Mitre Attack Data Sources

32

Mitre Attack Data Objects

99

Total Techniques and Sub-techniques

552

Total Techniques

185

## Total Sub-Techniques

# 367

## Mitre Attack Data Sources

| DS |
| --- |
| Active Directory |
| Application Log |
| Cloud Service |
| Cloud Storage |
| Cluster |
| Command |
| Container |
| Drive |
| Driver |
| File |
| Firewall |
| Firmware |
| Group |
| Image |
| Instance |
| Kernel |
| Logon Session |
| Module |
| Network Share |
| Network Traffic |
| Pod |
| Process |
| Scheduled Job |
| Script |
| Sensor Health |
| Service |
| Snapshot |
| User Account |
| Volume |
| WMI |
| Web Credential |
| Windows Registry |

# Mitre Attack Data Objects

| DS |
| --- |
| Active Directory: Active Directory Credential Request |
| Active Directory: Active Directory Object Access |
| Active Directory: Active Directory Object Creation |
| Active Directory: Active Directory Object Deletion |
| Active Directory: Active Directory Object Modification |
| Application Log: Application Log Content |
| Cloud Service: Cloud Service Disable |
| Cloud Service: Cloud Service Enumeration |
| Cloud Service: Cloud Service Metadata |
| Cloud Service: Cloud Service Modification |
| Cloud Storage: Cloud Storage Access |
| Cloud Storage: Cloud Storage Creation |
| Cloud Storage: Cloud Storage Deletion |
| Cloud Storage: Cloud Storage Enumeration |
| Cloud Storage: Cloud Storage Metadata |
| Cloud Storage: Cloud Storage Modification |
| Cluster: Cluster Metadata |
| Command: Command Execution |
| Container: Container Creation |
| Container: Container Enumeration |
| Container: Container Metadata |
| Container: Container Start |
| Drive: Drive Access |
| Drive: Drive Creation |
| Drive: Drive Modification |
| Driver: Driver Load |
| Driver: Driver Metadata |
| File: File Access |
| File: File Content |
| File: File Creation |
| File: File Deletion |
| File: File Metadata |
| File: File Modification |
| Firewall: Firewall Disable |
| Firewall: Firewall Enumeration |
| Firewall: Firewall Metadata |
| Firewall: Firewall Rule Modification |
| Firmware: Firmware Modification |
| Group: Group Enumeration |
| Group: Group Metadata |
| Group: Group Modification |
| Image: Image Creation |
| Image: Image Deletion |
| Image: Image Metadata |
| Image: Image Modification |
| Instance: Instance Creation |
| Instance: Instance Deletion |
| Instance: Instance Enumeration |
| Instance: Instance Metadata |
| Instance: Instance Modification |

| DS |
| --- |
| Instance: Instance Start |
| Instance: Instance Stop |
| Kernel: Kernel Module Load |
| Logon Session: Logon Session Creation |
| Logon Session: Logon Session Metadata |
| Module: Module Load |
| Network Share: Network Share Access |
| Network Traffic: Network Connection Creation |
| Network Traffic: Network Traffic Content |
| Network Traffic: Network Traffic Flow |
| Pod: Pod Creation |
| Pod: Pod Enumeration |
| Pod: Pod Metadata |
| Pod: Pod Modification |
| Process: OS API Execution |
| Process: Process Access |
| Process: Process Creation |
| Process: Process Metadata |
| Process: Process Termination |
| Scheduled Job: Scheduled Job Creation |
| Scheduled Job: Scheduled Job Metadata |
| Scheduled Job: Scheduled Job Modification |
| Script: Script Execution |
| Sensor Health: Host Status |
| Service: Service Creation |
| Service: Service Metadata |
| Service: Service Modification |
| Snapshot: Snapshot Creation |
| Snapshot: Snapshot Deletion |
| Snapshot: Snapshot Enumeration |
| Snapshot: Snapshot Metadata |
| Snapshot: Snapshot Modification |
| User Account: User Account Authentication |
| User Account: User Account Creation |
| User Account: User Account Deletion |
| User Account: User Account Metadata |
| User Account: User Account Modification |
| Volume: Volume Creation |
| Volume: Volume Deletion |
| Volume: Volume Enumeration |
| Volume: Volume Metadata |
| Volume: Volume Modification |
| WMI: WMI Creation |
| Web Credential: Web Credential Creation |
| Web Credential: Web Credential Usage |
| Windows Registry: Windows Registry Key Access |
| Windows Registry: Windows Registry Key Creation |
| Windows Registry: Windows Registry Key Deletion |
| Windows Registry: Windows Registry Key Modification |

