Eviction Strategies Tool Playbook

Title: Ransomware via Admin Credential Phish + No MFA + VPN Reuse
Template: no template used
Created: 2025-07-30T00:00:00Z
Updated: 2025-07-30T00:00:00Z
Version: 2

Techniques & Mappings

Technique	Confidence	Mapped Countermeasures
T1566.002: Phishing: Spearphishing Link	confirmed	CM0002
T1078: Valid Accounts	confirmed	CM0063, CM0065
T1021.001: Remote Services: Remote Desktop Protocol	confirmed	CM0065
T1486: Data Encrypted for Impact	confirmed	CM0065
T1556.006: Modify Authentication Process: Multi-Factor Authentication	confirmed	
T1110.003: Brute Force: Password Spraying	suspected	CM0028
T1566: Phishing	suspected	CM0004, CM0009, CM0035, CM0059
(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

CM0063: Investigate Suspicious Login Attempts

Details

- **ID:** CM0063
- **Version:** 1.0
- **Created:** 14 March 2025
- **Modified:** 14 March 2025
- **Type:** Examine
- **Status:** Active

Intended Outcome

Investigating suspicious login attempts detects adversary credential access and lateral movement.

Introduction

Cyber responders should follow best practices regarding monitoring systems for potential breaches. Two areas for consideration are external logins and internal logins. Adversaries may continue to use credential access techniques and/or abuse valid accounts after eradication and recovery efforts.

External Login Attempts

External attacks for credential access will be for initial access to the environment. Investigate web application authentication logs, associated IP addresses, and frequency of http requests. An additional area of investigation is remote logins. Network activity should be monitored for signs of brute force, failed login attempts, and origin source.

Internal Login Attempts

Internal login attempts may occur when an account in the environment has been compromised and the adversary is looking to move laterally or escalate privileges. Internal logins are suspicious if a logged in user or device is attempting to access accounts or devices not within the scope of their duties or usual activities.

Preparation

No Preparation content identified.

Risks

No Risks content identified.

Guidance

To investigate suspicious login attempts, consider these 4 "W"s:

- Who: The user(s) attempting to gain access,
- When: At what times were access attempts occurring and frequency of attempts,
- Where: The associated IP/MAC address the requests are coming from, and
- What: The platform to be accessed (host, network service, web application, etc).

After applying these 4 "W"s, it may be necessary to lock the account and send a notification to the affected user(s) to reset their secrets.

Incident Counter Strategies

To counter suspicious login attempts, it may be necessary to move an account to a protected users security group or an equivalent. Doing so will help protect against credential theft for both devices and users. Another strategy will be to tune EDR, SIEMs, threat hunting tools, etc., to an ongoing threat actors potential targets. This will be

useful in restricting an adversary's actions, determining their goals, and removing them from all affected systems.

Windows Event Logs

Responders should review event logs in case of an incident to check for suspicious activity. These logs can be found in C:\Windows\System32\winevt\Logs\ or in event viewer's Window's Security logs and filtering for event IDs

- Event ID: 4624 Captures successful logon events and will be an important log to monitor. This log also captures "Logontypes" with types 3, 9, and 10 being most important for suspicious activity. - Logon type 3 refers to users logging in through network shares such as SMB. Adversaries will often use pass-the-hash or a discovered password to get an interactive shell or discover more information using a user's credentials. - Logontype 9 can be suspicous if a regular user uses the "runas" command to perform actions as another user on the network. - Logontype 10 captures remote log-in such as WinRM and RDP which is often used by adversaries that have stolen credentials.
- Event ID: 4625 Captures failed logon events and will an another important event to monitor. It will be important to pay attention to the status codes which are in hexadecimal format. - 0xC000006F describes a user that attempts to log-in outside of work hours. If the machine is configured to reject logon attempts outside of duty hours, this could be an indicator of attack (IoA). - 0xc000015b describes a user that attempts to log-in to a machine not associated with their account. This could be a sign of pivoting attempts by an adversary and should be monitored.
- Event ID: 4648 Captures logons using explicit credentials such as with the "runas" command.

Enable Auditing

To enable auditing of logon events on a host follow these steps: Open gpmc.msc -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy -> Audit Account Logon Events -> Checkmark Success and Failure. The steps are the same for Active directory except for these additional steps: Open gpmc.msc on domain controller -> Select Domain -> right-click domain and click "Create a GPO in this domain, and Link it here" -> Enter a GPO name -> Right click on new GPO and select edit. Then follow the rest of the steps from enabling on a host.

Post-Incident Activities

After an incident occurs, compromised accounts should be monitored to verify no backdoor access mechanisms remains. This would include verifying vulnerabilities that were patched have not created another vulnerability that allows access to the same or different accounts.

