Eviction Strategies Tool Playbook

**Title:** Comprehensive Endpoint & Organizational Hardening

**Template:** no template used

**Created:** 2025-07-31T00:00:00Z

**Updated:** 2025-07-31T00:00:00Z

**Version:** 2

# Techniques & Mappings

| Technique | Confidence | Mapped Countermeasures |
| --- | --- | --- |
| T1566.001: Phishing: Spearphishing Attachment | confirmed | CM0002, CM0010, CM0100 |
| T1059: Command and Scripting Interpreter | confirmed | CM0004, CM0012, CM0009 |
| T1200: Hardware Additions | confirmed | CM0059, CM0102 |
| T1078: Valid Accounts | confirmed | CM0012, CM0028, CM0105 |
| T1486: Data Encrypted for Impact | confirmed | CM0035, CM0062, CM0040 |
| T1021.001: Remote Services: Remote Desktop Protocol | confirmed | CM0012, CM0028 |
| T1204: User Execution | confirmed | CM0100 |
| T1087: Account Discovery | confirmed | CM0101 |
| T1005: Data from Local System | confirmed | CM0030 |
| T1490: Inhibit System Recovery | confirmed | CM0040 |
| T1555: Credentials from Password Stores | confirmed | CM0100 |
| T1562: Impair Defenses | confirmed | CM0106 |
| T1071: Application Layer Protocol | confirmed | CM0103 |
| (Additional Countermeasures) | - |  |

# Countermeasures

## CM0002: Enable Email Attachment Filtering and Message Authentication

### Details

* **ID:** CM0002
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Enable
* **Status:** Active

### Intended Outcome

Enabling email attachment filtering and enabling message authentication restricts adversary initial access using malicious files.

### Introduction

An email gateway can filter incoming and outgoing email messages based on specified parameters. Email gateways provide a high level of control over what emails are to be filtered out and how. The attachment scanning capability commonly available with email gateways allows organizations to automatically scan email attachments and perform different tasks on them (hash checking, filetype checking, etc.) and then filter them out based on different criteria. Examples of file types typically blocked: .com, .exe, .dll, .ps1, .ps1xml, .msh, .cmd, .bat, .hta, .jar, .ws, .wsc, .rar, .bz2, .gz, .tar, .msi, .msu, .tmp, .iso, .img, .xls, .xlt, .xlm

Sender Policy Framework (SPF) serves as an email authentication mechanism that verifies the IP address of the sending server matches the domain name of the sender's email address. Implementing SPF helps to prevent spoofing attacks. Spoofing attacks can increase the likelihood of an authentic looking attachment with a malicious payload reaching an employee's inbox.

Domain Keys Identified Mail (DKIM) provides an additional layer of email authentication that helps to confirm the integrity of messages via digital signatures and can help prevent email tampering that might occur in transit from one location to another.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email authentication protocol that allows control over how an organization's emails should be handled should they fail SPF or DKIM checks, which can help to prevent email spoofing. DMARC can also generate reports on other useful email authentication measures such as Certificate Authorities Authorization (CAA), Authenticated Received Chain (ARC), and the Domain Name System-Based Authentication of Named Entities (DANE).

### Preparation

* Deploy and configure an email gateway.
* Compile an up-to-date list of suitable or unsuitable file types that you wish the email gateway to either block or allow.
* Ensure that the appropriate allowlist/denylist that best suits the organization's business needs and security requirements is/are configured and up to date.
* Ensure that email file attachment hashes are being compared to a reliable and reputable database of known malicious hashes and that any files with a matching hash from the database are blocked. This can be performed either via the email gateway, or a third-party solution that is properly integrated with the email gateway. However, security teams should understand that just because a file's hash doesn't match a previously identified signature, this does not mean the file is verified to be safe as packing and obfuscating malicious files is comparatively easy for threat actors.

### Risks

* This countermeasure can break legitimate functionality.
* A phased implementation can reveal potential issues involving improper quarantining or blocking. During the first phase, e-mails to be quarantined are flagged and monitored, allowing issues to be identified and resolved. E-mails are quarantined in a subsequent phase.

### Guidance

#### Email Gateway Configuration

* Configure an email gateway to filter incoming and outgoing email messages based on specific parameters.
* Enable the attachment scanning capability to automatically scan email attachments (hash checking, filetype checking, etc.) and filter them based on specified criteria. If this capability does not exist on your solution, consider supplementing with antivirus integration.

#### Anti-Spoofing and Email Authentication Mechanisms

* Implement Sender Policy Framework (SPF) to help prevent spoofing attacks. Ensure emails with attachments that fail SPF checks are rejected, quarantined, or flagged as suspicious.
* Ensure email services support Domain Keys Identified Mail (DKIM). Configure DKIM settings for action if an email fails to pass a DKIM check.
* Verify that your email services support Domain-based Message Authentication, Reporting, and Conformance (DMARC) and configure DMARC settings to specify the actions to be taken if an email fails to pass a check.

#### User/Employee Training

* Provide education and training to inform users of the risks and best practices associated with email attachments.

### References

* Filtering and blocking email attachments using Trend Micro's Messaging products | <https://success.trendmicro.com/en-US/solution/KA-0003827>
* Defense Evasion and Phishing Emails | <https://redcanary.com/blog/defense-evasion-and-phishing-emails/>
* Spearphishing Attachment | <https://redcanary.com/threat-detection-report/techniques/spearphishing-attachment/>
* Mail flow best practices for Exchange Online, Microsoft 365, and Office 365 (overview) | <https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/mail-flow-best-practices/>
* Anti-spoofing protection in EOP | <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-spoofing-about/>
* Strategies to Mitigate Cyber Security Incidents | <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents>
* Configure trusted ARC sealers | <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-arc-exceptions-to-mark-trusted-arc-senders/>
* What is Certification Authority Authorization? | <https://pkic.org/2013/09/25/what-is-certification-authority-authorization/>
* Phishing | <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>

## CM0010: Enable Internet Protocol (IP) Address Allowlists

### Details

* **ID:** CM0010
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Enable
* **Status:** Active

### Intended Outcome

Enabling Internet Protocol (IP) address allowlists restricts adversary
initial access and command and control using unverified IP addresses.

### Introduction

There are numerous open-source and commercially available solutions for
IP allowlisting.

### Preparation

No Preparation content identified.

### Risks

* This countermeasure may block legitimate activity.
* IP allowlisting risks blocking legitimate and/or mission essential connections.

### Guidance

On the host

* Check the firewall (Windows, UFW, etc.) for the presence of specific IP addresses for whitelisting.
* If not present, create an inbound rule for specifically approved IP addresses.

On the Enterprise

* Maintain a list of allowed IP addresses.
* Import the allowlist into the endpoint detection/protection solution or via the main firewall.
* Process requests for adding new IP addresses to the allowlist.

