Enterprise Tactics

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10	8	10	14	20	14	44	17	32	9	17	18	9	14

Reconnaissance (10)
- **Active Scanning (3)**: Scanning IP Blocks; Vulnerability Scanning; Wordlist Scanning
- **Gather Victim Host Information (4)**: Hardware; Software; Firmware; Client Configurations
- **Gather Victim Identity Information (3)**: Credentials; Email Addresses; Employee Names
- **Gather Victim Network Information (6)**: Domain Properties; DNS; Network Trust Dependencies; Network Topology; IP Addresses; Network Security Appliances
- **Gather Victim Org Information (4)**: Determine Physical Locations; Business Relationships; Identify Business Tempo; Identify Roles
- **Phishing for Information (3)**: Spearphishing Service; Spearphishing Attachment; Spearphishing Link; Spearphishing Voice
- **Search Closed Sources (2)**: Threat Intel Vendors; Purchase Technical Data
- **Search Open Technical Databases (5)**: DNS/Passive DNS; WHOIS; Digital Certificates; CDNs; Scan Databases
- **Search Open Websites/Domains (3)**: Social Media; Search Engines; Code Repositories
- **Search Victim-Owned Websites**

Resource Development (8)
- **Acquire Access**
- **Acquire Infrastructure (8)**: Domains; DNS Server; Virtual Private Server; Server; Botnet; Web Services; Serverless; Malvertising
- **Compromise Accounts (3)**: Social Media Accounts; Email Accounts; Cloud Accounts
- **Compromise Infrastructure (8)**: Domains; DNS Server; Virtual Private Server; Server; Botnet; Web Services; Serverless; Network Devices
- **Develop Capabilities (4)**: Malware; Code Signing Certificates; Digital Certificates; Exploits
- **Establish Accounts (3)**: Social Media Accounts; Email Accounts; Cloud Accounts
- **Obtain Capabilities (7)**: Malware; Tool; Code Signing Certificates; Digital Certificates; Exploits; Vulnerabilities; Artificial Intelligence
- **Stage Capabilities (6)**: Upload Malware; Upload Tool; Install Digital Certificate; Drive-by Target; Link Target; SEO Poisoning; Content Injection

Initial Access (10)
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- **Phishing (4)**: Spearphishing Attachment; Spearphishing Link; Spearphishing via Service; Spearphishing Voice
- Replication Through Removable Media
- **Supply Chain Compromise (3)**: Compromise Software Dependencies and Development Tools; Compromise Software Supply Chain; Compromise Hardware Supply Chain
- Trusted Relationship
- **Valid Accounts (4)**: Default Accounts; Domain Accounts; Local Accounts; Cloud Accounts

Execution (14)
- Cloud Administration Command
- **Command and Scripting Interpreter (11)**: PowerShell; AppleScript; Windows Command Shell; Unix Shell; Visual Basic; Python; JavaScript; Network Device CLI; Cloud API; AutoHotKey & AutoIT; Lua
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- **Inter-Process Communication (3)**: Component Object Model; Dynamic Data Exchange; XPC Services
- Native API
- **Scheduled Task/Job (5)**: At; Cron; Scheduled Task; Systemd Timers; Container Orchestration Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- **System Services (2)**: Launchctl; Service Execution
- **User Execution (3)**: Malicious Link; Malicious File; Malicious Image
- Windows Management Instrumentation

Persistence (20)
- **Account Manipulation (7)**: Additional Cloud Credentials; Additional Email Delegate Permissions; Additional Cloud Roles; SSH Authorized Keys; Device Registration; Additional Container Cluster Roles; Additional Local or Domain Groups
- BITS Jobs
- **Boot or Logon Autostart Execution (14)**: 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
- **Boot or Logon Initialization Scripts (5)**: Logon Script (Windows); Login Hook; Network Logon Script; RC Scripts; Startup Items
- Browser Extensions
- Compromise Host Software Binary
- **Create Account (3)**: Local Account; Domain Account; Cloud Account
- **Create or Modify System Process (5)**: Launch Agent; Systemd Service; Windows Service; Launch Daemon; Container Service
- **Event Triggered Execution (17)**: 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; AppInit DLLs; Application Shimming; Image File Execution Options Injection; PowerShell Profile; Emond; Component Object Model Hijacking; Installer Packages; Udev Rules
- External Remote Services
- **Hijack Execution Flow (13)**: 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; AppDomainManager
- Implant Internal Image
- **Modify Authentication Process (9)**: Domain Controller Authentication; Password Filter DLL; Pluggable Authentication Modules; Network Device Authentication; Reversible Encryption; Multi-Factor Authentication; Hybrid Identity; Network Provider DLL; Conditional Access Policies
- **Office Application Startup (6)**: Office Template Macros; Office Test; Outlook Forms; Outlook Home Page; Outlook Rules; Add-ins; Power Settings
- **Pre-OS Boot (5)**: System Firmware; Component Firmware; Bootkit; ROMMONkit; TFTP Boot
- **Scheduled Task/Job (5)**: At; Cron; Scheduled Task; Systemd Timers; Container Orchestration Job
- **Server Software Component (5)**: SQL Stored Procedures; Transport Agent; Web Shell; IIS Components; Terminal Services DLL
- **Valid Accounts (4)**: Default Accounts; Domain Accounts; Local Accounts; Cloud Accounts

