System Services: Service Execution

Other sub-techniques of System Services (2)

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (`services.exe`) is an interface to manage and manipulate services.[1] The service control manager is accessible to users via GUI components as well as system utilities such as `sc.exe` and Net.

PsExec can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.[2] Tools such as PsExec and `sc.exe` can accept remote servers as arguments and may be used to conduct remote execution.

Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This technique is the execution used in conjunction with Windows Service during service persistence or privilege escalation.

ID: T1569.002

Sub-technique of: T1569

ⓘ

Tactic: Execution

ⓘ

Platforms: Windows

ⓘ

Supports Remote: Yes

Version: 1.2

Created: 10 March 2020

Last Modified: 15 October 2024

Version Permalink

Procedure Examples

ID	Name	Description
S0504	Anchor	Anchor can create and execute services to load its payload.[3][4]
G0050	APT32	APT32's backdoor has used Windows services as a way to execute its malicious payload. [5]
G0082	APT38	APT38 has created new services or modified existing ones to run executables, commands, or scripts.[6]
G0087	APT39	APT39 has used post-exploitation tools including RemCom and the Non-sucking Service Manager (NSSM) to execute processes.[7][8]
G0096	APT41	APT41 used svchost.exe and Net to execute a system service installed to launch a Cobalt Strike BEACON loader.[9][10]
C0040	APT41 DUST	APT41 DUST used Windows services to execute DUSTPAN.[11]
S0438	Attor	Attor's dispatcher can be executed as a service.[12]
S0606	Bad Rabbit	Bad Rabbit drops a file named `infpub.dat` into the Windows directory and is executed through SCManager and `rundll.exe`.
S0127	BBSRAT	BBSRAT can start, stop, or delete services.[13]
G0108	Blue Mockingbird	Blue Mockingbird has executed custom-compiled XMRIG miner DLLs by configuring them to execute via the "wercplsupport" service.[14]
S1063	Brute Ratel C4	Brute Ratel C4 can create Windows system services for execution.[15]
G0114	Chimera	Chimera has used PsExec to deploy beacons on compromised systems.[16]
S0660	Clambling	Clambling can create and start services on a compromised host.[17]
S0154	Cobalt Strike	Cobalt Strike can use PsExec to execute a payload on a remote host. It can also use Service Control Manager to start new services.[18][19][20]
S1111	DarkGate	DarkGate tries to elevate privileges to `SYSTEM` using PsExec to locally execute as a service, such as `cmd /c c:\temp\PsExec.exe -accepteula -j -d -s [Target Binary]`.[21]
S1134	DEADWOOD	DEADWOOD can be executed as a service using various names, such as `ScDeviceEnums`.[22]
S0363	Empire	Empire can use PsExec to execute a payload on a remote host.[23]
G0037	FIN6	FIN6 has created Windows services to execute encoded PowerShell commands.[24]
S0032	gh0st RAT	gh0st RAT can execute its service if the Service key exists. If the key does not exist, gh0st RAT will create and run the service.[25]
S0697	HermeticWiper	HermeticWiper can create system services to aid in executing the payload.[26][27][28]
S0698	HermeticWizard	HermeticWizard can use `OpenRemoteServiceManager` to create a service.[29]
S0376	HOPLIGHT	HOPLIGHT has used svchost.exe to execute a malicious DLL .[30]
S0203	Hydraq	Hydraq uses svchost.exe to execute a malicious DLL included in a new service group.[31]
S0398	HyperBro	HyperBro has the ability to start and stop a specified service.[32]
S0357	Impacket	Impacket contains various modules emulating other service execution tools such as PsExec.[33]

ID	Name	Description
G1032	INC Ransom	INC Ransom has run a file encryption executable via `Service Control Manager/7045;winupd,%SystemRoot%\winupd.exe,user mode service,demand start,LocalSystem`.[34]
S0260	InvisiMole	InvisiMole has used Windows services as a way to execute its malicious payload.[35]
S1132	IPsec Helper	IPsec Helper is run as a Windows service in victim environments.[22]
G0004	Ke3chang	Ke3chang has used a tool known as RemoteExec (similar to PsExec) to remotely execute batch scripts and binaries.[36]
S0250	Koadic	Koadic can run a command on another machine using PsExec.[37]
S0451	LoudMiner	LoudMiner started the cryptomining virtual machine as a service on the infected machine.[38]
S1060	Mafalda	Mafalda can create a remote service, let it run once, and then delete it.[39]
G1036	Moonstone Sleet	Moonstone Sleet used intermediate loader malware such as YouieLoader and SplitLoader that create malicious services.[40]
S0039	Net	The `net start` and `net stop` commands can be used in Net to execute or stop Windows services.[41]
S0056	Net Crawler	Net Crawler uses PsExec to perform remote service manipulation to execute a copy of itself as part of lateral movement.[42]
S0457	Netwalker	Operators deploying Netwalker have used psexec and certutil to retrieve the Netwalker payload.[43]
S0368	NotPetya	NotPetya can use PsExec to help propagate itself across a network.[44][45]
S0439	Okrum	Okrum's loader can create a new service named NtmsSvc to execute the payload.[46]
S0365	Olympic Destroyer	Olympic Destroyer utilizes PsExec to help propagate itself across a network.[47]
C0006	Operation Honeybee	During Operation Honeybee, threat actors ran `sc start` to start the COMSysApp as part of the service hijacking and `sc stop` to stop and reconfigure the COMSysApp.[48]
C0014	Operation Wocao	During Operation Wocao, threat actors created services on remote systems for execution purposes.[49]
S0664	Pandora	Pandora has the ability to install itself as a Windows service.[50]
S0378	PoshC2	PoshC2 contains an implementation of PsExec for remote execution.[51]
S0238	Proxysvc	Proxysvc registers itself as a service on the victim's machine to run as a standalone process.[52]
S0029	PsExec	Microsoft Sysinternals PsExec is a popular administration tool that can be used to execute binaries on remote systems using a temporary Windows service.[2]
S0192	Pupy	Pupy uses PsExec to execute a payload or commands on a remote host.[53]
S0583	Pysa	Pysa has used PsExec to copy and execute the ransomware.[54]
S0481	Ragnar Locker	Ragnar Locker has used sc.exe to execute a service that it creates.[55]
S0166	RemoteCMD	RemoteCMD can execute commands remotely by creating a new service on the remote system.[56]
S0140	Shamoon	Shamoon creates a new service named "ntssrv" to execute the payload. Shamoon can also spread via PsExec.[57][58]
G0091	Silence	Silence has used Winexe to install a service on the remote system.[59][60]

