	CHIED	Description	manningtyne	target ID	target type	target name	target ref	Ba fs	Advanced hunting action type	Dependencies
Block credential stealing from the Windows local security authority	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	This rule helps prevent credential stealing by locking down Local Security Authority Subsystem Service (LSASS). LSASS authenticates users who sign in on a Windows computer. Microsoft Defender Credential Guard in Windows normally prevents	mitigates	T1003.001	sub-technique	LSASS Memory	attack-pattern65f2d882-3f41-4d48-8a06- 29af77ec9f90	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules-	AsrLsassCredentialTheftAudited	Microsoft Defender Antivirus
subsystem (Isass.exe)		LSASS authenticates users who sign in on a Windows computer. Microsoft Defender Credential Guard in Windows normally prevents attempts to extract credentials from LSASS. Some organizations can't enable Credential Guard on all of their computers because of					29af77ec9f90	endpoint/attack-surface-reduction-rules- reference#block-credential-stealing-from-the-	AsrLsassCredentialTheftBlocked	
		attempts to extract credentials from LSASS. Some organizations can't enable Credential Guard on all of their computers because of compatibility issues with custom smartcard drivers or other programs that load into the Local Security Authority (LSA). In these cases, attackers can use tools like Ministra to scrace cleared casswords and MTM hashes from LSASS.	1					windows-local-security-authority-subsystem		
		By default the state of this rule is set to block. In most cases, many processes make calls to LSASS for access rights that are not needed.	1							
		For example, such as when the initial block from the ASR rule results in a subsequent call for a lesser privilege which subsequently succeeds. For information about the types of rights that are typically requested in process calls to LSASS, see: Process Security and	1							
		Access Rights.								
		Enabling this rule doesn't provide additional protection if you have LSA protection enabled since the ASR rule and LSA protection work similarly. However, when LSA protection cannot be enabled, this rule can be configured to provide equivalent protection against malware								
		that target Isass.exe.								
Block execution of potentially obfuscated scripts	5beb7ete-fd9a-4556-801d-275e5ffc04cc	This rule detects suspicious properties within an obfuscated script.	mitigates	T1027.010	sub-technique	Command Obfuscation	attack-patternd511a686-4a33-41d5-bc95- c343875d1377	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules-	AsrObfuscatedScriptAudited	Microsoft Defender Antivirus, AntiMaly
		PowerShell scripts are now supported for the "Block execution of potentially obfuscated scripts" rule.					C3436/3013//	reference#block-execution-of-potentially-	AS ODIESCATEDOCREU	acan interface (Arrai)
		Script obfuscation is a common technique that both malware authors and legitimate applications use to hide intellectual property or decrease script loading times. Malware authors also use obfuscation to make malicious code harder to read, which hampers close	1					obfuscated-scripts		
		scrutiny by humans and security software.								
Block execution of potentially obfuscated scripts	5beb7efe-fd9a-4556-801d-275e5ffc04cc	This rule detects suspicious properties within an obfuscated script. Important:	mitigates	T1027.013	sub-technique	Encrypted/Encoded File	attack-pattern0d91b3c0-5e50-47c3-949a- 2a796f04d144	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules-	AsrObfuscatedScriptAudited AsrObfuscatedScriptBlocked	Microsoft Defender Antivirus, AntiMalv Scan Interface (AMSI)
		PowerShell scripts are now supported for the "Block execution of potentially obfuscated scripts" rule. Script obluscation is a common technique that both malware authors and legitimate applications use to hide intellectual property or						reference#block-execution-of-potentially- obfuscated-scripts		(* 127)
		decrease script loading times. Malware authors also use obfuscation to make malicious code harder to read, which hampers close						opruscateo-scripts		
	r0033r00.d16d.4114.a5a0.dr9b3a7d2reh	scrutiny by humans and security software. This rule blocks the use of executable files that are identified as copies of Windows system tools. These files are either duplicates or	<u> </u>	T1036 002			attack-patternbd5b58a4-a52d-4a29-bc0d-	https://learn.microsoft.com/en.us/defender-		Microsoft Dafander Antivirus
Block use of copied or impersonated system tools (preview)	cuusacuu-a16a-4114-a5au-ac9asa/azcea	Inis rule blocks the use or executable files that are identified as copies of windows system tools. These files are either dupicates or Impostors of the original system tools.	mtigates	110.96.003	sub-technique	Rename System Utilities	attack-patternbbbbb8a4-ab20-4a29-bc06- 3f1d3968eb6b	mtps://learn.microsom.com/en-us/desender- endpoint/attack-surface-reduction-rules- reference#block-use-of-copied-or-impersonate/		MICROSOT Detender Antivirus
		impostors of the original system tools. Some mall closus programs may try to copy or impersonate Windows system tools to avoid detection or gain privileges. Allowing such executable files can lead to potential attacks. This rule prevents propagation and execution of such duplicates and impostors of the						reference#block-use-of-copied-or-impersonates system-tools-preview	·	
		system tools on Windows machines.						,		
		Note: This capability is currently in preview. Additional upgrades to improve efficacy are under development.	1							
Block use of copied or impersonated system tools (preview)	c0033c00-d16d-4114-a5a0-dc9b3a7d2ceb	This rule blocks the use of executable files that are identified as copies of Windows system tools. These files are either duplicates or	mitigates	T1036.005	sub-technique	Rename System Utilities	attack-pattern1c4e5d32-1fe9-4116-9d9d-	https://learn.microsoft.com/en-us/defender-		Microsoft Defender Antivirus