Privilege Escalation (14)
- **Abuse Elevation Control Mechanism (6)**: Setuid and Setgid; Bypass User Account Control; Sudo and Sudo Caching; Elevated Execution with Prompt; Temporary Elevated Cloud Access; TCC Manipulation
- **Access Token Manipulation (5)**: Token Impersonation/Theft; Create Process with Token; Make and Impersonate Token; Parent PID Spoofing; SID-History Injection
- **Account Manipulation (7)**: Additional Cloud Credentials; Additional Email Delegate Permissions; Additional Cloud Roles; SSH Authorized Keys; Device Registration; Additional Container Cluster Roles; Additional Local or Domain Groups
- **Boot or Logon Autostart Execution (14)**: 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
- **Boot or Logon Initialization Scripts (5)**: Logon Script (Windows); Login Hook; Network Logon Script; RC Scripts; Startup Items
- **Create or Modify System Process (5)**: Launch Agent; Systemd Service; Windows Service; Launch Daemon; Container Service
- **Domain or Tenant Policy Modification (2)**: Group Policy Modification; Trust Modification; Escape to Host
- **Event Triggered Execution (17)**: 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; AppInit DLLs; Application Shimming; Image File Execution Options Injection; PowerShell Profile; Emond; Component Object Model Hijacking; Installer Packages; Udev Rules; External Remote Services
- **Exploitation for Privilege Escalation**
- **Hijack Execution Flow (13)**: 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; AppDomainManager; Implant Internal Image
- **Modify Authentication Process (9)**: Domain Controller Authentication; Password Filter DLL; Pluggable Authentication Modules; Network Device Authentication; Reversible Encryption; Multi-Factor Authentication; Hybrid Identity; Network Provider DLL; Conditional Access Policies
- **Process Injection (12)**: 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; ListPlanting
- **Scheduled Task/Job (5)**: At; Cron; Scheduled Task; Systemd Timers; Container Orchestration Job
- **Valid Accounts (4)**: Default Accounts; Domain Accounts; Local Accounts; Cloud Accounts

Defense Evasion (44)
- **Abuse Elevation Control Mechanism (6)**: Setuid and Setgid; Bypass User Account Control; Sudo and Sudo Caching; Elevated Execution with Prompt; Temporary Elevated Cloud Access; TCC Manipulation
- **Access Token Manipulation (5)**: Token Impersonation/Theft; Create Process with Token; Make and Impersonate Token; Parent PID Spoofing; SID-History Injection
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- **Domain or Tenant Policy Modification (2)**: Group Policy Modification; Trust Modification; Escape to Host
- **Execution Guardrails (2)**: Environmental Keying; Mutual Exclusion
- Exploitation for Defense Evasion
- **File and Directory Permissions Modification (2)**: Windows File and Directory Permissions Modification; Linux and Mac File and Directory Permissions Modification
- **Hide Artifacts (12)**: Hidden Files and Directories; Hidden Users; Hidden Window; NTFS File Attributes; Hidden File System; Run Virtual Instance; VBA Stomping; Email Hiding Rules; Resource Forking; Process Argument Spoofing; Ignore Process Interrupts; File/Path Exclusions
- **Hijack Execution Flow (13)**: 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; AppDomainManager; Implant Internal Image
- **Impair Defenses (11)**: 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 or Modify Cloud Logs; Safe Mode Boot; Downgrade Attack; Spoof Security Alerting; Disable or Modify Linux Audit System; Impersonation
- **Indicator Removal (10)**: 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; Relocate Malware; Indirect Command Execution
- **Masquerading (10)**: Invalid Code Signature; Right-to-Left Override; Rename System Utilities; Masquerade Task or Service; Match Legitimate Name or Location; Space after Filename; Double File Extension; Masquerade File Type; Break Process Trees; Manipulate Account Name
- **Modify Authentication Process (9)**: Domain Controller Authentication; Password Filter DLL; Pluggable Authentication Modules; Network Device Authentication; Reversible Encryption; Multi-Factor Authentication; Hybrid Identity; Network Provider DLL; Conditional Access Policies
- **Modify Cloud Compute Infrastructure (5)**: Create Snapshot; Create Cloud Instance; Delete Cloud Instance; Revert Cloud Instance; Modify Cloud Compute Configurations
- Modify Cloud Resource Hierarchy
- Modify Registry
- **Modify System Image (2)**

