MITRE Enterprise ATT&CK™ Framework

<table>
<tr><th>Persistence</th><th>Privilege Escalation</th><th>Defense Evasion</th><th>Credential Access</th><th>Discovery</th><th>Lateral Movement</th><th>Execution</th><th>Collection</th><th>Exfiltration</th><th>Command and Control</th></tr>
<tr><td colspan="3">Image File Execution Options Injection</td><td>Forced Authentication</td><td>Network Share Discovery</td><td colspan="2">AppleScript</td><td>Man in the Browser</td><td rowspan="2">Exfiltration Over Physical Medium</td><td>Multi-hop Proxy</td></tr>
<tr><td colspan="3">Plist Modification</td><td>Hooking</td><td>System Time Discovery</td><td colspan="2">Third-party Software</td><td>Browser Extensions</td><td>Domain Fronting</td></tr>
<tr><td colspan="3">Valid Accounts</td><td>Password Filter DLL</td><td>Peripheral Device Discovery</td><td colspan="2">Windows Remote Management</td><td>Video Capture</td><td rowspan="2">Exfiltration Over Command and Control Channel</td><td>Data Encoding</td></tr>
<tr><td colspan="3">DLL Search Order Hijacking</td><td>LLMNR/NBT-NS Poisoning</td><td>Account Discovery</td><td>SSH Hijacking</td><td>LSASS Driver</td><td>Audio Capture</td><td>Remote File Copy</td></tr>
<tr><td colspan="2">AppCert DLLs</td><td>Process Doppelgänging</td><td>Securityd Memory</td><td>File and Directory Discovery</td><td rowspan="2">Distributed Component Object Model</td><td>Dynamic Data Exchange</td><td>Automated Collection</td><td>Scheduled Transfer</td><td>Multi-Stage Channels</td></tr>
<tr><td colspan="2">Hooking</td><td>Mshta</td><td>Private Keys</td><td rowspan="2">System Information Discovery</td><td>Mshta</td><td>Clipboard Data</td><td>Data Encrypted</td><td>Web Service</td></tr>
<tr><td colspan="2">Startup Items</td><td>Hidden Files and Directories</td><td>Keychain</td><td>Pass the Ticket</td><td>Local Job Scheduling</td><td>Email Collection</td><td>Automated Exfiltration</td><td rowspan="2">Standard Non-Application Layer Protocol</td></tr>
<tr><td colspan="2">Launch Daemon</td><td>Launchctl</td><td>Input Prompt</td><td rowspan="2">Security Software Discovery</td><td rowspan="2">Replication Through Removable Media</td><td>Trap</td><td>Screen Capture</td><td rowspan="2">Exfiltration Over Other Network Medium</td></tr>
<tr><td colspan="2">Dylib Hijacking</td><td>Space after Filename</td><td>Bash History</td><td>Source</td><td>Data Staged</td><td rowspan="2">Communication Through Removable Media</td></tr>
<tr><td colspan="2">Application Shimming</td><td>LC_MAIN Hijacking</td><td rowspan="2">Two-Factor Authentication Interception</td><td rowspan="2">System Network Connections Discovery</td><td>Windows Admin Shares</td><td>Launchctl</td><td>Input Capture</td><td rowspan="2">Exfiltration Over Alternative Protocol</td></tr>
<tr><td colspan="2">AppInit DLLs</td><td>HISTCONTROL</td><td>Remote Desktop Protocol</td><td>Space after Filename</td><td rowspan="2">Data from Network Shared Drive</td><td>Multilayer Encryption</td></tr>
<tr><td colspan="2">Web Shell</td><td>Hidden Users</td><td>Account Manipulation</td><td rowspan="2">System Owner/User Discovery</td><td>Pass the Hash</td><td rowspan="2">Execution through Module Load</td><td>Data Transfer Size Limits</td><td rowspan="2">Standard Application Layer Protocol</td></tr>
<tr><td colspan="2">Service Registry Permissions Weakness</td><td>Clear Command History</td><td rowspan="2">Replication Through Removable Media</td><td>Exploitation of Vulnerability</td><td>Data from Local System</td><td>Data Compressed</td></tr>
<tr><td colspan="2">Scheduled Task</td><td>Gatekeeper Bypass</td><td rowspan="2">System Network Configuration Discovery</td><td>Shared Webroot</td><td>Regsvcs/Regasm</td><td>Data from Removable Media</td><td></td><td>Commonly Used Port</td></tr>
<tr><td colspan="2">New Service</td><td>Hidden Window</td><td>Input Capture</td><td>Logon Scripts</td><td>InstallUtil</td><td></td><td></td><td rowspan="2">Standard Cryptographic Protocol</td></tr>
<tr><td colspan="2">File System Permissions Weakness</td><td rowspan="2">Deobfuscate/Decode Files or Information</td><td>Network Sniffing</td><td rowspan="2">Application Window Discovery</td><td>Remote Services</td><td>Regsvr32</td><td></td><td></td></tr>
<tr><td colspan="2">Path Interception</td><td>Credential Dumping</td><td rowspan="2">Application Deployment Software</td><td>Execution through API</td><td></td><td></td><td rowspan="2">Custom Cryptographic Protocol</td></tr>