### References

* Security - Firewall | <https://ubuntu.com/server/docs/firewalls>
* iptables(8) - Linux man page | <https://linux.die.net/man/8/iptables>
* How to Add IP Address in Windows Firewall | <https://web.archive.org/web/20240616112618/https://www.oryon.net/knowledge-base/article/how-to-add-ip-address-in-windows-firewall/>
* Uncomplicated Firewall | <https://wiki.archlinux.org/title/Uncomplicated_Firewall>

## CM0100: Restrict and Monitor Remote Procedure Calls (RPC)

### Details

* **ID:** CM0100
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Disable, Examine
* **Status:** Active

### Intended Outcome

Restricting and monitoring Remote Procedure Calls (RPC) limits opportunities for an adversary to conduct reconnaissance and achieve execution, lateral movement, and privilege escalation via RPC abuse.

### Introduction

Remote Procedure Call (RPC) is a protocol native to the Windows operating system that enables inter-process communication (IPC) both locally and remotely. RPC is ubiquitous in a Windows environment and although necessary, significantly expands the attack surface. RPC can be abused by adversaries to achieve reconnaissance, execution, lateral movement, and privilege escalation.

RPC cannot be completely blocked, but it can be filtered and monitored. RPC filtering is a capability native to Windows that is facilitated by the Windows Filtering Platform (WFP) via netsh.exe. Another option to consider is the [RPC Firewall](https://github.com/zeronetworks/rpcfirewall) by Zero Networks. This free and open-source tool may offer additional capabilities to enable defenders to more granularly filter and monitor RPC traffic.

### Preparation

* Audit RPC traffic to assess a baseline and identify anomalous traffic.
* RPC filtering can be used to proactively prevent RPC abuse. A deny list can be created to block RPC interfaces and reduce the attack surface introduced by the protocol.

### Risks

RPC filtering is a complex topic that requires responders to be familiar with both the protocol and it's attack surface. Inadvertently blocking necessary RPC traffic can introduce the risk of operational disruption.

### Guidance

#### Restrict

RPC can be restricted by leveraging native RPC filtering capabilities via netsh.exe or by implementing the RPC Firewall. Consider filtering, at a minimum, the following:

* + Permit only specific privileged users to create services remotely.
  + Permit only specific hosts to modify registry data remotely.
  + Prevent scheduled tasks from being created remotely.
  + Only permit Kerberos authentication to a specific RPC endpoint.
  + Block connections to an RPC endpoint made over specific named pipes.

##### RPC Filtering via netsh.exe

* Consider the following process to create an RPC filter:
  + Add a rule - `netsh rpc filter add rule...`
  + Add conditions to the rule - `add condition field...`
  + Add the rule to a filter - `add filter...`

##### RPC Filtering via RPC Firewall

* Consider the following process to create an RPC filter:
  + Identify the Universally Unique Identifier (UUID) and the Opnum (the number of a specific function of an RPC interface) of the RPC call.
  + Collect whitelisted IPs of endpoints that should be permitted to access RPC methods.
  + Block/allow/audit the call.

#### Monitor

* Monitoring RPC traffic is necessary to prevent and detect RPC abuse. RPC auditing can be implemented via the WFP and netsh.exe or via the RPC Firewall. Successful and failed connections should be captured in the Security Event Log and forwarded to a centralized location for detection and analysis.

### References

* Stopping Lateral Movement via the RPC Firewall | <https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall>
* A Definitive Guide to the Remote Procedure Call (RPC) Filter | <https://www.akamai.com/blog/security/guide-rpc-filter>
* Filtering Layer Identifiers | <https://learn.microsoft.com/en-us/windows/win32/fwp/management-filtering-layer-identifiers->
* The Dark Side of Microsoft Remote Procedure Call Protocols | <https://redcanary.com/blog/threat-detection/msrpc-to-attack/>
* RPC Firewall | <https://github.com/zeronetworks/rpcfirewall>

## CM0004: Enable Windows Defender Exploit Guard (WDEG) Attack Surface Reduction (ASR) Rules

### Details

* **ID:** CM0004
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Enable
* **Status:** Active

### Intended Outcome

Enabling Windows Defender Exploit Guard (WDEG) Attack Surface Reduction (ASR) rules restricts adversary lateral movement and persistence using malicious files and scripts.

### Introduction

ASR is a ruleset and subcomponent of WDEG, specifically designed to block processes and activities commonly used by malware to infect computers. ASR rules target specific software behaviors e.g., launching files and scripts, running (obfuscated) scripts, and deviations from typical application behavior.

### Preparation

* Microsoft Defender for Endpoint with real-time and cloud-delivery protection is enabled.
* Microsoft Defender is the primary anti-virus solution.
* No Microsoft Defender component is more than two versions old.

### Risks

No Risks content identified.

### Guidance

Assess the status of ASR and identify gaps in coverage. Survey the attack surface management card in the Microsoft 365 Defender portal and determine whether standard and/or other rules are applied, the mode in which they are configured, and any existing exclusions.

Microsoft recommends beginning by enabling the three standard protection rules: block credential stealing from LSASS, abuse of exploited vulnerable signed drivers, and persistence via WMI event subscription. These three rules can typically be implemented with little impact to business function. ASR can be configured using Microsoft Endpoint Manager, Group Policy, and/or PowerShell Cmdlets.

Additional rules to consider are listed below.

#### Standard Protection Rules

The minimum set of rules which Microsoft recommends you always enabled, while you are evaluating the impact and configuration needs of the other
ASR rules. These rules typically have minimal-to-no noticeable impact on the end user.

| Rule | Mapped to TTPs |
| --- | --- |
| Block abuse of exploited vulnerable signed driver | [T1068](https://attack.mitre.org/techniques/T1068) - Exploitation for Privilege Escalation |
| Block credential stealing from the Windows local security authority subsystem (lsass.exe) | [T1003.001](https://attack.mitre.org/techniques/T1003/001) - OS Credential Dumping: LSASS Memory |
| Block persistence through WMI event subscription | [T1546.003](https://attack.mitre.org/techniques/T1546/003) - Event Triggered Execution: WMI Event Subscription |

#### Other Rules

Rules that require some measure of following the documented deployment steps (Plan \> Test \> Enable \> Operationalize).