		impostors of the original system tools. Some malicious programs may try to copy or impersonate Windows system tools to avoid detection or gain privileges. Allowing such					59e3925bd6a2	endpoint/attack-surface-reduction-rules- reference#block-use-of-copied-or-impersonate		
		executable files can lead to potential attacks. This rule prevents propagation and execution of such duplicates and impostors of the system tools on Windows machines.						system-tools-preview		
		Note:	1							1
		This capability is currently in preview. Additional upgrades to improve efficacy are under development.						https://learn.microsoft.com/en.us/defender.	Ast Psever Wmi Child Process Audited	
lock process creations originating from PSExec and WM1 commands	g1e49aac-8f56-4280-b9ba-993a6d77406c	This rule blocks processes created through PsExec and WMI from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command and control purposes, or to spread an infection throughout an	mitigates	11047	technique	Windows Management Instrumentation	attack-pattern01a5a209-b94c-450b-b7f9- 946497d91055	endpoint/attack-surface-reduction-rules-	AsrPsexecWmiChildProcessAudited AsrPsexecWmiChildProcessBlocked	Microsoft Defender Antivirus
		organization's network.						reference#block-process-creations-originating-		1
		Warning: Only use this rule if you're managing your devices with Intune or another MDM solution. This rule is incompatible with management	1		1			from-psexec-and-wmi-commands		1
		through Microsoft Endpoint Configuration Manager because this rule blocks WMI commands the Configuration Manager client uses to function correctly.								1
lock Office applications from injecting code into other processes	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	This rule blocks code injection attempts from Office apps into other processes.	mitigates	T1055	technique	Process Injection	attack-pattern43e7dc91-05b2-474c-b9ac-	https://learn.microsoft.com/en-us/defender-	AsrOfficeProcessInjectionAudited	Microsoft Defender Antivirus
		Note:	"				2ed4fe101f4d	endpoint/attack-surface-reduction-rules-	AsrOfficeProcessInjectionBlocked	1
		The Block applications from injecting code into other processes ASR rule does not support WARN mode. Important:						reference#block-office-applications-from- injecting-code-into-other-processes		1
		Infinitude requires restarting Microsoft 365 Apps (Office applications) for the configuration changes to take effect. Attackers might attempt to use Office apps to migrate malicious code into other processes through code injection, so the code can								1
		masquerade as a clean process.								
1		There are no known legitimate business purposes for using code injection. This rule applies to Word, Excel, OneNote, and PowerPoint.								
llock JavaScript or VBScript from launching downloaded executable	d3e037e1-3eb8-44c8-a917-57927947596d	This rule prevents scripts from launching potentially malicious downloaded content. Malware written in JavaScript or VBScript often acts	mitigates	T1059.005	sub-technique	Visual Basic	attack-patterndfd7cc1d-e1d8-4394-a198-	https://learn.microsoft.com/en-us/defender-	AsrScriptExecutableDownloadAudited	Microsoft Defender Antivirus, AMSI
ontent		as a downloader to fetch and launch other malware from the Internet. Although not common, line-of-business applications sometimes use scripts to download and launch installers.	1				97c4cab8aa67	endpoint/attack-surface-reduction-rules- reference#block-javascript-or-vbscript-from-	AsrScriptExecutableDownloadBlocked	
			1					launching-downloaded-executable-content		
llock JavaScript or VBScript from launching downloaded executable	d3e037e1-3eb8-44c8-a917-57927947596d	This rule prevents scripts from launching potentially malicious downloaded content. Malware written in JavaScript or VBScript often acts as a downloader to fetch and launch other malware from the internet.	mitigates	T1059.007	sub-technique	JavaScript	attack-pattern0f4a0c76-ab2d-4cb0-85d3- 3f0efb8cba0d	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules-	AsrScriptExecutableDownloadAudited AsrScriptExecutableDownloadBlocked	Microsoft Defender Antivirus, AMSI
Content		Although not common, line-of-business applications sometimes use scripts to download and launch installers.	1				STOCKED CO.	reference#block-javascript-or-vbscript-from- launching-downloaded-executable-content	Par Delipte Consideration of the Consideration of t	
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5	This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, vulnerable signed drivers can be exploited by	mitigator	Tince	technique	Exploitation for Brigilaria Erralation	attack-patternb21c3b2d-02e6-45b1-980b-	launching-downloaded-executable-content https://learn.microsoft.com/en-us/defender-	AsrVulnerableSignedDriverAudited	Microsoft Defender Antivirus
	30100312-0/3E-4103-3017-3002-0403CE3	into our prevents an approximation uniting a doubleader spired or rections is in-one-wind, volune above spired or rections to include applications of the spiral provides or spiral or cases to the kernel. Vulnerable signed drivers enable attackers to disable or circumvent security solutions, eventually leading to system compromise.	mugates	11000	technique	exportation of Privilege escatation	e69051040839	endpoint/attack-surface-reduction-rules-	AsrVulnerableSignedDriverBlocked	Priciosoli Deletidei Altivitus
		circumvent security solutions, eventually leading to system compromise. The Block abuse of exploited vulnerable signed drivers rule doesn't block a driver already existing on the system from being loaded.						reference#block-abuse-of-exploited-vulnerable- signed-drivers		
Block untrusted and unsigned processes that run from USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	With this rule, admins can prevent unsigned or untrusted executable files from running from USB removable drives, including SD cards.	mitigates	T1091		Replication Through Removable Media	attack-pattern3b744087-9945-4a6f-91e8- 9dbceda417a4	https://learn.microsoft.com/en-us/defender-	AsrUntrustedUsbProcessAudited	Microsoft Defender Antivirus
