Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions	Scheduled Task			Binary Padding	Credentials in Registry	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Exfiltration Over Physical Medium	Remote Access Tools
Trusted Relationship	LSASS Driver		Extra Window Memory Injection		Exploitation for Credential Access					Port Knocking
Supply Chain Compromise	Local Job Scheduling		Access Token Manipulation			Network Share Discovery	Distributed Component Object Model	Video Capture	Exfiltration Over Command and Control Channel	Multi-hop Proxy
	Trap		Bypass User Account Control		Forced Authentication			Audio Capture		Domain Fronting
Spearphishing Attachment	Launchctl		Process Injection		Hooking	Peripheral Device Discovery	Remote File Copy	Automated Collection		Data Encoding
	Signed Binary Proxy Execution	Image File Execution Options Injection			Password Filter DLL		Pass the Ticket	Clipboard Data	Data Encrypted	Remote File Copy
Exploit Public-Facing Application		Plist Modification			LLMNR/NBT-NS Poisoning	File and Directory Discovery	Replication Through Removable Media	Email Collection	Automated Exfiltration	Multi-Stage Channels
	User Execution	Valid Accounts						Screen Capture	Exfiltration Over Other Network Medium	Web Service
Replication Through Removable Media	Exploitation for Client Execution	DLL Search Order Hijacking			Private Keys	Permission Groups Discovery	Windows Admin Shares	Data Staged		Standard Non-Application Layer Protocol
		AppCert DLLs		Signed Script Proxy Execution	Keychain		Pass the Hash	Input Capture	Exfiltration Over Alternative Protocol	
Spearphishing via Service	CMSTP	Hooking			Input Prompt	Process Discovery	Third-party Software	Data from Network Shared Drive		
	Dynamic Data Exchange	Startup Items		DCShadow	Bash History	System Network Connections Discovery	Shared Webroot		Data Transfer Size Limits	Connection Proxy
Spearphishing Link	Mshta	Launch Daemon		Port Knocking	Two-Factor Authentication Interception		Logon Scripts	Data from Local System		Multilayer Encryption
Drive-by Compromise	AppleScript	Dylib Hijacking		Indirect Command Execution		System Owner/User Discovery	Windows Remote Management	Man in the Browser	Data Compressed	Standard Application Layer Protocol
Valid Accounts	Source	Application Shimming						Data from Removable Media	Scheduled Transfer	
	Space after Filename	AppInit DLLs		BITS Jobs	Replication Through Removable Media	System Network Configuration Discovery	Application Deployment Software			Commonly Used Port
	Execution through Module Load	Web Shell		Control Panel Items						Standard Cryptographic Protocol
		Service Registry Permissions Weakness		CMSTP	Input Capture	Application Window Discovery	SSH Hijacking			
	Regsvcs/Regasm	New Service		Process Doppelgänging	Network Sniffing		AppleScript			Custom Cryptographic Protocol
	InstallUtil	File System Permissions Weakness		Mshta	Credential Dumping	Password Policy Discovery	Taint Shared Content			
	Regsvr32	Path Interception		Hidden Files and Directories	Kerberoasting		Remote Desktop Protocol			Data Obfuscation
	Execution through API	Accessibility Features			Securityd Memory	System Time Discovery				Custom Command and Control Protocol
	PowerShell	Port Monitors		Space after Filename	Brute Force	Account Discovery	Remote Services			
	Rundll32	Kernel Modules and Extensions	Sudo Caching	LC_MAIN Hijacking	Account Manipulation	System Information Discovery				Communication Through Removable Media
	Third-party Software		SID-History Injection	HISTCONTROL	Credentials in Files					
	Scripting	Port Knocking	Sudo	Hidden Users		Security Software Discovery				
	Graphical User Interface	SIP and Trust Provider Hijacking	Setuid and Setgid	Clear Command History						Multiband Communication
	Command-Line Interface		Exploitation for Privilege Escalation	Gatekeeper Bypass		Network Service Scanning				
		Screensaver		Hidden Window						Fallback Channels
	Service Execution	Browser Extensions		Deobfuscate/Decode Files or Information		Remote System Discovery				Uncommonly Used Port
	Windows Remote Management	Re-opened Applications								
		Rc.common		Trusted Developer Utilities		Query Registry				
	Signed Script Proxy Execution	Login Item				System Service Discovery				
		LC_LOAD_DYLIB Addition		Component Object Model Hijacking						
	Control Panel Items									
	Trusted Developer Utilities	Hidden Files and Directories		InstallUtil						
	Windows Management Instrumentation	Office Application Startup		Regsvr32						
		External Remote Services		Code Signing						
		Netsh Helper DLL		Modify Registry						
		Component Object Model Hijacking		Component Firmware						
		Redundant Access		Redundant Access						
		Security Support Provider		File Deletion						
		Bootkit		Web Service						
		Hypervisor		Timestomp						
		Registry Run Keys / Start Folder		NTFS File Attributes						
		Logon Scripts		Process Hollowing						
		Modify Existing Service		Disabling Security Tools						
		Shortcut Modification		Rundll32						
		System Firmware		DLL Side-Loading						
		Winlogon Helper DLL		Indicator Removal on Host						
		Time Providers		Scripting						
		BITS Jobs		Indicator Blocking						
		Launch Agent		Software Packing						
		.bash_profile and .bashrc		Masquerading						
		Create Account		Obfuscated Files or Information						
		Authentication Package		Signed Binary Proxy Execution						
		Component Firmware		Exploitation for Defense Evasion						
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking						
		Change Default File Association		Launchctl						
				Install Root Certificate						
				Network Share Connection Removal						
				Regsvcs/Regasm						
				Indicator Removal from Tools						
				Rootkit						

THE MITRE ATT&CK™ ENTERPRISE FRAMEWORK

ATTACK.MITRE.ORG

ATT&CK™

MITRE