| Rule | Mapped to TTPs |
| --- | --- |
| Block Adobe Reader from creating child processes | [T1203](https://attack.mitre.org/techniques/T1203) - Exploitation for Client Execution |
| Block all Office applications from creating child processes | [T1203](https://attack.mitre.org/techniques/T1203) - Exploitation for Client Execution |
| Block executable content from email client and webmail | [T1566](https://attack.mitre.org/techniques/T1566) - Phishing |
| Block executable files from running unless they meet a prevalence, age, or trusted list criterion |  |
| Block execution of potentially obfuscated scripts | [T1027](https://attack.mitre.org/techniques/T1027) - Obfuscated Files or Information |
| Block JavaScript or VBScript from launching downloaded executable content | [T1059.005](https://attack.mitre.org/techniques/T1059/005) - Command and Scripting Interpreter: Visual Basic, [T1059.007](https://attack.mitre.org/techniques/T1059/007) - Command and Scripting Interpreter: JavaScript |
| Block Office applications from creating executable content | [T1204.002](https://attack.mitre.org/techniques/T1204/002) - User Execution: Malicious File |
| Block Office applications from injecting code into other processes | [T1055](https://attack.mitre.org/techniques/T1055) - Process Injection, [T1204.002](https://attack.mitre.org/techniques/T1204/002) - User Execution: Malicious File |
| Block Office communication application from creating child processes |  |
| Block process creations originating from PSExec and WMI commands | [T1569.002](https://attack.mitre.org/techniques/T1569/002) - System Services: Service Execution, [T1047](https://attack.mitre.org/techniques/T1047) - Windows Management Instrumentation |
| Block untrusted and unsigned processes that run from USB | [T1091](https://attack.mitre.org/techniques/T1091) - Replication Through Removable Media |
| Block Win32 API calls from Office macros | [T1204.002](https://attack.mitre.org/techniques/T1204/002) - User Execution: Malicious File |
| Use advanced protection against ransomware |  |

#### Deployment Modes

* Audit mode - used to evaluate how ASR rules would affect the organization if enabled
* Block mode - prevents execution
* Warn mode - warns of execution
* Not configured/disabled

##### Exclusions

Files and folders can be specified for exclusion from ASR rule evaluation. While exclusions may be necessary to ensure normal operations, it is important to note that exclusions could introduce vulnerability and should be carefully evaluated.

A typical implementation process includes the following steps:

#### Plan

The first step in preparing to deploy ASR rules is planning. Key to the planning process is identifying key stakeholders and critical business operations.

* Identify business units - ASR rollout should be contingent upon distribution and usage of software, shared folders, and scripts
* Identify ASR rules champions to assist during rollout, preliminary testing, and implementation
* Inventory business apps - understanding applications and processes used across the organization is critical to the success of ASR rule deployment
* Define ASR rules reporting and response teams - determine the person/team responsible for gathering reports, with whom to share the reports, and how to escalate identified threats/issues
* Determine deployment rings - Leverage deployment rings for phased rollout of ASR rules

#### Test

The second step in preparing to deploy ASR rules is testing. Testing the deployment of ASR rules is critical to ensuring the maximum likelihood of success while minimizing the chance of disrupting regular business operations.

* Enable ASR rule in audit mode
* Review reporting in the Microsoft 365 Defender portal
* Assess impact
* Define exclusions to deploy ASR rules without negatively impacting operations

#### Enable

This step is intended to be the limited and scalable rollout of the tested ASR rules to the first test ring.

* Set ASR rule to block or warn
* Assess impact from the reporting page in Microsoft 365 Defender portal and seek feedback from the ASR champions
* Refine exclusions
* Problematic rules should be switched back into audit mode

#### Operationalize

After the ASR rule is deployed, it is critical to implement processes to
monitor and respond to ASR events.

* Monitor for false positives
* Review ASR rule reports regularly to stay abreast of rule-reported events
* Engage in ASR rule hunting to proactively inspect events

### References

* Enable attack surface reduction rules | <https://learn.microsoft.com/en-us/defender-endpoint/enable-attack-surface-reduction>
* Attack surface reduction rules deployment overview | <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment>
* Attack surface reduction rules reference | <https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference>
* Plan attack surface reduction rules deployment | <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment-plan>
* Test attack surface reduction rules | <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment-test>
* Implement attack surface reduction rules | <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment-implement>
* Operationalize attack surface reduction rules | <https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-deployment-operationalize>

## CM0012: Disable or Restrict Distributed Component Object Model (DCOM) Protocol

### Details

* **ID:** CM0012
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Disable
* **Status:** Active

### Intended Outcome

Disabling or restricting the Distributed Component Object Model (DCOM)
protocol blocks or restricts adversary lateral movement using malicious
COM objects.

### Introduction

DCOM is a technology that enables software component communication and interaction between software components directly over a network enabling distributed computing and inter-process communication. In many organizations, DCOM has been replaced by the .NET Framework, RESTful APIs, and Web Services. However, DCOM is still an essential technology for some organizations because it is required by some applications and legacy systems.

### Preparation

* Determine necessity of permitting DCOM in the environment.
* Determine whether blocking the protocol to specific systems, such as kiosks, fileservers, etc. is sufficient to harden security.

### Risks

* This countermeasure may block legitimate activity. This countermeasure should only be implemented by organizations for which DCOM is not an essential technology.
* Disabling DCOM may impact the functionality of applications and services that rely on it. Potential problems include:
  + Any COM objects that can be started remotely may not function correctly.
  + The local COM+ snap-in will not be able to connect to remote servers to enumerate their COM+ catalog.
  + Certificate auto-enrollment may not function correctly.
  + WMI queries against remote servers may not function correctly.
  + Disabling DCOM by modifying the registry may occur if the registry is modified incorrectly. To limit the damage caused by incorrectly modifying the registry, administrators should modify the registry using the GPO method, and ensure that the registry is backed up prior to attempted modifications.

### Guidance

If reliant on DCOM, organizations should ensure all updates to the
protocol\'s implementation have been installed, including DCOM updates
released by Microsoft.

Otherwise, if DCOM is not required, follow the guidelines below.

#### Disable DCOM using GPO

DCOM can be disabled across multiple systems using a Group Policy Object
(GPO) created or modified within the Group Policy Management Console.
Specifically, system administrators can disable DCOM by selecting the
\"Enabled\" option for \"Default Properties\" located at Computer
Configuration \> Policies \> Administrative Templates \> System \>
Distributed COM

#### Disable DCOM using Dcomcnfg.exe

DCOM can be disabled by running Dcomcnfg.exe and clearing the \"Enable
Distributed COM on this Computer\" checkbox within the Default
Properties tab of the window. Afterwards, administrators should apply
the changes and restart the operating system for the changes to take
effect. Dcomcnfg.exe can be further used to configure DCOM, including
access to highly sensitive
objects.

#### Block DCOM with Windows Firewall

Under appropriate circumstances, security teams may want to consider
restricting DCOM on systems by blocking port 135 to reduce DCOM
functionality. DCOM uses port 135 for the initial session creation.
Blocking port 135 will inhibit remote procedure call (RPC) and remote
management of endpoints disrupting communication between workstations
and Domain Controllers and disrupting SMB file-sharing on Windows
servers.

#### Harden Systems

Verify that other mitigations that prevent an adversary from enabling DCOM or potentially performing other malicious activities are implemented alongside any decision to disable or restrict DCOM. This may require disabling the remote registry and implementing GPOs which harden access privileges.

#### Create DCOM Baseline

Security teams should create a baseline for DCOM usage in their networks
so anomalous DCOM activity can be detected.

