Command and Scripting Interpreter: PowerShell

Other sub-techniques of Command and Scripting Interpreter (11)

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.[1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

A number of PowerShell-based offensive testing tools are available, including Empire, PowerSploit, PoshC2, and PSAttack.[2]

PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).[3][4][5]

ID: T1059.001

Sub-technique of: T1059

ⓘ

Tactic: Execution

ⓘ

Platforms: Windows

ⓘ

Supports Remote: Yes

Contributors: Mayuresh Dani, Qualys; Praetorian; Ross Brittain

Version: 1.4

Created: 09 March 2020

Last Modified: 15 October 2024

Version Permalink

Procedure Examples

ID	Name	Description
C0025	2016 Ukraine Electric Power Attack	During the 2016 Ukraine Electric Power Attack, Sandworm Team used PowerShell scripts to run a credential harvesting tool in memory to evade defenses.[6]
C0034	2022 Ukraine Electric Power Attack	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilized a PowerShell utility called TANKTRAP to spread and launch a wiper using Windows Group Policy.[7]
S0677	AADInternals	AADInternals is written and executed via PowerShell.[8]
S1129	Akira	Akira will execute PowerShell commands to delete system volume shadow copies.[9]
S0622	AppleSeed	AppleSeed has the ability to execute its payload via PowerShell.[10]
G0073	APT19	APT19 used PowerShell commands to execute payloads.[11]
G0007	APT28	APT28 downloads and executes PowerShell scripts and performs PowerShell commands.[12][13][14]
G0016	APT29	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke.[15][16][17][18]
G0022	APT3	APT3 has used PowerShell on victim systems to download and run payloads after exploitation.[19]
G0050	APT32	APT32 has used PowerShell-based tools, PowerShell one-liners, and shellcode loaders for execution.[20][21][22]
G0064	APT33	APT33 has utilized PowerShell to download files from the C2 server and run various scripts. [23][24]
G0082	APT38	APT38 has used PowerShell to execute commands and other operational tasks.[25]
G0087	APT39	APT39 has used PowerShell to execute malicious code.[26][27]
G0096	APT41	APT41 leveraged PowerShell to deploy malware families in victims' environments.[28][29]
G1023	APT5	APT5 has used PowerShell to accomplish tasks within targeted environments.[30]
G0143	Aquatic Panda	Aquatic Panda has downloaded additional scripts and executed Base64 encoded commands in PowerShell.[31]
S0129	AutoIt backdoor	AutoIt backdoor downloads a PowerShell script that decodes to a typical shellcode loader.[32]
S1081	BADHATCH	BADHATCH can utilize `powershell.exe` to execute commands on a compromised host.[33][34]
S0234	Bandook	Bandook has used PowerShell loaders as part of execution.[35]
S0534	Bazar	Bazar can execute a PowerShell script received from C2.[36][37]
S1070	Black Basta	Black Basta has used PowerShell scripts for discovery and to execute files over the network.[38][39][40]
S0521	BloodHound	BloodHound can use PowerShell to pull Active Directory information from the target environment.[41]
G0108	Blue Mockingbird	Blue Mockingbird has used PowerShell reverse TCP shells to issue interactive commands over a network connection.[42]

