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.

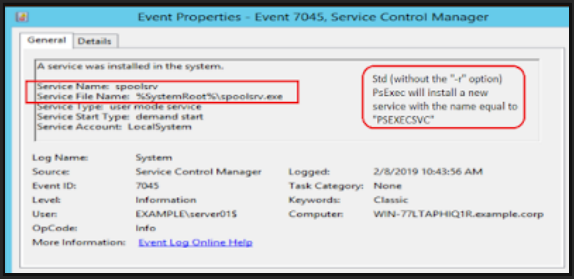
Existing detection of PSEXEC can be easily bypassed:

- 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)

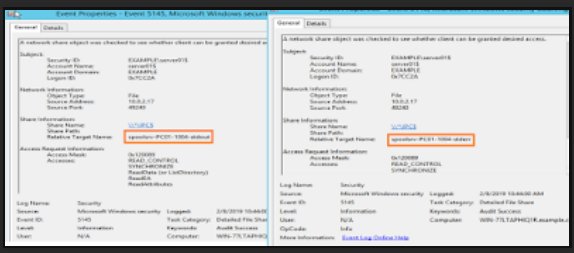
Proposed detection rely on EventID 5145 "Network File Share Access", that logs in the relative target name field traces of remote access to PSEXECSVC named pipes, with the following format:

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

Below an example of the left traces:



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.



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

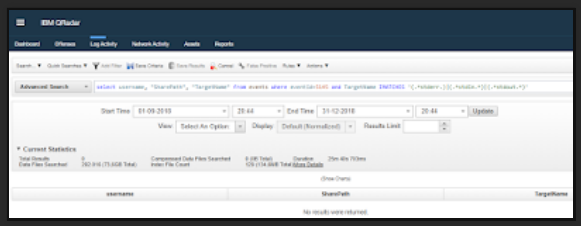
Blog Archive

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

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

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