References

- How to investigate user logins | https://www.cybertriage.com/blog/training/how-to-investigate-user-logins-intro-to-incident-response-triage-2021/
- Audit logon events | https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-logon-events
- Windows Security Log Event ID 4624 | https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624
- Windows Security Log Event ID 4625 | https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4625
- 4624 (S): An account was successfully logged on | https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624
- How to See Who Logged Into a Computer | https://www.howtogeek.com/124313/how-to-see-who-logged-into-a-computer-and-when/
- Check User Login History in Windows Active Directory | https://www.lepide.com/how-to/audit-who-logged-into-a-computer-and-when.html

- Audit logon Events | https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-logon-events
- How to Detect Pass-The-Hash Attacks | https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/

CM0065: Isolate Endpoints from Network

Details

- **ID:** CM0065
- **Version:** 1.0
- **Created:** 14 March 2025
- **Modified:** 14 March 2025
- **Type:** Disable
- **Status:** Active

Intended Outcome

Isolating an endpoint from the network blocks adversary initial access, lateral movement, and command and control to and from the host on a network.

Introduction

An endpoint is any physical or virtual device or node on a network which is the ultimate destination of communications encompassing laptops, desktops, workstations, smartphones, servers, IoT devices, virtual machines, and other computing devices linked within an enterprise environment.

Adversaries that compromise an endpoint can perform a range of techniques to accomplish their objectives. By isolating a compromised endpoint, responders will be able to contain an incident by preventing the threat from issuing C2 commands and/or moving laterally across a network. Endpoint isolation can further disrupt or otherwise limit additional network-centric activities ranging from discovery, collection, and exfiltration - although automated actions that do not require realtime communication with the adversary may still occur.

Preparation

- Ensure plans, procedures, and authorities are in place to enable rapid containment of compromised endpoints.
- This countermeasure requires effective asset management and assumes use of endpoint management software or endpoint detection and response (EDR).
- Having backups or redundant devices available to replace the compromised endpoint will mitigate the likelihood of operational interruption.

Risks

- Isolating critical endpoints may disrupt important business operations. Responders should factor in potential operational impacts into their decision-making process.

Guidance

Software solutions (e.g. CrowdStrike, Defender for Endpoint, SentinalOne, etc.) may be used to quickly segregate endpoints from the rest of the network. Alternatly, teams may configure endpoint solutions to automatically isolate devices via workflows or playbooks under circumstances that warrant immediate containment.

In some cases, system administrators may want to consider either logically segregating virtual separation or physical disconnection from the network.

While the steps to perform endpoint isolation vary depending on the circumstances of the incident, the characteristics of the network, and the options available to the organization, the following general steps are as follow:

- Identify compromised endpoint(s)
- Understand the compromised endpoint(s) purpose to assess the potential for operational impact
    - Identify the type of endpoint (mobile device, workstation, server, etc.)
    - Determine the endpoint's function (desktop, web server, application server, etc.)

    - Identify to whom the endpoint is assigned and the individual's role (business function, administrator, c-suite/leadership, etc.)
- Isolate the endpoint(s) from the network
    - As part of isolation, responders may freeze system processes and prevent user interaction and perform a forensic capture of the device.
- Investigate and eradicate the threat
- Prioritize recovery according to endpoint criticality
- Redeploy in a phased approach
- Monitor restored endpoints for persistent malicious activity

References

- IR in focus: Isolating & containing a confirmed threat | https://redcanary.com/blog/incident-response/ir-containment-isolation/
- Endpoint Isolation | https://thewatchman.pro/endpoint-isolation/

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
Contact Info: Contact CISA at contact@mail.cisa.dhs.gov for questions about this tool. Visit the CISA Incident Reporting System (https://myservices.cisa.gov/irf) to securely report cyber incidents to CISA.

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/

Contact Info: Contact CISA at contact@mail.cisa.dhs.gov for questions about this tool. Visit the CISA Incident Reporting System (https://myservices.cisa.gov/irf) to securely report cyber incidents to CISA.

- LocalService Account | https://learn.microsoft.com/en-us/windows/win32/services/localservice-account

Contact Info: Contact CISA at contact@mail.cisa.dhs.gov for questions about this tool. Visit the CISA Incident Reporting System (https://myservices.cisa.gov/irf) to securely report cyber incidents to CISA.

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

Rule	Mapped to TTPs
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

Contact Info: Contact CISA at contact@mail.cisa.dhs.gov for questions about this tool. Visit the CISA Incident Reporting System (https://myservices.cisa.gov/irf) to securely report cyber incidents to CISA.

- 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

Contact Info: Contact CISA at contact@mail.cisa.dhs.gov for questions about this tool. Visit the CISA Incident Reporting System (https://myservices.cisa.gov/irf) to securely report cyber incidents to CISA.

- 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

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/

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/

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