MITRE ATT&CK
EXPANDED DEFENSIVE ANALYSIS

Comprehensive Detection Engineering Reference

120 Techniques Across 12 Tactics

Version 1.0 | January 2026

UNCLASSIFIED

Table of Contents

TA0001 - Initial Access

Initial Access techniques represent methods adversaries use to gain their first foothold in a target network. Detection focuses on perimeter telemetry, email gateways, and endpoint indicators of initial compromise.

Previously Documented (3)

- T1566 - Phishing
- T1190 - Exploit Public-Facing Application
- T1133 - External Remote Services

Additional Techniques (7)

T1189 - Drive-by Compromise

Adversaries compromise websites visited by targets to deliver exploits or malware. Users are compromised simply by visiting a legitimate but infected site.

Detection Opportunities

- Browser exploit telemetry from EDR (suspicious child processes from browser)
- Network indicators: connections to known exploit kit infrastructure
- Endpoint: unexpected file writes from browser process to temp directories
- Memory protection events (DEP/ASLR violations in browser context)

Key Log Sources

- Sysmon Event 1: Browser spawning cmd.exe, powershell.exe, wscript.exe
- Sysmon Event 11: File creation in %TEMP% from browser process
- Proxy logs: Connections to categorized malicious domains
- Windows Defender Exploit Guard: Exploit protection events

Sigma Detection

```
title: Browser Spawning Suspicious Process
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        ParentImage|endswith:
            - '\chrome.exe'
            - '\firefox.exe'
            - '\msedge.exe'
            - '\iexplore.exe'
        Image|endswith:
            - '\cmd.exe'
            - '\powershell.exe'
            - '\wscript.exe'
            - '\mshta.exe'
    condition: selection
level: high
```

Mitigations

- Browser isolation / sandboxing
- Exploit protection (Windows Defender Exploit Guard)
- Regular browser patching
- Web content filtering

T1195 - Supply Chain Compromise

Adversaries manipulate products or delivery mechanisms before receipt by the end consumer. This includes compromising software updates, development tools, or hardware.

Detection Opportunities

- Software integrity verification (hash comparison against known-good)
- Unexpected network connections from trusted software
- Code signing certificate anomalies
- Build pipeline monitoring for unauthorized changes

Key Log Sources

- Software deployment logs (SCCM, Intune, WSUS)
- Code signing verification events
- Network connections from newly updated software
- File integrity monitoring on critical binaries

Mitigations

- Vendor security assessment
- Software bill of materials (SBOM) tracking
- Binary authorization / allowlisting
- Network segmentation for build systems

T1199 - Trusted Relationship

Adversaries abuse trusted third-party relationships to gain access. MSPs, contractors, and business partners with network access are common vectors.

Detection Opportunities

- Unusual access patterns from partner accounts
- Geographic anomalies (partner accessing from unexpected locations)
- Access outside normal business hours
- Lateral movement from partner-connected systems

Key Log Sources

- VPN authentication logs with source IP geolocation
- Azure AD / Okta sign-in logs for partner accounts
- Network flow from partner VLANs/subnets
- Privileged access from partner identities

Sigma Detection

```
title: Partner Account Accessing Sensitive Resources
logsource:
    product: azure
    service: signinlogs
detection:
    selection:
        UserPrincipalName|contains: '#EXT#'  # External/guest
        ResourceDisplayName|contains:
            - 'Azure Key Vault'
            - 'Azure SQL'
    condition: selection
level: medium
```

Mitigations

- Zero-trust architecture for partner access
- Just-in-time access provisioning
- Continuous access evaluation
- Network segmentation for partner connections

T1078 - Valid Accounts

Adversaries obtain and use legitimate credentials to gain initial access. Credentials may be stolen, purchased, or obtained through social engineering.

Detection Opportunities

- Impossible travel (login from geographically distant locations)
- New device fingerprints for existing accounts
- Credential stuffing patterns (many accounts, few passwords)
- Service account interactive logons

Key Log Sources

- Windows Security 4624/4625 (Logon Success/Failure)
- Azure AD Sign-in logs with risk scores
- VPN authentication with device fingerprinting
- UEBA platforms for behavioral baselines

Sigma Detection

```
title: Multiple Failed Logins Followed by Success
logsource:
    product: windows
    service: security
detection:
    selection_fail:
        EventID: 4625
    selection_success:
        EventID: 4624
    timeframe: 5m
    condition: selection_fail | count() by TargetUserName > 5
              and selection_success
level: medium
```

Mitigations

- Multi-factor authentication everywhere
- Conditional access policies
- Password breach monitoring (Have I Been Pwned integration)
- Privileged access workstations

T1091 - Replication Through Removable Media

Adversaries use removable media (USB drives) to introduce malware into air-gapped or isolated networks.

Detection Opportunities

- USB device insertion events
- Autorun execution attempts
- File execution from removable drives
- DLP alerts on sensitive data to removable media

Key Log Sources

- Windows Security 4663 (Object Access) on removable drives
- Sysmon Event 1 with Image path containing drive letters E:-Z:
- USB device connection events (PnP logs)
- Group Policy: Removable Storage Access audit events

Sigma Detection

```
title: Execution from Removable Media
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|re: '^[D-Z]:\\\\'  # Non-C drive
    filter:
        Image|startswith: 'D:\\'  # DVD drive if applicable
    condition: selection and not filter
level: medium
```

Mitigations

- Disable autorun/autoplay
- USB device allowlisting
- Endpoint DLP for removable media
- Physical USB port blocking for sensitive systems

T1200 - Hardware Additions

Adversaries introduce rogue hardware (network implants, keyloggers, USB devices) to gain access or exfiltrate data.

Detection Opportunities

- New device enumeration events
- Unexpected network device discovery (NAC)
- USB device class anomalies (HID devices from unexpected vendors)
- Physical security monitoring

Key Log Sources

- Windows PnP device installation events
- Network Access Control (NAC) alerts
- DHCP new lease events for unknown MAC addresses
- Switch port security violations

Mitigations

- 802.1X port-based authentication
- USB device class restrictions via GPO
- Physical security controls
- Regular network device inventory

T1566.001/002 - Spearphishing Attachment/Link

Targeted phishing with malicious attachments or links directed at specific individuals or organizations.

Detection Opportunities

- Email attachment analysis (sandbox detonation)
- URL reputation and age scoring
- Macro execution from Office documents
- User-reported phishing correlation

Key Log Sources

- Email gateway logs with attachment hashes
- Office 365 Advanced Threat Protection alerts
- Sysmon Event 1: Office apps spawning suspicious processes

- Proxy logs for clicked URLs

Sigma Detection

```
title: Office Application Spawning Script Interpreter
logsource:
    product: windows
    category: process_creation
detection:
    selection_parent:
        ParentImage|endswith:
            - '\WINWORD.EXE'
            - '\EXCEL.EXE'
            - '\POWERPNT.EXE'
    selection_child:
        Image|endswith:
            - '\powershell.exe'
            - '\cmd.exe'
            - '\wscript.exe'
            - '\cscript.exe'
            - '\mshta.exe'
    condition: selection_parent and selection_child
level: high
```

Mitigations

- Email attachment sandboxing
- Attack Surface Reduction rules for Office
- Protected View enforcement
- User security awareness training

TA0002 - Execution

Execution techniques represent methods adversaries use to run malicious code on target systems. Detection focuses on process creation, script execution, and API abuse patterns.

Previously Documented (3)

- T1059 - Command and Scripting Interpreter
- T1106 - Native API
- T1203 - Exploitation for Client Execution

Additional Techniques (7)

T1047 - Windows Management Instrumentation

Adversaries use WMI to execute commands locally or remotely. WMI provides powerful system management capabilities that can be abused for code execution.

Detection Opportunities

- WMI process creation events (wmiprvse.exe spawning processes)
- WMI subscription persistence (Event Consumers)
- Remote WMI connections (DCOM traffic on TCP 135)
- WMI query patterns for reconnaissance

Key Log Sources

- Sysmon Event 1: wmiprvse.exe as parent process
- Sysmon Event 19/20/21: WMI Event Subscription
- Windows WMI-Activity/Operational log
- Network: DCOM/RPC traffic on 135/TCP

Sigma Detection

```
title: WMI Spawning Suspicious Process
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        ParentImage|endswith: '\wmiprvse.exe'
        Image|endswith:
            - '\powershell.exe'
            - '\cmd.exe'
            - '\rundll32.exe'
    condition: selection
level: high
```

Mitigations

- Restrict WMI permissions via GPO
- Disable remote WMI where not required
- Monitor WMI subscription creation
- Application allowlisting

T1053.005 - Scheduled Task

Adversaries abuse Windows Task Scheduler to execute code at specified times or intervals, often for persistence or privilege escalation.