		Blocked file types include executable files (such as.exe, .dll, or .scr) Important:					9dbceda417a4	endpoint/attack-surface-reduction-rules- reference#block-untrusted-and-unsigned-	AsrUntrustedUsbProcessBlocked	
Block Win32 API calls from Office macros	92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b	Files copied from the USB to the disk drive will be blocked by this rule if and when it's about to be executed on the disk drive.	- William -	71.100	and a large	Nation 179	attack-pattern391d824f-0ef1-47a0-b0ee-	processes-that-run-from-usb	AsrOfficeMacroWin32ApiCallsAudited	Missessi Patendar Inthiana MIPI
SIDER WILISZ APT CARS HOLLOWING HINGCOS	926971a1+2601-4476-0006-900004000C70	This rule prevents VBA macros from calling Win32 APIs. Office VBA enables Win32 API calls. Malware can abuse this capability, such as calling Win32 APIs to launch malicious shellcode without	mugates	11100	technique	Native Art	c59a75e27670	endpoint/attack-surface-reduction-rules-	AsrOfficeMacroWin32ApiCallsBlocked	Priciosoli Deletidei Altivitos, Ariai
		writing anything directly to disk. Most organizations don't rely on the ability to call Win32 APIs in their day-to-day functioning, even if they use macros in other ways						reference#block-win32-api-calls-from-office- macros		
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access.	mitigates	T1137	technique	Office Application Startup	attack-pattern2c4d4e92-0ccf-4a97-b54c-	https://learn.microsoft.com/en-us/defender-	AsrOfficeChildProcessAudited	Microsoft Defender Antivirus
		Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate					86d962988a53	endpoint/attack-surface-reduction-rules- reference#block-all-office-applications-from-	AsrOfficeChildProcessBlocked	
		exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.						creating-child-processes		
llock Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access.	mitidates	T1137 001	sub-technique	Office Template Macros	attack-pattern79a47ad0-fc3b-4821-9f01-	https://learn.microsoft.com/en.us/defender-		Missessen Defender februar
, , , , , , , , , , , , , , , , , , , ,		Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate	1				a026b1ddba21			
		exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	İ					endpoint/attack-surface-reduction-rules-	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	PICTOSOIL Deletides Altanios
			I.					reference#block-all-office-applications-from- creating-child-processes		Prictoson Deterior Antiviros
llock Office application from creating child processes								reference#block-all-office-applications-from- creating-child-processes	AsrOfficeChildProcessBlocked	PILLIOSON DESERVATOS
	d4f940ab-401b-4efc-aadc-ad5f3c50688a		mitigates	T1137.002	sub-technique	OfficeTest	attack-patterned7efd4d-ce28-4a19-a8e6- c58011eb2c7a	reference#block-all-office-applications-from- creating-child-processes https://learn.microsoft.com/en-us/defender- endopint/attack-surface-reduction-rules-		Microsoft Defender Antivirus
	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access. Creating multicusus child processes is a common multaure strategy. Nature that abuses Office as a vector office num VBA macros and exploit Code to download and attempt or num more payloads. However, some legitizate tilen-of-business applications might also generate	mitigates	T1137.002	sub-technique	Office Test	attack-pattern-ed7efd4d-ce28-4a19-a8e6- c58011eb2c7a	reference#block-all-office-applications-from- creating-child-processes https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-all-office-applications-from-	AsrOfficeChildProcessBlocked	Microsoft Defender Anthrirus
		This rule blocks Office apport from creating child processes. Office apportincipal Wlord, Excel, PowerPaint, OneNote, and Access. Creating malicious child processes is a common mulmous entrating. Malanee that abuses Office as a vector office mun vilkal macros and expositor code to download and artiferng to non mey polavids. However, own negligitate liter of downloads supplication may all do sognerate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.	mitigates		sub-technique			reference#block-all-office-applications-from- creating-child-processes https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-all-office-applications-from- creating-child-processes	Aur Office ChildProcessBlocked Aur Office ChildProcessAudited Aur Office ChildProcessBlocked	
lock Office application from creating child processes	04/940ab-401b-4efc-aadc-ad5f3c50688a 04/940ab-401b-4efc-aadc-ad5f3c50688a	This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNode, and Access. Creating mail-induced rules processes is a common rules settinge, Anhance that all notes Office as a vestor others not visit flamances and expect code is demanded and army four runes regulars. Memore, a rune all notes of the size as a vestor others not visit flamances and expect code is demanded and army four runes regulars. Memore, a rune all notes in the office abusines applicate on rules and processes to the other purposes. Excels a special regular point or unity Power Settle In configure specially applicate to the common processes. The common processes are all the processes of the common processes and the common processes of the common processes are all the common processes. The common processes are all the common processes are all the common processes and the common processes are all the common processes and the common processes are all the common processes and the common processes are all the common processes are a	mitigates mitigates	T1137.002	sub-technique sub-technique	Office Test Outlook Forms	attack-patterna9e2cea0-c805-4bt8-9e31-	reference Effack - all-office- applications in om- creating-child-processes https://lea.m.microsoft.com/en-us/defender- endpoint/attack.surface-reduction-rules- reference Effack-all-office- applications- from- creating-child-processes https://lea.m.microsoft.com/en-us/defender-	Arr Office ChildProcessBlocked Arr Office ChildProcessAudited Arr Office ChildProcessBlocked Arr Office ChildProcessBlocked Arr Office ChildProcessBlocked	Microsoft Defender Antivirus Microsoft Defender Antivirus
