

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 Weventutil
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)

(transactions.resourcename in ("Windows Security","Sysmon")) AND transactions.eventtype in ("5145")

TODAY LAST 24 HOURS LAST 7 DAYS LAST 30 DAYS PREVIOUS WEEK PREVIOUS MONTH PREVIOUS 3 MONTHS PREVIOUS 6 MONTHS PREVIOUS 12 MONTHS

Real Time From 09/24/2021 to 09/24/2021

ANOMALIES 9 **USERS** **ACCOUNTS** **ENTITIES** **ROLES** **ENTITLEMENTS** **ACCOUNT ENTITLEMENTS** **RESOURCES** **PEER GROUPS** **DYNAMIC PEER GROUPS** **WATCHLISTS** **ASSETS**

Attributes Hide **OPTIONS** **... Show Chart**

Showing 9 of 9

Employee ID 1
Title 1
Department 1
Manager 1
Account Name 0
Resource Name 1
Machine ID 0
IP Address 2
Anomaly 2
commandline 0
computername 0
destaddress 0
destport 0
Event Type 1

Time Event

23:52:28 09/24/2021

Employee ID = Administrator Resource Name = Windows Security Event Type = 5145 IP Address = 192.168.118.144 Account Name = Audit Date = 09/24/2021 23:53:10 Event Day = 09/24/2021 keywords = -9214364837600034816 restrictedadminmode = channel = Security layername = opcode = Info type = eventreceivedtime = 2021-09-24 23:52:30 remotemachineid = targetlinkedlogonid = targetusername = hostname = HYDRA-DC.MARVEL.local protocol = Impackagename = host = subjectuserid = S-1-5-21-3688015610-2013655948-1090528724-1104 logversion = 1 iport = 50446 targetusersid = sourcemodulename = GuruculWindowsFull2016 authenticationpackagename = recordnumber = 68006237 version = 0 filterid = targetoutbounddomainname = elevatedtoken = severityvalue = 2 logontypefile = task = 12811 port = targetoutboundusername = impersonationlevel = opcodevalue = 0 destport = remoteuserid = transmittedservices = destaddress = subjectdomainname = MARVEL virtualaccount = subjectlogonid = 0x136996 targetlogonid = sourceport = keylength = workstationname = logonprocessname = tokenlevationtype = direction = severity = INFO logonguid = processname = sourcename = Microsoft-Windows-Security-Auditing message = A network share object was checked to see whether client can be granted desired access. Security ID: S-1-5-21-3688015610-2013655948-1090528724-1104 Account Name: fcastle Account Domain: MARVEL Logon ID: 0x136996 Network Information Object Type: File Source Address: 192.168.118.144 Source Port: 50446 Share Information\Share Name: \\IPCS\Share Path: Relative Target Name: spools Access Request Information:Access Mask: 0x3 Accesses: ReadData (or ListDirectory) WriteData (or AddFile) Access Check Results: - threadid = 112 activitiyid = subjectusername = fcastle application = providerguid = (54849625-5478-4994-A5BA-3E3B0328C30D) newprocessname = processid = 4 targetdomainname = layerid = sourceaddress = category = Detailed File Share sourcemoduletype = im_msvisatalog

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 spools.exe or generation of Event ID 7031 showing unexpected termination of print spooler service:

Spools 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 – spools.exe

(transactions.eventtype in ("4688")) AND transactions.newprocessname in ("C:\Windows\System32\WerFault.exe")

TODAY LAST 24 HOURS LAST 7 DAYS LAST 30 DAYS PREVIOUS WEEK PREVIOUS MONTH PREVIOUS 3 MONTHS PREVIOUS 6 MONTHS PREVIOUS 12 MONTHS