Detection Opportunities

- Task creation events (Security 4698)
- schtasks.exe command-line patterns
- Tasks with suspicious actions (encoded commands, remote paths)
- Tasks created by unusual parent processes

Key Log Sources

- Windows Security 4698 (Scheduled Task Created)
- Windows Security 4702 (Scheduled Task Updated)
- Sysmon Event 1: schtasks.exe execution
- Task Scheduler Operational log

Sigma Detection

```
title: Scheduled Task Created via Command Line
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\schtasks.exe'
        CommandLine|contains: '/create'
    suspicious:
        CommandLine|contains:
            - 'powershell'
            - 'cmd /c'
            - 'encoded'
            - 'bypass'
    condition: selection and suspicious
level: high
```

Mitigations

- Restrict task creation to administrators
- Audit scheduled task changes
- Block AT command via GPO
- Review tasks pointing to writable locations

T1059.001 - PowerShell

PowerShell is extensively abused for execution due to its deep Windows integration, .NET access, and scripting capabilities.

Detection Opportunities

- Script Block Logging (Event 4104)
- Suspicious command-line patterns (-enc, -nop, downloadstring)
- PowerShell loading unusual assemblies
- Constrained Language Mode bypass attempts

Key Log Sources

- PowerShell Script Block Logging (4104)
- PowerShell Module Logging (4103)
- Sysmon Event 1: PowerShell with suspicious arguments
- AMSI events for script content inspection

Sigma Detection

```
title: Suspicious PowerShell Download Cradle
logsource:
    product: windows
    category: ps_script
detection:
    selection:
        ScriptBlockText|contains:
            - 'DownloadString'
            - 'DownloadFile'
            - 'DownloadData'
            - 'Net.WebClient'
            - 'Start-BitsTransfer'
            - 'Invoke-WebRequest'
            - 'iwr '
            - 'wget '
            - 'curl '
    condition: selection
level: high
```

Mitigations

- Enable Constrained Language Mode
- Require script signing (AllSigned execution policy)
- Deploy PowerShell v5+ for enhanced logging
- AMSI integration for real-time inspection

T1059.003 - Windows Command Shell

cmd.exe is used to execute commands and batch scripts. Its ubiquity makes it a common execution vehicle.

Detection Opportunities

- Unusual parent processes spawning cmd.exe
- Command-line obfuscation patterns (^, %, environment variables)
- Batch file execution from suspicious locations
- Chained commands with suspicious patterns

Key Log Sources

- Sysmon Event 1: cmd.exe with full command line
- Windows Security 4688 with command-line auditing
- Process ancestry tracking

Sigma Detection

```
title: Obfuscated Command Line
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\cmd.exe'
    obfuscation:
        CommandLine|re: '.*\^.{1,3}\^.*\^.*'
    env_vars:
        CommandLine|contains:
            - '%COMSPEC%'
            - '%APPDATA%'
    condition: selection and (obfuscation or env_vars)
level: medium
```

Mitigations

- Application allowlisting
- Command-line logging and analysis
- Restrict cmd.exe execution via AppLocker
- Block batch file execution from temp directories

T1059.005 - Visual Basic

VBScript and VBA macros are abused for initial execution, often delivered via Office documents or standalone scripts.

Detection Opportunities

- wscript.exe/cscript.exe spawning suspicious processes
- VBS file creation in temp directories
- Office macro execution indicators
- Script content via AMSI

Key Log Sources

- Sysmon Event 1: wscript.exe/cscript.exe execution
- Sysmon Event 11: .vbs file creation
- AMSI events for VBScript content
- Office macro execution events

Sigma Detection

```
title: WScript Spawning PowerShell
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        ParentImage|endswith:
            - '\wscript.exe'
            - '\cscript.exe'
        Image|endswith:
            - '\powershell.exe'
            - '\cmd.exe'
    condition: selection
level: high
```

Mitigations

- Disable Windows Script Host via GPO
- Block macro execution in Office
- Attack Surface Reduction rules
- Application allowlisting

T1204 - User Execution

Adversaries rely on users to execute malicious payloads through social engineering. This includes opening attachments, clicking links, or running downloaded files.

Detection Opportunities

- Execution from browser download directories
- Execution from email attachment temp paths
- Zone.Identifier (Mark of the Web) on executed files
- User double-clicking unusual file types

Key Log Sources

- Sysmon Event 1: Execution from Downloads, Temp paths
- Sysmon Event 15: Alternate Data Stream (Zone.Identifier)
- Explorer.exe child process monitoring
- Email client spawning executables

Sigma Detection

```
title: Execution from User Download Directory
```

```
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|contains:
            - '\Downloads\\'
            - '\Temp\\'
        Image|endswith:
            - '.exe'
            - '.scr'
            - '.pif'
    condition: selection
level: medium
```

Mitigations

- User security awareness training
- SmartScreen enforcement
- Application allowlisting
- Email attachment restrictions

T1569.002 - Service Execution

Adversaries execute code by creating or modifying Windows services. Services run with elevated privileges and persist across reboots.

Detection Opportunities

- Service installation events (System 7045)
- sc.exe command-line patterns
- Services with suspicious binary paths
- Services running from temp or user directories

Key Log Sources

- Windows System 7045 (Service Installed)
- Windows System 7036 (Service State Change)
- Sysmon Event 1: sc.exe, services.exe children
- Registry: HKLM\SYSTEM\CurrentControlSet\Services

Sigma Detection

```
title: Suspicious Service Installation
logsource:
    product: windows
    service: system
detection:
    selection:
        EventID: 7045
    suspicious_path:
        ImagePath|contains:
            - '\Temp\\'
            - '\Users\\'
            - 'cmd.exe'
            - 'powershell'
    condition: selection and suspicious_path
level: high
```

Mitigations

- Restrict service creation to administrators
- Monitor service binary paths
- Application allowlisting for service binaries
- Audit service configuration changes

TA0003 - Persistence

Persistence techniques allow adversaries to maintain access across system restarts, credential changes, or other interruptions. Detection focuses on registry modifications, scheduled tasks, and startup locations.

Previously Documented (3)

- T1547 - Boot/Logon Autostart Execution
- T1053 - Scheduled Task/Job
- T1136 - Create Account

Additional Techniques (7)

T1543.003 - Windows Service

Adversaries create or modify Windows services for persistence. Services start automatically and run with SYSTEM privileges.

Detection Opportunities

- New service creation events
- Service binary path modifications
- Services with unusual characteristics (no description, random names)
- Service failure recovery actions pointing to malicious binaries

Key Log Sources

- Windows System 7045 (Service Installed)
- Sysmon Event 12/13: Service registry modifications
- Sysmon Event 1: sc.exe execution
- Registry: HKLM\SYSTEM\CurrentControlSet\Services

Sigma Detection

```
title: Service Installed with Suspicious Binary Path
logsource:
    product: windows
    service: system
detection:
    selection:
        EventID: 7045
    suspicious:
        ImagePath|contains:
            - '.ps1'
            - 'powershell'
            - '\AppData\\'
            - '\Temp\\'
            - 'cmd /c'
    condition: selection and suspicious
```

```
level: critical
```

Mitigations

- Service creation restrictions
- Application allowlisting for service binaries
- Monitor service configuration registry keys
- Regular service inventory review

T1546.001 - Change Default File Association

Adversaries modify file associations to execute malicious code when users open specific file types.

Detection Opportunities

- Registry modifications to file association keys
- HKCR or UserChoice registry changes
- Unexpected handlers for common file types

Key Log Sources

- Sysmon Event 12/13: Registry changes to HKCR
- Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
- Process creation with unusual parent for file type

Sigma Detection

```
title: File Association Registry Modification
logsource:
    product: windows
    category: registry_set
detection:
    selection:
        TargetObject|contains:
            - '\shell\open\command'
            - 'HKCR\\'
        TargetObject|endswith:
            - '.txt'
            - '.doc'
            - '.pdf'
    condition: selection
level: high
```

Mitigations

- Restrict registry write access to association keys
- Monitor file association changes
- Application allowlisting

T1546.003 - Windows Management Instrumentation Event Subscription

Adversaries use WMI event subscriptions to trigger code execution based on system events, providing persistent and stealthy execution.

Detection Opportunities

- WMI subscription creation events
- Unusual WMI consumers (CommandLineEventConsumer, ActiveScriptEventConsumer)
- Subscription filters monitoring sensitive events

Key Log Sources

- Sysmon Event 19: WMI Event Filter
- Sysmon Event 20: WMI Event Consumer
- Sysmon Event 21: WMI Event Consumer to Filter
- WMI-Activity/Operational log

Sigma Detection

```
title: WMI Event Subscription Created
logsource:
    product: windows
    category: wmi_event
detection:
    selection:
        EventID:
            - 19
            - 20
            - 21
    suspicious_consumer:
        Consumer|contains:
            - 'CommandLineEventConsumer'
            - 'ActiveScriptEventConsumer'
    condition: selection and suspicious_consumer
level: critical
```

Mitigations

- Monitor WMI subscription creation
- Restrict WMI namespace permissions
- Regular WMI subscription audit
- Disable WMI where not required

T1546.008 - Accessibility Features

Adversaries replace accessibility features (sethc.exe, utilman.exe) with malicious binaries for persistence and privilege escalation at the login screen.