# Number of Techniques and Sub-techniques covered per data source/data object pair

| DS | count |
|---|---|
| Command: Command Execution | 243 |
| Process: Process Creation | 197 |
| File: File Modification | 95 |
| Network Traffic: Network Traffic Content | 89 |
| Network Traffic: Network Traffic Flow | 84 |
| File: File Creation | 82 |
| Process: OS API Execution | 76 |
| Network Traffic: Network Connection Creation | 58 |
| Windows Registry: Windows Registry Key Modification | 56 |
| Application Log: Application Log Content | 50 |
| Module: Module Load | 49 |
| File: File Access | 45 |
| File: File Metadata | 32 |
| Logon Session: Logon Session Creation | 31 |
| Script: Script Execution | 21 |
| User Account: User Account Authentication | 20 |
| Process: Process Access | 18 |
| Sensor Health: Host Status | 15 |
| Windows Registry: Windows Registry Key Creation | 15 |
| Service: Service Creation | 14 |
| Active Directory: Active Directory Object Modification | 13 |
| Service: Service Metadata | 11 |
| Driver: Driver Load | 10 |
| File: File Deletion | 10 |
| Process: Process Metadata | 10 |
| Firmware: Firmware Modification | 9 |
| Scheduled Job: Scheduled Job Creation | 8 |
| Active Directory: Active Directory Credential Request | 7 |
| User Account: User Account Metadata | 7 |
| Container: Container Creation | 6 |
| Drive: Drive Modification | 6 |
| File: File Content | 6 |
| User Account: User Account Creation | 6 |
| User Account: User Account Modification | 6 |
| Web Credential: Web Credential Usage | 6 |
| Windows Registry: Windows Registry Key Access | 6 |
| Drive: Drive Access | 5 |
| Instance: Instance Creation | 5 |
| Logon Session: Logon Session Metadata | 5 |
| Service: Service Modification | 5 |
| Active Directory: Active Directory Object Creation | 4 |
| Drive: Drive Creation | 4 |
| Image: Image Creation | 4 |
| Instance: Instance Start | 4 |
| Network Share: Network Share Access | 4 |
| Windows Registry: Windows Registry Key Deletion | 4 |
| Container: Container Start | 3 |
| Firewall: Firewall Disable | 3 |
| Firewall: Firewall Rule Modification | 3 |

| DS | count |
|---|---|
| Instance: Instance Deletion | 3 |
| Instance: Instance Metadata | 3 |
| Process: Process Termination | 3 |
| Snapshot: Snapshot Creation | 3 |
| Web Credential: Web Credential Creation | 3 |
| Active Directory: Active Directory Object Access | 2 |
| Active Directory: Active Directory Object Deletion | 2 |
| Cloud Service: Cloud Service Disable | 2 |
| Cloud Service: Cloud Service Enumeration | 2 |
| Cloud Service: Cloud Service Modification | 2 |
| Cloud Storage: Cloud Storage Metadata | 2 |
| Cloud Storage: Cloud Storage Modification | 2 |
| Driver: Driver Metadata | 2 |
| Firewall: Firewall Enumeration | 2 |
| Firewall: Firewall Metadata | 2 |
| Group: Group Enumeration | 2 |
| Group: Group Metadata | 2 |
| Group: Group Modification | 2 |
| Image: Image Metadata | 2 |
| Instance: Instance Modification | 2 |
| Instance: Instance Stop | 2 |
| Kernel: Kernel Module Load | 2 |
| Scheduled Job: Scheduled Job Metadata | 2 |
| Scheduled Job: Scheduled Job Modification | 2 |
| Snapshot: Snapshot Deletion | 2 |
| Snapshot: Snapshot Modification | 2 |
| Volume: Volume Deletion | 2 |
| WMI: WMI Creation | 2 |
| Cloud Service: Cloud Service Metadata | 1 |
| Cloud Storage: Cloud Storage Access | 1 |
| Cloud Storage: Cloud Storage Creation | 1 |
| Cloud Storage: Cloud Storage Deletion | 1 |
| Cloud Storage: Cloud Storage Enumeration | 1 |
| Cluster: Cluster Metadata | 1 |
| Container: Container Enumeration | 1 |
| Container: Container Metadata | 1 |
| Image: Image Deletion | 1 |
| Image: Image Modification | 1 |
| Instance: Instance Enumeration | 1 |
| Pod: Pod Creation | 1 |
| Pod: Pod Enumeration | 1 |
| Pod: Pod Metadata | 1 |
| Pod: Pod Modification | 1 |
| Snapshot: Snapshot Enumeration | 1 |
| Snapshot: Snapshot Metadata | 1 |
| User Account: User Account Deletion | 1 |
| Volume: Volume Creation | 1 |
| Volume: Volume Enumeration | 1 |
| Volume: Volume Metadata | 1 |
| Volume: Volume Modification | 1 |