Credential Access (17)
- **Adversary-in-the-Middle (4)**: LLMNR/NBT-NS Poisoning and SMB Relay; ARP Cache Poisoning; DHCP Spoofing; Evil Twin
- **Brute Force (4)**: Password Guessing; Password Cracking; Password Spraying; Credential Stuffing
- **Credentials from Password Stores (6)**: Keychain; Securityd Memory; Credentials from Web Browsers; Windows Credential Manager; Password Managers; Cloud Secrets Management Stores; Exploitation for Credential Access; Forced Authentication
- **Forge Web Credentials (2)**: Web Cookies; SAML Tokens
- **Input Capture (4)**: Keylogging; GUI Input Capture; Web Portal Capture; Credential API Hooking
- **Modify Authentication Process (9)**: Domain Controller Authentication; Password Filter DLL; Pluggable Authentication Modules; Network Device Authentication; Reversible Encryption; Multi-Factor Authentication; Hybrid Identity; Network Provider DLL; Conditional Access Policies
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- **OS Credential Dumping (8)**: LSASS Memory; Security Account Manager; NTDS; LSA Secrets; Cached Domain Credentials; DCSync; Proc Filesystem; /etc/passwd and /etc/shadow; Steal Application Access Token; Steal or Forge Authentication Certificates
- **Steal or Forge Kerberos Tickets (5)**: Golden Ticket; Silver Ticket; Kerberoasting; AS-REP Roasting; Ccache Files; Steal Web Session Cookie
- **Unsecured Credentials (8)**: Credentials In Files; Credentials in Registry; Bash History; Private Keys; Cloud Instance Metadata API; Group Policy Preferences; Container API; Chat Messages

Discovery (32)
- **Account Discovery (4)**: Local Account; Domain Account; Email Account; Cloud Account
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- **Permission Groups Discovery (3)**: Local Groups; Domain Groups; Cloud Groups
- Process Discovery
- Query Registry
- Remote System Discovery
- **Software Discovery (1)**: Security Software Discovery
- System Information Discovery
- **System Location Discovery (1)**: System Language Discovery
- **System Network Configuration Discovery (2)**: Internet Connection Discovery; Wi-Fi Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- **Virtualization/Sandbox Evasion (3)**: System Checks; User Activity Based Checks; Time Based Evasion

Lateral Movement (9)
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- **Remote Service Session Hijacking (2)**: SSH Hijacking; RDP Hijacking
- **Remote Services (7)**: Remote Desktop Protocol; SMB/Windows Admin Shares; Distributed Component Object Model; SSH; VNC; Windows Remote Management; Cloud Services; Direct Cloud VM Connections
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- **Use Alternate Authentication Material (4)**: Application Access Token; Pass the Hash; Pass the Ticket; Web Session Cookie

Collection (17)
- **Adversary-in-the-Middle (4)**: LLMNR/NBT-NS Poisoning and SMB Relay; ARP Cache Poisoning; DHCP Spoofing; Evil Twin
- **Archive Collected Data (3)**: Archive via Utility; Archive via Library; Archive via Custom Method
- **Audio Capture**: Automated Collection; Browser Session Hijacking; Clipboard Data; Data from Cloud Storage
- **Data from Configuration Repository (2)**: SNMP (MIB Dump); Network Device Configuration Dump
- **Data from Information Repositories (5)**: Confluence; Sharepoint; Code Repositories; Customer Relationship Management Software; Messaging Applications
- **Data from Local System**: Data from Network Shared Drive; Data from Removable Media
- **Data Staged (2)**: Local Data Staging; Remote Data Staging
- **Email Collection (3)**: Local Email Collection; Remote Email Collection; Email Forwarding Rule
- **Input Capture (4)**: Keylogging; GUI Input Capture; Web Portal Capture; Credential API Hooking
- **Screen Capture**: Video Capture

