVault Backup buffer overflow atte mpt 1:46474 Drop and generate

events

SERVER-OTHER SAP NetWeaver dir content listing attempt 1:30928 Drop and generate

events

SERVER-OTHER Spring Data Commons remote code execution attempt 1: 46473 Drop and generate

events

SERVER-OTHER Symantec Endpoint Protection Manager cross site requ est forgery attempt 1:39404 Drop and generate SERVER-OTHER TLS client hello session resumption detected 3:41547 Generate events

events

SERVER-OTHER TopSec Firewall cookie header command injection atte mpt 1:42232 Drop and generate

events

SERVER-OTHER Trend Micro local node.js http command execution att empt 1:37285 Drop and generate

events

SERVER-OTHER Trend Micro local node.js http command execution att empt 1:37286 Drop and generate

events

SERVER-OTHER Trend Micro local node.js http command execution att empt 1:37287 Drop and generate

events

SERVER-OTHER TRUFFLEHUNTER SFVRT-1008 attack attempt 100173 3:176 82 Drop and generate

events

SERVER-OTHER TRUFFLEHUNTER TALOS-2017-0379 attack attempt 3:43558 Generate events

SERVER-OTHER TRUFFLEHUNTER TALOS-2017-0421 attack attempt 3:44189 Drop and generate

events

SERVER-OTHER TRUFFLEHUNTER TALOS-2018-0627 attack attempt 3:47234 Drop and generate

events

SERVER-OTHER Wordpress CMS platform denial of service attempt 1: 45598 Drop and generate

events

SERVER-OTHER Wordpress linenity theme LFI attempt 1:30769 Drop and generate

events

SERVER-OTHER Xerox DocuShare SQL injection attempt 1:31300 Drop and generate

events

SERVER-SAMBA Microsoft Windows SMBv2/SMBv3 Buffer Overflow attemp t 1:41499 Drop and generate

events

SERVER-SAMBA Samba is\_known\_pipe arbitrary module load code execu tion attempt 1:43004 Drop and generate

events

SERVER-WEBAPP /etc/passwd file access attempt 1:31289 Drop and generate

events

SERVER-WEBAPP Advantech WebAccess Dashboard remote code execution attempt 1:41026

SERVER-WEBAPP AlienVault OSSIM av-centerd get\_license command inj ection attempt 1:31505 Drop and generate

events

SERVER-WEBAPP AlienVault OSSIM av-centerd get\_log\_line command in jection attempt 1:31506 Drop and generate SERVER-WEBAPP AlienVault OSSIM av-centerd update\_system\_info\_debi an\_package command injection attempt 1:31330 Drop and generate SERVER-WEBAPP AlienVault OSSIM nfsen.php command injection attemp t 1:43534 Drop and generate

events

events

events

SERVER-WEBAPP AlienVault OSSIM nfsen.php command injection attemp t 1:43535 Drop and generate

events

SERVER-WEBAPP AlienVault OSSIM nfsen.php command injection attemp t 1:43536 Drop and generate

events

SERVER-WEBAPP AlienVault OSSIM remote\_task command injection atte mpt 1:31823 Drop and generate

events

SERVER-WEBAPP Allen-Bradley Compact Logix cross site scripting at tempt 1:37622 Drop and generate

events

SERVER-WEBAPP Allen-Bradley Compact Logix cross site scripting at tempt 1:37623 Drop and generate

events

SERVER-WEBAPP Allen-Bradley Compact Logix cross site scripting at tempt 1:37624 Drop and generate SERVER-WEBAPP Apache Commons Library FileUpload unauthorized Java object upload attempt 1:41390 Drop and generate SERVER-WEBAPP Apache Struts remote code execution attempt 1:47649 Drop and generate SERVER-WEBAPP Arcserve Unified Data Protection export servlet dir ectory traversal attempt 1:34878 Drop and generate SERVER-WEBAPP Arcserve Unified Data Protection export servlet dir ectory traversal attempt 1:34879 Drop and generate SERVER-WEBAPP Arcserve Unified Data Protection export servlet dir ectory traversal attempt 1:34880 Drop and generate SERVER-WEBAPP Arcserve Unified Data Protection reportFileServlet directory traversal attempt 1:34881 Drop and generate SERVER-WEBAPP Arcserve Unified Data Protection reportFileServlet directory traversal attempt 1:34882 Drop and generate SERVER-WEBAPP Arcserve Unified Data Protection reportFileServlet directory traversal attempt 1:34883 Drop and generate SERVER-WEBAPP Arris VAP2500 tools\_command.php command execution attempt 1:32742 Drop and generate