ID	Name	Description
S0360	BONDUPDATER	BONDUPDATER is written in PowerShell.[43][44]
G0060	BRONZE BUTLER	BRONZE BUTLER has used PowerShell for execution.[45]
S1039	Bumblebee	Bumblebee can use PowerShell for execution.[46]
C0018	C0018	During C0018, the threat actors used encoded PowerShell scripts for execution.[47][48]
C0021	C0021	During C0021, the threat actors used obfuscated PowerShell to extract an encoded payload from within an .LNK file.[49][50]
C0032	C0032	During the C0032 campaign, TEMP.Veles used PowerShell to perform timestomping.[51]
S0674	CharmPower	CharmPower can use PowerShell for payload execution and C2 communication.[52]
G0114	Chimera	Chimera has used PowerShell scripts to execute malicious payloads and the DSInternals PowerShell module to make use of Active Directory features.[53][54]
S1149	CHIMNEYSWEEP	CHIMNEYSWEEP can invoke the PowerShell command `[Reflection.Assembly]::LoadFile(\"%s\")\n$i=\"\"\n$r=[%s]::%s(\"%s\",[ref] $i)\necho $r,$i\n` to execute secondary payloads.[55]
G1021	Cinnamon Tempest	Cinnamon Tempest has used PowerShell to communicate with C2, download files, and execute reconnaissance commands.[56]
S0660	Clambling	The Clambling dropper can use PowerShell to download the malware.[57]
G0080	Cobalt Group	Cobalt Group has used powershell.exe to download and execute scripts.[58][59][60][61][62][63]
S0154	Cobalt Strike	Cobalt Strike can execute a payload on a remote host with PowerShell. This technique does not write any data to disk.[64][65] Cobalt Strike can also use PowerSploit and other scripting frameworks to perform execution.[66][67][68][69]
S0126	ComRAT	ComRAT has used PowerShell to load itself every time a user logs in to the system. ComRAT can execute PowerShell scripts loaded into memory or from the file system.[70][71]
G0142	Confucius	Confucius has used PowerShell to execute malicious files and payloads.[72]
S0591	ConnectWise	ConnectWise can be used to execute PowerShell commands on target machines.[73]
G0052	CopyKittens	CopyKittens has used PowerShell Empire.[74]
S1155	Covenant	Covenant can create PowerShell-based launchers for Grunt installation.[75]
S0488	CrackMapExec	CrackMapExec can execute PowerShell commands via WMI.[76]
S1023	CreepyDrive	CreepyDrive can use Powershell for execution, including the cmdlets `Invoke-WebRequest` and `Invoke-Expression` .[77]
S1024	CreepySnail	CreepySnail can use PowerShell for execution, including the cmdlets `Invoke-WebRequst` and `Invoke-Expression` .[77]
S0625	Cuba	Cuba has been dropped onto systems and used for lateral movement via obfuscated PowerShell scripts.[78]
G1012	CURIUM	CURIUM has leveraged PowerShell scripts for initial process execution and data gathering in victim environments.[79]
G1034	Daggerfly	Daggerfly used PowerShell to download and execute remote-hosted files on victim systems.[80]

ID	Name	Description
G0079	DarkHydrus	DarkHydrus leveraged PowerShell to download and execute additional scripts for execution.[81][82]
G0105	DarkVishnya	DarkVishnya used PowerShell to create shellcode loaders.[83]
S0673	DarkWatchman	DarkWatchman can execute PowerShell commands and has used PowerShell to execute a keylogger.[84]
G0009	Deep Panda	Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.[85]
S0354	Denis	Denis has a version written in PowerShell.[22]
S0695	Donut	Donut can generate shellcode outputs that execute via PowerShell.[86]
S0186	DownPaper	DownPaper uses PowerShell for execution.[87]
G0035	Dragonfly	Dragonfly has used PowerShell scripts for execution.[88][89]
G1006	Earth Lusca	Earth Lusca has used PowerShell to execute commands.[90]
S0554	Egregor	Egregor has used an encoded PowerShell command by a service created by Cobalt Strike for lateral movement.[91]
G1003	Ember Bear	Ember Bear has used PowerShell commands to gather information from compromised systems, such as email servers.[92]
S0367	Emotet	Emotet has used Powershell to retrieve the malicious payload and download additional resources like Mimikatz. [93][94][95][96][97]
S0363	Empire	Empire leverages PowerShell for the majority of its client-side agent tasks. Empire also contains the ability to conduct PowerShell remoting with the `Invoke-PSRemoting` module.[98][99]
S0512	FatDuke	FatDuke has the ability to execute PowerShell scripts.[100]
S0679	Ferocious	Ferocious can use PowerShell scripts for execution.[101]
G0051	FIN10	FIN10 uses PowerShell for execution as well as PowerShell Empire to establish persistence.[102][98]
G1016	FIN13	FIN13 has used PowerShell commands to obtain DNS data from a compromised network.[103]
G0037	FIN6	FIN6 has used PowerShell to gain access to merchant's networks, and a Metasploit PowerShell module to download and execute shellcode and to set up a local listener.[104][105][106]
G0046	FIN7	FIN7 used a PowerShell script to launch shellcode that retrieved an additional payload.[107][108][109][110]
G0061	FIN8	FIN8's malicious spearphishing payloads are executed as PowerShell. FIN8 has also used PowerShell for lateral movement and credential access.[111][112][113][114]
S0381	FlawedAmmyy	FlawedAmmyy has used PowerShell to execute commands.[115]
G0117	Fox Kitten	Fox Kitten has used PowerShell scripts to access credential data.[116]
C0001	Frankenstein	During Frankenstein, the threat actors used PowerShell to run a series of Base64-encoded commands that acted as a stager and enumerated hosts.[117]