Real Time From 09/24/2021 to 09/24/2021

ACTIVITIES 4 **ANOMALIES** **USERS** **ACCOUNTS** **ENTITIES** **ROLES** **ENTITLEMENTS** **ACCOUNT ENTITLEMENTS** **RESOURCES** **PEER GROUPS** **DYNAMIC PEER GROUPS** **WATCHLISTS** **ASSETS**

Attributes Hide **OPTIONS** **... Show Chart**

Showing 4 of 4

Employee ID 1
Title 1
Department 1
Manager 1
Account Name 0
Resource Name 1
Machine ID 0
IP Address 2
Anomaly 2
commandline 0
computername 0
destaddress 0
destport 0
Event Type 1
hostname 1
image 4
message 1
newprocessname 1

Time Event

23:52:29 09/24/2021

Employee ID = Administrator Resource Name = Windows Security Event Type = 4688 IP Address = Account Name = Audit Date = 09/24/2021 23:53:07 Event Day = 09/24/2021 keywords = -9214364837600034816 restrictedadminmode = channel = Security layername = opcode = Info type = eventreceivedtime = 2021-09-24 23:52:30 remotemachineid = targetlinkedlogonid = targetusername = - hostname = HYDRA-DC.MARVEL.local protocol = Impackagename = host = subjectuserid = S-1-5-18 sourcemodulename = GuruculWindowsFull2016 authenticationpackagename = recordnumber = 68006255 version = 2 filterid = targetoutbounddomainname = elevatedtoken = severityvalue = 2 logontypefile = task = 13312 port = targetoutboundusername = impersonationlevel = opcodevalue = 0 destport = remoteuserid = transmittedservices = destaddress = subjectdomainname = MARVEL virtualaccount = subjectlogonid = 0x3e7 targetlogonid = 0x0 sourceport = keylength = workstationname = logonprocessname = tokenlevationtype = %x1936 direction = severity = INFO logonguid = processname = sourcename = Microsoft-Windows-Security-Auditing message = A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: HYDRA-DCS Account Domain: MARVEL Logon ID: 0x2E7 Target Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0xb60 New Process Name: C:\Windows\System32\WerFault.exe Token Elevation Type: %x1936 Mandatory Label: S-1-16-16384 Creator Process ID: 0xc0 Creator Process Name: C:\Windows\System32\spools.exe Process Command Line: Token Elevation Type: indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator. threadid = 112 activitiyid = subjectusername = HYDRA-DCS application = providerguid = (54849625-5478-4994-A5BA-3E3B0328C30D) newprocessname = C:\Windows\System32\WerFault.exe

Spools Suspicious Loaded Modules

Detection Case 3:

Spools Spawning rundll32

Detects Spools with a child process of rundll32.exe.

(((transactions.eventtype in ('4688')) AND transactions.newprocessname in ('C:\Windows\System32\rundll32.exe'))

Today Last 24 Hours Last 7 Days Last 30 Days Previous Week Previous Month Previous 3 Months Previous 6 Months Previous 12 Months Real Time From 09/24/2021 to 09/24/2021

ACTIVITIES ANOMALIES USERS ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS DYNAMIC PEER GROUPS WATCHLISTS ASSETS

Attributes Hide Options Show

Employee ID
Title
Department
Manager
Account Name
Resource Name
Machine ID
IP Address
Anomaly
commandline
computename
destaddress
destport
Event Type
hostname
image
message