events

events

events

events

events

events

events

events

events

events

SERVER-WEBAPP Avtech IP Camera unauthenticated config access atte mpt 1:40446 Drop and generate

events

SERVER-WEBAPP Axis M3004 remote code execution attempt 1:43625 Drop and generate

events

SERVER-WEBAPP BA Systems BAS Web information disclosure attempt 1 :46805 Drop and generate

events

SERVER-WEBAPP BA Systems BAS Web information disclosure attempt 1 :46806 Drop and generate

events

SERVER-WEBAPP Bassmaster Batch remote code execution attempt 1:40 865 Drop and generate SERVER-WEBAPP Beijing Hanbang Hanbanggaoke IP camera admin passwo rd change attempt 1:45314 Drop and generate SERVER-WEBAPP Belkin F9K1122 webpage buffer overflow attempt 1:40 047 Drop and generate

events

events

events

SERVER-WEBAPP Blueimp jQuery File Upload arbitrary PHP file uploa d attempt 1:48263 Drop and generate

events

SERVER-WEBAPP carel plantvisorpro3 directory traversal attempt 1: 41781 Drop and generate

events

SERVER-WEBAPP carel plantvisorpro3 directory traversal attempt 1: 41782 Drop and generate

events

SERVER-WEBAPP CCTV-DVR command injection attempt 1:47358 Drop and generate

events

SERVER-WEBAPP Centreon cmdGetExample.php SQL injection attempt 1: 35016 Drop and generate

events

SERVER-WEBAPP Centreon displayServiceStatus.php command injection attempt 1:32352 Drop and generate

events

SERVER-WEBAPP Centreon GetXMLTrapsForVendor.php SQL injection att empt 1:35014 Drop and generate

events

SERVER-WEBAPP Centreon GetXmlTree.php SQL injection attempt 1:350 15 Drop and generate

events

SERVER-WEBAPP Centreon makeXML\_ListMetrics.php SQL injection atte mpt 1:35017 Drop and generate

events

SERVER-WEBAPP CGit cgit\_clone\_objects function directory traversa l attempt 1:47464 Drop and generate

events

SERVER-WEBAPP CGit cgit\_clone\_objects function directory traversa l attempt 1:47465 Drop and generate

events

SERVER-WEBAPP CGit cgit\_clone\_objects function directory traversa l attempt 1:47466 Drop and generate

events

SERVER-WEBAPP Cisco ACS unsafe Java object deserialization attemp t 3:45870 Drop and generate

events

SERVER-WEBAPP Cisco ASA WebVPN memory corruption attempt 3:41538 Drop and generate

events

SERVER-WEBAPP Cisco ESA internal testing interface access attempt 3:40275 Drop and generate SERVER-WEBAPP Cisco FirePOWER Management Center sajaxintf.cgi com mand injection attempt 3:39897 Drop and generate SERVER-WEBAPP Cisco Firepower Management Console 6.0 local file i nclude attempt 1:41356 Drop and generate SERVER-WEBAPP Cisco Identity Services Engine default password aut hentication attempt 3:37358 Drop and generate SERVER-WEBAPP Cisco Integrated Management Controller and UCS Dire ctor directory traversal attempt 3:35941 Drop and generate SERVER-WEBAPP Cisco Meraki default admin credentials attempt 1:41 446 Drop and generate

events

events

events

events

events

events

SERVER-WEBAPP Cisco NX-OS NX-API privilege escalation attempt 3:4 6992 Drop and generate SERVER-WEBAPP Cisco Prime Data Center Network Manager FileUploadS ervlet arbitrary file upload attempt 1:29141 Drop and generate SERVER-WEBAPP Cisco Prime Data Center Network Manager FileUploadS ervlet arbitrary file upload attempt 1:29142 Drop and generate SERVER-WEBAPP Cisco Prime Data Center Network Manager processImag eSave.jsp directory traversal attempt 1:29041 Drop and generate SERVER-WEBAPP Cisco Prime Data Center Network Manager processImag eSave.jsp directory traversal attempt 1:29042 Drop and generate SERVER-WEBAPP Cisco TelePresence command injection attempt 3:4767 9 Drop and generate

events

events

events

events

events

events

SERVER-WEBAPP Cisco TelePresence command injection attempt 3:4768 0 Drop and generate

events

SERVER-WEBAPP Cisco UCS Central Web Framework remote file include attempt 3:38543 Drop and generate