Detection Opportunities

- File modifications to accessibility binaries
- Image File Execution Options debugger keys

- Accessibility binaries spawning unexpected processes

Key Log Sources

- Sysmon Event 11: File creation/modification of sethc.exe, utilman.exe
- Sysmon Event 12/13: IFEO registry modifications
- File integrity monitoring on System32 accessibility binaries

Sigma Detection

```
title: Image File Execution Options Debugger for Accessibility
logsource:
    product: windows
    category: registry_set
detection:
    selection:
        TargetObject|contains: 'Image File Execution Options'
        TargetObject|endswith:
            - 'sethc.exe\Debugger'
            - 'utilman.exe\Debugger'
            - 'osk.exe\Debugger'
            - 'narrator.exe\Debugger'
            - 'magnify.exe\Debugger'
    condition: selection
level: critical
```

Mitigations

- File integrity monitoring on accessibility binaries
- Protect IFEO registry keys
- Remove accessibility features from sensitive systems
- Restrict console access to servers

T1547.001 - Registry Run Keys / Startup Folder

Adversaries add entries to registry Run keys or Startup folders to execute code when users log in.

Detection Opportunities

- Registry modifications to Run/RunOnce keys
- File creation in Startup folders
- Unusual executables in autostart locations

Key Log Sources

- Sysmon Event 12/13: Run key modifications
- Sysmon Event 11: File creation in Startup folders
- Autoruns comparison for new entries

Critical Registry Paths

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
```

Sigma Detection

```
title: Suspicious Run Key Registration
logsource:
    product: windows
    category: registry_set
detection:
    selection:
        TargetObject|contains:
            - '\CurrentVersion\Run'
    suspicious:
        Details|contains:
            - 'powershell'
            - 'cmd.exe'
            - '\AppData\\'
            - '\Temp\\'
    condition: selection and suspicious
level: high
```

Mitigations

- Application allowlisting
- Restrict write access to Run keys
- Monitor Startup folder changes
- Regular autoruns baseline comparison

T1574.001 - DLL Search Order Hijacking

Adversaries place malicious DLLs in locations searched before legitimate DLLs, causing applications to load attacker code.

Detection Opportunities

- DLL loads from unusual paths
- Unsigned DLLs loaded by signed executables
- DLL creation in application directories
- Known DLL name in unexpected location

Key Log Sources

- Sysmon Event 7: Image Loaded (DLL loading)
- Sysmon Event 11: DLL file creation
- Process Monitor for DLL search order analysis

Sigma Detection

```
title: DLL Loaded from Suspicious Path
```

```
logsource:
    product: windows
    category: image_load
detection:
    selection:
        ImageLoaded|contains:
            - '\Users\\'
            - '\Temp\\'
            - '\AppData\Local\Temp'
    filter:
        Signed: 'true'
    condition: selection and not filter
level: medium
```

Mitigations

- Enable SafeDllSearchMode
- Use absolute paths in applications
- Code signing enforcement
- Application allowlisting

T1505.003 - Web Shell

Adversaries install web shells on internet-facing servers for persistent remote access and command execution.

Detection Opportunities

- File creation in web directories
- Web server process spawning cmd.exe/powershell.exe
- Unusual HTTP POST requests to static files
- Known web shell signatures

Key Log Sources

- Sysmon Event 1: w3wp.exe/httpd spawning shells
- Sysmon Event 11: File creation in wwwroot, htdocs
- Web server access logs: POST to .aspx/.php/.jsp
- File integrity monitoring on web roots

Sigma Detection

```
title: IIS Worker Spawning Suspicious Process
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        ParentImage|endswith: '\w3wp.exe'
        Image|endswith:
            - '\cmd.exe'
            - '\powershell.exe'
            - '\whoami.exe'
            - '\net.exe'
    condition: selection
level: critical
```

Mitigations

- File integrity monitoring on web directories
- Web application firewall (WAF)
- Restrict web server process permissions
- Regular web directory scans

TA0004 - Privilege Escalation

Privilege Escalation techniques allow adversaries to gain higher-level permissions. Detection focuses on token manipulation, exploitation indicators, and elevation events.

Previously Documented (3)

- T1055 - Process Injection
- T1548 - Abuse Elevation Control Mechanism
- T1068 - Exploitation for Privilege Escalation

Additional Techniques (7)

T1134 - Access Token Manipulation

Adversaries manipulate access tokens to operate under different security contexts, enabling privilege escalation or impersonation.

Detection Opportunities

- Token impersonation API calls (SetThreadToken, ImpersonateLoggedOnUser)
- Process with unexpected token
- Logon events with unusual authentication packages
- Token theft from high-privilege processes

Key Log Sources

- Windows Security 4624 Type 9 (NewCredentials)
- Windows Security 4648 (Explicit Credential Logon)
- ETW: Microsoft-Windows-Kernel-Audit-API-Calls
- EDR telemetry for token manipulation APIs

Sigma Detection

```
title: RunAs with Explicit Credentials
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4648
    filter_legitimate:
        ProcessName|endswith:
            - '\svchost.exe'
            - '\services.exe'
    condition: selection and not filter_legitimate
level: medium
```

Mitigations

- Credential Guard
- Protected Users security group
- Limit token privileges on accounts
- Monitor high-privilege account usage

T1134.001 - Token Impersonation/Theft

Adversaries duplicate access tokens from other processes to assume their security context, often targeting SYSTEM tokens.

Detection Opportunities

- OpenProcessToken on high-value targets
- DuplicateTokenEx calls across privilege boundaries
- Process with mismatched user and token

Key Log Sources

- Sysmon Event 10: Process Access with TOKEN_DUPLICATE
- ETW kernel audit events
- EDR behavioral detection

Mitigations

- Run services with minimal required privileges
- Enable Credential Guard
- Protected Processes for sensitive services

T1055.001 - Dynamic-link Library Injection

Adversaries inject DLLs into running processes to execute code in their context, evading detection and gaining process privileges.

Detection Opportunities

- CreateRemoteThread to load DLL
- Unsigned DLL loaded into signed process
- DLL loaded from unusual path
- Known process loading unexpected modules

Key Log Sources

- Sysmon Event 7: Image Loaded (DLL)
- Sysmon Event 8: CreateRemoteThread
- EDR DLL injection detection

Sigma Detection

```
title: CreateRemoteThread into Sensitive Process
logsource:
    product: windows
    category: create_remote_thread
```

```
detection:
    selection:
        EventID: 8
        TargetImage|endswith:
            - '\lsass.exe'
            - '\csrss.exe'
            - '\winlogon.exe'
            - '\services.exe'
    condition: selection
level: critical
```

Mitigations

- Application allowlisting
- Code integrity policies
- Protected Process Light (PPL)
- EDR with injection detection

T1055.003 - Thread Execution Hijacking

Adversaries suspend a thread in a target process, modify its context to point to malicious code, then resume execution.

Detection Opportunities

- SuspendThread/ResumeThread API patterns
- SetThreadContext on remote processes
- Thread context pointing to unusual memory regions

Key Log Sources

- ETW thread tracing
- EDR behavioral detection
- Memory forensics for modified thread contexts

Mitigations

- Protected Process Light for sensitive processes
- Code integrity enforcement
- EDR with thread monitoring

T1055.012 - Process Hollowing

Adversaries create a process in suspended state, hollow out its memory, inject malicious code, then resume execution.

Detection Opportunities

- Process created suspended then resumed
- Memory section unmapped and rewritten
- Process image path doesn't match in-memory code

- Sysmon Event 25 (Process Tampering)

Key Log Sources

- Sysmon Event 25: Process Tampering
- Sysmon Event 1: Process with suspicious parent/child
- EDR memory scanning
- Process hollowing detection via memory analysis

Sigma Detection

```
title: Process Tampering Detected
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 25
        Type: 'Image is replaced'
    condition: selection
level: critical
```

Mitigations

- EDR with memory protection
- Exploit protection (CFG, ACG)
- Code integrity policies

T1548.002 - Bypass User Account Control

Adversaries bypass UAC to execute code with elevated privileges without prompting the user.

Detection Opportunities

- Known UAC bypass binaries (fodhelper, eventvwr, computerdefaults)
- Auto-elevated COM objects with modified registry
- DLL hijacking in auto-elevated processes
- Environment variable manipulation for bypass

Key Log Sources

- Sysmon Event 1: UAC bypass binary execution
- Sysmon Event 12/13: Registry modifications for bypass
- Windows Security 4688 with elevated token

Sigma Detection