ID	Name	Description
G0093	GALLIUM	GALLIUM used PowerShell for execution to assist in lateral movement as well as for dumping credentials stored on compromised machines.[118]
G0084	Gallmaker	Gallmaker used PowerShell to download additional payloads and for execution.[119]
G0047	Gamaredon Group	Gamaredon Group has used obfuscated PowerShell scripts for staging.[120]
S1117	GLASSTOKEN	GLASSTOKEN can use PowerShell for command execution.[121]
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has staged and executed PowerShell scripts on compromised hosts.[122]
S1138	Gootloader	Gootloader can use an encoded PowerShell stager to write to the Registry for persistence.[123][124]
G0078	Gorgon Group	Gorgon Group malware can use PowerShell commands to download and execute a payload and open a decoy document on the victim's machine.[125]
S0417	GRIFFON	GRIFFON has used PowerShell to execute the Meterpreter downloader TinyMet.[126]
G0125	HAFNIUM	HAFNIUM has used the Exchange Power Shell module `Set-OabVirtualDirectoryPowerShell` to export mailbox data.[127][128]
S0151	HALFBAKED	HALFBAKED can execute PowerShell scripts.[107]
S0037	HAMMERTOSS	HAMMERTOSS is known to use PowerShell.[129]
S0499	Hancitor	Hancitor has used PowerShell to execute commands.[130]
S0170	Helminth	One version of Helminth uses a PowerShell script.[131]
G1001	HEXANE	HEXANE has used PowerShell-based tools and scripts for discovery and collection on compromised hosts.[132][133][134]
C0038	HomeLand Justice	During HomeLand Justice, threat actors used PowerShell cmdlets New-MailboxSearch and Get-Recipient for discovery.[135][136]
G0100	Inception	Inception has used PowerShell to execute malicious commands and payloads.[137][138]
G0119	Indrik Spider	Indrik Spider has used PowerShell Empire for execution of malware.[139][140]
S1132	IPsec Helper	IPsec Helper can run arbitrary PowerShell commands passed to it.[141]
S0389	JCry	JCry has used PowerShell to execute payloads.[142]
S0648	JSS Loader	JSS Loader has the ability to download and execute PowerShell scripts.[143]
S0387	KeyBoy	KeyBoy uses PowerShell commands to download and execute payloads.[144]
S0526	KGH_SPY	KGH_SPY can execute PowerShell commands on the victim's machine.[145]
G0094	Kimsuky	Kimsuky has executed a variety of PowerShell scripts including Invoke-Mimikatz.[146][147][148][149][150]
S0250	Koadic	Koadic has used PowerShell to establish persistence.[151]
S0669	KOCTOPUS	KOCTOPUS has used PowerShell commands to download additional files.[151]
S0356	KONNI	KONNI used PowerShell to download and execute a specific 64-bit version of the malware.[152][153]