events

SERVER-WEBAPP Cisco Unified MeetingPlace password change policy b ypass attempt 3:35347 Drop and generate

events

SERVER-WEBAPP Cisco WebEx Meetings Server command injection attempt 3:36913 Drop and generate SERVER-WEBAPP Cisco WebEx Meetings Server config\_dmz remote code execution attempt 3:40240 Drop and generate SERVER-WEBAPP D-Link DCS-900 Series Network Camera arbitrary file upload attempt 1:37242 Drop and generate

events

events

events

SERVER-WEBAPP D-Link DIR Series Routers HNAP stack buffer overflo w attempt 1:40750 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt 1:48141 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt 1:48142 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt 1:48143 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt 1:48172 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt 1:48173 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt 1:48174 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt 1 :48097 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt 1 :48098 Drop and generate

events

SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt 1 :48099 Drop and generate

events

SERVER-WEBAPP D-Link DSL-2750B routers login.cgi command injectio n attempt 1:46735 Drop and generate

events

SERVER-WEBAPP D-Link DSL-2750B routers login.cgi command injectio n attempt 1:46736 Drop and generate

events

SERVER-WEBAPP D-Link DSL-2750B routers login.cgi command injectio n attempt 1:46737 Drop and generate

events

SERVER-WEBAPP D-Link hedwig.cgi directory traversal attempt 1:444 54 Drop and generate SERVER-WEBAPP D-Link hedwig.cgi NTP service configuration command injection attempt 1:44453 Drop and generate SERVER-WEBAPP D-Link multiple products HNAP SOAPAction header com mand injection attempt 1:34300 Drop and generate SERVER-WEBAPP D-Link router unauthorised DNS change attempt 1:391 92 Drop and generate

events

events

events

events

SERVER-WEBAPP DD-WRT httpd cgi-bin remote command execution attempt 1:26275 Drop and generate SERVER-WEBAPP Dell SonicWall GMS set\_time\_config XMLRPC method co mmand injection attempt 1:39743 Drop and generate SERVER-WEBAPP Delta IEM DIAEnergie file upload attempt 1:45250 Drop and generate

events

events

events

SERVER-WEBAPP Dicoogle directory traversal attempt 1:47664 Drop and generate

events

SERVER-WEBAPP Drupal 8 remote code execution attempt 1:46316 Drop and generate

events

SERVER-WEBAPP Drupal Coder Module insecure remote file deserializ ation attempt 1:39645 Drop and generate

events

SERVER-WEBAPP Drupal RESTWS restws\_page\_callback command injectio n attempt 1:39725 Drop and generate

events

SERVER-WEBAPP Drupal RESTWS restws\_page\_callback command injectio n attempt 1:39726 Drop and generate

events

SERVER-WEBAPP Drupal unsafe internal attribute remote code execut ion attempt 1:46451 Drop and generate

events

SERVER-WEBAPP Embedded php in Exif data upload attempt 1:30249 Drop and generate

events

SERVER-WEBAPP Embedthis GoAhead CGI information disclosure attemp t 1:45218 Drop and generate

events

SERVER-WEBAPP Embedthis GoAhead LD\_preload code execution attempt 1:45219 Drop and generate SERVER-WEBAPP EMC Connectrix Manager FileUploadController directo ry traversal attempt 1:29390 Drop and generate SERVER-WEBAPP EMC Connectrix Manager FileUploadController directo ry traversal attempt 1:29391 Drop and generate SERVER-WEBAPP EMC Connectrix Manager FileUploadController directo ry traversal attempt 1:29392 Drop and generate SERVER-WEBAPP EMC Connectrix Manager ManualBootImageUpload direct ory traversal attempt 1:29485 Drop and generate SERVER-WEBAPP EMC Connectrix Manager ManualBootImageUpload direct ory traversal attempt 1:29486 Drop and generate SERVER-WEBAPP EMC Connectrix Manager ManualBootImageUpload direct ory traversal attempt 1:29487 Drop and generate SERVER-WEBAPP EMC Connectrix Manager ManualBootImageUpload direct ory traversal attempt 1:29488 Drop and generate SERVER-WEBAPP Fireeye Java decompiler reflection remote code exec ution attempt 1:37135 Drop and generate

events

events

events

events

events

events

events

events

events

SERVER-WEBAPP Fireeye Java decompiler reflection remote code exec ution attempt 1:37137 Drop and generate

