ATT&CK Matrix for Enterprise

ID: TA0040 Impact

11 Techniques

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

- T1529 - System Shutdown/Reboot
- T1489 - Service Stop
- T1496 - Resource Hijacking
- T1498 - Network Denial of Service
  - Direct Network Flood
  - Reflection Amplification
- T1490 - Inhibit System Recovery
- T1495 - Firmware Corruption
- T1531 - Account Access Removal
- T1485 - Data Destruction
- T1486 - Data Encrypted for Impact
- T1565 - Data Manipulation
  - Stored Data Manipulation
  - Transmitted Data Manipulation
  - Runtime Data Manipulation
- T1491 - Defacement
  - Internal Defacement
  - External Defacement
- T1561 - Disk Wipe
  - Disk Content Wipe
  - Disk Structure Wipe
- T1499 - Endpoint Denial of Service
  - OS Exhaustion Flood
  - Service Exhaustion Flood
  - Application Exhaustion Flood
  - Application or System Exploitation

ID: TA0010 Exfiltration

9 Techniques

The adversary is trying to steal data.

- T1537 - Transfer Data to Cloud Account
- T1029 - Scheduled Transfer
- T1567 - Exfiltration Over Web Service
  - Exfiltration to Code Repository
  - Exfiltration to Cloud Storage
- T1052 - Exfiltration Over Physical Medium
  - Exfiltration over USB
- T1020 - Automated Exfiltration
  - Traffic Duplication
- T1030 - Data Transfer Size Limits
- T1048 - Exfiltration Over Alternative Protocol
  - Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted Non-C2 Protocol
- T1041 - Exfiltration Over C2 Channel
- T1011 - Exfiltration Over Other Network Medium
  - Exfiltration Over Bluetooth

ID: TA0011 Command and Control

16 Techniques

The adversary is trying to communicate with compromised systems to control them.

- Dead Drop Resolver
- Bidirectional Communication
- One Way Communication
- T1071 - Application Layer Protocol
  - Web Protocols
  - File Transfer Protocols
  - Mail Protocols
  - DNS
- T1092 - Communication Through Removable Media
- T1132 - Data Encoding
  - Standard Encoding
  - Non-Standard Encoding
- T1001 - Data Obfuscation
  - Junk Data
  - Steganography
  - Protocol Impersonation
- T1568 - Dynamic Resolution
  - Fast Flux DNS
  - Domain Generation Algorithms
  - DNS Calculation
- T1573 - Encrypted Channel
  - Symmetric Cryptography
  - Asymmetric Cryptography
- T1008 - Fallback Channels
- T1105 - Ingress Tool Transfer
- T1104 - Multi-Stage Channels
- T1095 - Non-Application Layer Protocol
- T1571 - Non-Standard Port
- T1572 - Protocol Tunneling
- T1090 - Proxy
  - Internal Proxy
  - External Proxy
  - Multi-hop Proxy
  - Domain Fronting
- T1219 - Remote Access Software
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1102 - Web Service
  - Dead Drop Resolver
  - Bidirectional Communication
  - One Way Communication

ID: TA0009 Collection

17 Techniques

The adversary is trying to gather data of interest to their goal.

- T1123 - Audio Capture
- T1119 - Automated Collection
- T1185 - Browser Session Hijacking
- T1115 - Clipboard Data
- T1530 - Data from Cloud Storage
- T1602 - Data from Configuration Repository
  - SNMP (MIB Dump)
  - Network Device Configuration Dump
- T1213 - Data from Information Repositories
  - Confluence
  - Sharepoint
  - Code Repositories
- T1005 - Data from Local System
- T1039 - Data from Network Shared Drive
- T1025 - Data from Removable Media
- T1074 - Data Staged
  - Local Data Staging
  - Remote Data Staging
- T1114 - Email Collection
  - Local Email Collection
  - Remote Email Collection
  - Email Forwarding Rule
- T1056 - Input Capture
  - Keylogging
  - GUI Input Capture
  - Web Portal Capture
  - Credential API Hooking
- T1113 - Screen Capture
- T1125 - Video Capture
- T1071 - Application Layer Protocol
  - Web Protocols
  - File Transfer Protocols
  - Mail Protocols
  - DNS
- T1092 - Communication Through Removable Media
- T1132 - Data Encoding
  - Standard Encoding
  - Non-Standard Encoding
- T1001 - Data Obfuscation
  - Junk Data
  - Steganography
  - Protocol Impersonation
- T1568 - Dynamic Resolution
  - Fast Flux DNS
  - Domain Generation Algorithms
  - DNS Calculation
- T1573 - Encrypted Channel
  - Symmetric Cryptography
  - Asymmetric Cryptography
- T1008 - Fallback Channels
- T1105 - Ingress Tool Transfer
- T1104 - Multi-Stage Channels
- T1095 - Non-Application Layer Protocol
- T1571 - Non-Standard Port
- T1572 - Protocol Tunneling
- T1090 - Proxy
  - Internal Proxy
  - External Proxy
  - Multi-hop Proxy
  - Domain Fronting
- T1219 - Remote Access Software
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1102 - Web Service
  - Dead Drop Resolver
  - Bidirectional Communication
  - One Way Communication