```
title: UAC Bypass via fodhelper
logsource:
    product: windows
    category: process_creation
detection:
    selection_parent:
        ParentImage|endswith: '\fodhelper.exe'
    selection_child:
        Image|endswith:
            - '\cmd.exe'
            - '\powershell.exe'
    condition: selection_parent and selection_child
level: critical
```

Mitigations

- Set UAC to 'Always Notify'
- Remove users from local Administrators
- Monitor auto-elevate binaries
- Application allowlisting

T1078.002 - Domain Accounts

Adversaries use compromised domain credentials to escalate privileges across the domain.

Detection Opportunities

- Domain admin logon to workstations
- Tier model violations (T0 creds on T1/T2)
- Unusual service account usage
- Privileged account logon from unexpected sources

Key Log Sources

- Windows Security 4624/4672 (Logon with Special Privileges)
- Azure AD Privileged Identity Management logs
- Domain Controller authentication logs

Sigma Detection

```
title: Domain Admin Logon to Workstation
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4624
        LogonType: 10  # RemoteInteractive
    admin_groups:
        TargetUserName|endswith:
            - '-admin'
            - '_admin'
            - 'administrator'
    workstation:
        WorkstationName|startswith: 'WS'
    condition: selection and admin_groups and workstation
```

```
level: high
```

Mitigations

- Tiered administration model
- Privileged Access Workstations (PAW)
- Just-In-Time privileged access
- Protected Users security group

TA0005 - Defense Evasion

Defense Evasion techniques help adversaries avoid detection. Detection paradoxically focuses on identifying evasion attempts through behavioral analysis and integrity monitoring.

Previously Documented (4)

- T1027 - Obfuscated Files or Information
- T1562 - Impair Defenses
- T1070 - Indicator Removal
- T1497 - Virtualization/Sandbox Evasion

Additional Techniques (6)

T1036 - Masquerading

Adversaries manipulate features of artifacts to appear legitimate, including renaming executables, modifying timestamps, or mimicking system files.

Detection Opportunities

- Executables in system paths with unusual metadata
- Known system binary name from non-system location
- Process name/path mismatch
- Timestamp anomalies (timestomping)

Key Log Sources

- Sysmon Event 1: Compare Image vs OriginalFileName
- Sysmon Event 2: File creation time modification
- File metadata analysis (VersionInfo vs filename)

Sigma Detection

```
title: Renamed System Binary
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        OriginalFileName:
            - 'cmd.exe'
            - 'powershell.exe'
    filter:
        Image|endswith:
            - '\cmd.exe'
            - '\powershell.exe'
    condition: selection and not filter
level: high
```

Mitigations

- Application allowlisting with path rules
- Monitor for OriginalFileName mismatches
- File integrity monitoring on system directories

T1070.001 - Clear Windows Event Logs

Adversaries clear Windows event logs to remove evidence of intrusion activity.

Detection Opportunities

- Event log cleared events (1102, 104)
- wevtutil.exe execution
- Gaps in event log timeline
- Log file access/deletion

Key Log Sources

- Windows Security 1102 (Audit Log Cleared)
- Windows System 104 (Log Cleared)
- Sysmon Event 1: wevtutil.exe cl command

Sigma Detection

```
title: Security Event Log Cleared
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 1102
    condition: selection
level: critical
```

Mitigations

- Forward logs to remote SIEM immediately
- Restrict log management permissions
- Alert on log clearing events
- Immutable backup logging

T1218 - System Binary Proxy Execution

Adversaries use signed system binaries to proxy execution of malicious code, bypassing application controls.

Detection Opportunities

- LOLBins with suspicious command-line arguments
- Signed binaries loading unsigned content
- Unusual parent-child process relationships

Key Log Sources

- Sysmon Event 1: LOLBin execution patterns
- Sysmon Event 7: DLL loads from LOLBins
- Command-line analysis for abuse patterns

Common LOLBins

- mshta.exe - Execute HTA files
- rundll32.exe - Execute DLL exports
- regsvr32.exe - Register/execute COM servers
- certutil.exe - Download and decode files
- msiexec.exe - Execute MSI packages
- cmstp.exe - Execute INF files

Sigma Detection

```
title: Certutil Download
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\certutil.exe'
        CommandLine|contains:
            - 'urlcache'
            - '-decode'
            - '/decode'
    condition: selection
level: high
```

Mitigations

- Application allowlisting with argument rules
- Block unnecessary LOLBins via WDAC
- Monitor LOLBin command-line patterns

T1218.011 - Rundll32

Adversaries use rundll32.exe to execute malicious DLLs and their exports, often with obfuscated arguments.

Detection Opportunities

- Rundll32 loading DLLs from unusual paths
- Unusual export names or ordinals
- Network connections from rundll32
- Rundll32 spawning child processes

Key Log Sources

- Sysmon Event 1: rundll32.exe command line
- Sysmon Event 3: Network from rundll32
- Sysmon Event 7: DLLs loaded by rundll32

Sigma Detection

```
title: Rundll32 Executing DLL from Temp
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\rundll32.exe'
        CommandLine|contains:
            - '\Temp\\'
            - '\AppData\\'
            - 'javascript:'
    condition: selection
level: high
```

Mitigations

- Monitor rundll32 execution patterns
- Application allowlisting
- Block rundll32 network access

T1553 - Subvert Trust Controls

Adversaries subvert security controls that rely on trust, including code signing and certificate validation.

Detection Opportunities

- Installation of untrusted root certificates
- Mark-of-the-Web bypass attempts
- Catalog file modifications
- Authenticode validation failures

Key Log Sources

- Windows CAPI2 logs (Certificate validation)
- Sysmon Event 12/13: Certificate store modifications
- Windows Defender SmartScreen events

Sigma Detection

```
title: Root Certificate Installed
logsource:
    product: windows
    category: registry_set
detection:
    selection:
        TargetObject|contains:
            - '\ROOT\Certificates'
            - '\AuthRoot\Certificates'
    condition: selection
level: high
```

Mitigations

- Restrict certificate installation to administrators
- Monitor certificate stores
- Enable Certificate Transparency logging
- Code signing enforcement

T1620 - Reflective Code Loading

Adversaries load code directly into process memory without writing to disk, evading file-based detection.

Detection Opportunities

- Memory allocation with RWX permissions
- PE headers in non-image memory regions
- Unbacked executable memory
- Process with loaded modules not on disk

Key Log Sources

- ETW: Microsoft-Windows-Threat-Intelligence
- EDR memory telemetry
- Memory forensics for unbacked code

Sigma Detection

```
title: PowerShell Loading Assembly from Memory
logsource:
    product: windows
    category: ps_script
detection:
    selection:
        ScriptBlockText|contains:
            - '[System.Reflection.Assembly]::Load'
            - 'Reflection.Assembly'
            - 'LoadMethod'
    condition: selection
level: high
```

Mitigations

- AMSI integration for script inspection
- Memory protection (ACG, CIG)
- EDR with memory scanning

- Constrained Language Mode

TA0006 - Credential Access

Credential Access techniques allow adversaries to steal credentials. Detection focuses on access to credential stores, authentication anomalies, and known credential theft tool patterns.

Previously Documented (3)

- T1003 - OS Credential Dumping
- T1555 - Credentials from Password Stores
- T1110 - Brute Force

Additional Techniques (7)

T1558 - Steal or Forge Kerberos Tickets

Adversaries steal or forge Kerberos tickets to move laterally or escalate privileges. Includes Kerberoasting, Golden/Silver tickets.

Detection Opportunities

- TGS requests for service accounts (Kerberoasting)
- Encryption downgrade to RC4 (0x17)
- TGT requests without pre-authentication (AS-REP roasting)
- Ticket encryption type anomalies

Key Log Sources

- Windows Security 4769 (Kerberos Service Ticket)
- Windows Security 4768 (Kerberos TGT Request)
- Windows Security 4771 (Kerberos Pre-auth Failed)
- Domain Controller Kerberos logs

Sigma Detection

```
title: Kerberoasting - RC4 Service Ticket
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4769
        TicketEncryptionType: '0x17'  # RC4
        ServiceName|endswith: '$': false
    filter:
        ServiceName: 'krbtgt'
    condition: selection and not filter
level: high
```

Mitigations

- Use AES-only Kerberos encryption
- Strong passwords for service accounts
- Group Managed Service Accounts (gMSA)
- Monitor TGS requests for service accounts

T1552 - Unsecured Credentials

Adversaries search for credentials stored insecurely in files, registry, or environment variables.

Detection Opportunities

- Access to known credential file locations
- Registry queries for stored credentials
- File searches for password patterns
- Access to cloud metadata endpoints

Key Log Sources

- Sysmon Event 1: findstr, select-string with password patterns
- File access auditing on sensitive locations
- Registry auditing on credential keys

Sigma Detection