# Number of Techniques covered per data source/data object pair

| DS | count |
|---|---|
| Command: Command Execution | 88 |
| Process: Process Creation | 78 |
| Network Traffic: Network Traffic Content | 40 |
| Network Traffic: Network Traffic Flow | 39 |
| Process: OS API Execution | 38 |
| Network Traffic: Network Connection Creation | 30 |
| File: File Modification | 29 |
| File: File Creation | 28 |
| Application Log: Application Log Content | 22 |
| File: File Access | 21 |
| Windows Registry: Windows Registry Key Modification | 19 |
| Module: Module Load | 14 |
| File: File Metadata | 12 |
| Logon Session: Logon Session Creation | 11 |
| Script: Script Execution | 11 |
| Active Directory: Active Directory Object Modification | 7 |
| User Account: User Account Authentication | 7 |
| Windows Registry: Windows Registry Key Creation | 7 |
| Process: Process Access | 6 |
| Service: Service Metadata | 6 |
| Driver: Driver Load | 5 |
| File: File Deletion | 5 |
| Sensor Health: Host Status | 5 |
| Service: Service Creation | 5 |
| Container: Container Creation | 4 |
| Firmware: Firmware Modification | 4 |
| Process: Process Metadata | 4 |
| Drive: Drive Access | 3 |
| Drive: Drive Creation | 3 |
| Drive: Drive Modification | 3 |
| Image: Image Creation | 3 |
| Instance: Instance Creation | 3 |
| Instance: Instance Metadata | 3 |
| Logon Session: Logon Session Metadata | 3 |
| Network Share: Network Share Access | 3 |
| User Account: User Account Metadata | 3 |
| User Account: User Account Modification | 3 |
| Windows Registry: Windows Registry Key Access | 3 |
| Windows Registry: Windows Registry Key Deletion | 3 |
| Active Directory: Active Directory Credential Request | 2 |
| Active Directory: Active Directory Object Creation | 2 |
| Cloud Service: Cloud Service Enumeration | 2 |
| Cloud Storage: Cloud Storage Metadata | 2 |
| Cloud Storage: Cloud Storage Modification | 2 |
| Container: Container Start | 2 |
| File: File Content | 2 |
| Instance: Instance Deletion | 2 |
| Instance: Instance Start | 2 |
| Process: Process Termination | 2 |
| Snapshot: Snapshot Creation | 2 |

| DS | count |
|---|---|
| Snapshot: Snapshot Deletion | 2 |
| Snapshot: Snapshot Modification | 2 |
| User Account: User Account Creation | 2 |
| Volume: Volume Deletion | 2 |
| Web Credential: Web Credential Usage | 2 |
| Active Directory: Active Directory Object Access | 1 |
| Active Directory: Active Directory Object Deletion | 1 |
| Cloud Service: Cloud Service Disable | 1 |
| Cloud Service: Cloud Service Metadata | 1 |
| Cloud Service: Cloud Service Modification | 1 |
| Cloud Storage: Cloud Storage Access | 1 |
| Cloud Storage: Cloud Storage Creation | 1 |
| Cloud Storage: Cloud Storage Deletion | 1 |
| Cloud Storage: Cloud Storage Enumeration | 1 |
| Cluster: Cluster Metadata | 1 |
| Container: Container Enumeration | 1 |
| Container: Container Metadata | 1 |
| Driver: Driver Metadata | 1 |
| Firewall: Firewall Disable | 1 |
| Firewall: Firewall Enumeration | 1 |
| Firewall: Firewall Metadata | 1 |
| Firewall: Firewall Rule Modification | 1 |
| Group: Group Enumeration | 1 |
| Group: Group Metadata | 1 |
| Group: Group Modification | 1 |
| Image: Image Deletion | 1 |
| Image: Image Metadata | 1 |
| Image: Image Modification | 1 |
| Instance: Instance Enumeration | 1 |
| Instance: Instance Modification | 1 |
| Instance: Instance Stop | 1 |
| Kernel: Kernel Module Load | 1 |
| Pod: Pod Creation | 1 |
| Pod: Pod Enumeration | 1 |
| Pod: Pod Metadata | 1 |
| Pod: Pod Modification | 1 |
| Scheduled Job: Scheduled Job Creation | 1 |
| Scheduled Job: Scheduled Job Metadata | 1 |
| Scheduled Job: Scheduled Job Modification | 1 |
| Service: Service Modification | 1 |
| Snapshot: Snapshot Enumeration | 1 |
| Snapshot: Snapshot Metadata | 1 |
| User Account: User Account Deletion | 1 |
| Volume: Volume Creation | 1 |
| Volume: Volume Enumeration | 1 |
| Volume: Volume Metadata | 1 |
| Volume: Volume Modification | 1 |
| WMI: WMI Creation | 1 |
| Web Credential: Web Credential Creation | 1 |

