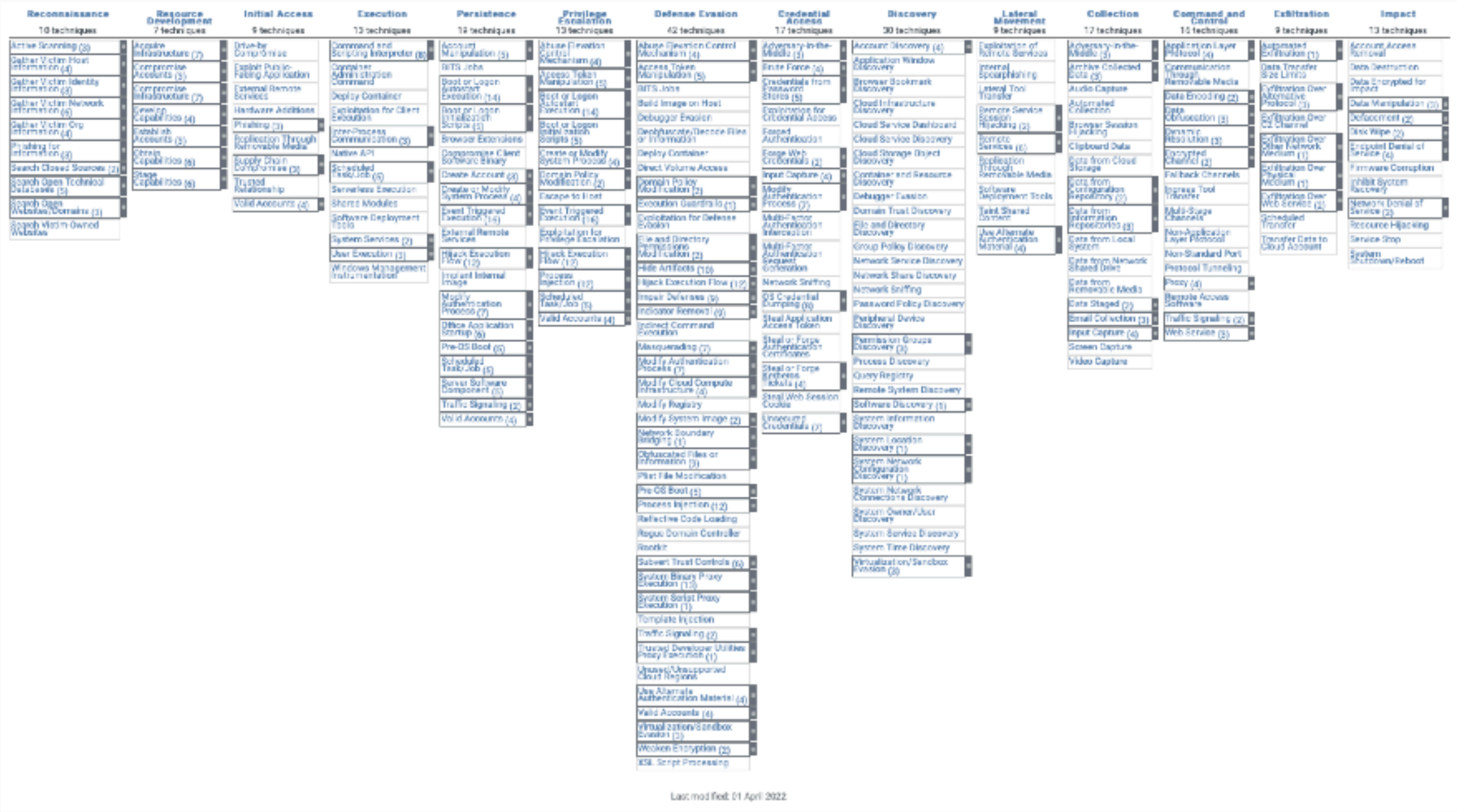
➡ Mitre Attack Matrix

# Endpoint Protection



**Reconnaissance**
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

**Resource Development**
7 techniques

- Acquire Infrastructure (7)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

**Initial Access**
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

**Execution**
13 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

**Persistence**
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

**Privilege Escalation**
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

**Defense Evasion**
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (7)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (3)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (6)
- System Binary Proxy Execution (13)
- System Script Proxy Execution (1)
- Template Injection
- Traffic Signaling (2)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