### References

* How to disable DCOM support in Windows | <https://support.microsoft.com/en-us/topic/how-to-disable-dcom-support-in-windows-2bb8c280-9698-7f9c-bf67-2625a5873c7b>
* New lateral movement techniques abuse DCOM technology | <https://www.cybereason.com/blog/dcom-lateral-movement-techniques>
* KB5004442---Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414) | <https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c>
* Lateral Movement using DCOM Objects - How to do it the right way? | <https://www.scorpiones.io/articles/lateral-movement-using-dcom-objects>

## CM0009: Update Domain Name Service (DNS) Deny List

### Details

* **ID:** CM0009
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Refresh
* **Status:** Active

### Intended Outcome

Updating the Domain Name Service (DNS) deny list blocks adversary command and control (C2).

### Introduction

Adversaries who acquire infrastructure can use bad domains to run C2-based offensive operations.

### Preparation

No Preparation content identified.

### Risks

* Blocking domains can unintentionally prevent access to domains that that are needed for the enterprise.

### Guidance

DNS blacklists or deny lists are often to filter and block emails containing known bad domains. They can also be used to block, blocks of IP addresses or even an internet service provider known for spam. There are two ways to block a domain:

* Domain redirect - A domain redirect will redirect a flagged domain to a quarantine zone.
* Request denied - A request denied will refuse DNS queries from flagged domains.

### References

* What is a DNSBL? | <https://whatismyipaddress.com/dnsbl-blacklist>
* DNS Blocking: A Viable Strategy in Malware Defense | <https://insights.sei.cmu.edu/blog/dns-blocking-a-viable-strategy-in-malware-defense/>

## CM0059: Configure Tactical Privileged Access Workstation

### Details

* **ID:** CM0059
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Enable
* **Status:** Active

### Intended Outcome

Configuring a tactical privileged access workstation (PAW) enables privileged administrators to respond to an incident while minimizing the exposure of privileged administrator accounts.

### Introduction

A privileged access workstation (PAWs) is a dedicated computer environment that allows accounts with elevated permissions, such as Tier-0 domain administrators, to access and configure highly-sensitive accounts, resources, and functions. PAWs are deployed to enforce the separation of security tiers. Properly configured PAWs ensure the device, accounts, and tools exist within the same security tier, thus minimizing the potential attack surface.

If properly implemented, the tactical PAWs will enable privileged administrators to respond with the required degree of privilege while reducing the risk of exposure from other security tiers. Note that the tactical deployment of PAWs will not protect an environment from an adversary that has already achieved privileged access.

### Preparation

* Ideally, PAWs will be configured prior to an incident as configuring dedicated PAWs can be time consuming. If this in not the case, PAWs will need to be rapidly configured with dedicated hardware and software to enable incident response and reduce exposure.

### Risks

* Leveraging a fresh PAW to facilitate incident response may result in unforeseen difficulties, including software components breaking or security controls interfering with what a responder needs to accomplish to remediate the compromise.

### Guidance

* Create a secure administrative Active Directory organizational unit (OU) structure to host the privileged access workstation (PAW).
* Implement Microsoft Windows Privileged Access Workstation (PAW) Security Technical Implementation Guides (STIG) to quickly minimize the attack surface area of PAWs. The Windows PAW STIG provides configuration and installation requirements for dedicated Windows workstations used exclusively for remote administrative management of designated high-value IT resources.
* Treat the PAW as if it were an air-gapped machine. This means ensuring all remote access is disabled and blocked to prevent unauthorized access.
* Configure the domain administrator account (or other accounts with similarly expansive privilege sets) to only permit authentication from the newly provisioned PAWs. Continue to abide by the principle of least privilege.
* Ensure firewall rules permit only communications with the AD server and utilize a jump box / jump server between the PAW and compromised computing environment. All outbound connections to the Internet from the PAW should be blocked.
* Ensure physical hardware supports the latest Trusted Platform Module and encryption.
* Require multi-factor authentication (MFA) for all accounts operating on PAW(s).
* Avoid the use of wireless network communications and rely on wired network connections wherever possible.
* Document use of USB storage media or peripherals. Avoid reuse of peripherals that were ever used on the compromised computing environment.
* Only run the necessary tooling to carry out system administration duties to minimize its attack surface. Adding unnecessary tools will risk introducing potential vulnerabilities to an otherwise secure workstation.

### References

* Implementing a Zero Trust strategy after compromise recovery | <https://www.microsoft.com/en-us/security/blog/2022/09/14/implementing-a-zero-trust-strategy-after-compromise-recovery/>
* Privileged access: Strategy | <https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-strategy>
* Privileged access deployment | <https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment>
* Microsoft Windows Privileged Access Workstation (PAW) STIG - Ver 2, Rel 3 | <https://public.cyber.mil/u_ms_windows_paw_v2r3_stig/>
* Using Privileged Access Workstations (PAWs) to Protect the Cloud | <https://www.beyondtrust.com/blog/entry/using-privileged-access-workstations-to-protect-the-cloud>

## CM0102: Remove Cached Domain Credentials From Workstation

### Details

* **ID:** CM0102
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Eliminate
* **Status:** Active

### Intended Outcome

Removing cached domain credentials from workstations prevents adversaries from pursuing credential access via password stores and OS credential dumping.

### Introduction

Caching domain credentials locally allows users to log-in if domain controller(s) are down. Adversaries abuse this functionality by dumping cached credentials using tools such as mimikatz.

### Preparation

* Identify which users, if any, should have credentials cached to maintain business operations or communications.

### Risks

* Users won't be able to login if authentication servers are down and domain controller authentication is required.
* Users won't be able to access networked resources.

### Guidance

#### Configure via Group Policy

Open gpedit.msc -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Double-click Policy Named, "Interactive logon: Number of previous logons to cache (in case domain controller is not available)." -> Select 0
This will set previous cached credentials to zero. run gpuupdate force

#### Configure via Registry

Open regedit.exe -> Navigate to HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ -> Double-Click "cachedlogonscount" -> Set Value to 0.

Restart will be required to enforce changes.

### References

* How to remove saved domain credentials from workstation | <https://learn.microsoft.com/en-us/answers/questions/1611007/how-to-remove-saved-domain-credentials-from-a-work>
* Mimikatz | <https://redcanary.com/threat-detection-report/threats/mimikatz/>
* Credential Dumping: Domain Cache Credential | <https://www.hackingarticles.in/credential-dumping-domain-cache-credential/>
* Campus Active Directory - Windows Endpoints - Caching Credentials for Remote Users | <https://kb.wisc.edu/iam/page.php?id=114011#:~:text=Caching%20credentials%20is%20a%20feature,no%20domain%20controllers%20are%20available.>

## CM0028: Reset Service Account Passwords

### Details

* **ID:** CM0028
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Refresh
* **Status:** Active

### Intended Outcome

Resetting service account passwords restricts adversary persistence and lateral movement using valid accounts.

