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

# MITRE ATT&CK® Enterprise Framework

**attack.mitre.org**

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

Matrix current as of February 2020