lock Office application from creating child processes		This state blocks Office apps from creating child processes. Office apps include Word, Jack Freen Part III. Ownshoot, and Access and explain client of the control of the c	mitigates mitigates		tsub-technique sub-technique			reference EMDAC Aut - office - applications - from- creating - full-d processes https://learn.microsoft.com/en-us/defender- endpoint/attack.osurface-teduction-rufes- reference EMDAC - all-office-applications-from- creating-rufe-processes https://learn.microsoft.com/en-us/defender- endpoint/attack.osurface-reduction-rufes- serference EMDAC - all-office-applications-from- reference EMDAC - all-office-applications-from-	Aur Office ChildProcessBlocked Aur Office ChildProcessAudited Aur Office ChildProcessBlocked	
llock. Office application from creating child processes		This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNode, and Access. Creating mail-induced rules processes is a common rules settinge, Anhance that all notes Office as a vestor others not visit flamances and expect code is demanded and army four runes regulars. Memore, a rune all notes of the size as a vestor others not visit flamances and expect code is demanded and army four runes regulars. Memore, a rune all notes in the office abusines applicate on rules and processes to the other purposes. Excels a special regular point or unity Power Settle In configure specially applicate to the common processes. The common processes are all the processes of the common processes and the common processes of the common processes are all the common processes. The common processes are all the common processes are all the common processes and the common processes are all the common processes and the common processes are all the common processes and the common processes are all the common processes are a	mitigates mitigates		sub-technique sub-technique		attack-patterna9e2cea0-c805-4bt8-9e31-	reference EMDAC - All-office - applications- from- creating-child-processes https://learn.mrccrost.com/en-us/defender- endpoint/attack.susface-reduction-rules- reference EMDAC - All-office-applications-from- creating-child-processes https://learn.mrccrost.com/en-us/defender- endpoint/attack.susface-reduction-rules- redocinit/attack.susface-reduction-rules-	Arr Office ChildProcessBlocked Arr Office ChildProcessAudited Arr Office ChildProcessBlocked Arr Office ChildProcessBlocked Arr Office ChildProcessBlocked	
liock.Office application from creating child processes		This raid block is Office agos from creating child processes. Office agas include Word, Excel, PowerPain, OneMode, and Access. Creating mail conceives a common makenes strategy. Administrated abuses Office as a vector when new Villa macros and control of the conceive and control one of the control of the	mitigates mitigates mitigates		sub-technique sub-technique sub-technique		attack-pattern-a5e2cea0-c805-4b8-9e31- f5l0513a:3634 attack-pattern-bf147104-abf9-4221-95d1-	reference effaces all offices applications from creating child processes HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan.	Asr Office ChildProcessition ked	
	d48940ab-401b-4etc-aadc-ad553c50688a	Threat doubted office stays from creating cyclid process. Other any particular Wast. Excel. Presented Control, and Access	mitigates mitigates mitigates		sub-technique sub-technique sub-technique		attack-patterna9e2cea0-c805-4bt8-9e31-	inferior extilació al office applications from creating child program and consistent and program and consistent and consistent and applications and consistent and consistent and exploration and consistent and consistent and program	Arr Office ChildProcessBlocked Arr Office ChildProcessAudited Arr Office ChildProcessBlocked Arr Office ChildProcessBlocked Arr Office ChildProcessBlocked	
	d48940ab-401b-4etc-aadc-ad553c50688a	The state of the case in the case of the c	mitigates mitigates mitigates		sub-technique sub-technique sub-technique		attack-pattern-a5e2cea0-c805-4b8-9e31- f5l0513a:3634 attack-pattern-bf147104-abf9-4221-95d1-	reference effaces all offices applications from creating child processes HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan. HTSp.//Insan.microsof.com/on-autofetodor-insan.	Asr Office ChildProcessition ked	
	d48940ab-401b-4etc-aadc-ad553c50688a	The state of the case in the case of the c	mitigates mitigates mitigates		sub-technique sub-technique sub-technique sub-technique		attack-pattern - 26x2cca0 c805-458-5e31- 180691a-3634 attack-pattern - 26147104-ab9-4221-56d1- e81569696441	reference (ESCA) - 30 (Rec. applications from casting-citida processor au site from the particular and course au site from integration and course au site from integration and course and course produced training and considerations from course (Course au site from from the course au site from course (Course au site from course au s	Au Office Child Process Blocked Au Office Child Process Austral Au Office Child Process Blocked Au Office Child Process Austral Au Office Child Process Blocked	
tock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The state of the case in the case of the c	mitigates mitigates mitigates	71137.004	sub-technique sub-technique sub-technique sub-technique		attack-pattern-a5e2cea0-c805-4b8-9e31- f5l0513a:3634 attack-pattern-bf147104-abf9-4221-95d1-	reference tractice, also disc-applications from creating-riddly processing. Integral from a record acception - scheduler enoquentization is and control or scheduler enoquentization is and since-applications from creating-riddly processing and since-applications from creating-riddly processing and since-applications from creating-riddly processing and since-applications from creating-riddly processing and integral ratios and since-applications from creating-riddly processing and integral ratios. The since applications from creating-riddly processing and integral ratios and control or scheduler intermediated in since applications from creating-riddly processing and intermediated in since applications from creating-riddly processing and integral ratios and since-applications from creating-riddly processing and the creating-riddly processing and the creating-riddly processing and the creating-riddly processing and creating-riddly processing and the creating-riddly processing and creating-riddly processing and the creating-riddly processing the creating-riddly the creating-ri	Au Office Childrine ceditioned Aur Office Childrine cedulated Aur Office Childrine ceditioned Aur Office Childrine ceditioned Aur Office Childrine ceditioned Aur Office Childrine cedulated	