ID	Name	Description
S0533	SLOTHFULMEDIA	SLOTHFULMEDIA has the capability to start services.[61]
S0491	StrongPity	StrongPity can install a service to execute itself as a service.[62][63]
S0663	SysUpdate	SysUpdate can manage services and processes.[50]
S0668	TinyTurla	TinyTurla can install itself as a service on compromised machines.[64]
S0612	WastedLocker	WastedLocker can execute itself as a service.[65]
S0689	WhisperGate	WhisperGate can download and execute AdvancedRun.exe via `sc.exe`.[66][67]
S0191	Winexe	Winexe installs a service on the remote system, executes the command, then uninstalls the service.[68]
S0176	Wingbird	Wingbird uses services.exe to register a new autostart service named "Audit Service" using a copy of the local lsass.exe file.[69][70]
S0141	Winnti for Windows	Winnti for Windows can run as a service using svchost.exe.[71]
G0102	Wizard Spider	Wizard Spider has used `services.exe` to execute scripts and executables during lateral movement within a victim's network. Wizard Spider has also used batch scripts that leverage PsExec to execute a previously transferred ransomware payload on a victim's network.[72][73][74]
S0123	xCmd	xCmd can be used to execute binaries on remote systems by creating and starting a service.[75]
S0412	ZxShell	ZxShell can create a new service for execution.[76]

Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running. [77]
M1026	Privileged Account Management	Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level.
M1022	Restrict File and Directory Permissions	Ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

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>Monitor executed commands and arguments that may abuse the Windows service control manager to execute malicious commands or payloads.
Analytic 1- Commands abusing Windows service control manager.
sourcetype=WinEventLog:Security OR sourcetype=Powershell OR sourcetype=Sysmon EventCode IN (1,4688,4104) | search command_line IN ("sc.exe", "net start", "net stop", "psexec.exe")| where user!="SYSTEM" // Exclude common system-level activities</td></tr>
<tr><td>DS0029</td><td>Network Traffic</td><td>Network Traffic Flow</td><td>Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.</td></tr>
<tr><td>DS0009</td><td>Process</td><td>Process Creation</td><td>Monitor for newly executed processes that may abuse the Windows service control manager to execute malicious commands or payloads.
Events 4688 (Microsoft Windows Security Auditing) and 1 (Microsoft Windows Sysmon) provide context of Windows processes creation that can be used to implement this detection.
This detection is based on uncommon process and parent process relationships. Service Control Manager spawning command shell is a good starting point. Add more suspicious relationships based on the reality of your network environment.
In order to reduce false positives, you can also filter the CommandLine event field using parameters such as /c which carries out the command specified by the parent process.
Analytic 1 - Service Execution
(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="WinEventLog:Security" EventCode="4688") | WHERE Image LIKE "services.exe" AND Image LIKE "cmd.exe"</td></tr>
<tr><td>DS0019</td><td>Service</td><td>Service Creation</td><td>Monitor newly constructed services that abuse control manager to execute malicious commands or payloads.
Analytic 1 - Suspicious Service Creation
sourcetype=WinEventLog:Security OR sourcetype=WinEventLog:System EventCode=4697 OR EventCode=7045| table _time, user, service_name, service_file_name, process_id| where service_file_name != "legitimate_software_path" // Exclude legitimate services</td></tr>
<tr><td>DS0024</td><td>Windows Registry</td><td>Windows Registry Key Modification</td><td>Monitor for changes made to windows registry keys and/or values that may abuse the Windows service control manager to execute malicious commands or payloads.
Analytic 1 - Registry changes related to service execution.
sourcetype=WinEventLog:Security OR sourcetype=Sysmon EventCode=13 OR EventCode=4657| search registry_path IN ("HKLM\SYSTEM\CurrentControlSet\Services")| where registry_value != "legitimate_software_registry*" // Filter out common services</td></tr>
</table>