**Credential Access**
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

**Discovery**
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

**Lateral Movement**
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

**Collection**
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

**Command and Control**
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

**Exfiltration**
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

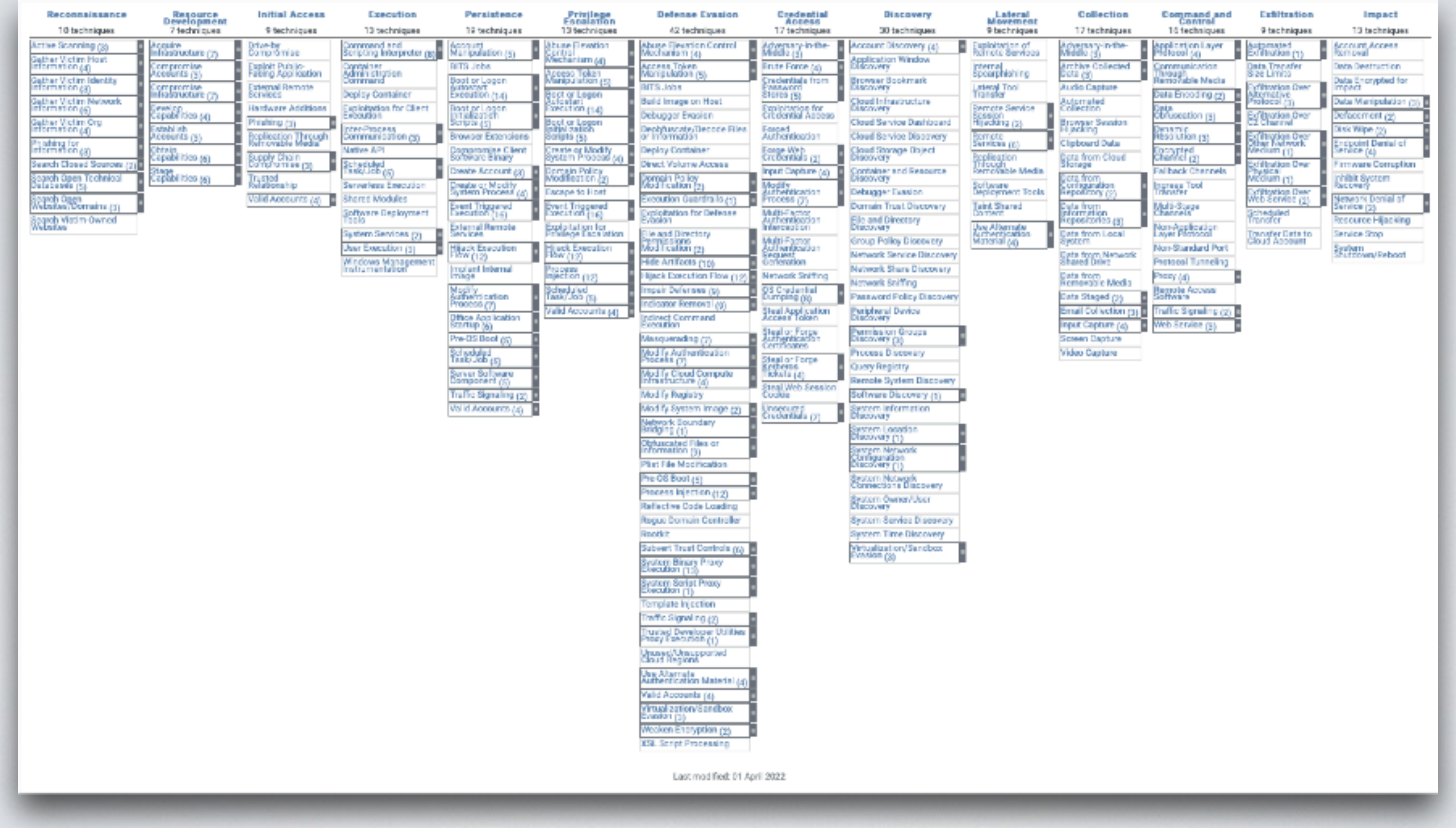
**Impact**
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Last modified: 01 April 2022