ID: TA0008 Lateral Movement

9 Techniques

The adversary is trying to move through your environment.

- T1550 - Use Alternate Authentication Material
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie
- T1080 - Taint Shared Content
- T1072 - Software Deployment Tools
- T1091 - Replication Through Removable Media
- T1210 - Exploitation of Remote Services
- T1534 - Internal Spearphishing
- T1570 - Lateral Tool Transfer
- T1563 - Remote Service Session Hijacking
  - SSH Hijacking
  - RDP Hijacking
- T1021 - Remote Services
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - Distributed Component Object Model
  - SSH
  - VNC
  - Windows Remote Management

ID: TA0007 Discovery

30 Techniques

The adversary is trying to figure out your environment.

- T1087 - Account Discovery
  - Local Account
  - Domain Account
  - Email Account
  - Cloud Account
- T1010 - Application Window Discovery
- T1217 - Browser Bookmark Discovery
- T1580 - Cloud Infrastructure Discovery
- T1538 - Cloud Service Dashboard
- T1526 - Cloud Service Discovery
- T1619 - Cloud Storage Object Discovery
- T1613 - Container and Resource Discovery
- T1622 - Debugger Evasion
- T1482 - Domain Trust Discovery
- T1083 - File and Directory Discovery
- T1615 - Group Policy Discovery
- T1046 - Network Service Discovery
- T1135 - Network Share Discovery
- T1040 - Network Sniffing
- T1120 - Peripheral Device Discovery
- T1069 - Permission Groups Discovery
  - Local Groups
  - Domain Groups
  - Cloud Groups
- T1057 - Process Discovery
- T1012 - Query Registry
- T1018 - Remote System Discovery
- T1082 - System Information Discovery
- T1016 - System Network Configuration Discovery
  - Internet Connection Discovery
- T1049 - System Network Connections Discovery
- T1033 - System Owner/User Discovery
- T1007 - System Service Discovery
- T1014 - Rootkit
- T1497 - Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion
- T1124 - System Time Discovery
- T1007 - System Service Discovery
- T1033 - System Owner/User Discovery
- T1049 - System Network Connections Discovery
- T1016 - System Network Configuration Discovery
  - Internet Connection Discovery
- T1614 - System Location Discovery
  - System Language Discovery
- T1082 - System Information Discovery
- T1518 - Software Discovery
  - Security Software Discovery
- T1018 - Remote System Discovery
- T1012 - Query Registry
- T1057 - Process Discovery
- T1069 - Permission Groups Discovery
  - Local Groups
  - Domain Groups
  - Cloud Groups
- T1120 - Peripheral Device Discovery
- T1201 - Password Policy Discovery