```
title: Searching for Credentials in Files
logsource:
    product: windows
    category: process_creation
detection:
    selection_tool:
        Image|endswith:
            - '\findstr.exe'
            - '\select-string'
    selection_pattern:
        CommandLine|contains:
            - 'password'
            - 'credential'
            - 'secret'
            - 'key'
    condition: selection_tool and selection_pattern
level: medium
```

Mitigations

- Remove credentials from scripts and configs
- Use credential managers and vaults
- Audit sensitive file access
- Rotate exposed credentials

T1557 - Adversary-in-the-Middle

Adversaries intercept authentication traffic to capture credentials. Includes LLMNR/NBT-NS poisoning, ARP spoofing, and Kerberos interception.

Detection Opportunities

- Multiple LLMNR/NBT-NS responses
- ARP table anomalies
- NetNTLM authentication to unexpected hosts
- SMB connections to non-server IPs

Key Log Sources

- Network: LLMNR (UDP 5355), NBT-NS (UDP 137) traffic
- Windows Security 4624 with unexpected network address
- IDS signatures for poisoning attacks
- Switch ARP table monitoring

Mitigations

- Disable LLMNR and NBT-NS
- Enable SMB signing
- Network segmentation
- DHCP snooping and dynamic ARP inspection

T1539 - Steal Web Session Cookie

Adversaries steal web session cookies to hijack authenticated sessions without needing credentials.

Detection Opportunities

- Access to browser cookie databases
- Cookie file copying or exfiltration
- Browser credential store access
- Session anomalies (cookie used from different IP)

Key Log Sources

- Sysmon Event 1: Access to browser profiles
- File access auditing on cookie databases
- Web application logs for session anomalies

Cookie Locations

```
Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies
Firefox: %APPDATA%\Mozilla\Firefox\Profiles\*.default\cookies.sqlite
Edge: %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cookies
```

Mitigations

- Endpoint DLP for cookie file access
- Short session timeouts

- Continuous session validation
- Bind sessions to client characteristics

T1111 - Multi-Factor Authentication Interception

Adversaries intercept MFA codes through phishing proxies, malware, or social engineering.

Detection Opportunities

- Authentication from known phishing infrastructure
- Rapid MFA code reuse
- Session establishment from proxy infrastructure
- Push notification spam patterns

Key Log Sources

- Azure AD/Identity Provider sign-in logs
- MFA provider audit logs
- Network connections to known phishing infrastructure

Mitigations

- Phishing-resistant MFA (FIDO2, Windows Hello)
- Number matching for push notifications
- Conditional access policies
- Certificate-based authentication

T1187 - Forced Authentication

Adversaries force authentication attempts to capture credentials, often via UNC paths or embedded content.

Detection Opportunities

- SMB authentication to external IPs
- WebDAV authentication attempts
- Office documents with external resources
- Shortcut files pointing to UNC paths

Key Log Sources

- Windows Security 4624/4625 with external IPs
- Sysmon Event 3: SMB connections to internet
- Firewall logs: Outbound SMB (445/TCP)

Sigma Detection

```
title: SMB Connection to External IP
logsource:
    product: windows
    category: network_connection
detection:
    selection:
        DestinationPort: 445
        Initiated: 'true'
    filter_internal:
        DestinationIp|startswith:
            - '10.'
            - '172.16.'
            - '192.168.'
    condition: selection and not filter_internal
level: high
```

Mitigations

- Block outbound SMB at firewall
- Disable NTLM where possible
- Configure Windows to restrict outbound auth

T1040 - Network Sniffing

Adversaries capture network traffic to extract credentials and other sensitive information.

Detection Opportunities

- Promiscuous mode on network interfaces
- Known sniffing tool execution
- Packet capture file creation
- Unusual network driver activity

Key Log Sources

- Sysmon Event 1: tcpdump, wireshark, windump execution
- Sysmon Event 11: .pcap file creation
- Network device logs for promiscuous mode

Sigma Detection

```
title: Network Capture Tool Execution
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith:
            - '\tcpdump.exe'
            - '\windump.exe'
            - '\tshark.exe'
            - '\dumpcap.exe'
    condition: selection
level: medium
```

Mitigations

- Network encryption (TLS everywhere)
- Network segmentation
- 802.1X port authentication
- Application allowlisting

TA0007 - Discovery

Discovery techniques help adversaries learn about the target environment. Detection focuses on reconnaissance command patterns and unusual enumeration activity.

Previously Documented (3)

- T1087 - Account Discovery
- T1082 - System Information Discovery
- T1046 - Network Service Discovery

Additional Techniques (7)

T1083 - File and Directory Discovery

Adversaries enumerate files and directories to find sensitive data, credentials, or understand the environment.

Detection Opportunities

- Recursive directory listing commands
- Searches for sensitive file patterns
- Access to many directories in short time

Key Log Sources

- Sysmon Event 1: dir, tree, get-childitem commands
- File access auditing for sensitive directories
- EDR file system telemetry

Sigma Detection

```
title: Recursive Directory Listing
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        CommandLine|contains:
            - 'dir /s'
            - 'tree /f'
            - 'Get-ChildItem -Recurse'
            - 'gci -r'
    condition: selection
level: low
```

Mitigations

- Least privilege file access
- Data classification and access controls

- Monitor bulk file enumeration

T1057 - Process Discovery

Adversaries enumerate running processes to understand security tools, identify targets, or find processes to inject into.

Detection Opportunities

- Process enumeration commands
- API-based process listing
- Queries for security product processes

Key Log Sources

- Sysmon Event 1: tasklist, ps, get-process
- ETW process enumeration events

Sigma Detection

```
title: Security Product Process Discovery
logsource:
    product: windows
    category: process_creation
detection:
    selection_tool:
        Image|endswith:
            - '\tasklist.exe'
            - '\wmic.exe'
    selection_security:
        CommandLine|contains:
            - 'antivirus'
            - 'defender'
            - 'crowdstrike'
            - 'carbon'
    condition: selection_tool and selection_security
level: medium
```

Mitigations

- Behavioral baseline for enumeration
- Deception (fake security processes)

T1018 - Remote System Discovery

Adversaries enumerate remote systems on the network to identify targets for lateral movement.

Detection Opportunities

- Net view, ping sweep, nltest commands
- LDAP queries for computer objects
- ARP scanning activity

Key Log Sources

- Sysmon Event 1: net view, nltest, dsquery computer
- Network: ICMP echo patterns, SMB enumeration
- Domain Controller LDAP logs

Sigma Detection

```
title: Remote System Discovery via Net
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\net.exe'
        CommandLine|contains:
            - 'view'
            - 'session'
            - 'computer'
    condition: selection
level: low
```

Mitigations

- Network segmentation
- Disable unnecessary protocols
- Honeypots for enumeration detection

T1069 - Permission Groups Discovery

Adversaries enumerate local and domain groups to understand privilege levels and identify targets.

Detection Opportunities

- Group enumeration commands
- LDAP queries for group membership
- Unusual BloodHound-style enumeration

Key Log Sources

- Sysmon Event 1: net group, net localgroup
- Windows Security 4799 (Security Group Enumeration)
- Domain Controller LDAP query logs

Sigma Detection

```
title: Domain Admin Group Enumeration
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        CommandLine|contains:
            - 'net group "domain admins"'
            - 'net group "enterprise admins"'
            - 'Get-ADGroupMember'
    condition: selection
level: medium
```

Mitigations

- Tiered administration model
- Limit group enumeration permissions
- Monitor LDAP queries

T1016 - System Network Configuration Discovery

Adversaries enumerate network configuration to understand connectivity, routes, and identify pivot targets.

Detection Opportunities

- ipconfig, netstat, route commands
- Network interface enumeration APIs
- Discovery command stacking

Key Log Sources

- Sysmon Event 1: ipconfig, netstat, arp, route
- Command-line logging correlation

Sigma Detection

```
title: Network Configuration Discovery
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith:
            - '\ipconfig.exe'
            - '\netstat.exe'
            - '\arp.exe'
            - '\route.exe'
    condition: selection
level: informational
```

Mitigations

- Behavioral baseline
- Network segmentation

T1033 - System Owner/User Discovery

Adversaries identify the current user and other logged-on users to understand the context and identify targets.

Detection Opportunities

- whoami, query user, qwinsta commands
- Enumeration of logged-on sessions

Key Log Sources

- Sysmon Event 1: whoami, query user
- Command-line patterns

Sigma Detection