# Endpoint Protection

➡ Mitre Attack Matrix

➡ 

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 13 techniques | 19 techniques | 13 techniques | 42 techniques | 17 techniques | 30 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |
| Active Scanning (3) | Acquire Infrastructure (7) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (5) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Adversary-in-the-Middle (3) | Account Discovery (4) | Exploitation of Remote Services | Adversary-in-the-Middle (3) | Application Layer Protocol (4) | Automated Exfiltration (1) | Account Access Removal |
| Gather Victim Host Information (4) | Compromise Accounts (3) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Brute Force (4) | Application Window Discovery | Internal Spearphishing | Archive Collected Data (3) | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (3) | Compromise Infrastructure (7) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (14) | Boot or Logon Autostart Execution (14) | BITS Jobs | Credentials from Password Stores (5) | Browser Bookmark Discovery | Lateral Tool Transfer | Audio Capture | Data Encoding (2) | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Automated Collection | Data Obfuscation (3) | Exfiltration Over C2 Channel | Data Manipulation (3) |
| Gather Victim Org Information (4) | Establish Accounts (3) | Phishing (3) | Inter-Process Communication (3) | Browser Extensions | Create or Modify System Process (4) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (6) | Browser Session Hijacking | Dynamic Resolution (3) | Exfiltration Over Other Network Medium (1) | Defacement (2) |
| Phishing for Information (3) | Obtain Capabilities (6) | Replication Through Removable Media | Native API | Compromise Client Software Binary | Domain Policy Modification (2) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Encrypted Channel (2) | Exfiltration Over Physical Medium (1) | Disk Wipe (2) |
| Search Closed Sources (2) | Stage Capabilities (6) | Supply Chain Compromise (3) | Scheduled Task/Job (5) | Create Account (3) | Escape to Host | Deploy Container | Input Capture (4) | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Fallback Channels | Exfiltration Over Web Service (2) | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5) | | Trusted Relationship | Serverless Execution | Create or Modify System Process (4) | Event Triggered Execution (16) | Direct Volume Access | Modify Authentication Process (7) | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository (2) | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Search Open Websites/Domains (3) | | Valid Accounts (4) | Shared Modules | Event Triggered Execution (16) | Exploitation for Privilege Escalation | Domain Policy Modification (2) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material (4) | Data from Information Repositories (3) | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| Search Victim-Owned Websites | | | Software Deployment Tools | External Remote Services | Hijack Execution Flow (12) | Execution Guardrails (1) | Multi-Factor Authentication Request Generation | Domain Trust Discovery | | Data from Local System | Non-Application Layer Protocol | | Network Denial of Service (2) |
| | | | System Services (2) | Hijack Execution Flow (12) | Process Injection (12) | Exploitation for Defense Evasion | Network Sniffing | File and Directory Discovery | | Data from Network Shared Drive | Non-Standard Port | | Resource Hijacking |
| | | | User Execution (3) | Implant Internal Image | Scheduled Task/Job (5) | File and Directory Permissions Modification (2) | OS Credential Dumping (8) | Group Policy Discovery | | Data from Removable Media | Protocol Tunneling | | Service Stop |
| | | | Windows Management Instrumentation | Modify Authentication Process (7) | Valid Accounts (4) | Hide Artifacts (10) | Steal Application Access Token | Network Service Discovery | | Data Staged (2) | Proxy (4) | | System Shutdown/Reboot |
| | | | | Office Application Startup (6) | | Hijack Execution Flow (12) | Steal or Forge Authentication Certificates | Network Share Discovery | | Email Collection (3) | Remote Access Software | | |
| | | | | Pre-OS Boot (5) | | Impair Defenses (9) | Steal or Forge Kerberos Tickets (4) | Network Sniffing | | Input Capture (4) | Traffic Signaling (2) | | |
| | | | | Scheduled Task/Job (5) | | Indicator Removal (6) | Steal Web Session Cookie | Password Policy Discovery | | Screen Capture | Web Service (3) | | |
| | | | | Server Software Component (5) | | Indirect Command Execution | Unsecured Credentials (7) | Peripheral Device Discovery | | Video Capture | | | |
| | | | | Traffic Signaling (2) | | Masquerading (7) | | Permission Groups Discovery (3) | | | | | |
| | | | | Valid Accounts (4) | | Modify Authentication Process (7) | | Process Discovery | | | | | |
| | | | | | | Modify Cloud Compute Infrastructure (4) | | Query Registry | | | | | |
| | | | | | | Modify Registry | | Remote System Discovery | | | | | |
| | | | | | | Modify System Image (2) | | Software Discovery (1) | | | | | |
| | | | | | | Network Boundary Bridging (1) | | System Information Discovery | | | | | |
| | | | | | | Obfuscated Files or Information (9) | | System Location Discovery (1) | | | | | |
| | | | | | | Plist File Modification | | System Network Configuration Discovery (1) | | | | | |
| | | | | | | Pre-OS Boot (5) | | System Network Connections Discovery | | | | | |
| | | | | | | Process Injection (12) | | System Owner/User Discovery | | | | | |
| | | | | | | Reflective Code Loading | | System Service Discovery | | | | | |
| | | | | | | Rogue Domain Controller | | System Time Discovery | | | | | |
| | | | | | | Rootkit | | Virtualization/Sandbox Evasion (3) | | | | | |
| | | | | | | Subvert Trust Controls (6) | | | | | | | |
| | | | | | | System Binary Proxy Execution (13) | | | | | | | |
| | | | | | | System Script Proxy Execution (1) | | | | | | | |
| | | | | | | Template Injection | | | | | | | |
| | | | | | | Traffic Signaling (2) | | | | | | | |
| | | | | | | Trusted Developer Utilities Proxy Execution (1) | | | | | | | |
| | | | | | | Unused/Unsupported Cloud Regions | | | | | | | |
| | | | | | | Use Alternate Authentication Material (4) | | | | | | | |
| | | | | | | Valid Accounts (4) | | | | | | | |
| | | | | | | Virtualization/Sandbox Evasion (3) | | | | | | | |
| | | | | | | Weaken Encryption (2) | | | | | | | |
| | | | | | | XSL Script Processing | | | | | | | |

Last modified: 01 April 2022