MENA SEC Applied Security Research

Home About us

Wednesday, 6 February 2019

Threat Hunting #3 - Detecting PsExec execution using event 5145

PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.

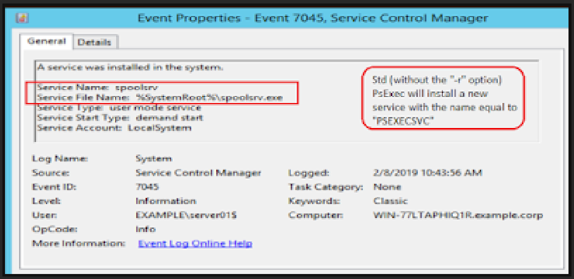
Existing detection of PSEXEC can be easily bypassed:

- PSEXEC Service created - logged by EventID 7045 "Service Creation" ["**psexec -r spoolsvr**" option allow to bypass this one]
- Remote registry change due to accepting Eula (not valid for other PSEXEC implementation in Python or PowerShell)

Proposed detection rely on EventID 5145 "Network File Share Access", that logs in the relative target name field traces of remote access to PSEXECSVC named pipes, with the following format:

<psexecsvc|chosen service name with the "-r" option>-<machine-name>-<5-random-numbers>-<stdin|stderr|stdout>)

Below an example of the left traces:



Event Properties - Event 7045, Service Control Manager

General | Details

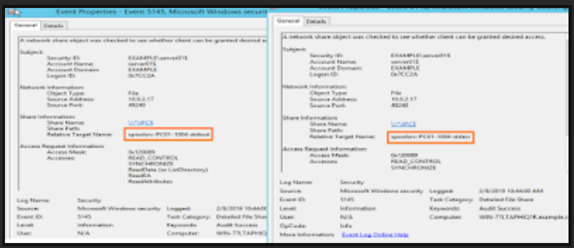
A service was installed in the system.

Service Name: spoolsrv
Service File Name: %SystemRoot%\spoolsrv.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Std (without the "-r" option) PsExec will install a new service with the name equal to "PSEXECSVC"

Log Name:	System		
Source:	Service Control Manager	Logged:	2/8/2019 10:43:56 AM
Event ID:	7045	Task Category:	None
Level:	Information	Keywords:	Classic
User:	EXAMPLE\server01$	Computer:	WIN-77LTAPHIQ1R.example.corp
OpCode:	Info		
More Information:	Event Log Online Help		

As can be seen above, with the "psexec -r spoolsrv \\target -s cmd" (rename) option, standard detection based on service name can be easily bypassed.



Event Properties - Event 5145, Microsoft Windows securi

General | Details

A network share object was checked to see whether client can be granted desired a

Subject:
Security ID: EXAMPLE\server01$
Account Name: server01$
Account Domain: EXAMPLE
Logon ID: 0x7CC2A

Network Information:
Object Type: File
Source Address: 10.0.2.17
Source Port: 49240

Share Information:
Share Name: *\IPC$
Share Path:
Relative Target Name: spoolsrv-PC01-1004-stdout

Access Request Information:
Access Mask: 0x120089
Accesses: READ_CONTROL
SYNCHRONIZE
ReadData (or ListDirectory)
ReadEA
ReadAttributes

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/8/2019 10:44:0
Event ID:	5145	Task Category:	Detailed File Shar
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-77LTAPHIQ

General | Details

A network share object was checked to see whether client can be granted desired access.

Subject:
Security ID: EXAMPLE\server01$
Account Name: server01$
Account Domain: EXAMPLE
Logon ID: 0x7CC2A

Network Information:
Object Type: File
Source Address: 10.0.2.17
Source Port: 49240

Share Information:
Share Name: *\IPC$
Share Path:
Relative Target Name: spoolsrv-PC01-1004-stderr

Access Request Information:
Access Mask: 0x120089
Accesses: READ_CONTROL
SYNCHRONIZE

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/8/2019 10:44:00 AM
Event ID:	5145	Task Category:	Detailed File Share
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-77LTAPHIQ1R.example.c
OpCode:	Info		
More Information:	Event Log Online Help		

Luckily we still have (for now) a unique string in the 5145 event that we can use to detect PSEXEC ("stdin", "stdout" and "stderr").

Blog Archive

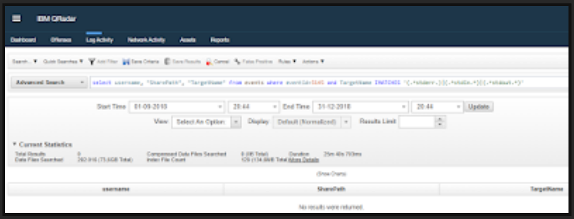
► 2022 (2)
► 2021 (3)
► 2020 (4)
▼ 2019 (39)
► November (2)
► July (1)
► April (3)
► March (7)
▼ February (26)
Threat Hunting #24 - RDP over a Reverse SSH Tunnel
Threat Hunting #23 - Microsoft Windows DNS Server ...
IronPort: Password-Protected Archives
Threat Hunting #22 - Detecting user accounts set w...
Threat Hunting #21 - Hiding in plain sights with r...
IronPort: Blacklisted Attachments
Threat Hunting #20 - Detecting Process Doppelgängi...
Threat Hunting #19 - Procdump or Taskmgr - memory ...
Threat Hunting #18 - Run/RunOnce - Shell-Core El...
Threat Hunting #17 - Suspicious System Time Change
Threat Hunting #16 - Lateral Movement via DCOM - S...
Threat Hunting #15 - Detecting Doc with Macro invo...
Threat Hunting #14 - RDP Hijacking via RDPWRAP | f...
Threat Hunting #13 - Detecting CACTUSTORCH using S...
Threat Hunting #12 - Suspicious strings in Regist...
Threat Hunting #11 - Exposed Passwords
Threat Hunting #10 - Renamed/Modified Windows (ab)...

Detection Logic:

- [EventID=5145 and TargetFileName contains *-stdin or *-stdout or *-stderr]
- [EventID=5145 and not TargetFileName contains *psexecsvc*) and TargetFileName contains *-stdin or *-stdout or *-stderr] -> means attacker changed default psexec service name.

IBM Qradar hunting AQL:

select username, "SharePath", "TargetName" from events where eventid=5145 and TargetName IMATCHES '(.*stderr.)|(.*stdin.*)|(.*\stdout.*)'



And if PsExec is somehow used by IT personnel, then try the following AQL looking for renamed PSEXEC service name: (i.e. psexec -r notPsExecSvc \\host -u account$ -p Passw0rd!123 -s cmd.exe)

select username, "SharePath", "TargetName" from events where eventid=5145 and TargetName IMATCHES '(.*stderr.)|(.*stdin.*)|(.*stdout.*)' and not (TargetName IMATCHES '(?i)(.*PSEXECSVC.*)')

References:

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=5145
https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

Posted by MENASEC at 21:26

Labels: 5145, 7045, paexec, psexec, psexec_psh

No comments:

Post a Comment

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Threat Huting #9 - Impacket\Secretdump remote exec...
Threat H... Detecting trac... confi...
Thre... BloodHound\Sharphoun...
Threat Hunting #6 - Hiding in plain sights with re...
Threat Hunting #5 - Detecting enumeration of users...
Threat Hunting #4 - Detecting Excel/Word documents...
Threat Hunting #3 - Detecting PsExec execution usi...
Threat Hunting #2 - Detecting PsLoggedOn exec usin...
Threat Hunting #1 - RDP Hijacking traces - Part 1