ID	Name	Description
G0032	Lazarus Group	Lazarus Group has used PowerShell to execute commands and malicious code.[154]
G0140	LazyScripter	LazyScripter has used PowerShell scripts to execute malicious code.[151]
G0065	Leviathan	Leviathan has used PowerShell for execution.[155][156][157][158]
S0680	LitePower	LitePower can use a PowerShell script to execute commands.[101]
S0681	Lizar	Lizar has used PowerShell scripts.[159]
S0447	Lokibot	Lokibot has used PowerShell commands embedded inside batch scripts.[160]
S1141	LunarWeb	LunarWeb has the ability to run shell commands via PowerShell.[161]
S1060	Mafalda	Mafalda can execute PowerShell commands on a compromised machine.[162]
G0059	Magic Hound	Magic Hound has used PowerShell for execution and privilege escalation.[163][164][165][166][167]
G0045	menuPass	menuPass uses PowerSploit to inject shellcode into PowerShell.[168][169]
S0688	Meteor	Meteor can use PowerShell commands to disable the network adapters on a victim machines.[170]
S0553	MoleNet	MoleNet can use PowerShell to set persistence.[171]
G0021	Molerats	Molerats used PowerShell implants on target machines.[172]
S0256	Mosquito	Mosquito can launch PowerShell Scripts.[173]
G1019	MoustachedBouncer	MoustachedBouncer has used plugins to execute PowerShell scripts.[174]
G0069	MuddyWater	MuddyWater has used PowerShell for execution.[175][176][177][178][179][180][181][182][183][184]
G0129	Mustang Panda	Mustang Panda has used malicious PowerShell scripts to enable execution.[185][186]
S0457	Netwalker	Netwalker has been written in PowerShell and executed directly in memory, avoiding detection.[187][188]
S0198	NETWIRE	The NETWIRE binary has been executed via PowerShell script.[189]
S0385	njRAT	njRAT has executed PowerShell commands via auto-run registry key persistence.[190]
G0133	Nomadic Octopus	Nomadic Octopus has used PowerShell for execution.[191]
G0049	OilRig	OilRig has used PowerShell scripts for execution, including use of a macro to run a PowerShell command to decode file contents.[43][192][193]
C0022	Operation Dream Job	During Operation Dream Job, Lazarus Group used PowerShell commands to explore the environment of compromised victims.[194]
C0014	Operation Wocao	During Operation Wocao, threat actors used PowerShell on compromised systems.[195]
S0352	OSX_OCEANLOTUS.D	OSX_OCEANLOTUS.D uses PowerShell scripts.[196]
G0040	Patchwork	Patchwork used PowerSploit to download payloads, run a reverse shell, and execute malware on the victim's machine.[197][198]
C0036	Pikabot Distribution February 2024	Pikabot Distribution February 2024 passed execution from obfuscated JavaScript files to PowerShell scripts to download and install Pikabot.[199]