# Number of Sub-Techniques covered per data source/data object pair

| DS | count |
|---|---|
| Command: Command Execution | 155 |
| Process: Process Creation | 119 |
| File: File Modification | 66 |
| File: File Creation | 54 |
| Network Traffic: Network Traffic Content | 49 |
| Network Traffic: Network Traffic Flow | 45 |
| Process: OS API Execution | 38 |
| Windows Registry: Windows Registry Key Modification | 37 |
| Module: Module Load | 35 |
| Application Log: Application Log Content | 28 |
| Network Traffic: Network Connection Creation | 28 |
| File: File Access | 24 |
| File: File Metadata | 20 |
| Logon Session: Logon Session Creation | 20 |
| User Account: User Account Authentication | 13 |
| Process: Process Access | 12 |
| Script: Script Execution | 10 |
| Sensor Health: Host Status | 10 |
| Service: Service Creation | 9 |
| Windows Registry: Windows Registry Key Creation | 8 |
| Scheduled Job: Scheduled Job Creation | 7 |
| Active Directory: Active Directory Object Modification | 6 |
| Process: Process Metadata | 6 |
| Active Directory: Active Directory Credential Request | 5 |
| Driver: Driver Load | 5 |
| File: File Deletion | 5 |
| Firmware: Firmware Modification | 5 |
| Service: Service Metadata | 5 |
| File: File Content | 4 |
| Service: Service Modification | 4 |
| User Account: User Account Creation | 4 |
| User Account: User Account Metadata | 4 |
| Web Credential: Web Credential Usage | 4 |
| Drive: Drive Modification | 3 |
| User Account: User Account Modification | 3 |
| Windows Registry: Windows Registry Key Access | 3 |
| Active Directory: Active Directory Object Creation | 2 |
| Container: Container Creation | 2 |
| Drive: Drive Access | 2 |
| Firewall: Firewall Disable | 2 |
| Firewall: Firewall Rule Modification | 2 |
| Instance: Instance Creation | 2 |
| Instance: Instance Start | 2 |
| Logon Session: Logon Session Metadata | 2 |
| Web Credential: Web Credential Creation | 2 |
| Active Directory: Active Directory Object Access | 1 |
| Active Directory: Active Directory Object Deletion | 1 |
| Cloud Service: Cloud Service Disable | 1 |
| Cloud Service: Cloud Service Modification | 1 |
| Container: Container Start | 1 |

| DS | count |
|---|---|
| Drive: Drive Creation | 1 |
| Driver: Driver Metadata | 1 |
| Firewall: Firewall Enumeration | 1 |
| Firewall: Firewall Metadata | 1 |
| Group: Group Enumeration | 1 |
| Group: Group Metadata | 1 |
| Group: Group Modification | 1 |
| Image: Image Creation | 1 |
| Image: Image Metadata | 1 |
| Instance: Instance Deletion | 1 |
| Instance: Instance Modification | 1 |
| Instance: Instance Stop | 1 |
| Kernel: Kernel Module Load | 1 |
| Network Share: Network Share Access | 1 |
| Process: Process Termination | 1 |
| Scheduled Job: Scheduled Job Metadata | 1 |
| Scheduled Job: Scheduled Job Modification | 1 |
| Snapshot: Snapshot Creation | 1 |
| WMI: WMI Creation | 1 |
| Windows Registry: Windows Registry Key Deletion | 1 |

