PrintNightmare Detection

Monday, September 27, 2021 10:05 AM

Start Time	End Time
2021-09-24 23:51:05	2021-09-24 23:53:34

- 13 Anomalies flagged

CAR-2013-05-005: SMB Copy and Execution1
GSE-T1021 - Remote Services - Unusual Remote SSH Connection - AWS
GSE-Abnormally High Number Of Endpoint Changes By User - Windows Security Abnormally High Number Of Endpoint Changes By User
CAR-2021-01-002: Unusually Long Command Line Strings
CAR-2016-03-001: Host Discovery Commands
CAR-2021-01-003: Clearing Windows Logs with Wevtutil
GSE-Defense Evasion - T1027 - Obfuscated Files or Information - Unusual Process Executed by User
CAR-2013-07-001: Suspicious Arguments
GSE-New Login User Getting Elevated Privileges - Windows Security
CAR-2013-05-005: SMB Copy and Execution
CAR-2014-03-006: RunDLL32.exe monitoring
CAR-2020-11-005: Clear Powershell Console Command History

1.
transactions.ipaddress in ("192.168.118.144") <----- Kali IP

192.168.118.144 is a new IP address we are seeing

Event ID: 4624: An account was successfully logged on
Logon Type: 3 <-- Network logon
Elevated Token: Yes

(transactions.resourcename not in ("Unix Processes")) AND anomaly in ("GSE-New Login User Getting Elevated Privileges - Windows Security")

Model Flagged: GSE-New Login User Getting Elevated Privileges - Windows Security
Event ID: 4672 - Special Privileges assigned to new logon
Privileges: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege SeEnableDelegationPrivilege

Event type: 1116 - Microsoft Defender - Microsoft Defender Antivirus has detected malware or other potentially unwanted software
Severity: Severe

Detection case 1

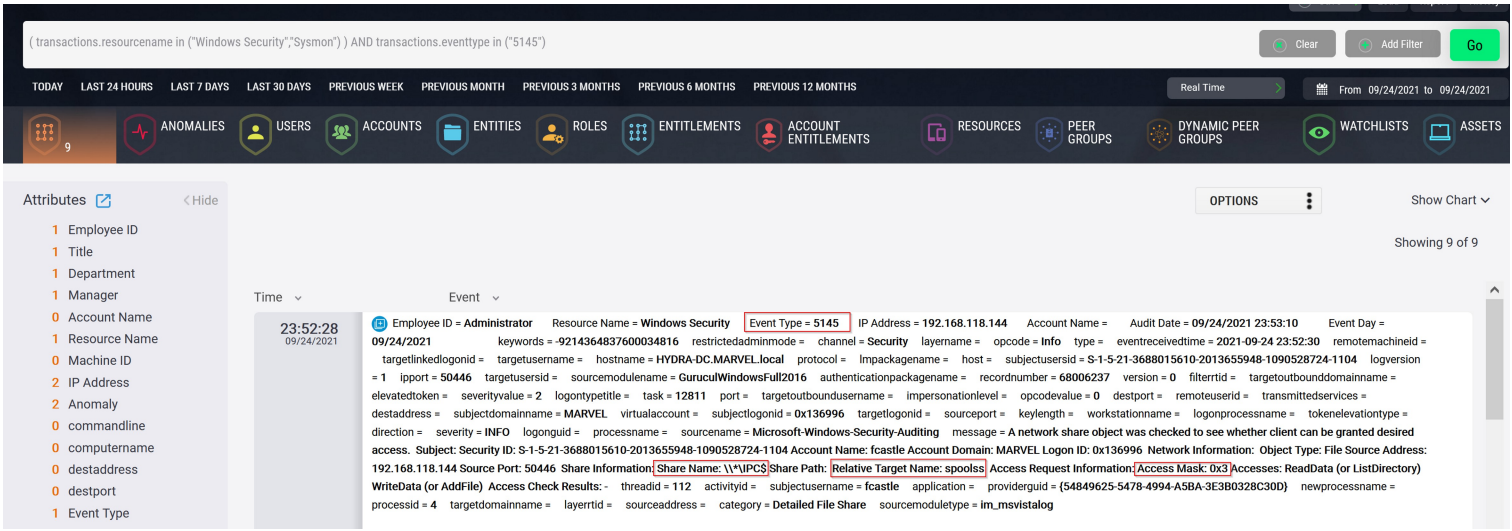
Detecting remote print spooler driver load using file share logs:

- Event Code – 5145
- ShareName – *\IPC$
- AccessMask – 0x3
- RelativeTargetName – spoolss

Event ID: 5145: A network share object was accessed.

and

Event ID: 5145 A network share object was checked to see whether client can be granted desired access
Account accessed: fcastle on
domain Marvel.local
Share Name: *\IPC$
The IPC$ share is also known as a null session connection. By using this session, Windows lets anonymous users perform certain activities, such as enumerating the names of domain accounts and network shares.
Relative Target Name: **spoolss**
Access Request Information: **Access Mask: 0x3** Accesses: ReadData (or ListDirectory) WriteData (or AddFile)