```
title: User Discovery Commands
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith:
            - '\whoami.exe'
            - '\query.exe'
            - '\qwinsta.exe'
    suspicious:
        CommandLine|contains:
            - '/priv'
            - '/all'
            - '/groups'
    condition: selection and suspicious
level: low
```

Mitigations

- Behavioral baseline
- Monitor enumeration stacking

T1482 - Domain Trust Discovery

Adversaries enumerate domain trusts to identify paths for lateral movement across trust boundaries.

Detection Opportunities

- nltest /domain_trusts command
- LDAP queries for trust objects
- BloodHound trust enumeration

Key Log Sources

- Sysmon Event 1: nltest, dsquery trusteddomain
- Domain Controller LDAP logs

- Active Directory audit logs

Sigma Detection

```
title: Domain Trust Discovery
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        CommandLine|contains:
            - 'nltest /domain_trusts'
            - 'Get-ADTrust'
            - 'dsquery trustedDomain'
    condition: selection
level: medium
```

Mitigations

- SID filtering on trusts
- Selective authentication
- Monitor trust enumeration

TA0008 - Lateral Movement

Lateral Movement techniques allow adversaries to move through the network. Detection focuses on authentication patterns, remote execution, and network connections.

Previously Documented (3)

- T1021 - Remote Services
- T1550 - Use Alternate Authentication Material
- T1570 - Lateral Tool Transfer

Additional Techniques (7)

T1021.001 - Remote Desktop Protocol

Adversaries use RDP for interactive access to remote systems. RDP provides full GUI access but leaves significant logs.

Detection Opportunities

- RDP logon events (Type 10)
- Unexpected RDP sources
- RDP from non-workstation systems
- Multiple RDP sessions from single source

Key Log Sources

- Windows Security 4624 LogonType 10
- Windows Security 4778/4779 (Session reconnect/disconnect)
- TerminalServices-LocalSessionManager logs
- Network: 3389/TCP connections

Sigma Detection

```
title: RDP from Non-Workstation
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4624
        LogonType: 10
    filter:
        IpAddress|startswith: '10.10.20.'  # Workstation VLAN
    condition: selection and not filter
level: medium
```

Mitigations

- Network Level Authentication (NLA)

- Restrict RDP to jump servers
- MFA for RDP
- RDP gateway with logging

T1021.002 - SMB/Windows Admin Shares

Adversaries use SMB and administrative shares (C$, ADMIN$, IPC$) for lateral movement and file transfer.

Detection Opportunities

- Admin share access events
- File copies to ADMIN$
- Unusual SMB connections between workstations
- PsExec-style execution via shares

Key Log Sources

- Windows Security 5140/5145 (Share Access)
- Sysmon Event 3: SMB connections
- Sysmon Event 11: File creation on admin shares

Sigma Detection

```
title: Admin Share Access
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 5145
        ShareName|contains:
            - 'ADMIN$'
            - 'C$'
    condition: selection
level: medium
```

Mitigations

- Disable admin shares where not needed
- Network segmentation
- SMB signing
- Monitor admin share access

T1021.003 - Distributed Component Object Model

Adversaries use DCOM for remote code execution, often via Office applications or system objects.

Detection Opportunities

- DCOM network connections

- MMC20, ShellWindows, ShellBrowserWindow abuse
- Office spawning processes via DCOM

Key Log Sources

- Windows Security 4688: Process creation via DCOM
- Sysmon Event 3: DCOM network (135/TCP + dynamic)
- Sysmon Event 1: mmc.exe, excel.exe spawning processes remotely

Sigma Detection

```
title: DCOM Remote Process Creation
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        ParentImage|endswith:
            - '\mmc.exe'
            - '\excel.exe'
            - '\outlook.exe'
        Image|endswith:
            - '\cmd.exe'
            - '\powershell.exe'
    condition: selection
level: high
```

Mitigations

- Disable DCOM where not required
- DCOM security configuration
- Monitor known DCOM abuse patterns

T1021.004 - SSH

Adversaries use SSH for lateral movement, especially in Linux environments or hybrid networks.

Detection Opportunities

- SSH authentication events
- SSH from unusual sources
- SSH key usage anomalies
- Interactive SSH sessions to servers

Key Log Sources

- Linux auth.log: SSH authentication events
- Windows OpenSSH logs
- Network: 22/TCP connections
- SSH audit logs

Sigma Detection

```
title: SSH Brute Force Attempt
logsource:
    product: linux
    service: auth
detection:
    selection:
        pam_message: 'authentication failure'
    timeframe: 1m
    condition: selection | count() by src_ip > 10
level: high
```

Mitigations

- Key-based authentication only
- SSH jump servers
- Fail2ban or similar
- MFA for SSH

T1021.006 - Windows Remote Management

Adversaries use WinRM for remote PowerShell execution and management.

Detection Opportunities

- WinRM authentication events
- PowerShell remoting sessions
- wsmprovhost.exe execution

Key Log Sources

- Windows Security 4624 Type 3 with WinRM
- PowerShell Operational logs (Event 40961, 40962)
- Sysmon Event 1: wsmprovhost.exe
- Network: 5985/5986 (HTTP/HTTPS)

Sigma Detection

```
title: WinRM Remote PowerShell Session
logsource:
    product: windows
    service: powershell
detection:
    selection:
        EventID: 4103
        HostApplication|contains: 'wsmprovhost'
    condition: selection
level: medium
```

Mitigations

- Restrict WinRM to management networks
- Require HTTPS for WinRM
- Enable PowerShell logging
- Use constrained endpoints

T1534 - Internal Spearphishing

Adversaries send phishing emails from compromised internal accounts to move laterally.

Detection Opportunities

- Internal email with malicious content
- Unusual sender patterns
- Internal emails with external characteristics

Key Log Sources

- Email gateway logs for internal traffic
- Exchange Message Tracking logs
- DLP alerts on internal mail

Mitigations

- Internal email scanning
- DLP for internal communications
- User awareness training

T1563 - Remote Service Session Hijacking

Adversaries hijack existing remote sessions (RDP, SSH) to take over legitimate user connections.

Detection Opportunities

- Session shadow/takeover commands
- tscon.exe execution
- Session state changes

Key Log Sources

- Sysmon Event 1: tscon.exe execution
- Windows TerminalServices logs
- Session disconnect/reconnect events

Sigma Detection

```
title: RDP Session Hijacking
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\tscon.exe'
    condition: selection
level: critical
```

Mitigations

- Restrict session takeover permissions
- Monitor tscon usage
- Disable RDP session shadowing

TA0009 - Collection

Collection techniques allow adversaries to gather data of interest. Detection focuses on access to sensitive data, staging activity, and collection tool patterns.

Previously Documented (3)

- T1113 - Screen Capture
- T1056 - Input Capture
- T1560 - Archive Collected Data

Additional Techniques (7)

T1005 - Data from Local System

Adversaries collect sensitive data from local filesystems including documents, databases, and configuration files.

Detection Opportunities

- Bulk file access patterns
- Access to sensitive directories
- Staging of collected files

Key Log Sources

- Sysmon Event 11: File reads in sensitive directories
- Windows Security 4663 (Object Access)
- DLP file access events

Sigma Detection

```
title: Access to Sensitive File Types
logsource:
    product: windows
    category: file_access
detection:
    selection:
        TargetFilename|endswith:
            - '.docx'
            - '.xlsx'
            - '.pdf'
            - '.pst'
    bulk:
        | count() by ProcessId > 50
    timeframe: 5m
    condition: selection and bulk
level: medium
```

Mitigations

- Data Loss Prevention (DLP)
- File access auditing
- Data classification
- Endpoint detection for bulk access

T1039 - Data from Network Shared Drive

Adversaries collect data from network shares accessible from compromised systems.

Detection Opportunities

- Bulk file access on shares
- Unusual share enumeration
- Access from unexpected hosts

Key Log Sources

- Windows Security 5145 (Share Access)
- File server access logs
- Network: SMB read patterns

Mitigations

- Least privilege share access
- Share access auditing
- DLP on file servers

T1025 - Data from Removable Media

Adversaries collect data from removable media inserted into compromised systems.

Detection Opportunities

- USB device insertion events
- File reads from removable drives
- Bulk copy from removable media

Key Log Sources

- Windows PnP device events
- Sysmon Event 11: File operations on removable drives
- DLP removable media events

Mitigations

- USB device controls
- Endpoint DLP
- Encryption requirements for removable media

T1074 - Data Staged

Adversaries stage collected data in central locations before exfiltration, often using temp directories or hidden folders.

Detection Opportunities

- Large file creation in temp/staging directories
- Archive creation (zip, rar, 7z)
- Hidden directories with collected data

Key Log Sources

- Sysmon Event 11: File creation in staging paths
- Sysmon Event 1: Compression utilities
- File integrity monitoring

Sigma Detection

