Behavior Prevention on Endpoint, Mitigation M1040 - Enterprise

Archived: 2026-04-05 14:42:44 UTC

Enterprise T1059 Command and Scripting Interpreter

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic and JavaScript scripts from executing potentially malicious downloaded content [1].

.005 Visual Basic

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic scripts from executing potentially malicious downloaded content [1].

.007 JavaScript

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent JavaScript scripts from executing potentially malicious downloaded content [1].

Enterprise T1543 Create or Modify System Process

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[2] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed drivers.[3]

.003 Windows Service

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system.[2] On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed service drivers.[3]

Enterprise T1486 Data Encrypted for Impact

On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware.[1] In AWS environments, create an IAM policy to restrict or block the use of SSE-C on S3 buckets.[4]

Enterprise T1006 Direct Volume Access

Some endpoint security solutions can be configured to block some types of behaviors related to efforts by an adversary to create backups, such as command execution or preventing API calls to backup related services.

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent malware from abusing WMI to attain persistence.[1]

Enterprise T1564 .014 Hide Artifacts: Extended Attributes

During artifact review, packaging, or deployment stages, scan extended attributes alongside file contents to detect hidden payloads, obfuscated data, or suspicious attribute keys that may indicate malicious behavior.

Enterprise T1574 Hijack Execution Flow

Some endpoint security solutions can be configured to block some types of behaviors related to process injection/memory tampering based on common sequences of indicators (ex: execution of specific API functions).

.013 KernelCallbackTable

Some endpoint security solutions can be configured to block some types of behaviors related to process injection/memory tampering based on common sequences of indicators (ex: execution of specific API functions).

Enterprise T1559 Inter-Process Communication

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent DDE attacks and spawning of child processes from Office programs.[5][6]

.002 Dynamic Data Exchange

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent DDE attacks and spawning of child processes from Office programs.[5][6]

Enterprise T1036 Masquerading

Implement security controls on the endpoint, such as a Host Intrusion Prevention System (HIPS), to identify and prevent execution of potentially malicious files (such as those with mismatching file signatures).

.008 Masquerade File Type

Implement security controls on the endpoint, such as a Host Intrusion Prevention System (HIPS), to identify and prevent execution of files with mismatching file signatures.

Enterprise T1106 Native API

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office VBA macros from calling Win32 APIs. [1]

Enterprise T1027 Obfuscated Files or Information

On Windows 10+, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated payloads. [1]

.009 Embedded Payloads

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated scripts.[1]

.010 Command Obfuscation

On Windows 10+, enable Attack Surface Reduction (ASR) rules to block execution of potentially obfuscated scripts.[7]

.012 LNK Icon Smuggling

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated scripts or payloads.

.013 Encrypted/Encoded File

On Windows 10+, enable Attack Surface Reduction (ASR) rules to block execution of potentially obfuscated scripts.[8]

Security tools should be configured to analyze the encoding properties of files and detect anomalies that deviate from standard encoding practices.

.014 Polymorphic Code

On Windows 10+, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated payloads

Enterprise T1137 Office Application Startup

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

.001 Office Template Macros

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

.002 Office Test

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

.003 Outlook Forms

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

.004 Outlook Home Page

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

.005 Outlook Rules

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

.006 Add-ins

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [1]

Enterprise T1003 OS Credential Dumping

On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. [1]

.001 LSASS Memory

On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. [1]

Enterprise T1055 Process Injection

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process. For example, on Windows 10, Attack Surface Reduction (ASR) rules may prevent Office applications from code injection. [1]

.001 Dynamic-link Library Injection

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.002 Portable Executable Injection

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.003 Thread Execution Hijacking

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.004 Asynchronous Procedure Call

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.005 Thread Local Storage

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.008 Ptrace System Calls

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.009 Proc Memory

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.011 Extra Window Memory Injection

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.012 Process Hollowing

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.013 Process Doppelgänging

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.014 VDSO Hijacking

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

.015 ListPlanting

Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process.

Enterprise T1091 Replication Through Removable Media

On Windows 10, enable Attack Surface Reduction (ASR) rules to block unsigned/untrusted executable files (such as .exe, .dll, or .scr) from running from USB removable drives. [1]

Enterprise T1216 .001 System Script Proxy Execution: PubPrn

On Windows 10, update Windows Defender Application Control policies to include rules that block the older, vulnerable versions of PubPrn.[9]

Enterprise T1569 System Services

On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running. [1]

.002 Service Execution

On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running. [1]

Enterprise T1204 User Execution

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent executable files from running unless they meet a prevalence, age, or trusted list criteria and to prevent Office applications from creating potentially malicious executable content by blocking malicious code from being written to disk. Note: cloud-delivered protection must be enabled to use certain rules. [1]

.002 Malicious File

On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria). Note: cloud-delivered protection must be enabled for certain rules. [1]

Enterprise T1047 Windows Management Instrumentation

On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by WMI commands from running. Note: many legitimate tools and applications utilize WMI for command execution. [1]