ID: TA0004 Privilege Escalation

- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- T1053 - Scheduled Task/Job
  - At
  - Cron
  - Scheduled Task
  - Systemd Timers
  - Container Orchestration Job
- T1055 - Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
  - Thread Execution Hijacking
  - Asynchronous Procedure Call
  - Thread Local Storage
  - Ptrace System Calls
  - Proc Memory
  - Extra Window Memory Injection
  - Process Doppelgänging
  - VDSO Hijacking
  - Listhijacking
- T1574 - Hijack Execution Flow
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - Dylib Hijacking
  - Executable Installer File Permissions Weakness
  - Hijacking
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - Path Interception by Unquoted Path
  - Services File Permissions Weakness
  - Services Registry Permissions Weakness
  - COR_PROFILER
  - KernelCallbackTable
- T1068 - Exploitation for Privilege Escalation
- T1546 - Event Triggered Execution
  - Change Default File Association
  - Screensaver
  - Windows Management Instrumentation Event Subscription
  - Unix Shell Configuration Modification
  - Trap
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - Applnit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - PowerShell Profile
  - Emond
  - Component Object Model Hijacking
  - Installer Packages
- T1548 - Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- T1134 - Access Token Manipulation
  - Token Impersonation/Theft
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
- T1547 - Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Print Processors
  - XDG Autostart Entries
  - Active Setup
  - Login Items
- T1037 - Boot or Logon Initialization Scripts
  - Logon Script (Windows)
  - Login Hook
  - Network Logon Script
  - RC Scripts
  - Startup Items
- T1543 - Create or Modify System Process
  - Launch Agent
  - System Service
  - Windows Service
  - Launch Daemon
- T1484 - Domain Policy Modification
  - Group Policy Modification
  - Domain Trust Modification
- T1611 - Escape to Host

@hackinarticles

https://github.com/SigniteTechnologies

https://in.linkedin.com/company/hackingarticles

ID: TA0043 Reconnaissance

10 Techniques

The adversary is trying to gather information they can use to plan future operations.

- T1594 - Search Victim-Owned Websites
- T1593 - Search Open Websites/Domains
  - Social Media
  - Search Engines
  - Code Repositories
- T1596 - Search Open Technical Databases
  - DNS/Passive DNS
  - WHOIS
  - Digital Certificates
  - CDNs
  - Scan Databases
- T1597 - Search Closed Sources
  - Threat Intel Vendors
  - Purchase Technical Data
- T1598 - Phishing for Information
  - Spearphishing Service
  - Spearphishing Attachment
  - Spearphishing Link
- T1595 - Active Scanning
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- T1592 - Gather Victim Host Information
  - Hardware
  - Software
  - Firmware
  - Client Configurations
- T1589 - Gather Victim Identity Information
  - Credentials
  - Email Addresses
  - Employee Names
- T1590 - Gather Victim Network Information
  - Domain Properties
  - DNS
  - Network Trust Dependencies
  - Network Topology
  - IP Addresses
  - Network Security Appliances
- T1591 - Gather Victim Org Information
  - Determine Physical Locations
  - Business Relationships
  - Identify Business Tempo
  - Identify Roles

ID: TA0042 Resource Development

7 Techniques

The adversary is trying to establish resources they can use to support operations.

- T1608 - Stage Capabilities
  - Upload Malware
  - Upload Tool
  - Install Digital Certificate
  - Drive-by Target
  - Link Target
  - SEO Poisoning
- T1588 - Obtain Capabilities
  - Malware
  - Tool
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Vulnerabilities
- T1585 - Establish Accounts
  - Social Media Accounts
  - Email Accounts
  - Cloud Accounts
- T1583 - Acquire Infrastructure
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
  - Serverless
- T1586 - Compromise Accounts
  - Social Media Accounts
  - Email Accounts
  - Cloud Accounts
- T1584 - Compromise Infrastructure
  - Domains
  - DNS Server
  - Virtual Private Server
  - Server
  - Botnet
  - Web Services
  - Serverless
- T1587 - Develop Capabilities
  - Malware
  - Code Signing Certificates
  - Digital Certificates
  - Exploits

ID: TA0001 Initial Access

9 Techniques

The adversary is trying to get into your network.

- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- T1189 - Drive by Compromise
- T1190 - Exploit Public-Facing Application
- T1133 - External Remote Services
- T1200 - Hardware Additions
- T1566 - Phishing
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- T1091 - Replication Through Removable Media
- T1195 - Supply Chain Compromise
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
- T1199 - Trusted Relationship
- T1659 - Content Injection

ID: TA0002 Execution

13 Techniques

The adversary is trying to run malicious code.

- T1047 - Windows Management Instrumentation
- T1204 - User Execution
  - Malicious Link
  - Malicious File
  - Malicious Image
- T1569 - System Services
  - Launchctl
  - Service Execution
- T1072 - Software Deployment Tools
- T1129 - Shared Modules
- T1648 - Serverless Execution
- T1059 - Command and Scripting Interpreter
  - PowerShell
  - AppleScript
  - Windows Command Shell
  - Unix Shell
  - Visual Basic
  - Python
  - JavaScript
  - Network Device CLI
- T1609 - Container Administration Command
- T1610 - Deploy Container
- T1203 - Exploitation for Client Execution
- T1559 - Inter-Process Communication
  - Component Object Model
  - Dynamic Data Exchange
  - XPC Services
- T1106 - Native API
- T1053 - Scheduled Task/Job
  - At
  - Cron
  - Scheduled Task
  - Systemd Timers
  - Container Orchestration Job

ID: TA0003 Persistence

19 Techniques

The adversary is trying to maintain their foothold.

- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1505 - Server Software Component
  - SQL Stored Procedures
  - Transport Agent
  - Web Shell
  - IIS Components
  - Terminal Services DLL
- T1053 - Scheduled Task/Job
  - At
  - Cron
  - Scheduled Task
  - Systemd Timers
  - Container Orchestration Job
- T1542 - Pre-OS Boot
  - System Firmware
  - Component Firmware
  - Bootkit
  - TFTP Boot
  - ROMMONkit
- T1137 - Office Application Startup
  - Office Template Macros
  - Office Test
  - Outlook Forms
  - Outlook Home Page
  - Outlook Rules
  - Add-ins
- T1556 - Modify Authentication Process
  - Domain Controller Authentication
  - Password Filter DLL
  - Pluggable Authentication Modules
  - Network Device Authentication
  - Reversible Encryption
  - Multi Factor Authentication
  - Hybrid Identity
- T1525 - Implant Internal Image
- T1574 - Hijack Execution Flow
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - Dylib Hijacking
  - Executable Installer File Permissions Weakness
  - Dynamic Linker Hijacking
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - Path Interception by Unquoted Path
  - Services File Permissions Weakness
  - Services Registry Permissions Weakness
  - COR_PROFILER
  - KernelCallbackTable
- T1098 - Account Manipulation
  - Additional Cloud Credentials
  - Additional Email Delegate Permissions
  - Additional Cloud Roles
  - SSH Authorized Keys
  - Device Registration
- T1197 - BITS Jobs
- T1547 - Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
  - Authentication Package
  - Time Providers
  - Winlogon Helper DLL
  - Security Support Provider
  - Kernel Modules and Extensions
  - Re-opened Applications
  - LSASS Driver
  - Shortcut Modification
  - Port Monitors
  - Print Processors
  - XDG Autostart Entries
  - Active Setup
  - Login Items
- T1037 - Boot or Logon Initialization Scripts
  - Logon Script (Windows)
  - Login Hook
  - Network Logon Script
  - RC Scripts
  - Startup Items
- T1176 - Browser Extensions
- T1554 - Compromise Client Software Binary
- T1136 - Create Account
  - Local Account
  - Domain Account
  - Cloud Account
- T1543 - Create or Modify System Process
  - Launch Agent
  - System Service
  - Windows Service
  - Launch Daemon
- T1546 - Event Triggered Execution
  - Change Default File Association
  - Screensaver
  - Windows Management Instrumentation Event Subscription
  - Unix Shell Configuration Modification
  - Trap
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - Accessibility Features
  - AppCert DLLs
  - Applnit DLLs
  - Application Shimming
  - Image File Execution Options Injection
  - PowerShell Profile
  - Emond
  - Component Object Model Hijacking
  - Installer Packages
- T1133 - External Remote Services

ID: TA0005 Defense Evasion

42 Techniques

The adversary is trying to avoid being detected.

