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

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

MITRE