tock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The state of the case in the case of the c	mitigates mitigates mitigates mitigates	71137.004	sub-technique sub-technique sub-technique sub-technique		attack-pattern - 26x2cca0 c805-458-5e31- 180691a-3634 attack-pattern - 26147104-ab9-4221-56d1- e81569696441	reference (ESCA) - 30 (Rec. applications from casting-citida processor au site from the particular and course au site from integration and course au site from integration and course and course produced training and considerations from course (Course au site from from the course au site from course (Course au site from course au s	Au Office Child Process Blocked Au Office Child Process Austral Au Office Child Process Blocked Au Office Child Process Austral Au Office Child Process Blocked	
lock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The control of the co	entigates entigates entigates entigates	71137.003 71137.004 71137.009	sub-ecchnique sub-ecchnique sub-ecchnique sub-ecchnique		STEAS pattern - Jeff-Lash-Cellis - 468 - 463 - 1005 1-3:2534 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 - 1005 1-3:2554 -	reference (Stock - als office- applications from centrify citied process of continues of continues of the continues of continues of continues of produced states as extracted on the continues of reference (Stock - als office- applications from centrify citied process or enduction reference centrify citied process or enduction reference continues of continues of continues of states of continues of continues of states of continues of reference continues of states of continues of continues of states br>states of states of states of states of states states of states s	Au Office Childrine cealitacead Aur Office Childrine cashudised	
lock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The state of the country of the coun	entigates mitigates mitigates mitigates mitigates	71137.004	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique		attack-pattern - 26x2cca0 c805-458-5e31- 180691a-3634 attack-pattern - 26147104-ab9-4221-56d1- e81569696441	información chia difeca applicationa fron- cistring childip processo. Intigo risuam encreada courren existénte en englicitationa de misco en endection relacional en entre combiona de difeca applicationa évano- sativa (childip processo. Intigo risuam encreada, comine existénte en entre control de difeca applicationa évano- cistring childip encreada comine a social desirador- ente encreada de difeca applicationa évano- cisativa (childip encreada comine a social entre en	Au Office Child Process Blocked Au Office Child Process Austral Au Office Child Process Blocked Au Office Child Process Austral Au Office Child Process Blocked	
lock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The state of the s	entigates entigates entigates entigates entigates	71137.003 71137.004 71137.009	sub-technique sub-technique sub-technique sub-technique sub-technique		#1005 pattern -#607c cod -009 -608 6x31- 6005 1x 8254 4 #1006 pattern -#161 104-889-422 1 66d1 - #11006 pattern -#161 104-889-422 1 66d1 - #11006 pattern -#161 105 276-227 4 455 -646x #11006 pattern -#161 105 276 -227 4 455 -646x	inference into Loca Julia (Dec. applications from creating child processing child processin	Au Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine ceanularised	
lock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The control of the country from control of the country of the coun	entigates entigates entigates entigates entigates	71137.003 71137.004 71137.009	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique		#1005 pattern -#607c cod -009 -608 6x31- 6005 1x 8254 4 #1006 pattern -#161 104-889-422 1 66d1 - #11006 pattern -#161 104-889-422 1 66d1 - #11006 pattern -#161 105 276-227 4 455 -646x #11006 pattern -#161 105 276 -227 4 455 -646x	reference tradics à ai office-applications from creating-riding processing-riding processing-riding processing-riding processing-riding processing-riding-rice-rice-rice-rice-rice-rice-rice-rice	Au Office Childrine estillacted Aur Office Childrine estillacted	
lock Office application from creating child processes	34840ab-401b-4efc-aadc-add5flc50688a 34840ab-401b-4efc-aadc-add5flc50688a	The control of the country from control of the country of the coun	entigates entigates entigates entigates entigates entigates	71137.003 71137.004 71137.009	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique		#1005 pattern -#607c cod -009 -608 6x31- 6005 1x 8254 4 #1006 pattern -#161 104-889-422 1 66d1 - #11006 pattern -#161 104-889-422 1 66d1 - #11006 pattern -#161 105 276-227 4 455 -646x #11006 pattern -#161 105 276 -227 4 455 -646x	reference tradics à ai office-applications from creating-riding processing-riding processing-riding processing-riding processing-riding processing-riding-rice-rice-rice-rice-rice-rice-rice-rice	Au Office Childrine estillacted Aur Office Childrine estillacted	
tock Office application from creating child processes	546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 26106680-1602-4648-86127-e+1dba1-c+868	The control of the cases in the control of the control of the case of the control of the control of the case of the control of the control of the case	entigates entigates entigates entigates entigates entigates	11137.003 11137.004 11137.005	sub-cectorique sub-cectorique sub-cectorique sub-cectorique sub-cectorique sub-cectorique sub-cectorique		STACK pattern - Jack 1280 - 4805 - 48	información chai disca-applications from carating child processor au distinuir con carating child processor au distinuir con targa (Plasa) and caracter con caractería con proposition de la contra con carating child processor. Al contra substitución de la contra substitución de substitución de la contra substitución de la contra subst	Au Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine cealularised Aur Office Childrine ceanularised	