events

SERVER-WEBAPP Fortinet FortiOS redir parameter cross site scripti ng attempt 1:45401 Drop and generate SERVER-WEBAPP FreePBX Framework Asterisk recording interface PHP unserialize code execution attempt 1:32753 Drop and generate SERVER-WEBAPP GE MDS PulseNet hidden credentials authentication attempt 1:36272 Drop and generate

events

events

events

SERVER-WEBAPP GPON Router authentication bypass and command injec tion attempt 1:46624 Drop and generate

events

SERVER-WEBAPP GPON Router authentication bypass and command injec tion attempt 1:46625 Drop and generate

events

SERVER-WEBAPP GPON Router authentication bypass and command injec tion attempt 1:46626 Drop and generate

events

SERVER-WEBAPP GPON Router authentication bypass and command injec tion attempt 1:46627 Drop and generate

events

SERVER-WEBAPP HNAP remote code execution attempt 1:29829 Drop and generate SERVER-WEBAPP HP Enterprise Vertica validateAdminConfig command i njection attempt 1:38879 Drop and generate

events

events

SERVER-WEBAPP HP IMC perfAccessMgrServlet arbitrary Java object d eserialization attempt 1:45885 Drop and generate

events

SERVER-WEBAPP HP IMC TopoMsgServlet arbitrary Java object deseria lization attempt 1:45748 Drop and generate

events

SERVER-WEBAPP HP IMC WebDM arbitrary Java object deserialization attempt 1:45617 Drop and generate SERVER-WEBAPP HP Intelligent Management Center BIMS UploadServlet arbitrary file upload attempt 1:28407 Drop and generate SERVER-WEBAPP HP LoadRunner Virtual User Generator EmulationAdmin directory traversal attempt 1:29017 Drop and generate SERVER-WEBAPP HP LoadRunner Virtual User Generator EmulationAdmin directory traversal attempt 1:29019 Drop and generate SERVER-WEBAPP HP System Management arbitrary command injection at tempt 1:27104 Drop and generate

events

events

events

events

events

SERVER-WEBAPP HP System Management arbitrary command injection at tempt 1:27105 Drop and generate

events

SERVER-WEBAPP Huawei DeviceUpgrade command injection attempt 1:45 117 Drop and generate SERVER-WEBAPP IBM OpenAdmin Tool SOAP welcomeService.php PHP code injection attempt 1:43147 Drop and generate SERVER-WEBAPP Java Library CommonsCollection unauthorized seriali zed object attempt 1:37859 Drop and generate SERVER-WEBAPP Java Library CommonsCollection unauthorized seriali zed object attempt 1:37860 Drop and generate SERVER-WEBAPP Java XML deserialization remote code execution atte mpt 1:44315 Drop and generate

events

events

events

events

events

SERVER-WEBAPP JBoss admin-console access 1:21517 Drop and generate

events

SERVER-WEBAPP JBoss JMX console access attempt 1:21516 Drop and generate

events

SERVER-WEBAPP JBoss JMXInvokerServlet access attempt 1:24343 Drop and generate

events

SERVER-WEBAPP JBoss web console access attempt 1:24342 Drop and generate

events

SERVER-WEBAPP Jenkins CI Server insecure deserialization command execution attempt 1:38894 Drop and generate SERVER-WEBAPP Jenkins Java SignedObject deserialization command e xecution attempt 1:45790 Drop and generate SERVER-WEBAPP Joomla DT Register SQL injection attempt 1:46333 Drop and generate

events

events

events

SERVER-WEBAPP Joomla DT Register SQL injection attempt 1:46334 Drop and generate

events

SERVER-WEBAPP Joomla JDatabaseDriverMysqli unserialize code execu tion attempt 1:37077 Drop and generate

events

SERVER-WEBAPP Joomla JDatabaseDriverMysqli unserialize code execu tion attempt 1:37078 Drop and generate

events

SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection att empt 1:46062 Drop and generate

events

SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection att empt 1:46063 Drop and generate

events

SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection att empt 1:46064 Drop and generate

events

SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injectio n attempt 1:46089 Drop and generate

events

SERVER-WEBAPP Joomla PostInstall Message SQL injection attempt 1: 47655 Drop and generate

events

SERVER-WEBAPP Joomla Proclaim biblestudy backup access attempt 1: 47613 Drop and generate

events

SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt 1:47 501 Drop and generate

events

SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt 1:47 502 Drop and generate

events

SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt 1:46337 Drop and generate