```
title: Data Staging via Archive Creation
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith:
            - '\7z.exe'
            - '\rar.exe'
            - '\zip.exe'
    staging:
        CommandLine|contains:
            - '\Temp\\'
            - '\AppData\\'
            - '\ProgramData\\'
    condition: selection and staging
level: medium
```

Mitigations

- Monitor staging directories
- DLP for archive creation
- Endpoint detection for staging patterns

T1114 - Email Collection

Adversaries collect email from local clients, servers, or cloud services for intelligence gathering.

Detection Opportunities

- PST/OST file access
- Mailbox export via PowerShell
- Graph API email access
- EWS bulk mail access

Key Log Sources

- Sysmon Event 11: PST/OST file operations
- Exchange audit logs
- Microsoft 365 Unified Audit Log
- Azure AD sign-in logs for mail apps

Sigma Detection

```
title: Outlook Data File Access
logsource:
    product: windows
    category: file_access
detection:
    selection:
        TargetFilename|endswith:
            - '.pst'
            - '.ost'
    filter:
        Image|endswith: '\OUTLOOK.EXE'
    condition: selection and not filter
level: high
```

Mitigations

- Mailbox audit logging
- DLP for email exports
- Restrict mail protocol access

T1115 - Clipboard Data

Adversaries capture clipboard contents to collect sensitive data like passwords or documents.

Detection Opportunities

- Clipboard API access
- Known clipboard stealing tools
- Persistent clipboard monitoring

Key Log Sources

- EDR clipboard access telemetry
- API monitoring for GetClipboardData
- Process behavior analysis

Mitigations

- EDR behavioral detection
- Clipboard history restrictions
- Application isolation

T1119 - Automated Collection

Adversaries use scripts or tools to automatically collect data based on patterns, file types, or locations.

Detection Opportunities

- Scripted file enumeration and collection
- Bulk file operations from scripts
- Known collection tool signatures

Key Log Sources

- Sysmon Event 1: Collection tool execution
- PowerShell script block logging
- File access patterns

Sigma Detection

```
title: Automated File Collection via PowerShell
logsource:
    product: windows
    category: ps_script
detection:
    selection:
        ScriptBlockText|contains:
            - 'Get-ChildItem'
            - '-Recurse'
    collection:
        ScriptBlockText|contains:
            - 'Copy-Item'
            - 'Compress-Archive'
            - '.zip'
    condition: selection and collection
level: medium
```

Mitigations

- DLP for bulk operations
- Script execution policies
- Endpoint detection

TA0011 - Command and Control

Command and Control techniques allow adversaries to communicate with compromised systems. Detection focuses on network patterns, protocol anomalies, and known C2 infrastructure.

Previously Documented (4)

- T1071 - Application Layer Protocol
- T1572 - Protocol Tunneling
- T1573 - Encrypted Channel
- T1090 - Proxy

Additional Techniques (6)

T1071.001 - Web Protocols (HTTP/S)

Adversaries use HTTP/S for C2 to blend with normal web traffic. Most C2 frameworks support HTTP/S as primary channel.

Detection Opportunities

- Beaconing patterns (regular intervals with jitter)
- Unusual user-agent strings
- POST requests to static-looking URLs
- Large outbound data transfers

Key Log Sources

- Proxy logs (URLs, user-agents, bytes transferred)
- Zeek http.log, ssl.log
- Firewall logs with URL filtering
- JA3/JA4 fingerprints

Sigma Detection

```
title: Potential C2 Beaconing
# Note: Typically implemented as SIEM correlation
# Look for:
# - Regular connection intervals (± jitter)
# - Same destination, same process
# - Low variance in request timing
# - Consistent payload sizes
```

Mitigations

- SSL inspection
- Domain categorization/reputation
- RITA/AC-Hunter for beacon detection

- JA3 blocking for known malware

T1071.004 - DNS

Adversaries use DNS for C2 communication, encoding commands in queries and responses.

Detection Opportunities

- Long DNS queries (encoded data)
- High volume of DNS requests
- TXT record queries
- Queries to low-reputation domains

Key Log Sources

- DNS query logs (internal resolvers)
- Sysmon Event 22 (DNS Query)
- Zeek dns.log
- Passive DNS

Sigma Detection

```
title: Potential DNS Tunneling
logsource:
    category: dns
detection:
    long_subdomain:
        query|re: '^[a-zA-Z0-9]{30,}\.'
    txt_records:
        query_type: 'TXT'
    timeframe: 1h
    condition: long_subdomain | count() > 100 or txt_records | count() > 50
level: high
```

Mitigations

- DNS query logging and analysis
- Block DNS over HTTPS (DoH) to external resolvers
- DNS reputation services
- Limit DNS query length

T1095 - Non-Application Layer Protocol

Adversaries use non-standard protocols (ICMP, raw TCP/UDP) for C2 to evade application-layer inspection.

Detection Opportunities

- ICMP tunneling (data in echo requests)
- Unusual protocol usage patterns
- High volume of non-standard traffic

Key Log Sources

- Zeek conn.log (protocol analysis)
- Firewall logs for unusual protocols
- IDS signatures for protocol anomalies

Mitigations

- Strict egress filtering
- Protocol inspection at firewall
- Block unnecessary protocols

T1132 - Data Encoding

Adversaries encode C2 data using standard encoding schemes (Base64, XOR) to evade inspection.

Detection Opportunities

- Base64 patterns in network traffic
- High entropy in HTTP parameters
- XOR patterns in payloads

Key Log Sources

- Proxy logs with full URL parameters
- Network packet inspection
- IDS content matching

Mitigations

- SSL inspection
- Deep packet inspection
- Behavioral analysis over signature

T1568 - Dynamic Resolution

Adversaries use dynamic techniques to determine C2 servers, including DGA (Domain Generation Algorithms) and fast-flux DNS.

Detection Opportunities

- DGA domain patterns (high entropy, random-looking)
- Queries to many NXDOMAINs
- Fast-flux DNS (rapidly changing IPs)

Key Log Sources

- DNS query logs with NXDOMAIN responses
- Domain reputation services
- Passive DNS for IP changes

Sigma Detection

```
title: Potential DGA Activity
logsource:
    category: dns
detection:
    selection:
        response_code: 'NXDOMAIN'
    timeframe: 1h
    condition: selection | count() by src_ip > 100
level: high
```

Mitigations

- DGA detection algorithms
- DNS sinkholing
- Threat intelligence feeds

T1105 - Ingress Tool Transfer

Adversaries transfer tools and malware into the environment after initial access.

Detection Opportunities

- File downloads from suspicious sources
- certutil, bitsadmin downloads
- PowerShell download cradles

Key Log Sources

- Sysmon Event 1: Download tool execution
- Sysmon Event 11: File creation from downloads
- Proxy logs for file downloads

Sigma Detection

```
title: Certutil Used for Download
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\certutil.exe'
        CommandLine|contains:
            - 'urlcache'
            - '-f'
            - 'http'
    condition: selection
level: high
```

Mitigations

- Application allowlisting

- Block LOLBins from network access
- Web filtering

TA0010 - Exfiltration

Exfiltration techniques allow adversaries to steal data from target networks. Detection focuses on unusual data transfers, protocol abuse, and known exfiltration patterns.

Previously Documented (3)

- T1041 - Exfiltration Over C2 Channel
- T1048 - Exfiltration Over Alternative Protocol
- T1567 - Exfiltration to Cloud Storage

Additional Techniques (7)

T1020 - Automated Exfiltration

Adversaries automate data exfiltration using scripts or scheduled tasks to continuously steal data.

Detection Opportunities

- Scheduled network transfers
- Scripts with upload functions
- Regular large outbound transfers

Key Log Sources

- Scheduled task logs
- Network flow analysis
- PowerShell logging

Mitigations

- DLP for network transfers
- Egress traffic monitoring
- Bandwidth anomaly detection

T1030 - Data Transfer Size Limits

Adversaries break data into smaller chunks to avoid detection thresholds for large transfers.

Detection Opportunities

- Many small transfers to same destination
- Chunked upload patterns
- Sustained low-bandwidth exfiltration

Key Log Sources

- Network flow with size analysis
- Proxy logs aggregated by destination
- DLP cumulative transfer tracking

Mitigations

- Cumulative transfer monitoring
- Per-destination volume tracking
- DLP with aggregation

T1048.002 - Exfiltration Over Asymmetric Encrypted Channel

Adversaries exfiltrate data over encrypted channels that are difficult to inspect.

Detection Opportunities

- Large uploads over HTTPS to unknown destinations
- Certificate anomalies
- JA3 fingerprint analysis

Key Log Sources

- SSL inspection logs
- Proxy logs with upload sizes
- Certificate transparency logs

Mitigations

- SSL inspection
- Category-based blocking
- Upload size monitoring

T1048.003 - Exfiltration Over Unencrypted Channel

Adversaries use unencrypted protocols (FTP, HTTP) that may bypass security controls focused on encrypted traffic.

Detection Opportunities

- FTP uploads
- HTTP POST with large bodies
- Clear-text protocols to external IPs

Key Log Sources

- Network flow for FTP (21/TCP)
- Proxy logs for HTTP uploads
- IDS for clear-text exfiltration

Mitigations

- Block unencrypted protocols outbound
- DLP for clear-text content
- Egress filtering

T1052 - Exfiltration Over Physical Medium

Adversaries use physical media (USB, external drives) to exfiltrate data, bypassing network controls entirely.

Detection Opportunities

- Large writes to removable media
- USB device insertion events
- DLP alerts on removable storage

Key Log Sources

- Windows PnP device logs
- DLP removable media events
- Sysmon Event 11: File writes to removable drives

Sigma Detection