## Techniques and Sub-Techniques not detectable by Mitre data sources

# 80

# Techniques and Sub-Techniques not detectable by Mitre data sources

| tactics | technique | ID |
|---|---|---|
| Resource Development | Acquire Infrastructure | T1583 |
| Resource Development | Acquire Infrastructure: Botnet | T1583.005 |
| Resource Development | Acquire Infrastructure: DNS Server | T1583.002 |
| Resource Development | Acquire Infrastructure: Domains | T1583.001 |
| Resource Development | Acquire Infrastructure: Server | T1583.004 |
| Resource Development | Acquire Infrastructure: Virtual Private Server | T1583.003 |
| Resource Development | Acquire Infrastructure: Web Services | T1583.006 |
| Resource Development | Compromise Accounts | T1586 |
| Resource Development | Compromise Accounts: Email Accounts | T1586.002 |
| Resource Development | Compromise Accounts: Social Media Accounts | T1586.001 |
| Resource Development | Compromise Infrastructure | T1584 |
| Resource Development | Compromise Infrastructure: Botnet | T1584.005 |
| Resource Development | Compromise Infrastructure: DNS Server | T1584.002 |
| Resource Development | Compromise Infrastructure: Domains | T1584.001 |
| Resource Development | Compromise Infrastructure: Server | T1584.004 |
| Resource Development | Compromise Infrastructure: Virtual Private Server | T1584.003 |
| Resource Development | Compromise Infrastructure: Web Services | T1584.006 |
| Resource Development | Develop Capabilities | T1587 |
| Resource Development | Develop Capabilities: Code Signing Certificates | T1587.002 |
| Resource Development | Develop Capabilities: Digital Certificates | T1587.003 |
| Resource Development | Develop Capabilities: Exploits | T1587.004 |
| Resource Development | Develop Capabilities: Malware | T1587.001 |
| Resource Development | Establish Accounts | T1585 |
| Resource Development | Establish Accounts: Email Accounts | T1585.002 |
| Resource Development | Establish Accounts: Social Media Accounts | T1585.001 |
| Execution | Exploitation for Client Execution | T1203 |
| Credential Access | Exploitation for Credential Access | T1212 |
| Defense Evasion | Exploitation for Defense Evasion | T1211 |
| Reconnaissance | Gather Victim Host Information | T1592 |
| Reconnaissance | Gather Victim Host Information: Client Configurations | T1592.004 |
| Reconnaissance | Gather Victim Host Information: Firmware | T1592.003 |
| Reconnaissance | Gather Victim Host Information: Hardware | T1592.001 |
| Reconnaissance | Gather Victim Host Information: Software | T1592.002 |
| Reconnaissance | Gather Victim Identity Information | T1589 |
| Reconnaissance | Gather Victim Identity Information: Credentials | T1589.001 |
| Reconnaissance | Gather Victim Identity Information: Email Addresses | T1589.002 |
| Reconnaissance | Gather Victim Identity Information: Employee Names | T1589.003 |
| Reconnaissance | Gather Victim Network Information | T1590 |
| Reconnaissance | Gather Victim Network Information: DNS | T1590.002 |
| Reconnaissance | Gather Victim Network Information: Domain Properties | T1590.001 |
| Reconnaissance | Gather Victim Network Information: IP Addresses | T1590.005 |
| Reconnaissance | Gather Victim Network Information: Network Security Appliances | T1590.006 |
| Reconnaissance | Gather Victim Network Information: Network Topology | T1590.004 |
| Reconnaissance | Gather Victim Network Information: Network Trust Dependencies | T1590.003 |
| Reconnaissance | Gather Victim Org Information | T1591 |
| Reconnaissance | Gather Victim Org Information: Business Relationships | T1591.002 |
| Reconnaissance | Gather Victim Org Information: Determine Physical Locations | T1591.001 |
| Reconnaissance | Gather Victim Org Information: Identify Business Tempo | T1591.003 |
| Reconnaissance | Gather Victim Org Information: Identify Roles | T1591.004 |
| Initial Access | Hardware Additions | T1200 |

| tactics | technique | ID |
|---|---|---|
| Defense Evasion | Obfuscated Files or Information: Indicator Removal from Tools | T1027.005 |
| Resource Development | Obtain Capabilities | T1588 |
| Resource Development | Obtain Capabilities: Code Signing Certificates | T1588.003 |
| Resource Development | Obtain Capabilities: Digital Certificates | T1588.004 |
| Resource Development | Obtain Capabilities: Exploits | T1588.005 |
| Resource Development | Obtain Capabilities: Malware | T1588.001 |
| Resource Development | Obtain Capabilities: Tool | T1588.002 |
| Resource Development | Obtain Capabilities: Vulnerabilities | T1588.006 |
| Reconnaissance | Search Closed Sources | T1597 |
| Reconnaissance | Search Closed Sources: Purchase Technical Data | T1597.002 |
| Reconnaissance | Search Closed Sources: Threat Intel Vendors | T1597.001 |
| Reconnaissance | Search Open Technical Databases | T1596 |
| Reconnaissance | Search Open Technical Databases: CDNs | T1596.004 |
| Reconnaissance | Search Open Technical Databases: DNS/Passive DNS | T1596.001 |
| Reconnaissance | Search Open Technical Databases: Digital Certificates | T1596.003 |
| Reconnaissance | Search Open Technical Databases: Scan Databases | T1596.005 |
| Reconnaissance | Search Open Technical Databases: WHOIS | T1596.002 |
| Reconnaissance | Search Open Websites/Domains | T1593 |
| Reconnaissance | Search Open Websites/Domains: Search Engines | T1593.002 |
| Reconnaissance | Search Open Websites/Domains: Social Media | T1593.001 |
| Resource Development | Stage Capabilities | T1608 |
| Resource Development | Stage Capabilities: Drive-by Target | T1608.004 |
| Resource Development | Stage Capabilities: Install Digital Certificate | T1608.003 |
| Resource Development | Stage Capabilities: Link Target | T1608.005 |
| Resource Development | Stage Capabilities: Upload Malware | T1608.001 |
| Resource Development | Stage Capabilities: Upload Tool | T1608.002 |
| Initial Access | Supply Chain Compromise | T1195 |
| Initial Access | Supply Chain Compromise: Compromise Hardware Supply Chain | T1195.003 |
| Initial Access | Supply Chain Compromise: Compromise Software Dependencies and Development Tools | T1195.001 |
| Initial Access | Supply Chain Compromise: Compromise Software Supply Chain | T1195.002 |