events

SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt 1:46338 Drop and generate SERVER-WEBAPP Joomla UsersController non-standard insecure accoun t registration method access attempt 1:40608 Drop and generate SERVER-WEBAPP Joomla UsersController non-standard insecure accoun t registration method access attempt 1:40609 Drop and generate SERVER-WEBAPP Kubernetes Kubelet arbitrary command execution atte mpt 3:46740 Drop and generate

events

events

events

events

SERVER-WEBAPP Kubernetes Kubelet arbitrary command execution atte mpt 3:46741 Drop and generate

events

SERVER-WEBAPP LifeSize UVC remote code execution attempt 1:30274 Drop and generate

events

SERVER-WEBAPP Linksys E-series HNAP TheMoon remote code execution attempt 1:29830 Drop and generate

events

SERVER-WEBAPP Linksys E-series HNAP TheMoon remote code execution attempt 1:29831 Drop and generate

events

SERVER-WEBAPP McAfee Virus Scan Linux cross site scripting attemp t 1:41521 Drop and generate

events

SERVER-WEBAPP McAfee Virus Scan Linux file existence test attempt 1:41516 Drop and generate

events

SERVER-WEBAPP McAfee Virus Scan Linux remote code execution attempt 1:41681 Drop and generate SERVER-WEBAPP Microsoft Office SharePoint malicious serialized vi ewstate evaluation attempt 1:27823 Drop and generate SERVER-WEBAPP Moxa AWK-3131A web application cross site scripting attempt 1:41102 Drop and generate

events

events

events

SERVER-WEBAPP Moxa AWK-3131A web application cross site scripting attempt 1:41103 Drop and generate

events

SERVER-WEBAPP Moxa AWK-3131A web application cross site scripting attempt 1:41104 Drop and generate

events

SERVER-WEBAPP Moxa AWK-3131A web application cross site scripting attempt 1:41105 Drop and generate

events

SERVER-WEBAPP Moxa MX Studio login page denial of service attempt 1:42222 Drop and generate

events

SERVER-WEBAPP Moxa private key disclosure attempt 1:42221 Drop and generate

events

SERVER-WEBAPP Multiple products DVR admin password leak attempt 1 :46825 Drop and generate

events

SERVER-WEBAPP Multiple routers getcfg.php credential disclosure attempt 1:44388 Drop and generate

events

SERVER-WEBAPP Nagios XI Incident Manager SQL injection attempt 3: 35930 Drop and generate

events

SERVER-WEBAPP Nagios XI Incident Manager SQL injection attempt 3: 35931 Drop and generate

events

SERVER-WEBAPP Nagios XI Incident Manager SQL injection attempt 3: 35932 Drop and generate SERVER-WEBAPP Netgear DGN1000 series routers arbitrary command ex ecution attempt 1:44688 Drop and generate SERVER-WEBAPP Netgear DGN1000 series routers authentication bypas s attempt 1:44687 Drop and generate

events

events

events

SERVER-WEBAPP Netgear DGN1000B setup.cgi parameter code execution attempt 1:29401 Drop and generate

events

SERVER-WEBAPP Netgear DGN1000B setup.cgi parameter code execution attempt 1:29402 Drop and generate SERVER-WEBAPP Netgear ReadyNAS Surveillance upgrade\_handle.php co mmand injection attempt 1:44471 Drop and generate SERVER-WEBAPP Netgear ReadyNAS Surveillance upgrade\_handle.php co mmand injection attempt 1:44472 Drop and generate SERVER-WEBAPP NetIQ Access Manager Identity Server directory trav ersal attempt 1:46348 Drop and generate

events

events

events

events

SERVER-WEBAPP NetIQ Access Manager Identity Server directory trav ersal attempt 1:46349 Drop and generate

events

SERVER-WEBAPP NetIQ Access Manager Identity Server directory trav ersal attempt 1:46350 Drop and generate SERVER-WEBAPP Oracle Application Testing Suite actionservlet dire ctory traversal attempt 1:38934 Drop and generate SERVER-WEBAPP Oracle Application Testing Suite directory traversa l attempt 1:38968 Drop and generate

events

events

events

SERVER-WEBAPP Oracle Application Testing Suite directory traversa l attempt 1:38969 Drop and generate