### Introduction

There are different types of service accounts: built-in service accounts, traditional service accounts, and managed service accounts.
Please refer to the Microsoft Service Account Selection Matrix below which provides guidance for what and when a particular service account should be used.

| Criterion | gMSA | sMSA | Computer Account | User account |
| --- | --- | --- | --- | --- |
| App runs on a single server | Yes | Yes. Use a gMSA if possible | Yes. Use an MSA if possible | Yes. Use an MSA if possible |
| App runs on multiple servers | Yes | No | No. Account is tied to the server. | Yes. Use an MSA if possible. |
| App runs behind a load balancer | Yes | No | No | Yes. Use only if you can't use a gMSA. |
| App runs on Windows Server 2008 R2 | No | Yes | Yes. Use an MSA if possible | Yes. Use an MSA if possible |
| App runs on Windows Server 2012 | Yes | Yes. Use a gMSA if possible | Yes. Use an MSA if possible. | Yes. Use an MSA if possible. |
| Requirement to restrict service account to single server | No | Yes | Yes. Use an sMSA if possible. | No |

In summary:

* All Service Accounts: Any Windows Desktop Operating System (preferably attached to Active Directory)
* Windows 2008 R2 and Above: Virtual Service Account or Standalone Managed Service Account
* Windows 2012 and Above: Group Managed Service Account

### Preparation

Documentation or knowledge of the purpose of the service accounts and potential impacts of a password reset is necessary to handle risks.

### Risks

* This countermeasure can break legitimate functionality.
* Resetting Service Account passwords may cause crashes in ongoing processes that have dependencies on services that require authentication. For example, processes that depend on scheduled tasks will fail to execute due to password changes.

### Guidance

#### Built-in Service Accounts

The accounts in this section do not have a password. Built-in service
accounts are: System Account, NetworkService Account, and
LocalService Account. These accounts do not appear in User
Management and cannot be added to groups in AD, but can be viewed in
Service Control Manager (SCM). Service Control Manager can be accessed
by pressing "Windows + R" to access the Run dialog box and entering
"services.msc".

#### Traditional Service Accounts

A "traditional" service account is a standard user account configured to
run one or more services. Administrators and users may use their account
to run services because it is quicker and more convenient. However, this
will lead to issues when trying to track down which accounts are
associated with which services. Another issue that arises is creating a
new account for each service or a group of related services. Not only is
this a tedious task, but it is also problematic if you must manage the
passwords for all of these accounts. There's also the risk of breaking
applications or services associated with the changed passwords.
Therefore, organizations set these accounts to never expire and never
update them.

A solution to counter this would be to configure a group(s) in Active
Directory that contains accounts responsible for service(s). Proper
record keeping of what services these accounts are responsible for
should be kept so planned password resets can be accompanied with
credential updates for services. Also, temporary service disruption can
be planned and accounted for. Password resets can be done through Active
Directory or by using PowerShell cmdlets.

For consideration, do not add service accounts to privileged user
groups. This would enable services to run with elevated privileges and
give an attacker the ability to escalate privileges by compromising a
service or account. Each service should have its own account for
auditing and security purposes.

#### Managed Service Accounts

Managed service accounts are designed for running services. Unique
passwords are automatically generated and changed every 30 days by
Active Directory. Interactive logon is not allowed; passwords are not
stored on the local system; and only Kerberos is used for
authentication. There are two types of managed service accounts,
standalone managed service accounts (sMSA) and group managed service
accounts.

Standalone managed service accounts (sMSAs) require windows server 2008
R2 and above. sMSAs can only run on one server; multiple services can be
run on that server. sMSAs cannot run scheduled tasks.

Group managed service accounts supersede sMSA and require Windows server
2012 or later. gMSAs can be used across multiple servers and can be used
to run scheduled tasks.

### References

* Windows LocalSystem vs. System | <https://serverfault.com/questions/168752/windows-localsystem-vs-system>
* Secure on-premises computer accounts with Active Directory | <https://learn.microsoft.com/en-us/entra/architecture/service-accounts-computer>
* Securing on-premises service accounts | <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-on-premises>
* LocalSystem Account | <https://learn.microsoft.com/en-us/windows/win32/services/localsystem-account>
* NetworkService Account | <https://learn.microsoft.com/en-us/windows/win32/services/networkservice-account>
* Local Accounts | <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts>
* LocalService Account | <https://learn.microsoft.com/en-us/windows/win32/services/localservice-account>
* Reset-ComputerMachinePassword | <https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/reset-computermachinepassword>
* Using Managed Service Accounts (MSA and gMSA) in Active Directory | <https://woshub.com/group-managed-service-accounts-in-windows-server-2012/>
* LocalService Account | <https://learn.microsoft.com/en-us/windows/win32/services/localservice-account>

## CM0105: Remove Malicious Enterprise Applications and Service Account Principals

### Details

* **ID:** CM0105
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Eliminate
* **Status:** Active

### Intended Outcome

Removing malicious applications and service account principals blocks an adversary's persistance via applications and service principals in the environment.

### Introduction

Adversaries may compromise legitimate enterprise applications with malicious code using hooks, payload injections, and other tactics to maintain persistence and evade defenses. Service principals are the identities of applications as stored in Entra ID, determining the resources an application is allowed to access. Compromised service principals lead to incorrect access controls and permissions.

Malicious Azure applications are a newer attack vector for adversaries since they are difficult to block and detect in an environment. Adversaries create a custom Azure application to use in a phishing attack, then use the Azure APIs to integrate with a victim's Microsoft 365 environment, obtain persistance, remotely execute code, or perform discovery on the organization. These applications do not require permission from Microsoft, come with valid Microsoft certificates, and they do not require code execution on endpoint devices, making detection via antivirus (AV) solutions or endpoint detection and response (EDR) difficult.

While a user is informed that an application is not published by Microsoft or their organization when they are prompted for authorization and permissions, this may be overlooked. Upon gaining access, attackers can access files, read and send emails, modify the calendar, and see all other users in the organization via user directories.

### Preparation

* Audit Enterprise Applications in the Azure portal to ensure all applications are known or trusted.
* Identify the impact removing the applications or service account principles will have on business operations.
* Identify if privileged or administrator credentials are compromised due to the malicious application and coordinate credential resets or other eviction techniques to eliminate all adversary access to/through the application.
* Determine the ID of the application(s) to be removed.
* Locate accounts using service principals and identify which ones are legitimate. Both Azure commandline interface (CLI) and PowerShell have commands to discover service principaled accounts.

### Risks

* Deleting legitimate applications can be disruptive to business operations; audit if applications are in use before deleting and alert users.
* Removing service principals can cause users to no longer have access to applications.
* Microsoft discourages organizations from completely disabling third-party applications. Instead, Microsoft recommends auditing 3rd party applications used by the organization and removing any that are not critical to business operations or have misconfigured permissions.

### Guidance

Authentication of the application is handled by Microsoft and users log in with valid credentials to their Office 365 instance, so multi-factor authentication (MFA) is not a useful mitigation for this tactic. Malicious applications should be deleted or disabled with revoked permissions, though deletion is recommended.