ock Office application from creating child processes	546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 26106680-1602-4648-86127-e+1dba1-c+868	The control of the co	entigates mitigates entigates entigates entigates	11137.003 11137.004 11137.005	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique		STACK pattern - Jack 1280 - 4805 - 48	información chia difeca applicationa front casting chiad porcesso de convenue subdenindo resignationa de convenue subdenindo en deputationa de convenue subdenindo en de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de convenue de de convenue de convenue de convenue de convenue de convenue de de convenue de convenue de convenue de convenue de convenue de de convenue de convenue de convenue de co	Au Office Childrine estillacted Aur Office Childrine estillacted	
ock Office application from creating child processes seck Office application from creating child processes	546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 546940a-4016-4et- aast-ast/01:00668a 26106680-1602-4648-86127-e+1dba1-c+868	The state of the company to the comp	entigates mitigates mitigates mitigates mitigates mitigates mitigates	11137.003 11137.004 11137.005	sub-eschrique sub-eschrique sub-eschrique sub-eschrique sub-eschrique sub-eschrique sub-eschrique		1826-9-281692862-1280-6855-488-6231- 6050-3-30534-688-6231- 6050-3-30534-688-6231-6050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3	información chais difeca applications from cesting child processor autorità del processor del proces	Au Office Childrine cealifacted Aur Office Childrine cealustied Aur Office Childrine cealusti	
lock Office application from creating child processes lock Office application from creating child processes lock Office application from creating child processes lock Office communication application from creating child processes lock Office application from creating child processes	546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a	The state of the company to the comp	entigates entigates entigates entigates entigates entigates	11137 2003 11137 2004 11137 2005 11137 2006	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique	Outlook Forms Outlook Home Page Outlook Home Page Outlook Rules Outlook Rules	STACK pattern - Jack 1480 - 6805 - 4818 - 6831 - 6805 - 6818 - 6831 - 6805 - 6818 - 6831 - 6805 - 6818 - 6831 - 6805 - 6818 - 6812 - 68	inference tradicio à si office applications from casting-citida processor. Integralizam, increased, coervie a sciedengar- sopportantata à sant e- endection national production and coervie a sciedengar- inference tradicio à si office applications from casting-citida processor. Integralizam, increased, coervier a sciedendar- resignaturative à son en endection en eta- dendiquentative à son en endection en eta- dendiquentative à son en endection et en en- creating-citida processor. Integralizam increased, comme en addictional entre creative, a del office applications from creating-citid processor. Integralizam an creased comme auditériales entre creative, a del office applications from creating-citida processor. Integralizam an creased comme auditériales endiquentativate à serie or endection nuides motivates en la comme auditériales endiquentativate à serie en endection nuides endiquentativate à serie en endection nui entre creativate en citique de entre creativate en citique en citique entre creativate en citique en citique entre creativate en citique en creativate en citique en creativate entre creativ	Au Office Childrine estillacied Aur Office Childrine estillacied	Microsoft Defender Antonius
lock Office application from creating child processes lock Office application from creating child processes lock Office application from creating child processes lock Office communication application from creating child processes lock Office application from creating child processes	546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a	The state of the control of the cont	entigates entigates entigates entigates entigates entigates	11137 2003 11137 2004 11137 2005 11137 2006	uub eechnique sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique	Outlook Forms Outlook Home Page Outlook Home Page Outlook Rules Outlook Rules	1826-9-281692862-1280-6855-488-6231- 6050-3-30534-688-6231- 6050-3-30534-688-6231-6050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3	información chais difeca applications from cesting child processor autorità del processor del proces	Au Office Childrine cealifacted Aur Office Childrine cealustied Aur Office Childrine cealusti	Microsoft Defender Antonius
ock Office application from creating child processes seck Office application from creating child processes	546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a 546940a-4016-4eht-aast-addict-50666a	The control of the case in the case of the	entigates entigates entigates entigates entigates entigates	11137 2003 11137 2004 11137 2005 11137 2006	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique	Outlook Forms Outlook Home Page Outlook Home Page Outlook Rules Outlook Rules	1826-9-281692862-1280-6855-488-6231- 6050-3-30534-688-6231- 6050-3-30534-688-6231-6050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3050-3-3	información chia difeca applicationa fron casting chial porcessor. Intiga l'imam increased courre existérinden dispositional and casting chial porcessor. Intiga l'imam increased courre existérinden dispositional chia de linica applicationa de una dispositional chia del l'image de l'i	Au Office Childrine cealifacted Aur Office Childrine cealustied Aur Office Childrine cealusti	Microsoft Defender Antivirus