ID	Name	Description
S0517	Pillowmint	Pillowmint has used a PowerShell script to install a shim database.[200]
G1040	Play	Play has used Base64-encoded PowerShell scripts to disable Microsoft Defender.[201]
G0033	Poseidon Group	The Poseidon Group's Information Gathering Tool (IGT) includes PowerShell components.[202]
S0150	POSHSPY	POSHSPY uses PowerShell to execute various commands, one to execute its payload.[203]
S1012	PowerLess	PowerLess is written in and executed via PowerShell without using powershell.exe.[204]
S0685	PowerPunch	PowerPunch has the ability to execute through PowerShell.[120]
S0441	PowerShower	PowerShower is a backdoor written in PowerShell.[137]
S0145	POWERSOURCE	POWERSOURCE is a PowerShell backdoor.[205][206]
S0194	PowerSploit	PowerSploit modules are written in and executed via PowerShell.[207][208]
S0393	PowerStallion	PowerStallion uses PowerShell loops to iteratively check for available commands in its OneDrive C2 server.[209]
S0223	POWERSTATS	POWERSTATS uses PowerShell for obfuscation and execution.[210][179][211][183]
S0371	POWERTON	POWERTON is written in PowerShell.[212]
S1046	PowGoop	PowGoop has the ability to use PowerShell scripts to execute commands.[183]
S0184	POWRUNER	POWRUNER is written in PowerShell.[43]
S1058	Prestige	Prestige can use PowerShell for payload execution on targeted systems.[213]
S0613	PS1	PS1 can utilize a PowerShell loader.[214]
S0196	PUNCHBUGGY	PUNCHBUGGY has used PowerShell scripts.[215]
S0192	Pupy	Pupy has a module for loading and executing PowerShell scripts.[216]
S1032	PyDCrypt	PyDCrypt has attempted to execute with PowerShell.[217]
S0583	Pysa	Pysa has used Powershell scripts to deploy its ransomware.[218]
S0650	QakBot	QakBot can use PowerShell to download and execute payloads.[219]
S0269	QUADAGENT	QUADAGENT uses PowerShell scripts for execution.[220]
S0241	RATANKBA	There is a variant of RATANKBA that uses a PowerShell script instead of the traditional PE form.[221][222]
G1039	RedCurl	RedCurl has used PowerShell to execute commands and to download malware.[223][224][225]
S0511	RegDuke	RegDuke can extract and execute PowerShell scripts from C2 communications.[100]
S0379	Revenge RAT	Revenge RAT uses the PowerShell command `Reflection.Assembly` to load itself into memory to aid in execution.[226]
S0496	REvil	REvil has used PowerShell to delete volume shadow copies and download files.[227][228][229][230]

ID	Name	Description
S0270	RogueRobin	RogueRobin uses a command prompt to run a PowerShell script from Excel.[81] To assist in establishing persistence, RogueRobin creates `%APPDATA%\OneDrive.bat` and saves the following string to it: `powershell.exe -WindowStyle Hidden -exec bypass -File "%APPDATA%\OneDrive.ps1"` .[231][81]
G1031	Saint Bear	Saint Bear relies extensively on PowerShell execution from malicious attachments and related content to retrieve and execute follow-on payloads.[232]
S1018	Saint Bot	Saint Bot has used PowerShell for execution.[232]
G0034	Sandworm Team	Sandworm Team has used PowerShell scripts to run a credential harvesting tool in memory to evade defenses.[233][6]
S1085	Sardonic	Sardonic has the ability to execute PowerShell commands on a compromised machine.[234]
S0053	SeaDuke	SeaDuke uses a module to execute Mimikatz with PowerShell to perform Pass the Ticket.[15]
S0382	ServHelper	ServHelper has the ability to execute a PowerShell script to get information from the infected host.[235]
S0546	SharpStage	SharpStage can execute arbitrary commands with PowerShell.[171][236]
S0450	SHARPSTATS	SHARPSTATS has the ability to employ a custom PowerShell script.[211]
G0121	Sidewinder	Sidewinder has used PowerShell to drop and execute malware loaders.[237]
G0091	Silence	Silence has used PowerShell to download and execute payloads.[238][239]
S0692	SILENTTRINITY	SILENTTRINITY can use PowerShell to execute commands.[240]
S0649	SMOKEDHAM	SMOKEDHAM can execute Powershell commands sent from its C2 server.[241]
S1086	Snip3	Snip3 can use a PowerShell script for second-stage execution.[242][243]
S0273	Socksbot	Socksbot can write and execute PowerShell scripts.[198]
C0024	SolarWinds Compromise	During the SolarWinds Compromise, APT29 used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and execute other commands.[244][245][246]
S1140	Spica	Spica can use an obfuscated PowerShell command to create a scheduled task for persistence.[247]
S0390	SQLRat	SQLRat has used PowerShell to create a Meterpreter session.[248]
S1030	Squirrelwaffle	Squirrelwaffle has used PowerShell to execute its payload.[249][250]
G0038	Stealth Falcon	Stealth Falcon malware uses PowerShell commands to perform various functions, including gathering system information via WMI and executing commands from its C2 server.[251]
S0491	StrongPity	StrongPity can use PowerShell to add files to the Windows Defender exclusions list.[252]
G1018	TA2541	TA2541 has used PowerShell to download files and to inject into various Windows processes.[253]
G0062	TA459	TA459 has used PowerShell for execution of a payload.[254]
G0092	TA505	TA505 has used PowerShell to download and execute malware and reconnaissance scripts.[255][256][257][258]