<tr><td colspan="2">Accessibility Features</td><td>Trusted Developer Utilities</td><td>Brute Force</td><td>Network Service Scanning</td><td>PowerShell</td><td></td><td></td></tr>
<tr><td colspan="2">Port Monitors</td><td>Regsvcs/Regasm</td><td>Credentials in Files</td><td>Query Registry</td><td>Remote File Copy</td><td>Rundll32</td><td></td><td></td><td>Data Obfuscation</td></tr>
<tr><td>Screensaver</td><td colspan="3">Exploitation of Vulnerability</td><td>Remote System Discovery</td><td>Taint Shared Content</td><td>Scripting</td><td></td><td></td><td rowspan="2">Custom Command and Control Protocol</td></tr>
<tr><td>LSASS Driver</td><td colspan="2">Extra Window Memory Injection</td><td></td><td rowspan="2">Permission Groups Discovery</td><td></td><td>Graphical User Interface</td><td></td><td></td></tr>
<tr><td>Browser Extensions</td><td colspan="2">Access Token Manipulation</td><td></td><td></td><td>Command-Line Interface</td><td></td><td></td><td>Connection Proxy</td></tr>
<tr><td>Local Job Scheduling</td><td colspan="2">Bypass User Account Control</td><td></td><td>Process Discovery</td><td></td><td>Scheduled Task</td><td></td><td></td><td>Uncommonly Used Port</td></tr>
<tr><td>Re-opened Applications</td><td colspan="2">Process Injection</td><td></td><td>System Service Discovery</td><td></td><td rowspan="2">Windows Management Instrumentation</td><td></td><td></td><td>Multiband Communication</td></tr>
<tr><td>Rc.common</td><td>SID-History Injection</td><td rowspan="2">Component Object Model Hijacking</td><td></td><td></td><td></td><td></td><td></td><td>Fallback Channels</td></tr>
<tr><td>Login Item</td><td>Sudo</td><td></td><td></td><td></td><td>Trusted Developer Utilities</td><td></td><td></td><td></td></tr>
<tr><td>LC_LOAD_DYLIB Addition</td><td>Setuid and Setgid</td><td>InstallUtil</td><td></td><td></td><td></td><td>Service Execution</td><td></td><td></td><td></td></tr>
<tr><td>Launch Agent</td><td></td><td>Regsvr32</td><td colspan="7"></td></tr>
<tr><td>Hidden Files and Directories</td><td></td><td>Code Signing</td><td colspan="7"></td></tr>
<tr><td>.bash_profile and .bashrc</td><td></td><td>Modify Registry</td><td colspan="7"></td></tr>
<tr><td>Trap</td><td></td><td>Component Firmware</td><td colspan="7"></td></tr>
<tr><td>Launchctl</td><td></td><td>Redundant Access</td><td colspan="7"></td></tr>
<tr><td>Office Application Startup</td><td></td><td>File Deletion</td><td colspan="7"></td></tr>
<tr><td>Create Account</td><td></td><td>Timestomp</td><td colspan="7"></td></tr>
<tr><td>External Remote Services</td><td></td><td>NTFS Extended Attributes</td><td colspan="7"></td></tr>
<tr><td>Authentication Package</td><td></td><td>Process Hollowing</td><td colspan="7"></td></tr>
<tr><td>Netsh Helper DLL</td><td></td><td>Disabling Security Tools</td><td colspan="7"></td></tr>
<tr><td rowspan="2">Component Object Model Hijacking</td><td></td><td>Rundll32</td><td colspan="7"></td></tr>
<tr><td></td><td>DLL Side-Loading</td><td colspan="7"></td></tr>
<tr><td>Redundant Access</td><td></td><td>Indicator Removal on Host</td><td colspan="7"></td></tr>
<tr><td>Security Support Provider</td><td></td><td rowspan="2">Indicator Removal from Tools</td><td colspan="7"></td></tr>
<tr><td rowspan="3">Windows Management Instrumentation Event Subscription</td><td></td><td colspan="7"></td></tr>
<tr><td></td><td>Indicator Blocking</td><td colspan="7"></td></tr>
<tr><td></td><td>Software Packing</td><td colspan="7"></td></tr>
<tr><td rowspan="2">Registry Run Keys / Start Folder</td><td></td><td>Masquerading</td><td colspan="7"></td></tr>
<tr><td></td><td rowspan="2">Obfuscated Files or Information</td><td colspan="7"></td></tr>
<tr><td rowspan="2">Change Default File Association</td><td></td><td colspan="7"></td></tr>
<tr><td></td><td>Binary Padding</td><td colspan="7"></td></tr>
<tr><td>Component Firmware</td><td></td><td>Install Root Certificate</td><td colspan="7"></td></tr>
<tr><td>Bootkit</td><td></td><td rowspan="2">Network Share Connection Removal</td><td colspan="7"></td></tr>
<tr><td>Hypervisor</td><td></td><td colspan="7"></td></tr>
<tr><td>Logon Scripts</td><td></td><td>Rootkit</td><td colspan="7"></td></tr>
<tr><td>Modify Existing Service</td><td></td><td>Scripting</td><td colspan="7"></td></tr>
</table>

attack.mitre.org

MITRE