## Windows only Techniques and Sub-techniques

# 125

## MacOS only Techniques and Sub-techniques

# 16

## Linux only Techniques and Sub-techniques

# 9

## Windows only Techniques and Sub-techniques

| tactics | technique | ID | DS |
|---|---|---|---|
| Credential Access | Steal or Forge Kerberos Tickets | T1558 | Active Directory: Active Directory Credential Request |
| Credential Access | Steal or Forge Kerberos Tickets: AS-REP Roasting | T1558.004 | Active Directory: Active Directory Credential Request |
| Credential Access | Steal or Forge Kerberos Tickets: Golden Ticket | T1558.001 | Active Directory: Active Directory Credential Request |
| Credential Access | Steal or Forge Kerberos Tickets: Kerberoasting | T1558.003 | Active Directory: Active Directory Credential Request |
| Defense Evasion, Lateral Movement | Use Alternate Authentication Material: Pass the Hash | T1550.002 | Active Directory: Active Directory Credential Request |
| Defense Evasion, Lateral Movement | Use Alternate Authentication Material: Pass the Ticket | T1550.003 | Active Directory: Active Directory Credential Request |
| Credential Access | OS Credential Dumping: DCSync | T1003.006 | Active Directory: Active Directory Object Access |
| Defense Evasion, Privilege Escalation | Domain Policy Modification: Group Policy Modification | T1484.001 | Active Directory: Active Directory Object Creation |
| Defense Evasion | Rogue Domain Controller | T1207 | Active Directory: Active Directory Object Creation |
| Defense Evasion, Privilege Escalation | Access Token Manipulation | T1134 | Active Directory: Active Directory Object Modification |
| Defense Evasion, Privilege Escalation | Access Token Manipulation: SID-History Injection | T1134.005 | Active Directory: Active Directory Object Modification |
| Persistence, Privilege Escalation | Boot or Logon Initialization Scripts: Network Logon Script | T1037.003 | Active Directory: Active Directory Object Modification |
| Defense Evasion | File and Directory Permissions Modification: Windows File and Directory Permissions Modification | T1222.001 | Active Directory: Active Directory Object Modification |
| Defense Evasion, Privilege Escalation | Abuse Elevation Control Mechanism: Bypass User Account Control | T1548.002 | Command: Command Execution |
| Defense Evasion, Privilege Escalation | Access Token Manipulation: Create Process with Token | T1134.002 | Command: Command Execution |
| Defense Evasion, Privilege Escalation | Access Token Manipulation: Make and Impersonate Token | T1134.003 | Command: Command Execution |
| Defense Evasion, Privilege Escalation | Access Token Manipulation: Token Impersonation/Theft | T1134.001 | Command: Command Execution |
| Defense Evasion, Persistence | BITS Jobs | T1197 | Command: Command Execution |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Active Setup | T1547.014 | Command: Command Execution |

| tactics | technique | ID | DS |
|---|---|---|---|
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Authentication Package | T1547.002 | Command: Command Execution |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | T1547.001 | Command: Command Execution |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Security Support Provider | T1547.005 | Command: Command Execution |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Time Providers | T1547.003 | Command: Command Execution |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Winlogon Helper DLL | T1547.004 | Command: Command Execution |
| Persistence, Privilege Escalation | Boot or Logon Initialization Scripts: Logon Script (Windows) | T1037.001 | Command: Command Execution |
| Execution | Command and Scripting Interpreter: PowerShell | T1059.001 | Command: Command Execution |
| Execution | Command and Scripting Interpreter: Windows Command Shell | T1059.003 | Command: Command Execution |
| Persistence, Privilege Escalation | Create or Modify System Process: Windows Service | T1543.003 | Command: Command Execution |
| Credential Access | Credentials from Password Stores: Windows Credential Manager | T1555.004 | Command: Command Execution |
| Defense Evasion | Direct Volume Access | T1006 | Command: Command Execution |
| Discovery | Domain Trust Discovery | T1482 | Command: Command Execution |
| Collection | Email Collection: Local Email Collection | T1114.001 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Accessibility Features | T1546.008 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: AppCert DLLs | T1546.009 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: AppInit DLLs | T1546.010 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Application Shimming | T1546.011 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Change Default File Association | T1546.001 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Component Object Model Hijacking | T1546.015 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Image File Execution Options Injection | T1546.012 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Netsh Helper DLL | T1546.007 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: PowerShell Profile | T1546.013 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Screensaver | T1546.002 | Command: Command Execution |
| Persistence, Privilege Escalation | Event Triggered Execution: Windows Management Instrumentation Event Subscription | T1546.003 | Command: Command Execution |
| Defense Evasion | Hide Artifacts: NTFS File Attributes | T1564.004 | Command: Command Execution |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: COR_PROFILER | T1574.012 | Command: Command Execution |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Services Registry Permissions Weakness | T1574.011 | Command: Command Execution |
| Defense Evasion | Impair Defenses: Disable Windows Event Logging | T1562.002 | Command: Command Execution |
| Defense Evasion | Indicator Removal on Host: Clear Windows Event Logs | T1070.001 | Command: Command Execution |
| Defense Evasion | Indicator Removal on Host: Network Share Connection Removal | T1070.005 | Command: Command Execution |
| Defense Evasion | Indirect Command Execution | T1202 | Command: Command Execution |
| Defense Evasion | Modify Registry | T1112 | Command: Command Execution |
| Credential Access | OS Credential Dumping: Cached Domain Credentials | T1003.005 | Command: Command Execution |
| Credential Access | OS Credential Dumping: LSA Secrets | T1003.004 | Command: Command Execution |
| Credential Access | OS Credential Dumping: LSASS Memory | T1003.001 | Command: Command Execution |
| Credential Access | OS Credential Dumping: NTDS | T1003.003 | Command: Command Execution |
| Credential Access | OS Credential Dumping: Security Account Manager | T1003.002 | Command: Command Execution |
| Discovery | Query Registry | T1012 | Command: Command Execution |
| Lateral Movement | Remote Service Session Hijacking: RDP Hijacking | T1563.002 | Command: Command Execution |
| Lateral Movement | Remote Services: SMB/Windows Admin Shares | T1021.002 | Command: Command Execution |
| Lateral Movement | Remote Services: Windows Remote Management | T1021.006 | Command: Command Execution |
| Execution, Persistence, Privilege Escalation | Scheduled Task/Job: At (Windows) | T1053.002 | Command: Command Execution |
| Execution, Persistence, Privilege Escalation | Scheduled Task/Job: Scheduled Task | T1053.005 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution | T1218 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: CMSTP | T1218.003 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Compiled HTML File | T1218.001 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Control Panel | T1218.002 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: InstallUtil | T1218.004 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Mshta | T1218.005 | Command: Command Execution |