Command and Control (18)
- **Application Layer Protocol (5)**: Web Protocols; File Transfer Protocols; Mail Protocols; DNS; Publish/Subscribe Protocols
- **Communication Through Removable Media**: Content Injection
- **Data Encoding (2)**: Standard Encoding; Non-Standard Encoding
- **Data Obfuscation (3)**: Junk Data; Steganography; Protocol or Service Impersonation
- **Dynamic Resolution (3)**: Fast Flux DNS; Domain Generation Algorithms; DNS Calculation
- **Encrypted Channel (2)**: Symmetric Cryptography; Asymmetric Cryptography
- **Fallback Channels**: Hide Infrastructure; Ingress Tool Transfer; Multi-Stage Channels; Non-Application Layer Protocol; Non-Standard Port; Protocol Tunneling
- **Proxy (4)**: Internal Proxy; External Proxy; Multi-hop Proxy; Domain Fronting
- **Remote Access Software**
- **Traffic Signaling (2)**: Port Knocking; Socket Filters
- **Web Service (3)**: Dead Drop Resolver; Bidirectional Communication; One-Way Communication

Exfiltration (9)
- **Automated Exfiltration (1)**: Traffic Duplication; Data Transfer Size Limits
- **Exfiltration Over Alternative Protocol (3)**: Exfiltration Over Symmetric Encrypted Non-C2 Protocol; Exfiltration Over Asymmetric Encrypted Non-C2 Protocol; Exfiltration Over Unencrypted Non-C2 Protocol; Exfiltration Over C2 Channel
- **Exfiltration Over Other Network Medium (1)**: Exfiltration Over Bluetooth
- **Exfiltration Over Physical Medium (1)**: Exfiltration over USB
- **Exfiltration Over Web Service (4)**: Exfiltration to Code Repository; Exfiltration to Cloud Storage; Exfiltration to Text Storage Sites; Exfiltration Over Webhook; Scheduled Transfer; Transfer Data to Cloud Account

Impact (14)
- Account access removal
- **Data Destruction (1)**: Lifecycle-Triggered Deletion; Data Encrypted for Impact
- **Data Manipulation (3)**: Stored Data Manipulation; Transmitted Data Manipulation; Runtime Data Manipulation
- **Defacement (2)**: Internal Defacement; External Defacement
- **Disk Wipe (2)**: Disk Content Wipe; Disk Structure Wipe
- **Endpoint Denial of Service (4)**: OS Exhaustion Flood; Service Exhaustion Flood; Application Exhaustion Flood; Application or System Exploitation; Financial Theft; Firmware Corruption; Inhibit System Recovery
- **Network Denial of Service (2)**: Direct Network Flood; Reflection Amplification
- **Resource Hijacking (4)**: Compute Hijacking; Bandwidth Hijacking; SMS Pumping; Cloud Service Hijacking; Service Stop; System Shutdown/Reboot

Traffic Signaling (2)
- Port Knocking
- Socket Filters

Valid Accounts (4)
- Default Accounts
- Domain Accounts
- Local Accounts
- Cloud Accounts

- Patch System Image
- Downgrade System Image

Network Boundary Bridging (1)
- Network Address Translation Traversal

Obfuscated Files or Information (14)
- Binary Padding
- Software Packing
- Steganography
- Compile After Delivery
- Indicator Removal from Tools
- HTML Smuggling
- Dynamic API Resolution
- Stripped Payloads
- Embedded Payloads
- Command Obfuscation
- Fileless Storage
- LNK Icon Smuggling
- Encrypted/Encoded File
- Polymorphic Code

Pre-OS Boot (5)
- System Firmware
- Component Firmware
- Bootkit
- ROMMONkit
- TFTP Boot

Process Injection (12)
- 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
- ListPlanting
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit

Subvert Trust Controls (6)
- Gatekeeper Bypass
- Code Signing
- SIP and Trust Provider Hijacking
- Install Root Certificate
- Mark-of-the-Web Bypass
- Code Signing Policy Modification

System Binary Proxy Execution (14)
- Compiled HTML File
- Control Panel
- CMSTP
- InstallUtil
- Mshta
- Msiexec
- Odbcconf
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Verclsid
- Mavinject
- MMC
- Electron Applications

System Script Proxy Execution (2)
- PubPrn
- SyncAppvPublishingServer
- Template Injection

Traffic Signaling (2)
- Port Knocking
- Socket Filters

Trusted Developer Utilities Proxy Execution (2)
- MSBuild
- ClickOnce
- Unused/Unsupported Cloud Regions

Use Alternate Authentication Material (4)
- Application Access Token
- Pass the Hash
- Pass the Ticket
- Web Session Cookie

Valid Accounts (4)
- Default Accounts
- Domain Accounts
- Local Accounts
- Cloud Accounts

Virtualization/Sandbox Evasion (3)
- System Checks
- User Activity Based Checks
- Time Based Evasion

Weaken Encryption (2)
- Reduce Key Space
- Disable Crypto Hardware

XSL Script Processing