#### Deleting applications through Azure portal or Microsoft Graph API

* Via the Azure portal, delete applications in the `Enterprise Applications` section under the `Azure Active Directory` tab.
* Via the Graph API, soft delete the application (recoverable for 30 days) using `DELETE /applications{id}`.
  + If you do not permanently delete the application, set up monitoring or logging to be alerted if the application state changes, such as being reenabled or recovered.
* Permanenetly delete the application using `DELETE /directory/deletedItems/{id}`.

#### Remediate service principals

* Rotate any KeyVault secrets that the service principal had access to in the following order:
  + Directly exposed secrets via the `GetSecrets` calls.
  + Other exposed secrets in KeyVault.
  + Other exposed secrets across other subscriptions.
* Remove service principals for malicious applications using the `Remove-ServicePrincipal` cmdlet, specifying the ID of the service principal.

### References

* Compromised and malicious applications investigation | <https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-compromised-malicious-app>
* Use service principals & managed identities | <https://learn.microsoft.com/en-us/azure/devops/integrate/get-started/authentication/service-principal-managed-identity?view=azure-devops>
* Securing service principals in Microsoft Entra ID | <https://learn.microsoft.com/en-us/entra/architecture/service-accounts-principal>
* Remove-ServicePrincipal | <https://learn.microsoft.com/en-us/powershell/module/exchange/remove-serviceprincipal?view=exchange-ps>

## CM0035: Configure Uniform Resource Locator (URL) Filtering

### Details

* **ID:** CM0035
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Enable
* **Status:** Active

### Intended Outcome

Configuring Uniform Resource Locator (URL) filtering restricts adversary initial access and execution via malicious URLs.

### Introduction

Uniform Resource Locator (URL) filtering, also known as web filtering, is used to control access to web pages by permitting or denying access when a user clicks on a link. URL filtering blocks compromised webpages used by adversaries to facilitate phishing attacks and malicious code execution.

URL filtering operates similarly to Domain Name System (DNS) filtering, although the latter blocks blocks DNS query requests for a domain.

Note that adversaries are able to generate new URLs, so manually updating URL filtering will not be sufficient for full protection against adversaries phishing attempts and should be paired with other, more sophisticated, methods of web security.

### Preparation

* No Preparation content identified.

### Risks

* Blocking legitimate URLs may disrupt business operations.

### Guidance

A URL filter is useful to configure for instances where a webpage on a domain is known to be or has been compromised or to meet business objectives.

#### Evaluating URLs during an Incident

* Check URLs against IoCs.
* Check clickable links/downloads available on the webpage.
* Check HTTP headers and Payloads using an intercept proxy such as, OWASP ZAP, to the site.
* View network traffic to suspicious URK using a protocol analyzer such as WireShark

#### Applying a Filter

Applying a filter can be based on an allow-list, block-list, or both.
There are multiple commercial tools that may be used to block malicious URLs (Cisco Umbrella, ZScaler, Palo Alto, etc). Organizations should consult their vendor for specific steps to block a known malicious URL. Commercial tools will also come with pre-built categories or URLs for preventative or post measures. Another, preventative step for consideration is blocking common mistypings of popular or common URLs used by staff to prevent typosquatting attacks.

### References

* What is URL Filtering | <https://www.zscaler.com/zpedia/what-is-url-filtering>
* URL Filtering | <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/url-filtering.pdf>
* Threat Hunting URLs for URLs as an IoC | <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/url-filtering.pdf>
* How to prevent and protect from typosquatting | <https://www.redpoints.com/blog/prevent-typosquatting/>

## CM0062: Monitor or Block Server Message Block (SMB) Protocol

### Details

* **ID:** CM0062
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Examine, Disable
* **Status:** Active

### Intended Outcome

Monitoring and/or blocking the Server Message Block (SMB) protocol detects and/or blocks adversary lateral movement and command and control using SMB.

### Introduction

No Introduction content identified.

### Preparation

* Determine the extent to which SMB is used in the environment.
* Determine the extent to which SMB has been secured in the environment.
* Identify distinctions between legitimate and malicious SMB usage.
* Identify opportunities for data collection.

### Risks

* Blocking SMB can impact the operation or functionality of systems in a domain by obstructing access to shared files, data, and/or devices.
* To minimize the likelihood of operational disruption, continually assess the effectiveness and efficiency of monitoring, collection, and detection. Take steps to minimize the likelihood of false positives.

### Guidance

#### Monitor

##### Collection

* Host-based agents should, to the extent possible, be configured to monitor files, processes, named pipes, logon sessions, network shares, network traffic, and command-line execution. These measures could provide insight into SMB abuse.
* Collect host-based logs (EDR, event logs, Sysmon, etc.). If available, consider collecting logs for process creation, file creation, named pipe creation, named pipe connection, and network connections. Consider reviewing windows security events for process creation, remote network authentication, special logons, and network share logs. Investigate instances of process execution from admin shares and file write on admin shares.

##### Detection

* Consider implementing detection logic that monitors for the following 3 conditions within a 10-minute period:
  + Successful logon event
  + A process launches in the ADMIN$ path on a remote host
  + A file share being opened repeatedly

#### Block

* Restrict or block all SMB communication between workstations to limit the likelihood of abusing the protocol to move laterally.
* Restrict or block SMB communications from workstations to servers where the business need for the protocol does not exist.

### References

* Restricting SMB Based Lateral Movement in a Windows Environment | <https://blog.palantir.com/restricting-smb-based-lateral-movement-in-a-windows-environment-ed033b888721>
* Offensive Lateral Movement | <https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f>
* Detecting Malicious C2 Activity - SpawnAs & SMB Lateral Movement in CobaltStrike | <https://dansec.medium.com/detecting-malicious-c2-activity-spawnas-smb-lateral-movement-in-cobaltstrike-9d518e68b64>
* SMB/Windows Admin Shares | <https://redcanary.com/threat-detection-report/techniques/windows-admin-shares/>

## CM0040: Clear Workstation and Server Domain Name Server (DNS) Caches

### Details

* **ID:** CM0040
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Eliminate
* **Status:** Active

### Intended Outcome

Clearing workstation and server Domain Name Server (DNS) cache terminates collection and command-and-control (C2) via corrupted DNS lookups.

### Introduction

The domain name system (DNS) cache is used to expedite the resolution of DNS queries for recently visited domains. Adversaries can poison the DNS cache by inserting or replacing records in the cache resulting in victims communicating with adversary-controlled infrastructure. By clearing the DNS cache, all stored queries, including malicious or corrupted IP-Domain mappings, will be purged.

### Preparation

* Capture all relevant forensic information before flushing cache.
* Ensure appropriate privileges are possessed by the user account issuing commands to clear the DNS cache.

### Risks

* Clearing the DNS cache will remove important forensic artifacts and IOCs. Ensure forensic captures of the DNS cache are taken prior to flushing.