| tactics | technique | ID | DS |
|---|---|---|---|
| Defense Evasion | Signed Binary Proxy Execution: Msiexec | T1218.007 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Odbcconf | T1218.008 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Regsvcs/Regasm | T1218.009 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Regsvr32 | T1218.010 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Rundll32 | T1218.011 | Command: Command Execution |
| Defense Evasion | Signed Binary Proxy Execution: Verclsid | T1218.012 | Command: Command Execution |
| Defense Evasion | Signed Script Proxy Execution | T1216 | Command: Command Execution |
| Defense Evasion | Signed Script Proxy Execution: PubPrn | T1216.001 | Command: Command Execution |
| Discovery | System Service Discovery | T1007 | Command: Command Execution |
| Execution | System Services: Service Execution | T1569.002 | Command: Command Execution |
| Discovery | System Time Discovery | T1124 | Command: Command Execution |
| Defense Evasion | Trusted Developer Utilities Proxy Execution | T1127 | Command: Command Execution |
| Defense Evasion | Trusted Developer Utilities Proxy Execution: MSBuild | T1127.001 | Command: Command Execution |
| Credential Access | Unsecured Credentials: Credentials in Registry | T1552.002 | Command: Command Execution |
| Credential Access | Unsecured Credentials: Group Policy Preferences | T1552.006 | Command: Command Execution |
| Execution | Windows Management Instrumentation | T1047 | Command: Command Execution |
| Initial Access, Lateral Movement | Replication Through Removable Media | T1091 | Drive: Drive Creation |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: LSASS Driver | T1547.008 | Driver: Driver Load |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Print Processors | T1547.012 | Driver: Driver Load |
| Defense Evasion, Persistence | Pre-OS Boot: Component Firmware | T1542.002 | Driver: Driver Metadata |
| Credential Access | Forced Authentication | T1187 | File: File Access |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Port Monitors | T1547.010 | File: File Creation |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Shortcut Modification | T1547.009 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: DLL Search Order Hijacking | T1574.001 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: DLL Side-Loading | T1574.002 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Executable Installer File Permissions Weakness | T1574.005 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Path Interception by PATH Environment Variable | T1574.007 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Path Interception by Search Order Hijacking | T1574.008 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Path Interception by Unquoted Path | T1574.009 | File: File Creation |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Services File Permissions Weakness | T1574.010 | File: File Creation |
| Credential Access, Defense Evasion, Persistence | Modify Authentication Process: Password Filter DLL | T1556.002 | File: File Creation |
| Defense Evasion | Subvert Trust Controls: Mark-of-the-Web Bypass | T1553.005 | File: File Creation |
| Lateral Movement | Taint Shared Content | T1080 | File: File Creation |
| Defense Evasion, Privilege Escalation | Process Injection: Process Doppelgänging | T1055.013 | File: File Metadata |
| Credential Access, Defense Evasion, Persistence | Modify Authentication Process: Domain Controller Authentication | T1556.001 | File: File Modification |
| Defense Evasion | Subvert Trust Controls: SIP and Trust Provider Hijacking | T1553.003 | File: File Modification |
| Defense Evasion, Persistence | Pre-OS Boot: System Firmware | T1542.001 | Firmware: Firmware Modification |
| Collection | Man in the Browser | T1185 | Logon Session: Logon Session Creation |
| Lateral Movement | Remote Services: Remote Desktop Protocol | T1021.001 | Logon Session: Logon Session Creation |
| Credential Access | Steal or Forge Kerberos Tickets: Silver Ticket | T1558.002 | Logon Session: Logon Session Metadata |
| Execution | Inter-Process Communication | T1559 | Module: Module Load |
| Execution | Inter-Process Communication: Component Object Model | T1559.001 | Module: Module Load |
| Execution | Inter-Process Communication: Dynamic Data Exchange | T1559.002 | Module: Module Load |
| Defense Evasion, Privilege Escalation | Process Injection: Dynamic-link Library Injection | T1055.001 | Module: Module Load |
| Lateral Movement | Remote Services: Distributed Component Object Model | T1021.003 | Module: Module Load |
| Execution | Shared Modules | T1129 | Module: Module Load |