ID	Name	Description
G0139	TeamTNT	TeamTNT has executed PowerShell commands in batch scripts.[259]
G0027	Threat Group-3390	Threat Group-3390 has used PowerShell for execution.[260][57]
G0076	Thrip	Thrip leveraged PowerShell to run commands to download payloads, traverse the compromised networks, and carry out reconnaissance.[261]
G1022	ToddyCat	ToddyCat has used Powershell scripts to perform post exploit collection.[262]
G0131	Tonto Team	Tonto Team has used PowerShell to download additional payloads.[263]
S0266	TrickBot	TrickBot has been known to use PowerShell to download new payloads, open documents, and upload data to command and control servers. [264]
C0030	Triton Safety Instrumented System Attack	In the Triton Safety Instrumented System Attack, TEMP.Veles used a publicly available PowerShell-based tool, WMImplant.[265]
G0010	Turla	Turla has used PowerShell to execute commands/scripts, in some cases via a custom executable or code from Empire's PSInject.[266][209][267] Turla has also used PowerShell scripts to load and execute malware in memory.
S0386	Ursnif	Ursnif droppers have used PowerShell in download cradles to download and execute the malware's full executable payload.[268]
S0476	Valak	Valak has used PowerShell to download additional modules.[269]
G1017	Volt Typhoon	Volt Typhoon has used PowerShell including for remote system discovery.[270][271][272]
S0670	WarzoneRAT	WarzoneRAT can use PowerShell to download files and execute commands.[273][274]
S0514	WellMess	WellMess can execute PowerShell scripts received from C2.[275][276]
S0689	WhisperGate	WhisperGate can use PowerShell to support multiple actions including execution and defense evasion.[277][278][279]
G1035	Winter Vivern	Winter Vivern passed execution from document macros to PowerShell scripts during initial access operations.[280] Winter Vivern used batch scripts that called PowerShell commands as part of initial access and installation operations.[281]
G0090	WIRTE	WIRTE has used PowerShell for script execution.[282]
G0102	Wizard Spider	Wizard Spider has used macros to execute PowerShell scripts to download malware on victim's machines.[283] It has also used PowerShell to execute commands and move laterally through a victim network.[284][285][286][287]
S1065	Woody RAT	Woody RAT can execute PowerShell commands and scripts with the use of .NET DLL, `WoodyPowerSession`.[288]
S0341	Xbash	Xbash can use scripts to invoke PowerShell to download a malicious PE executable or PE DLL for execution.[289]
S1151	ZeroCleare	ZeroCleare can use a malicious PowerShell script to bypass Windows controls.[290]
S0330	Zeus Panda	Zeus Panda uses PowerShell to download and execute the payload.[291]

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
M1045	Code Signing	Set PowerShell execution policy to execute only signed scripts.
M1042	Disable or Remove Feature or Program	It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.
M1038	Execution Prevention	Use application control where appropriate. PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`).[292]
M1026	Privileged Account Management	When PowerShell is necessary, consider restricting PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.[293] PowerShell JEA (Just Enough Administration) may also be used to sandbox administration and limit what commands admins/users can execute through remote PowerShell sessions.[294]