### Guidance

#### Clear DNS Cache

<b>Windows</b>

* To flush DNS on a local Windows device with Command Prompt, the command: `ipconfig /flushdns` can be used.
* To clear DNS on a Windows DNS server, the command-line tool Dnscmd can be used with `dnscmd <DNSServerName> /clearcache`
* System administrators can use the PowerShell cmdlets `Clear-DnsServerCache` and `Clear-DnsClientCache` respectively to clear resource records.

<b>Linux</b>

To flush DNS on a local Linux device with Terminal, the commands vary based on the DNS caching service installed.

* For `nscd`, use: `sudo /etc/init.d/nscd restart`
* For `dnsmasq`, use: `sudo /etc/init.d/dnsmasq restart`
* For `systemd-resolved`, use: `sudo systemd-resolve --flush-caches`. Confirm cache is cleared with the command `sudo systemd-resolve --statistics` and confirm "Current Cache Size 0".

<b>MacOS</b>

Clearing the DNS cache on Mac workstations depends on the version of MacOS employed. For MacOS 10.10.4 and above the command is `sudo killall -HUP mDNSResponder`.

Clearing DNS records can be automated using scripts or using tools such as SolarWinds Server & Application Monitor.

#### Restart DNS Service

System administrators should restart the DNS services ensure the cache is cleared. For example, with nscd or dnsmasq, the service can be restarted with `sudo systemctl restart nscd` or `sudo systemctl restart dnsmasq` respectively. If Windows PowerShell is being used for a Windows DNS server, system administrators can use `Restart-Service -Name DNS -Force`.

### References

* Flush DNS: What It Is & How to Easily Clear DNS Cache | <https://blog.hubspot.com/website/flush-dns>
* Simplified Guide on How to Clear DNS Server Cache on Windows | <https://www.dnsstuff.com/clear-flush-dns-server-cache-windows>
* Dnscmd | <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/dnscmd>
* Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise | <https://www.cisa.gov/news-events/analysis-reports/ar21-134a>

## CM0101: Block Applications in Writable Locations using AppLocker

### Details

* **ID:** CM0101
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Disable
* **Status:** Active

### Intended Outcome

Blocking applications in writable locations using AppLocker blocks execution by malware in compromised environments.

### Introduction

Adversaries deploy malware in furtherance of tactical objectives e.g. establish command-and-control or to achieve lateral movement, and persistence. In the event of a large-scale, malware-enabled compromise, AppLocker can be employed to halt the pace and extent of adversarial advance on the network.

AppLocker is an application control utility native to the Windows operating system (Windows 7 or more recent). AppLocker enables responders to permit or deny the execution of specific applications in writable locations by users. It can be configured to assess files based on the following attributes: digital signature, publisher, product, version, hash, and path.

This countermeasure is specific to blocking the execution of malware to enable containment. To do so, AppLocker requires the location or hash of the malware.

AppLocker can block the following filetypes:

| File Type | File Extension |
| --- | --- |
| :-------------- | --------------: |
| Executables | .exe, .dll, .ocx, .com |
| Windows Installers | .mst, .msi, .msp |
| Script Files | .bat, .ps1, .cmd, .js, .vbs |
| Packaged Application Installers | .appx |

### Preparation

* Enforce the principle of least privilege. Ensure users are not members of the local administrator group. AppLocker's default rule set allows local administrators to run executables, scripts, and installer files. If the adversary has elevated privileges, AppLocker's default ruleset should be considered nullified until privileges have been revoked.
* If AppLocker is not already enabled, the Application Identify service (AppIDSvc) must be started to enable AppLocker.
* Identify attributes of the malicious file e.g. path or file hash.

### Risks

* Application control can be a necessary component of the incident response process. It is not however, sufficient in and of itself, to stop the spread of malware, as it can be bypassed. AppLocker policies will not impede an adversary with elevated privileges.

### Guidance

AppLocker's deny list can be employed during incident response to contain the spread of malware.

#### Enable AppLocker and Apply Default Rules

* Use the GPMC to navigate to `Security Settings> Application Control Policies> AppLocker> Executable Rules` in the Group Policy object.
* Select `Executable Rules` and enable `Create Default Rules`.
* Define `Deny` rules based on file attributes and characteristics associated with files determined to be malicious.

##### Block by Location

AppLocker can be used to block execution by location. If blocking files by location is an option, assess locations that non-admins have permission to write to, and execute from. Take care not to block legitimate applications should they exist in these locations. Malware is commonly deployed to the following locations:

* `C:\Users\AppData\Local\Temp`
* `C:\Users\AppData\Local`
* `C:\Users\AppData`
* `C:\Users\AppData\Roaming`
* `C:\ProgramData`

##### Block by Filetype

AppLocker can be used to block filetypes from running in specific locations. Again, if this approach is an option, take care not to block the execution of legitimate applications. The following filetypes can be, but are not always, indicative of malware:

.ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .hlp, .ht, .hta, .inf, .ins, .isp, .jar, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .ocx, .pcd, .ps1, .reg, .scr, .sct, .shs, .svg, .url, .vb, .vbe, .vbs, .wbk, .wsc, .ws, .wsf, .wsh, .exe, .pif, .pub

#### Monitor

Audit

Monitoring is an essential component of effective application control. AppLocker allows rules to be configured to `Enforce` and/or `Audit`.
can be used during initial test and implementation to monitor effectiveness. It should also be configured to enable continual monitoring.

### References

* Administer AppLocker | <https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/applocker/administer-applocker>
* Understanding AppLocker Default Rules | <https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/understanding-applocker-default-rules>
* How to Prevent Ransomware: 5 Practical Techniques and Countermeasures | <https://redcanary.com/blog/threat-detection/how-to-prevent-ransomware/>

## CM0030: Remove Known Malware

### Details

* **ID:** CM0030
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Eliminate
* **Status:** Active

### Intended Outcome

Removing known malware terminates adversary collection, persistence, and
command and control using malware.

### Introduction

No Introduction content identified.

### Preparation

* Review malware eradication strategy to minimize chances of an adversary presence surviving or being reinstated after eradication steps have been implemented.
* Determine whether any specific vulnerabilities, if any, were used by or exploited to install the malware and investigate how to prevent future exploitation.

### Risks

* This countermeasure may have impacts that disrupt operations, including
  + Data loss: Data entered since the last clean backup may be lost.
  + Business disruption: Downtime during business hours may disrupt business.
* Errors can render this countermeasure ineffective.
* Confirm the integrity of any clean images/software prior to usage, to avoid the risk of re-infection.

### Guidance

The specifics on the eradication of malware, backdoors, and implants will vary with each instance. The following is a list of some recommended practices regarding malware eradication activities. Please note, this is not an exhaustive list.

* Search for Indicators of Compromise (IOCs) (IP addresses, domains, certificates).
* Search for Tactics, Techniques, and Procedures (TTPs) consistent with adversary activity.
* Exploit internal resources (threat intelligence feeds, logs, etc.) to inform understanding of the attack and pivot to discover additional IOCs and TTPs.
* Reimage affected systems by restoring to an original uncorrupted state.
* Rebuild or replace hardware in the event of hard to eradicate infections such as root kits.
* Replace compromised files with uncorrupted files.
* Install Patches to mitigate any existing vulnerabilities.
* Monitor the system to verify successful eradication.