- T1220 - XSL Script Processing
- T1400 - Weaken Encryption
  - Reduce Key Space
  - Disable Crypto Hardware
- T1497 - Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion
- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- T1550 - Use Alternate Authentication Material
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie
- T1535 - Unused/Unsupported Cloud Regions
- T1127 - Trusted Developer Utilities Proxy Execution
  - MSBuild
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1221 - Template Injection
- T1216 - System Script Proxy Execution
  - Pubprn
- T1218 - System Binary Proxy Execution
  - Compiled HTML File
  - Control Panel
  - CMSTP
  - Installutil
  - Mshta
  - Msiexec
  - Odbcconf
  - Regsvcs/Regasm
  - Regsvr32
  - Rundll32
  - Verclsid
  - Mavinject
  - WMIC
- T1553 - Subvert Trust Controls
  - Gatekeeper Bypass
  - Code Signing
  - SIP and Trust Provider Hijacking
  - Install Root Certificate
  - Mark-of-the-Web Bypass
  - Code Signing Policy Modification
- T1014 - Rootkit
- T1207 - Rogue Domain Controller
- T1620 - Reflective Code Loading
- T1055 - Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
  - Thread Execution Hijacking
  - Asynchronous Procedure Call
  - Thread Local Storage
  - Ptrace System Calls
  - Proc Memory
  - Extra Window Memory Injection
  - Process Hollowing
  - Process Doppelgänging
  - VDSO Hijacking
  - Listhijacking
- T1542 - Pre-OS Boot
  - System Firmware
  - Component Firmware
  - Bootkit
  - ROMMONkit
  - TFTP Boot
- T1647 - Plist File Modification
- T1027 - Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
  - HTML Smuggling
  - Dynamic API Resolution
  - Stripped Payloads
  - Embedded Payloads
- T1599 - Network Boundary Bridging
  - Network Address Translation Traversal
- T1601 - Modify System Image
  - Patch System Image
  - Downgrade System Image
- T1480 - Execution Guardrails
  - Environmental Keying
- T1211 - Exploitation for Defense Evasion
- T1222 - File and Directory Permissions Modification
  - Windows File and Directory Permissions Modification
  - Linux and Mac File and Directory Permissions Modification
- T1574 - Hijack Execution Flow
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - Dylib Hijacking
  - Executable Installer File Permissions Weakness
  - Dynamic Linker Hijacking
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - Path Interception by Unquoted Path
  - Services File Permissions Weakness
  - Services Registry Permissions Weakness
  - COR_PROFILER
  - KernelCallbackTable
- T1562 - Impair Defenses
  - Disable or Modify Tools
  - Disable Windows Event Logging
  - Impair Command History Logging
  - Disable or Modify System Firewall
  - Indicator Blocking
  - Disable or Modify Cloud Firewall
  - Disable Cloud Logs
  - Safe Mode Boot
  - Downgrade Attack
- T1070 - Indicator Removal
  - Clear Windows Event Logs
  - Clear Linux or Mac System Logs
  - Clear Command History
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
  - Clear Network Connection History and Configurations
  - Clear Mailbox Data
  - Clear Persistence
- T1556 - Modify Authentication Process
  - Domain Controller Authentication
  - Password Filter DLL
  - Pluggable Authentication Modules
  - Network Device Authentication
  - Reversible Encryption
  - Multi Factor Authentication
  - Hybrid Identity
- T1578 - Modify Cloud Compute Infrastructure
  - Create Snapshot
  - Create Cloud Instance
  - Delete Cloud Instance
  - Revert Cloud Instance
- T1112 - Modify Registry
- T1601 - Modify System Image
  - Patch System Image
  - Downgrade System Image
- T1599 - Network Boundary Bridging
  - Network Address Translation Traversal
- T1027 - Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
  - HTML Smuggling
  - Dynamic API Resolution
  - Stripped Payloads
  - Embedded Payloads
- T1647 - Plist File Modification
- T1542 - Pre-OS Boot
  - System Firmware
  - Component Firmware
  - Bootkit
  - ROMMONkit
  - TFTP Boot
- T1014 - Rootkit
- T1207 - Rogue Domain Controller
- T1620 - Reflective Code Loading
- T1553 - Subvert Trust Controls
  - Gatekeeper Bypass
  - Code Signing
  - SIP and Trust Provider Hijacking
  - Install Root Certificate
  - Mark-of-the-Web Bypass
  - Code Signing Policy Modification
- T1211 - Exploitation for Defense Evasion
- T1222 - File and Directory Permissions Modification
  - Windows File and Directory Permissions Modification
  - Linux and Mac File and Directory Permissions Modification
- T1562 - Impair Defenses
  - Disable or Modify Tools
  - Disable Windows Event Logging
  - Impair Command History Logging
  - Disable or Modify System Firewall
  - Indicator Blocking
  - Disable or Modify Cloud Firewall
  - Disable Cloud Logs
  - Safe Mode Boot
  - Downgrade Attack
- T1070 - Indicator Removal
  - Clear Windows Event Logs
  - Clear Linux or Mac System Logs
  - Clear Command History
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
  - Clear Network Connection History and Configurations
  - Clear Mailbox Data
  - Clear Persistence
- T1578 - Modify Cloud Compute Infrastructure
  - Create Snapshot
  - Create Cloud Instance
  - Delete Cloud Instance
  - Revert Cloud Instance
- T1112 - Modify Registry
- T1601 - Modify System Image
  - Patch System Image
  - Downgrade System Image
- T1599 - Network Boundary Bridging
  - Network Address Translation Traversal
- T1027 - Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
  - HTML Smuggling
  - Dynamic API Resolution
  - Stripped Payloads
  - Embedded Payloads
- T1647 - Plist File Modification
- T1542 - Pre-OS Boot
  - System Firmware
  - Component Firmware
  - Bootkit
  - ROMMONkit
  - TFTP Boot
- T1014 - Rootkit
- T1207 - Rogue Domain Controller
- T1620 - Reflective Code Loading
- T1553 - Subvert Trust Controls
  - Gatekeeper Bypass
  - Code Signing
  - SIP and Trust Provider Hijacking
  - Install Root Certificate
  - Mark-of-the-Web Bypass
  - Code Signing Policy Modification
- T1211 - Exploitation for Defense Evasion
- T1222 - File and Directory Permissions Modification
  - Windows File and Directory Permissions Modification
  - Linux and Mac File and Directory Permissions Modification
- T1574 - Hijack Execution Flow
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - Dylib Hijacking
  - Executable Installer File Permissions Weakness
  - Dynamic Linker Hijacking
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - Path Interception by Unquoted Path
  - Services File Permissions Weakness
  - Services Registry Permissions Weakness
  - COR_PROFILER
  - KernelCallbackTable
- T1562 - Impair Defenses
  - Disable or Modify Tools
  - Disable Windows Event Logging
  - Impair Command History Logging
  - Disable or Modify System Firewall
  - Indicator Blocking
  - Disable or Modify Cloud Firewall
  - Disable Cloud Logs
  - Safe Mode Boot
  - Downgrade Attack
- T1070 - Indicator Removal
  - Clear Windows Event Logs
  - Clear Linux or Mac System Logs
  - Clear Command History
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
  - Clear Network Connection History and Configurations
  - Clear Mailbox Data
  - Clear Persistence
- T1556 - Modify Authentication Process
  - Domain Controller Authentication
  - Password Filter DLL
  - Pluggable Authentication Modules
  - Network Device Authentication
  - Reversible Encryption
  - Multi Factor Authentication
  - Hybrid Identity
- T1578 - Modify Cloud Compute Infrastructure
  - Create Snapshot
  - Create Cloud Instance
  - Delete Cloud Instance
  - Revert Cloud Instance
- T1112 - Modify Registry