events

SERVER-WEBAPP Oracle Application Testing Suite directory traversa l attempt 1:38970 Drop and generate SERVER-WEBAPP Oracle application testing suite DownloadServlet di rectory traversal attempt 1:38789 Drop and generate SERVER-WEBAPP Oracle application testing suite DownloadServlet di rectory traversal attempt 1:38790 Drop and generate SERVER-WEBAPP Oracle application testing suite DownloadServlet di rectory traversal attempt 1:38791 Drop and generate SERVER-WEBAPP Oracle e-Business Suite HR\_UTIL\_DISP\_WEB SQL inject ion attempt 1:37687 Drop and generate SERVER-WEBAPP Oracle Fusion Middleware MapViewer arbitrary JSP fi le upload attempt 1:42951 Drop and generate SERVER-WEBAPP Oracle Fusion Middleware MapViewer directory traver sal attempt 1:42952 Drop and generate

events

events

events

events

events

events

events

SERVER-WEBAPP Oracle Fusion Middleware MapViewer directory traver sal attempt 1:42953 Drop and generate

events

SERVER-WEBAPP Oracle Fusion Middleware MapViewer directory traver sal attempt 1:42954 Drop and generate

events

SERVER-WEBAPP Oracle Identity Management authorization bypass att empt 3:35926 Drop and generate

events

SERVER-WEBAPP Oracle Identity Management remote file execution at tempt 3:35927 Drop and generate

events

SERVER-WEBAPP Oracle Weblogic default credentials login attempt 1 :40904 Drop and generate

events

SERVER-WEBAPP Oracle Weblogic default credentials login attempt 1 :40905 Drop and generate

events

SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload at tempt 1:47389 Drop and generate

events

SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload at tempt 1:47390 Drop and generate SERVER-WEBAPP Palo Alto Networks Firewall cms\_changeDeviceContext .esp session injection attempt 1:45236 Drop and generate SERVER-WEBAPP Palo Alto Networks Firewall router.php XML attribut e injection attempt 1:45235 Drop and generate

events

events

events

SERVER-WEBAPP PHPMailer command injection remote code execution attempt 1:41813 Drop and generate

events

SERVER-WEBAPP PHPMailer command injection remote code execution attempt 1:45917 Drop and generate

events

SERVER-WEBAPP PHPMailer command injection remote code execution attempt 1:41106 Drop and generate

events

SERVER-WEBAPP PHPUnit PHP remote code execution attempt 1:45749 Drop and generate SERVER-WEBAPP Pivotal Spring Data REST PATCH request remote code execution attempt 1:45976 Drop and generate SERVER-WEBAPP PrestaShop PS\_SAV\_IMAP\_URL command injection attemp t 1:48417 Drop and generate

events

events

events

SERVER-WEBAPP QNAP QCenter API account information disclosure att empt 1:47347 Drop and generate

events

SERVER-WEBAPP QNAP QCenter API set\_VM\_passwd command injection at tempt 1:47348 Drop and generate

events

SERVER-WEBAPP QNAP QCenter API set\_VM\_passwd command injection at tempt 1:47349 Drop and generate SERVER-WEBAPP Red Hat CloudForms agent controller filename direct ory traversal attempt 1:29296 Drop and generate SERVER-WEBAPP Red Hat CloudForms agent controller filename direct ory traversal attempt 1:29297 Drop and generate SERVER-WEBAPP RedHat JBoss Enterprise Application Platform JMX co de execution attempt 1:24642 Drop and generate SERVER-WEBAPP Reprise License Manager actserver stack buffer over flow attempt 1:38286 Drop and generate

events

events

events

events

events

SERVER-WEBAPP Reprise License Manager akey stack buffer overflow attempt 1:38287 Drop and generate

events

SERVER-WEBAPP Reprise License Manager licfile stack buffer overfl ow attempt 1:38288 Drop and generate

events

SERVER-WEBAPP RevSlider information disclosure attempt 1:34194 Drop and generate SERVER-WEBAPP Rocket Servergraph Admin Center userRequest and tsm Request command execution attempt 1:34948 Drop and generate SERVER-WEBAPP Rocket Servergraph Admin Center userRequest and tsm Request command execution attempt 1:34949 Drop and generate SERVER-WEBAPP Ruby on Rails arbitrary Ruby object deserialization attempt 1:33166 Drop and generate

events

events

events

events

SERVER-WEBAPP Ruby on Rails arbitrary Ruby object deserialization attempt 1:33167 Drop and generate

events

SERVER-WEBAPP SAP ConfigServlet command execution attempt 1:26929 Drop and generate

events

SERVER-WEBAPP Seagate NAS remote code execution attempt 1:33812 Drop and generate