### References

* Cybersecurity Incident & Vulnerability Response Playbooks | <https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>
* Computer Security Incident Handling Guide | <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

## CM0106: Eliminate Web Shells

### Details

* **ID:** CM0106
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Eliminate
* **Status:** Active

### Intended Outcome

Eliminating web shells removes malicious code from vulnerable web servers that enable initial access and persistence.

### Introduction

A web shell is malicious code that is written to a vulnerable web server.
Adversaries typically exploit server misconfigurations or software vulnerabilities to deploy web shells. Web shells provide adversaries with a foothold that enables them to execute commands, exfiltrate data, and upload additional files to expand access beyond the initial point of access.

### Preparation

* Verify that plans, procedures, and authorities are in place to enable rapid containment and eradication of adversary from the compromised server.
* Take steps to prepare for the operational interruptions incurred by taking a web server offline.

### Risks

* Eliminating web shells may require down-time and thus disrupt the availability of the compromised web server.
* Web shells are often used to achieve initial access and/or persistence. Additional tools, e.g. malware, are often deployed to enable the adversary to further compromise the environment. As such, additional countermeasures may be required to fully contain and eradicate the adversary from the compromised environment.

### Guidance

#### Detecting Web Shells

The following detection logic should be considered components of a broader defense-in-depth strategy, not stand-alone solutions.

* Compare files on web server with a known-good version. [Windiff](https://learn.microsoft.com/en-us/troubleshoot/windows-client/shell-experience/how-to-use-windiff-utility) is a tool developed by Microsoft for file and directory comparison. Another option to consider is [dirChecker](https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/dirChecker.ps1) by NSA Cyber.
* Detect anomalous user agents, referrer headers, and IP Addresses in web server logs. This detection logic is likely to result in a high rate of false positives and should be continually monitored and refined.
* Detect host-based artifacts for common web shells. Consider using a security scanning tool like [YARA](https://github.com/virustotal/yara/) and the [core web shell detection signatures](https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/core.webshell\_detection.yara)
* Detect network-based artifacts for common web shells.
* Detect unexpected network flows.

#### Eliminating Web Shells

* Isolate the compromised web server to reduce the likelihood of lateral movement.
* Preserve artifacts to enable further analysis.
  + Disk and memory artifacts.
  + Logs (operating system, web application, access, error, web application firewall, reverse proxy, content delivery network, DMZ firewall, and database logs).
* Delete the web shell.
* Change passwords for the web administrator, database user, hosting account, and remote access (FTP, SSH, etc.)
* Investigate the underlying vulnerability/cause of the breach.
* Restore from clean backup.
* Having identified the underlying vulnerability / misconfiguration that led to the breach remediate by patching and hardening the web application and/or web server.

### References

* Mitigating Web Shells | <https://github.com/nsacyber/Mitigating-Web-Shells>
* Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways | <https://www.cisa.gov/sites/default/files/2024-02/AA24-060B-Threat-Actors-Exploit-Multiple-Vulnerabilities-in-Ivanti-Connect-Secure-and-Policy-Secure-Gateways_0.pdf>
* Web Shells: Types, Mitigation & Removal | <https://blog.sucuri.net/2024/04/web-shells.html>
* Ghost in the Shell: Investigating Web Shell Attacks | <https://www.microsoft.com/en-us/security/blog/2020/02/04/ghost-in-the-shell-investigating-web-shell-attacks/>
* How to use Windiff.exe | <https://learn.microsoft.com/en-us/troubleshoot/windows-client/shell-experience/how-to-use-windiff-utility>
* dirChecker.ps1 | <https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/dirChecker.ps1>
* YARA | <https://github.com/virustotal/yara/>
* YARA rules for detecting common web shells | <https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/core.webshell_detection.yara>

## CM0103: Deny Logon as a Batch Job

### Details

* **ID:** CM0103
* **Version:** 1.0
* **Created:** 14 March 2025
* **Modified:** 14 March 2025
* **Type:** Disable
* **Status:** Active

### Intended Outcome

Denying log on as a batch job for a particular account disrupts the ability for an adversary to automate tasks or execute malicious scripts at specified times.

### Introduction

No Introduction content identified.

### Preparation

* Before assigning an account the "Deny log on as a batch job" user right, assess the impact of the countermeasure on the job activities of the affected accounts. If containing the adversary, consider first inhibiting their access to the compromised account by rotating the credentials of the compromised account.
* If "log on as a batch job" is required by a service account, create a Group Managed Service Account (gMSA) and delegate only the necessary privileges for the service running the task(s).

### Risks

* Removing the ability for a user or group to log on as a batch job may disrupt legitimate processes or services that rely on privilege. By default, logon as a batch job is enabled for administrators and backup operators on domain controllers and stand-alone servers so denying this ability may introduce downtime to domain controllers and administrative servers.

### Guidance

Ensure that the Guest user group is denied the ability to log on as a batch job. Extend "deny log on as a batch job" to Local Accounts, Domain Admins, Enterprise Admins, and all other user accounts as necessary.

Confirm Domain Admins and Enterprise Admins in an AD Domain are denied logons on lower trust systems and ensure auditing is configured to alert if modifications are made to properties or memberships of highly-privileged groups.

#### Remove the ability to log on as a batch job using Group Policy Management Console (GPMC)

After editing an existing Group Policy Object (GPO) or creating a new GPO, navigate to
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment
from the Group Policy Editor.

From here, the properties menu can be opened for "Deny log on as a batch job" and a user account or group added.

After updating "Deny log on as a batch job," open the properties window of "Log on as a batch job" and remove any unauthorized Users or Groups that possess the right to log on as a batch job. While "Deny log on as a batch job" overrides "Log on as a batch job," users should still be removed from the latter if a user has both.

After completing these steps, link the GPO to the appropriate domain, site, or organizational unit (OU) to apply the policy.

#### Remove the ability of a user to log on as a batch job using PowerShell

In addition to the above method, an administrator may use PowerShell to create a GPO and deny log on as a batch job.

### References

* Deny log on as a batch job | <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-batch-job>
* Log on as a batch job | <https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=LogonAsBatch>
* The "Deny log on as a batch job" user right will be configured to include "Guests". | <https://www.stigviewer.com/stig/windows_7/2012-07-02/finding/V-26483>
* Windows Server 2019 Deny log on as a batch job user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems. | <https://www.stigviewer.com/stig/windows_server_2019/2019-07-09/finding/V-93011>
* The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access. | <https://www.stigviewer.com/stig/windows_server_2016/2018-09-05/finding/V-73761>
* Appendix E: Securing Enterprise Admins Groups in Active Directory | <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-e--securing-enterprise-admins-groups-in-active-directory>