ID: TA0006 Credential Access

17 Techniques

The adversary is trying to steal account names and passwords.

- Credentials In Files
- Credentials in Registry
- Bash History
- Private Keys
- T1552 - Unsecured Credentials
  - Cloud Instance Metadata API
  - Group Policy Preferences
  - Container API
- T1557 - Adversary-in-the-Middle
  - LLMNR/NBT-NS Poisoning and SMB Relay
  - ARP Cache Poisoning
  - DHCP Spoofing
- T1110 - Brute Force
  - Password Guessing
  - Password Cracking
  - Password Spraying
  - Credential Stuffing
- T1555 - Credentials from Password Stores
  - Keychain
  - Securityd Memory
  - Credentials from Web Browsers
  - Windows Credential Manager
  - Password Managers
- T1212 - Exploitation for Credential Access
- T1187 - Forced Authentication
- T1606 - Forge Web Credentials
  - Web Cookies
  - SAML Tokens
- T1056 - Input Capture
  - Keylogging
  - GUI Input Capture
  - Web Portal Capture
  - Credential API Hooking
- T1556 - Modify Authentication Process
  - Domain Controller Authentication
  - Password Filter DLL
  - Pluggable Authentication Modules
  - Network Device Authentication
  - Reversible Encryption
  - Multi Factor Authentication
  - Hybrid Identity
- T1111 - Multi-Factor Authentication Interception
- T1621 - Multi-Factor Authentication Request Generation
- T1539 - Steal Web Session Cookie
- T1558 - Steal or Forge Kerberos Tickets
  - Golden Ticket
  - Silver Ticket
  - Kerberoasting
  - AS-REP Roasting
- T1649 - Steal or Forge Authentication Certificates
- T1528 - Steal Application Access Token
- T1003 - OS Credential Dumping
  - LSASS Memory
  - Security Account Manager
  - NTDS
  - LSA Secrets
  - Cached Domain Credentials
  - DCSync
  - Proc Filesystem
  - /etc/passwd and /etc/shadow
- T1040 - Network Sniffing