ock CIRCs application from creating child processes suck Office application from creating child processes	3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053	The state of the control of the cont	entigates entigates entigates entigates entigates entigates entigates	11137 2003 11137 2004 11137 2005 11137 2006	sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique sub-technique	Outlook Forms Outlook Home Page Outlook Home Page Outlook Rules Outlook Rules	#1806 pattern#6021.080 - 6886 - 6931 - 6990 1-38954 - 6986 - 6931 - 6990 1-38954 - 6986 - 6931 - 6990 1-38954 - 6990 1-3895	inference tradics à si office applications from cessing child processor. Intga/Flamm, increased, covere va solderinder- solopient fatales a les re- enfect don nider- inference fatales à si office applications s'on- cessing child processor. Intga/Flamm, increased, covere va solderinder- solopient fatales a les re- enfect don nider- opposite fatales a les re- enfect don nider- enfect de la re- solopient fatales a les re- processors. Intga/Flamm, increased, covere va solderinder- valopient fatales a les re- solopient fatales a les re- solo	Au Office Chalderine cealifacted Aur Office Chalderine cealulated	Microsoft Defender Antivirus
lock Office application from creating child processes suck Office application from creating child processes lock Office application from creating child processes	3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053	The state of the control of the cont		11137-003 11137-004 11137-006 11137-006		Outlook Forms Outlook Home Page Outlook Home Page Outlook Rules Outlook Rules Add-ins	1810-9-pattern - Jefc2-1820-0826-4828-6831- 1810-9-18-18-18-18-18-18-18-18-18-18-18-18-18-	información chais de caspiciacions de orientaria participación con la contra que de contra que de contra co	Au Office Childrine ceallacted Aur Office Childrine cealualised A	Nicrosoft Defender Antivirus
lock Office application from creating child processes	3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053 3455436-4016-44th-324th-325715:0000053	The control of the co		11137-003 11137-004 11137-006 11137-006		Outlook Forms Outlook Home Page Outlook Home Page Outlook Rules Outlook Rules Add-ins	#1806 pattern#6021.080 - 6886 - 6931 - 6990 1-38954 - 6986 - 6931 - 6990 1-38954 - 6986 - 6931 - 6990 1-38954 - 6990 1-3895	inference tradics à si office applications from cessing child processor. Intga/Flamm, increased, covere va solderinder- solopient fatales a les re- enfect don nider- inference fatales à si office applications s'on- cessing child processor. Intga/Flamm, increased, covere va solderinder- solopient fatales a les re- enfect don nider- opposite fatales a les re- enfect don nider- enfect de la re- solopient fatales a les re- processors. Intga/Flamm, increased, covere va solderinder- valopient fatales a les re- solopient fatales a les re- solo	Au Office Chalderine cealifacted Aur Office Chalderine cealulated	Nicrosoft Defender Antivirus

Nicologo de de discono con la contra de a contra de la contra dela contra de la contra del la contra	01440014 -474 400- 000- 04-00400	This rule blocks executable files, such as .exe, .dll, or .scr, from launching. Thus, launching untrusted or unknown executable files can be	militari na	71204	technique	User Execution	attack-pattern-9c32eb4d-805f-4fc5-bf60-	https://learn.microsoft.com/en.us/defender-	Asri IntrustedEvecutableAudited	Microsoft Defender Antivirus Cloud
Block executable files from running unless they meet a prevalence, age, or trusted list criteria		raily, as it eight not be intituly factor that files are mallocour, important. Interpolation of the property	mugares				c4d476c131b5	imper/mean.microsom.com/en-usoperenor- empoint/attack-author-crediction-tu- reterence-attock-executable-files-from-running- unless-they-med-a-prevalence-age-or-trusted- list-criterion	Asr Unitrusted Executable Blocked	Protection
Block Adobe Reader from creating child processes	7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c	This rule prevents attacks by lincking Adobe Reader from creating processes. **Halware can downsion and subunch prodoce and review our Adobe Reader through social engineering or exploits. By blocking child processes from being generated by Adobe Reader, malware attempting to use Adobe Reader as an attackvector are prevented from oppreading. presading.	mitigates	T1204.002	sub-technique	Maticious Fite	attack-pattern232b7f21-adf9-4b42-b936- b9d6f7df856e	https://learn.microsoft.com/en-usidefender- endpoint/attack-surface-reduction-rules- referenceEblock-adobe-reader-from-creating- child-processes	Asr Adobe Reader Child Process Audited Asr Adobe Reader Child Process Blocked	Microsoft Defender Antivirus
Block Office application from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a	This rate blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPrint, Crefelog, and Access. Creating millions child processes is a common malenate rate rate, Phalenate that absent Cliffice as sweet on their near Vell minror and explored to developed and their report near in orange pulpaded. However, zone singliment like neith quantities application like any place and explored processes can be applied to configurate or the common place of the processes of the	mitigates	T1204.002	sub-technique	Malicious File	attack-pattern232b7f21-adf9-4b42-b936- b9d6f7df856e	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-all-office-applications-from- creating-child-processes	AsrOfficeChildProcessAudited AsrOfficeChildProcessBlocked	Microsoft Defender Antivirus
Block executable content from email client and webmail	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	This rate blocks email opened within the Microsoft Outlook application, or Outlook.com and other popular webmist providers from propagating the foliologifie types: Executable files (such as. exe., off. ex. ex.). Executable files (such as. exe.). Executable files (such as. exe.). Exe. off. exe. exe. exe. exe. exe. exe. exe. e	mitigates	T1204.002	sub-technique	Malicious File	attack-pattern232b7f21-adf9-4b42-b936- b9d6f7df856e	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-executable-content-from-email- client-and-webmail	AsrExecutableEmailContentAudited AsrExecutableEmailContentBlocked	Microsoft Defender Antivirus