```
title: Large Write to Removable Media
logsource:
    product: windows
    category: file_event
detection:
    selection:
        TargetFilename|re: '^[D-Z]:\\\\'
    large_file:
        # Correlate with file size if available
    condition: selection
level: medium
```

Mitigations

- USB device controls
- Endpoint DLP
- Physical security

T1537 - Transfer Data to Cloud Account

Adversaries transfer data to cloud accounts they control, often using legitimate cloud sync clients.

Detection Opportunities

- Cloud sync to personal accounts
- New cloud app connections
- Large uploads to cloud storage

Key Log Sources

- CASB logs
- Cloud app audit logs
- Proxy logs for cloud storage APIs

Mitigations

- CASB controls
- Block personal cloud storage
- DLP for cloud apps

T1011 - Exfiltration Over Other Network Medium

Adversaries use alternative network paths (WiFi, cellular, Bluetooth) to exfiltrate data bypassing corporate network controls.

Detection Opportunities

- WiFi adapter activity on wired systems
- Mobile hotspot connections
- Bluetooth file transfers

Key Log Sources

- Wireless adapter events
- EDR network interface monitoring
- Physical security (RF detection)

Mitigations

- Disable unnecessary network adapters
- Wireless security monitoring
- Physical security controls

TA0040 - Impact

Impact techniques allow adversaries to disrupt operations, destroy data, or manipulate business processes. Detection focuses on destructive behaviors, service disruption, and data manipulation.

Previously Documented (3)

- T1486 - Data Encrypted for Impact (Ransomware)
- T1489 - Service Stop
- T1490 - Inhibit System Recovery

Additional Techniques (7)

T1485 - Data Destruction

Adversaries destroy data to disrupt operations or cover tracks. Unlike ransomware, data is permanently deleted rather than encrypted.

Detection Opportunities

- Mass file deletion events
- Wiper malware signatures
- Disk overwrite operations
- MBR/GPT modifications

Key Log Sources

- Sysmon Event 23: File Delete (archived)
- Sysmon Event 11: File operations
- VSS deletion events
- EDR disk operation telemetry

Sigma Detection

```
title: Mass File Deletion
logsource:
    product: windows
    category: file_delete
detection:
    selection:
        EventID: 23
    timeframe: 5m
    condition: selection | count() by Image > 100
level: critical
```

Mitigations

- Immutable backups
- File access controls

- EDR behavioral detection
- Volume Shadow Copy protection

T1491 - Defacement

Adversaries modify visual content (websites, desktops) to deliver messages or claim responsibility.

Detection Opportunities

- Web content file modifications
- Desktop wallpaper changes
- Website integrity monitoring

Key Log Sources

- File integrity monitoring on web roots
- Registry changes for desktop settings
- Web server access logs

Mitigations

- File integrity monitoring
- Web application firewall
- Content change alerting

T1498 - Network Denial of Service

Adversaries conduct DoS attacks to disrupt network availability.

Detection Opportunities

- Traffic volume anomalies
- Source IP diversity
- Protocol abuse patterns

Key Log Sources

- Network flow analysis
- Firewall connection logs
- DDoS mitigation appliance logs

Mitigations

- DDoS protection services
- Rate limiting
- Traffic scrubbing
- Anycast distribution

T1499 - Endpoint Denial of Service

Adversaries exhaust system resources to cause denial of service on specific endpoints.

Detection Opportunities

- CPU/memory exhaustion
- Disk space consumption
- Process resource abuse

Key Log Sources

- Performance counters
- System resource monitoring
- Process resource usage

Mitigations

- Resource quotas
- Process limits
- Monitoring and alerting

T1529 - System Shutdown/Reboot

Adversaries force system shutdowns to disrupt operations or complete malicious actions.

Detection Opportunities

- Shutdown/reboot commands
- Unexpected system restarts
- Scheduled shutdown tasks

Key Log Sources

- Windows Security 4608 (Windows Starting)
- Windows System 1074 (Shutdown Initiated)
- Sysmon Event 1: shutdown.exe execution

Sigma Detection

```
title: Forced System Shutdown
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        Image|endswith: '\shutdown.exe'
        CommandLine|contains:
            - '/s'
            - '/r'
            - '-s'
            - '-r'
    condition: selection
level: medium
```

Mitigations

- Restrict shutdown permissions
- Monitor shutdown events
- Redundant systems

T1531 - Account Access Removal

Adversaries delete or disable accounts to deny access to legitimate users.

Detection Opportunities

- Account deletion events
- Password resets on multiple accounts
- Account disable events

Key Log Sources

- Windows Security 4726 (Account Deleted)
- Windows Security 4725 (Account Disabled)
- Azure AD audit logs

Sigma Detection

```
title: Bulk Account Manipulation
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID:
            - 4725  # Disabled
            - 4726  # Deleted
    timeframe: 10m
    condition: selection | count() > 5
level: high
```

Mitigations

- Break-glass accounts
- Account deletion restrictions
- Backup authentication methods

T1565 - Data Manipulation

Adversaries modify data to affect business processes, corrupt information, or cause incorrect decisions.

Detection Opportunities

- Database modification anomalies
- Financial data changes
- Configuration modifications

Key Log Sources

- Database audit logs
- Application audit logs
- File integrity monitoring

Mitigations

- Data integrity monitoring
- Audit logging on critical data
- Change management controls
- Data validation

Appendix A: Detection Priority Matrix

Prioritization framework for detection development based on threat intelligence, organizational risk, and implementation complexity.

Priority	Criteria	Examples
P1 - Critical	Active threat, high impact, easy detection	Ransomware indicators, LSASS access, admin share access
P2 - High	Common technique, significant impact	PowerShell abuse, scheduled tasks, service installation
P3 - Medium	Moderate frequency, detectable with effort	WMI persistence, DLL hijacking, token manipulation
P4 - Low	Rare or difficult to detect reliably	Hardware implants, kernel exploits, custom protocols

Appendix B: Log Source Requirements

Minimum log sources required for comprehensive ATT&CK detection coverage.

Log Source	Coverage	Configuration
Sysmon	TA0002-TA0009	SwiftOnSecurity config + custom rules
Windows Security	TA0001, TA0003-TA0006, TA0008	4624, 4625, 4648, 4688, 4698, 4720, 5140
PowerShell	TA0002, TA0005	Script Block (4104), Module (4103)
DNS Logs	TA0011	Query logging on resolvers, Sysmon 22
Proxy/Firewall	TA0001, TA0010, TA0011	Full URL, user-agent, bytes
Zeek/Suricata	TA0008, TA0010, TA0011	conn, dns, http, ssl, files logs
Azure AD	TA0001, TA0006	Sign-in logs, audit logs, risky users
EDR	All tactics	Behavioral detection, telemetry

Appendix C: Sigma Rule Index

Summary of Sigma rules included in this document for implementation reference.

Tactic	Rule Name	Level
TA0001	Browser Spawning Suspicious Process	High
TA0001	Partner Account Accessing Sensitive Resources	Medium
TA0001	Office Application Spawning Script Interpreter	High
TA0002	WMI Spawning Suspicious Process	High
TA0002	Suspicious PowerShell Download Cradle	High
TA0003	Service Installed with Suspicious Binary Path	Critical
TA0003	WMI Event Subscription Created	Critical
TA0003	IIS Worker Spawning Suspicious Process	Critical
TA0004	CreateRemoteThread into Sensitive Process	Critical
TA0004	UAC Bypass via fodhelper	Critical
TA0005	Renamed System Binary	High
TA0005	Security Event Log Cleared	Critical
TA0006	Kerberoasting - RC4 Service Ticket	High
TA0006	SMB Connection to External IP	High
TA0007	Domain Admin Group Enumeration	Medium
TA0007	Domain Trust Discovery	Medium
TA0008	Admin Share Access	Medium
TA0008	RDP Session Hijacking	Critical
TA0009	Data Staging via Archive Creation	Medium
TA0009	Outlook Data File Access	High
TA0011	Potential DNS Tunneling	High
TA0011	Certutil Used for Download	High
TA0010	Large Write to Removable Media	Medium
TA0040	Mass File Deletion	Critical
TA0040	Forced System Shutdown	Medium