| tactics | technique | ID | DS |
|---|---|---|---|
| Defense Evasion | XSL Script Processing | T1220 | Module: Module Load |
| Defense Evasion | Template Injection | T1221 | Network Traffic: Network Connection Creation |
| Collection, Credential Access | Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay | T1557.001 | Network Traffic: Network Traffic Flow |
| Defense Evasion, Privilege Escalation | Access Token Manipulation: Parent PID Spoofing | T1134.004 | Process: OS API Execution |
| Collection, Credential Access | Input Capture: Credential API Hooking | T1056.004 | Process: OS API Execution |
| Defense Evasion, Privilege Escalation | Process Injection: Asynchronous Procedure Call | T1055.004 | Process: OS API Execution |
| Defense Evasion, Privilege Escalation | Process Injection: Extra Window Memory Injection | T1055.011 | Process: OS API Execution |
| Defense Evasion, Privilege Escalation | Process Injection: Portable Executable Injection | T1055.002 | Process: OS API Execution |
| Defense Evasion, Privilege Escalation | Process Injection: Process Hollowing | T1055.012 | Process: OS API Execution |
| Defense Evasion, Privilege Escalation | Process Injection: Thread Execution Hijacking | T1055.003 | Process: OS API Execution |
| Defense Evasion, Privilege Escalation | Process Injection: Thread Local Storage | T1055.005 | Process: OS API Execution |

# MacOS only Techniques and Sub-techniques

| tactics | technique | ID |
|---|---|---|
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Re-opened Applications | T1547.007 |
| Persistence, Privilege Escalation | Boot or Logon Initialization Scripts: Logon Script (Mac) | T1037.002 |
| Persistence, Privilege Escalation | Boot or Logon Initialization Scripts: Startup Items | T1037.005 |
| Execution | Command and Scripting Interpreter: AppleScript | T1059.002 |
| Persistence, Privilege Escalation | Create or Modify System Process: Launch Agent | T1543.001 |
| Persistence, Privilege Escalation | Create or Modify System Process: Launch Daemon | T1543.004 |
| Credential Access | Credentials from Password Stores: Keychain | T1555.001 |
| Persistence, Privilege Escalation | Event Triggered Execution: Emond | T1546.014 |
| Persistence, Privilege Escalation | Event Triggered Execution: LC_LOAD_DYLIB Addition | T1546.006 |
| Execution, Persistence, Privilege Escalation | Scheduled Task/Job: Launchd | T1053.004 |
| Defense Evasion | Subvert Trust Controls: Gatekeeper Bypass | T1553.001 |
| Execution | System Services: Launchctl | T1569.001 |
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: Plist Modification | T1547.011 |
| Defense Evasion, Persistence, Privilege Escalation | Hijack Execution Flow: Dylib Hijacking | T1574.004 |
| Defense Evasion | Hide Artifacts: Hidden Users | T1564.002 |
| Defense Evasion, Privilege Escalation | Abuse Elevation Control Mechanism: Elevated Execution with Prompt | T1548.004 |

## Linux only Techniques and Sub-techniques

| tactics | technique | ID |
|---|---|---|
| Persistence, Privilege Escalation | Boot or Logon Autostart Execution: XDG Autostart Entries | T1547.013 |
| Persistence, Privilege Escalation | Create or Modify System Process: Systemd Service | T1543.002 |
| Credential Access | OS Credential Dumping: /etc/passwd and /etc/shadow | T1003.008 |
| Credential Access | OS Credential Dumping: Proc Filesystem | T1003.007 |
| Execution, Persistence, Privilege Escalation | Scheduled Task/Job: At (Linux) | T1053.001 |
| Execution, Persistence, Privilege Escalation | Scheduled Task/Job: Systemd Timers | T1053.006 |
| Defense Evasion, Privilege Escalation | Process Injection: Proc Memory | T1055.009 |
| Defense Evasion, Privilege Escalation | Process Injection: VDSO Hijacking | T1055.014 |
| Defense Evasion, Privilege Escalation | Process Injection: Ptrace System Calls | T1055.008 |