Detection

<table>
<tr><th>ID</th><th>Data Source</th><th>Data Component</th><th>Detects</th></tr>
<tr><td>DS0017</td><td>Command</td><td>Command Execution</td><td>If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell. If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect malicious activity. It is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during execution (which is applied to .NET invocations).[295] PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added to PowerShell 4.0. Earlier versions of PowerShell do not have many logging features.[296] An organization can gather PowerShell execution details in a data analytic platform to supplement it with other data.
PowerShell can be used over WinRM to remotely run commands on a host. When a remote PowerShell session starts, svchost.exe executes wsmprovhost.exe
For this to work, certain registry keys must be set, and the WinRM service must be enabled. The PowerShell command Enter-PSSession -ComputerName \<RemoteHost> creates a remote PowerShell session.
Analytic 1 - Look for unusual PowerShell execution.
sourcetype=WinEventLog:Microsoft-Windows-PowerShell/Operational| search EventCode=4104| eval suspicious_cmds=if(like(Message, "%-EncodedCommand%") OR like(Message, "%Invoke-Expression%") OR like(Message, "%IEX%") OR like(Message, "%DownloadFile%"), "Yes", "No")| where suspicious_cmds="Yes"</td></tr>
<tr><td>DS0011</td><td>Module</td><td>Module Load</td><td>Monitor for loading and/or execution of artifacts associated with PowerShell specific assemblies, such as System.Management.Automation.dll (especially to unusual process names/locations).[3][4]
Analytic 1 - Processes loading PowerShell assemblies
sourcetype=WinEventLog:Microsoft-Windows-Sysmon/Operational| search EventCode=7 ImageLoaded IN ("C:\Windows\System32\System.Management.Automation.dll", "C:\Windows\System32\powershell.exe")</td></tr>
</table>

ID	Data Source	Data Component	Detects

DS0009	Process	Process Creation	Monitor for newly executed processes that may abuse PowerShell commands and scripts for execution. PowerShell is a scripting environment included with Windows that is used by both attackers and administrators. Execution of PowerShell scripts in most Windows versions is opaque and not typically secured by antivirus which makes using PowerShell an easy way to circumvent security measures. This analytic detects execution of PowerShell scripts.
			Powershell can be used to hide monitored command line execution such as:
			net usesc start
			Note: - The logic for Analytic 1 is based around detecting on non-interactive Powershell sessions (i.e., those not launched by a user through explorer.exe). This may lead to false positives when used in a production environment, so we recommend tuning any such analytics by including additional logic (e.g., looking for suspicious parent processes) that helps filter such events.- The logic for Analytic 2 is based around detecting on remote Powershell sessions. PowerShell can be used over WinRM to remotely run commands on a host. When a remote PowerShell session starts, svchost.exe executes wsmprovhost.exe.
			Analytic 1 - Non-interactive Powershell Sessions
			`(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="WinEventLog:Security" EventCode="4688") Image="powershell.exe" AND ParentImage!="explorer.exe"`
			Analytic 2 - Remote Powershell Sessions
			`(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="WinEventLog:Security" EventCode="4688") Image="wsmprovhost.exe" AND ParentImage="svchost.exe"`
			Analytic 3 - Powershell Execution
			`(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") Image="C:\Windows\\powershell.exe" ParentImage!="C:\Windows\explorer.exe"|stats values(CommandLine) as "Command Lines" values(ParentImage) as "Parent Images" by ComputerName`

		Process Metadata	Consider monitoring for Windows event ID (EID) 400, which shows the version of PowerShell executing in the `EngineVersion` field (which may also be relevant to detecting a potential Downgrade Attack) as well as if PowerShell is running locally or remotely in the `HostName` field. Furthermore, EID 400 may indicate the start time and EID 403 indicates the end time of a PowerShell session.[297]
DS0012	Script	Script Execution	Monitor for any attempts to enable scripts running on a system that would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent. Analytic 1 - Script Block Logging Events `(source=WinEventLog:"Microsoft-Windows-PowerShell/Operational" EventID="4104" AND Image="powershell.exe" AND (CommandLine="-enc" OR CommandLine="-ep bypass" OR CommandLine="-noni*")`