events

SERVER-WEBAPP Siemens IP-Camera credential disclosure attempt 1:3 9930 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler BackupAssociationServlet SQ L injection attempt 1:43195 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler BackupAssociationServlet SQ L injection attempt 1:43196 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler BackupExceptionsServlet SQL injection attempt 1:39331 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler BackupExceptionsServlet SQL injection attempt 1:39332 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler BexDriveUsageSummaryServlet SQL injection attempt 1:39336 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler BexDriveUsageSummaryServlet SQL injection attempt 1:39337 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler DuplicateFilesServlet SQL i njection attempt 1:39333 Drop and generate

events

events

events

events

events

events

events

events

SERVER-WEBAPP SolarWinds SRM Profiler DuplicateFilesServlet SQL i njection attempt 1:39334 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler FileActionAssignmentServlet SQL injection attempt 1:43197 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler FileActionAssignmentServlet SQL injection attempt 1:43198 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler HostStorageServlet SQL inje ction attempt 1:43199 Drop and generate

events

events

events

events

SERVER-WEBAPP SolarWinds SRM Profiler HostStorageServlet SQL inje ction attempt 1:43200 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler NbuErrorMessageServlet SQL injection attempt 1:43201 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler NbuErrorMessageServlet SQL injection attempt 1:43202 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler ProcessesServlet SQL inject ion attempt 1:43203 Drop and generate

events

events

events

events

SERVER-WEBAPP SolarWinds SRM Profiler ProcessesServlet SQL inject ion attempt 1:43204 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler QuantumMonitorServlet SQL i njection attempt 1:43205 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler QuantumMonitorServlet SQL i njection attempt 1:43206 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler ScriptServlet SQL injection attempt 1:39335 Drop and generate

events

events

events

events

SERVER-WEBAPP SolarWinds SRM Profiler ScriptServlet SQL injection attempt 1:39338 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler UserDefinedFieldConfigServl et SQL injection attempt 1:43207 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler UserDefinedFieldConfigServl et SQL injection attempt 1:43208 Drop and generate SERVER-WEBAPP SolarWinds SRM Profiler WindowsEventLogsServlet SQL injection attempt 1:39339 Drop and generate

events

events

events

events

SERVER-WEBAPP SolarWinds SRM Profiler XiotechMonitorServlet SQL i njection attempt 1:43210 Drop and generate

events

SERVER-WEBAPP SonicWall Secure Remote Access diagnostics command injection attempt 1:43645 Drop and generate SERVER-WEBAPP SonicWall Secure Remote Access diagnostics command injection attempt 1:43646 Drop and generate SERVER-WEBAPP SonicWall Secure Remote Access diagnostics command injection attempt 1:43647 Drop and generate SERVER-WEBAPP SonicWall Secure Remote Access viewcert command inj ection attempt 1:43688 Drop and generate SERVER-WEBAPP SonicWall Secure Remote Access viewcert command inj ection attempt 1:43689 Drop and generate SERVER-WEBAPP SonicWall Secure Remote Access viewcert command inj ection attempt 1:43690 Drop and generate SERVER-WEBAPP Sophos Web Protection Appliance sblistpack arbitrar y command execution attempt 1:27942 Drop and generate SERVER-WEBAPP Spring Security OAuth remote code execution attempt 1:46823 Drop and generate SERVER-WEBAPP Supermicro Intelligent Management Controller close\_ window.cgi buffer overflow attempt 1:31210 Drop and generate SERVER-WEBAPP Supermicro Intelligent Management Controller close\_ window.cgi buffer overflow attempt 1:31211 Drop and generate SERVER-WEBAPP Symantec Critical System Protection directory trave rsal attempt 1:34471 Drop and generate

events

events

events

events

events

events

events

events

events

events

events

SERVER-WEBAPP Symantec Decomposer Engine Dec2LHA buffer overflow attempt 1:39400 Drop and generate

events

SERVER-WEBAPP Symantec SEPM management console cross site scripti ng attempt 1:39398 Drop and generate SERVER-WEBAPP Synology DiskStation Manager SLICEUPLOAD remote com mand execution attempt 1:29387 Drop and generate SERVER-WEBAPP SysAid Enterprise auth bypass and remote file uploa d attempt 1:43237 Drop and generate SERVER-WEBAPP Trend Micro Mobile Security Enterprise web\_service. dll SQL injection attempt 1:44571 Drop and generate SERVER-WEBAPP Trend Micro Mobile Security Enterprise web\_service. dll SQL injection attempt 1:44572 Drop and generate SERVER-WEBAPP Trend Micro Mobile Security Enterprise web\_service. dll SQL injection attempt 1:44573 Drop and generate SERVER-WEBAPP Trend Micro proxy\_controller.php command injection attempt 1:44359 Drop and generate