Uhe advanced protection against ransomware	c1db55ab-c21a-4637-bb34-a12568109d35	Issue lay provides as entra layer of questions against assummans. It such softs client and close feveralists to determine whether a file excended a resonance. This made down this cold is that have one or more on of the following characteristics the determine whether a file excended is a sould regime file. The file is a sould regime file. The file is prevaled resolution of the control of a resonance. The risk detection of the control o	mitigates	11486	technique	Data Encrypted for Impact	attack-pattern-b80d107d-fa0d-4b60-9684- b0433e8bdaa0	https://lean.microsoft.com/en-us/defender- endpoint/attacks.urface-reduction-rules- reference Buse-advanced-protection-against- ransomware	Aer Ransomware Blocked Aur Ransomware Blocked	Microsoft Defender Anthirus, Cloud Probection
Block Webshell creation for Servers	a8f5898e-1dc8-49a9-9878-85004b8a61e6	The runk blocks web shall corgin creation on Microsoft Server, Exchange Role. Are betted licent is a specifically careful script that allows an attacker to control the compromised server. A web shell may include functionalities such as receiving and executing mallicious commande, downloading and executing mallicious files, stealing and entitiesting credentials and executing immunities. On the property of the p	mitigates	T1505.003	sub-technique	Web Shell	attack-pattern5d0d3609-d06d-49e1-b9c9- b544e0c618cb	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-webshell-creation-for-servers		Microsoft Defender Antivirus
Biock abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5	This rate prevents an application from writing a valenzable signed driver to disk. In the wild, valenzable signed drivers can be explored by the collapplications to that have sufficiently printingers. To glin access to the lenner, Municipable signed drivers can be attacked not disable or circi unwent security solutions, eventually isolating to system compromise. The Block above of explored valenzable signed drivers rate desort blocks a driver already existing on the system from being loaded.		71543	technique	Create or Modify System Process	attack-pattern106c0c16-bf73-4601-9aa8- 0945c2715ec5	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-abuse-of-exploited-vulnerable- signed-drivers	AsrVulnerableSignedDriverAudited AsrVulnerableSignedDriverBlocked	Microsoft Defender Antivirus
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5	This rule prevents an application from writing a vulnerable signed driver to disk. In-the-wild, vulnerable signed drivers can be exploited by the city applications to that have sufficient privileges. To glin access to the kernet Vulnerable signed drivers and is dashed or circiument security solutions, eventually isolading to system compromise. The disk of the control of the cont	mitigates	11543.003	sub-technique	Windows Service	attack-pattern2959d631-73td-46a1-abd2- 109d7dcede32	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-abuse-of-exploited-vulnerable- signed-drivers	AsrVulnerableSignedDriverAudited AsrVulnerableSignedDriverBlocked	Microsoft Defender Antivirus
Block persistence through WMI event subscription	e6db77e5-3dt2-4cf1-b95a-636979351e5b	This rule prevents real-are than absorption for statism prostations are as a device. Important International control of the property of the	mitigates	T1546.003	sub-technique	Windows Management Instrumentation Event Subscription	attack-pattern910906dd-8c0a-475a-9cc1- 5e029e2fad58	https://kean.microsoft.com/en-us/defender- endpoint/aft ack-surface-reduction-rules- reference@block-persistence-through-wmi-event- subscription	Asr Persistence ThroughWmiAsalt ted Asr Persistence ThroughWmiBlocked	Microsoft Defender Anthirus, RPC
Block rebooting machine in Safe Mode (preview)	33ddedf1 - 66e0-47cb-833e-de6133960387	This rule prevents the execution of commands to restart machines in Stalk Mode. So a diagnostic mode that confly loads the essential files and of viers needed for Windows to run. However, in Safe Mode, many accurally product as are either disabled or operate in a limited capacity, which allows attackers to further blanch tampering commands, or samply execute and encrypt all files on the machine. This rule blocks such attacks by preventing processes from restarting machines in Safe Mode.	mitigates	T1562.009	sub-technique	Safe Mode Boot	attack-pattern—28170e17-8384-415c-8486- 2e6b294cb803	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-rebooting-machine-in-safe- mode-preview		Microsoft Defender Antivirus
Block process creations originating from PSExec and WMI commands	d1e49aac-856-4280-b9ba-993a6d77406c	has all biolicy processes created from the many and the m	mitigates	11569.002	sub-technique	Service Execution	attack-pattern-r1951e8a-500e-4a26-8803- 76d95c-4554b4	https://learn.microsofi.com/en-us/defender- endpoint/attack.surface-reduction-rules- reference#block-process-creations-originating- trom-psexec-and-wmil-commands	Asr Psexec Wmi Child Process Audited Asr Psexec Wmi Child Process Blocked	Microsoft Defender Antivirus
Block process creations originating from PSExec and WMI commands	d1e49aac-856-4280-59ba-993a6d77406c	has a list locks processes created through Pickes, and 1999 from unuming flow Pickes, and 1999 from the making a lock process created by executions of the Pickes and 1999 from the pickes of the Pickes and 1999 from the pickes of the Pickes	mitigates	11570	technique	Lateral Tool Transfer	attack-pattern-b90072c-c00b-45e3-b3aa- 68560560d4c5	https://learn.microsoft.com/en-us/defender- endpoint/attack-surface-reduction-rules- reference#block-process-creations-originating- from-psexec-and-wmi-commands	Ast PseuecWmiChildProcessAudited Ast PseuecWmiChildProcessBlocked	Microsoft Defender Antivirus