Strong		Moderate		Lower		Minimal		Weakest		TBD	No Coverage
Initial Access	Execution	Persistence	Privilege Escalation	Defense evasion	Credential Access	Discovery	Lateral movement	Collection	Exfiltration	Command and Control	Impact
Hardware additions	Scheduled Task	User Execution	Modify Existing Service	Kernel Module and Execution	Deobfuscate / Decode Files for Information	Account Discovery	AppleScript	Data from Information Repositories	Exfiltration over Physical Medium	Remote Access Tools	Reduction of Enterprise Services
Trusted relationship	Local Job Scheduling	PowerShell	AppCert DLLs	Access Token Manipulation	Execution Guardrails	Application Window Discovery	Application Deployment Software	Video Captures	Exfiltration over Command and Control Channel	Commonly Used Ports	Total Loss of Enterprise Services
Supply Chain Compromise	BITS Jobs	Plistmodification	.bash_profile and .bashrc	Accessibility Features	Exploitation for Defense Evasion	Files and Directory Discovery	Distributed Component Object model	Audio Capture	Automated Exfiltration	Communication Through Removable Media	Data Encrypted for Impact
Drive by compromise	Traps	CMSTP Installs	Accessibility Features	Process Injection	Extra Window Memory Injection	Local Network Configuration Discovery	Exploitation of Remote Services	Automated Collection	Data Encrypted	Custom command and Control Protocol	Data Destruction
Exploit Public Facing Application	Launchcti	Command line interface	Authentication Packages	Exploitation of Vulnerability	File Permissions / Modifications	Network Service Scanning	Login Scripts	Clipboard Data	Data Compressed	Custom Cryptographic Protocol	Defacement
External Remote Services	Signed / Un-signed Scripting	Completed HTML File	Basic Input / Output System	Bypass User Account Controls	File System Logical Offsets	Peripheral Device Discovery	Pass the Hash	Data Staged	Data Transfer Size Limits	Data Encoding	Disk Wipe Content
Replication Through Removable Media	AppleScript	Control Panel Items	External Remote Services	Image File Execution Options Injection	Group Policy Modification	Permission Groups Discovery	Shared Webroot	Data from Local System	Exfiltration Over Other Physical Medium	Data Obfuscation	Disk Structure Wipe
Spear phishing attachment	Appinit DLLs	Dynamic Data Exchange	Bootkit	File System Permissions Weakness	Hidden Files and Directories	Browser bookmark discovery	Pass the Ticket	Email Collection	Exfiltration over Alternative Protocol	Port Knocking	Endpoint Denial of Service
Spear phishing link	DLL Injection	Execution Through API	Browser Extensions	Legitimate Credentials	Image File Execution Options Injection	File and Directory Discovery	Remove Desktop Protocol	Screen Capture	Scheduled Transfer	Multi-hop Proxy	Firmware Corruption
Spear phishing via service	DLL Search Order Hijacking	Execution Through Module Load	Change Default file association	Local Port Monitor	Indicator Blocking	Network Share Discovery	Remote File Copy	Input Capture		Domain Fronting	Inhibit System Recover
Business Partner Compromise	InstallUtil	Exploitation for Client Execution	Component Firmware	New Services	Indicator Removal from Tools	Network Sniffing	Remote Services	Data from Network Shared Drive		Fallback Channels	Network Denial of Service
Vendor Partner Compromise	Mshta	Graphical User Interface	Component Object Model Hijacking	Path Interception	Indicator Removal on Host	Password Policy Discovery	Replication Through Removable Media	Data from Removable Media		Multi-stage Channels	Resource Hijacking
Valid Accounts	Regsvcs/Regasm	Windows Remote Management	Account Creation	Scheduled Tasks	Indirect Command Execution	System Service Discovery	SSH Hijacking	Data from Local Systems		Multiband Communication	Runtime Data Manipulation
Valid Privileged Accounts	Regsvr32	Signed Script Proxy Execution	File System Permissions Weakness	Service Registry Permissions Weaknesses	Install Root Certificate	System Time Discovery	Tainted Shared Content	Man in the browser		Multilayer Encryption	Service Stop
Stolen Credentials	Registry Run Keys / Start Folder	Signed Binary Proxy Execution	Service Registry Permissions Weaknesses	Web Shell	Masquerading	Process Discovery	Third Party Software			Remote File Copy	Stored Data Manipulation
	Rundll32	Third Party Software	Legitimate Credentials	SID History Injection	Modify Registry	Query Registry	Windows Admin Shares			Standard Application Layer Protocol	Transmitted Data Manipulation
	Dylib Hijacking	Application Shimming	Local Port Monitor	Port Monitoring	Network Share Connection Removal	Remote System Discovery	Windows Remote Management			Standard Cryptographic Protocol	System Data Manipulation
	Service Execution	Service Execution	New Services	Valid Accounts	NTFS File Attributes	Security Software Discovery				Standard Non-Application Layer Protocol	
	LSASS Driver	Trusted Developer Utilities	Path Interception	Exploitation for Privilege Escalation	Obfuscated Files or Information	Virtualization / Sandbox Evasion				Uncommonly Used Ports	
	Registry Run Keys / Startup Folder	Windows Management Instrumentation	Redundant Access	Extra Window Memory Injection	Process Doppeganing					Web Services	
	Startup Items	port monitoring	Port Knocking	Bypass User Account Control	Process Hollowing					Connection Proxy	
	Launch Deamons	XSL Script Processing	SIP and Trust Provider Hijacking		Process Injection					Domain Generation Algorithms	
	Login Scripts	JSON	Screensaver		Redundant Injection					Multi-Band Communication	
	Application Shimming	XML / SXML	rc.common		Redundant Access					Multiplayer Encryption	
		xlsm / xlsb	login items		Signed Binary Proxy Execution					Peer Connections	
			LC-LOAD_DYUS Addition		Signed Script Proxy Execution						
			Re-opened Applications		SIP and Trust Provider Hijacking						
			Windows Helper DLL		Template Injection						
			Windows Management Instrumentation Event Subscription		Timestamp						
			System Firmware		Trusted Developer Utilities						
			Shortcut Modification		Valid Accounts						
			Netsh Helper DLL		Virtualization / Sandbox Evasion						
			Office Application Startup		Web Service						
			Time Providers		XSL Script Processing						
			Valid Accounts		Regsvcs / Regasm						
			Winlogon Helper DLL		Regsvr32						
			Hidden Files and Directories		Mshta						
			Hypervisor								