events

events

events

events

events

events

events

SERVER-WEBAPP Trend Micro proxy\_controller.php command injection attempt 1:44360 Drop and generate

events

SERVER-WEBAPP Trend Micro proxy\_controller.php command injection attempt 1:44361 Drop and generate SERVER-WEBAPP Trend Micro Threat Discovery Appliance logoff.cgi d irectory traversal attempt 1:42336 Drop and generate SERVER-WEBAPP Trend Micro widget system authentication bypass att empt 1:44582 Drop and generate

events

events

events

SERVER-WEBAPP Unitrends Enterprise Backup API SQL injection attempt 1:44657 Drop and generate

events

SERVER-WEBAPP Unitrends Enterprise Backup storage API command inj ection attempt 1:44658 Drop and generate

events

SERVER-WEBAPP UPnP AddPortMapping SOAP action command injection attempt 1:34799 Drop and generate

events

SERVER-WEBAPP Web Terria remote command execution attempt 1:31094 Drop and generate

events

SERVER-WEBAPP WebTester install2.php arbitrary command execution attempt 1:28288 Drop and generate SERVER-WEBAPP Western Digital MyCloud multi\_uploadify.php arbitra ry PHP file upload attempt 1:45479 Drop and generate SERVER-WEBAPP Western Digital MyCloud nas\_sharing.cgi backdoor ac count access attempt 1:45407 Drop and generate SERVER-WEBAPP WordPress get\_post authentication bypass attempt 1: 41495 Drop and generate

events

events

events

events

SERVER-WEBAPP WordPress get\_post authentication bypass attempt 1: 41496 Drop and generate

events

SERVER-WEBAPP WordPress get\_post authentication bypass attempt 1: 41497 Drop and generate

events

SERVER-WEBAPP Wordpress Mobile Detector Plugin remote file upload attempt 1:39349 Drop and generate

events

SERVER-WEBAPP Wordpress Mobile Detector Plugin remote file upload attempt 1:39350 Drop and generate

events

SERVER-WEBAPP WordPress pingback gethostbyname heap buffer overfl ow attempt 1:33275 Drop and generate

events

SERVER-WEBAPP WordPress pingback gethostbyname heap buffer overfl ow attempt 1:39925 Drop and generate

events

SERVER-WEBAPP Wordpress Symposium arbitrary PHP file upload attempt 1:40494 Drop and generate

events

SERVER-WEBAPP Wordpress Symposium arbitrary PHP file upload attempt 1:44236 Drop and generate

events

SERVER-WEBAPP Wordpress timthumb.php webshot source attack attemp t 1:31356 Drop and generate

events

SERVER-WEBAPP WordPress Ultimate Form Builder plugin SQL injectio n attempt 1:45075 Drop and generate

events

SERVER-WEBAPP WordPress Ultimate Form Builder plugin SQL injectio n attempt 1:45076 Drop and generate

events

SERVER-WEBAPP WordPress Ultimate Form Builder plugin SQL injectio n attempt 1:45077 Drop and generate

events

SERVER-WEBAPP WordPress wp-config.php access via directory traver sal attempt 1:41420 Drop and generate

events

SERVER-WEBAPP WordPress wp-config.php access via directory traver sal attempt 1:41421 Drop and generate

events

SERVER-WEBAPP WordPress XMLRPC pingback ddos attempt 1:40883 Drop and generate

events

SERVER-WEBAPP Zimbra remote code execution attempt 1:29027 Drop and generate

events

SERVER-WEBAPP ZyXEL TR-064 SetNTPServers command injection attemp t 1:40784 Drop and generate

events

SQL 1 = 0 - possible sql injection attempt 1:19440 Drop and generate

events

SQL 1 = 1 - possible sql injection attempt 1:19439 Drop and generate

events

SQL 1 = 1 - possible sql injection attempt 1:30040 Drop and generate

events

SQL 1 = 1 - possible sql injection attempt 1:30041 Drop and generate

events

SQL 1 = 1 - possible sql injection attempt 1:27287 Drop and generate

events

SQL generic sql with comments injection attempt - GET parameter 1 :16431 Drop and generate

events

SQL url ending in comment characters - possible sql injection att empt 1:19438 Drop and generate

events

SQL use of sleep function in HTTP header - likely SQL injection attempt 1:38993 Drop and generate

events