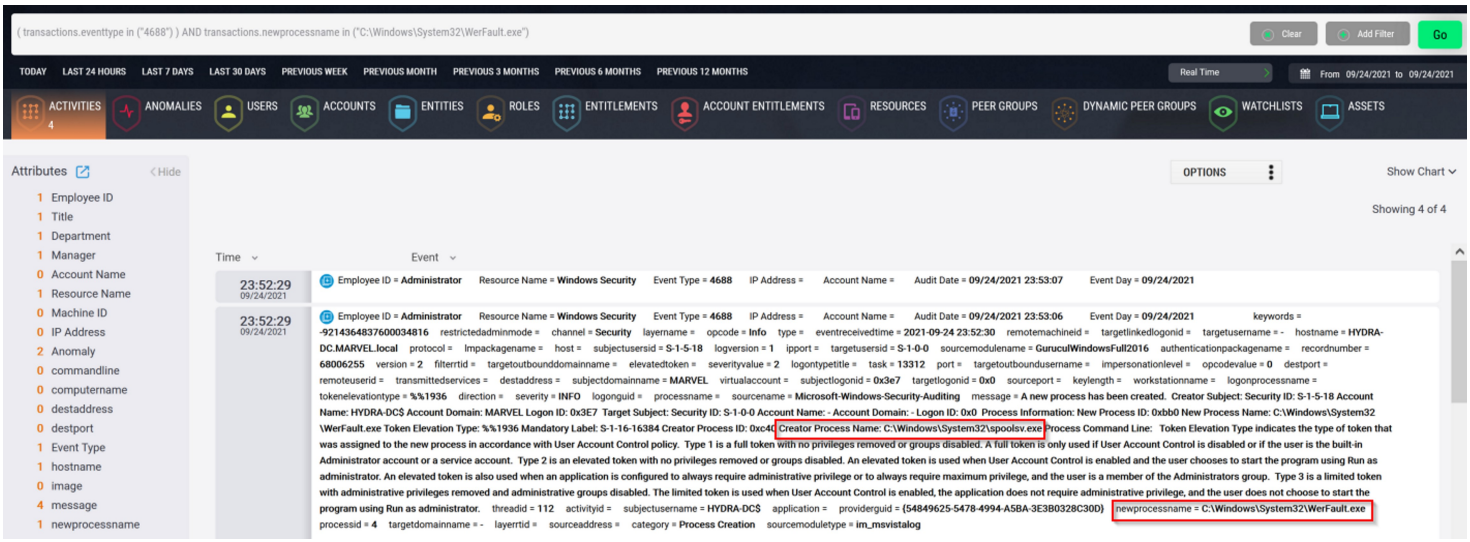
A generic way to hunt for Print Spooler exploitation is looking for error generated by print spooler due to loading of the payload DLL. This can be done either through looking for spawning of WerFault.exe by spoolsv.exe or generation of Event ID 7031 showing unexpected termination of print spooler service:

Spoolsv Suspicious Process Access:

Detection case 2

Abnormal parent-child relationship for the processes:

Event Code – 4688/1
Process Name – PowerShell.exe or cmd.exe or werfault.exe
Parent Process Name – spoolsv.exe

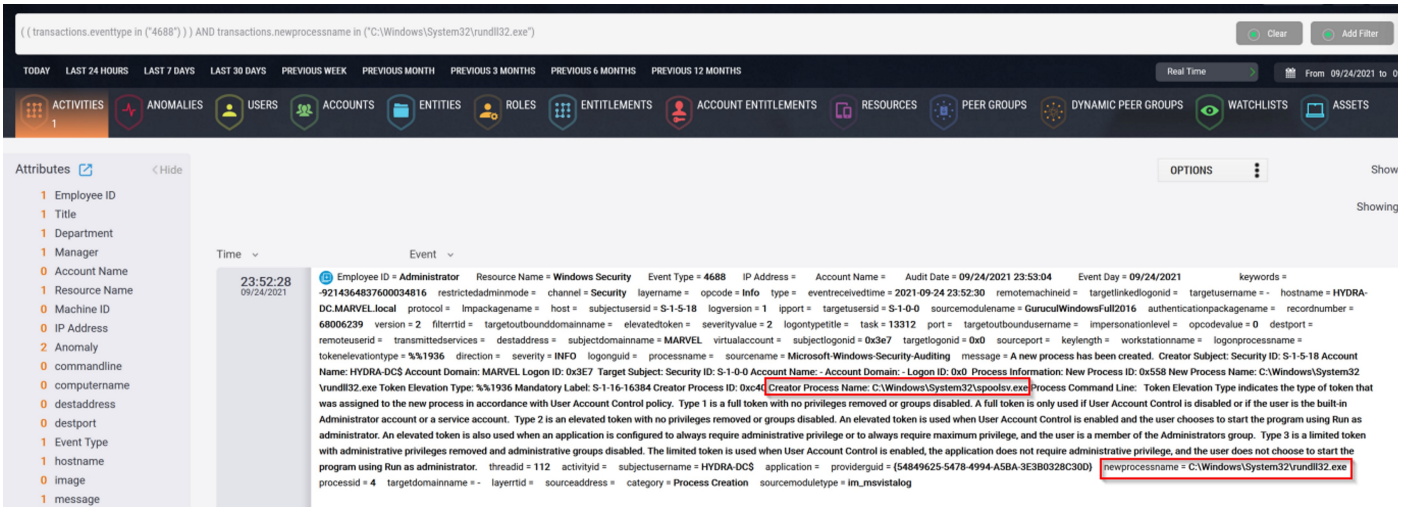


Spoolsv Suspicious Loaded Modules

Detection Case 3:

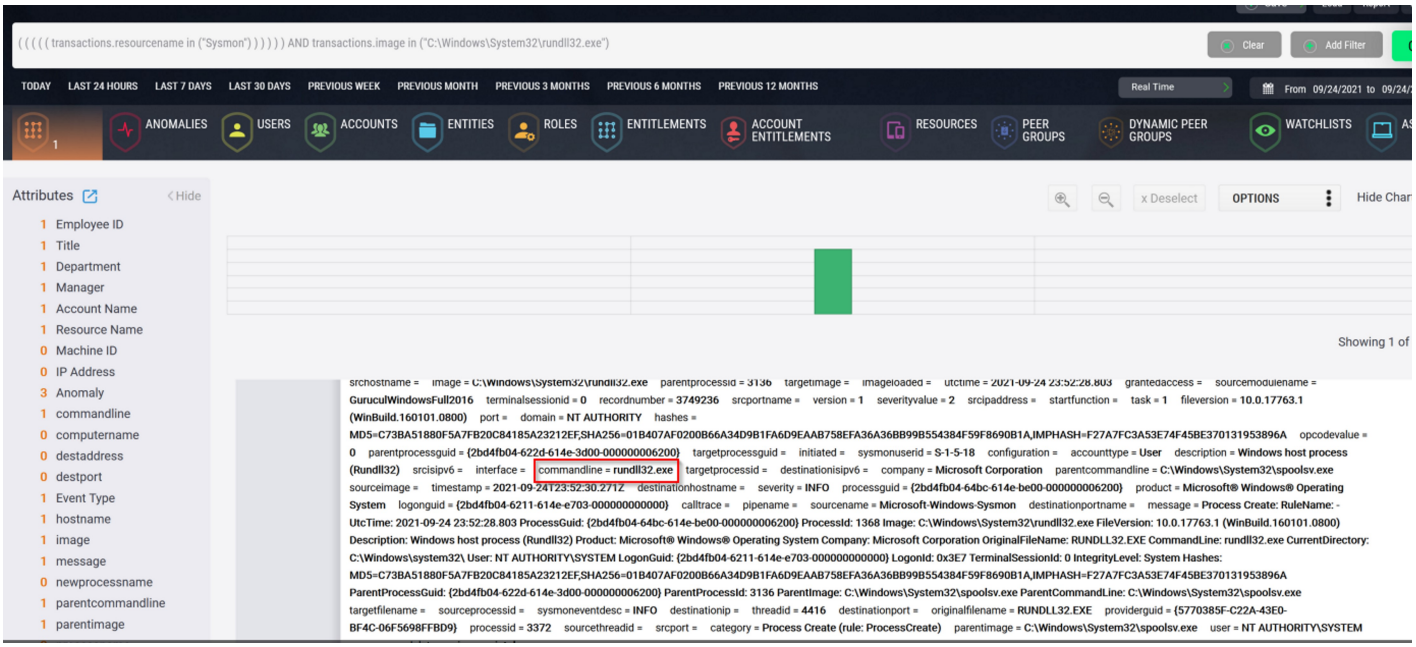
Spoolsv Spawning Rundll32

Detects Spoolsv with a child process of rundll32.exe.



SYSMON:

Suspicious Rundll32 no Command Line Arguments



MTRE

Detection	Techniques ID	Tactic(s)	Description
Spoolsv Spawning Rundll32 (New)	T1547.012	Persistence, Privilege Escalation	Detects Spoolsv with a child process of rundll32.exe
Spoolsv Suspicious Loaded Modules (New)	T1547.012	Persistence, Privilege Escalation	Identifies potentially suspicious module loads into Spoolsv.exe based on DLL loading from a specific path used by CVE-2021-34527
Spoolsv Suspicious Process Access (New)	T1068	Privilege Escalation	Identifies suspicious process access events from Spoolsv.exe to a Target process.
Suspicious Rundll32 no Command Line Arguments	T1218.011	Defense Evasion	Identifies Rundll32.exe with no command line arguments

Source:

https://www.exabeam.com/information-security/detecting-the-printnightmare-cve-2021-1675-34527-vulnerability-using-exabeam/
https://www.splunk.com/en_us/blog/security/i-pity-the-spool-detecting-printnightmare-cve-2021-34527.html