Time Event

23:52:28 09/24/2021 Employee ID = Administrator Resource Name = Windows Security Event Type = 4688 IP Address = Account Name = Audit Date = 09/24/2021 23:53:04 Event Day = 09/24/2021 keywords = -921436483760034816 restrictedadminmode = channel = Security layername = opcode = Info type = eventrceivedetime = 2021-09-24 23:52:20 remotemachineid = targetinkedgondid = targetusername = hostname = HYDRA-DC-MARVEL.local protocol = Impackagename = host = subjectuserid = S-1-5-18 logversion = 1 import = targetuserid = S-1-0 sourcemodulename = GuruculWindowsFull2016 authenticationpackagename = recordnumber = 68006239 version = 2 filterid = targetoutbounddomainname = elevatedtokken = severityvalue = 2 logontypefile = task = 13312 port = targetoutboundusername = impersonationlevel = opcodevalue = 0 destport = remoteuserid = transmittedservices = destaddress = subjectdomainname = MARVEL virtualaccount = subjectlogonid = 0x3e7 targetlogonid = 0x0 sourcereport = keylength = workstationname = logonprocessname = tokenlevellongtype = %1936 direction = severity = INFO logonguid = processname = sourcename = Microsoft-Windows-Security-Auditing message = A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: HYDRA-DC5 Account Domain: MARVEL Logon ID: 0x3e7 Target Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x558 New Process Name: C:\Windows\System32\rundll32.exe Token Elevation Type: %1936 Mandatory Label: S-1-16-16384 Creator Process ID: 0x40 [Creator Process Name: C:\Windows\System32\spoolsv.exe] Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator. threadid = 112 activitid = subjectusername = HYDRA-DC5 application = providerguid = {54849625-5478-4994-ASBA-3E3B032C83D0} newprocessname = C:\Windows\System32\rundll32.exe processid = 4 targetdomainname = - layerid = sourcereport = category = Process Creation sourcemoduletype = im_msvisatalog

SYSMON:

Suspicious Rundll32 no Command Line Arguments

(((((transactions.resourcename in ('Sysmon'))))) AND transactions.image in ('C:\Windows\System32\rundll32.exe'))

Today Last 24 Hours Last 7 Days Last 30 Days Previous Week Previous Month Previous 3 Months Previous 6 Months Previous 12 Months Real Time From 09/24/2021 to 09/24/2021

ACTIVITIES ANOMALIES USERS ACCOUNTS ENTITIES ROLES ENTITLEMENTS ACCOUNT ENTITLEMENTS RESOURCES PEER GROUPS DYNAMIC PEER GROUPS WATCHLISTS ASSETS

Attributes Hide Options Show

Employee ID
Title
Department
Manager
Account Name
Resource Name
Machine ID
IP Address
Anomaly
commandline
computename
destaddress
destport
Event Type
hostname
image
message
newprocessname
parentcommandline
parentimage

Time

23:52:28 09/24/2021

srchostname = image = C:\Windows\System32\rundll32.exe parentprocessid = 3136 targetimage = imageloaded = urctime = 2021-09-24 23:52:28.803 grantedaccess = sourcemodulename = GuruculWindowsFull2016 terminalsessionid = 0 recordnumber = 3749236 srcreportname = version = 1 srcipaddress = startfunction = task = 1 fileversion = 10.0.17763.1 (WinBuild.160101.0800) port = domain = NT AUTHORITY\hashes = MD5-C73BA51880F5A7FB20C84185A23212EFSHA256-01B407AF020B066A34D9B1FA6D9EAAB758FEFA36A36BB99B554384F59F8690B1AJMPHASH=F27A7FC3A53E74F45BE370131953896A opcodevalue = 0 parentprocessguid = {2bd4fb04-622d-614e-3d00-000000006200} targetprocessguid = initiated = sysmonuserid = S-1-5-18 configuration = accounttype = User description = Windows host process (Rundll32) srccipv6 = interface = commandline = rundll32.exe targetprocessid = destinationipv6 = company = Microsoft Corporation parentcommandline = C:\Windows\System32\spoolsv.exe sourcename = timestamp = 2021-09-24T23:52:30.271Z destinationhostname = severity = INFO processguid = {2bd4fb04-64bc-614e-be00-000000006200} product = Microsoft® Windows® Operating System logonguid = {2bd4fb04-6211-614e-e703-000000000000} calltrace = pipename = sourcename = Microsoft-Windows-Sysmon destinationportname = message = Process Create: RuleName: - UriTime: 2021-09-24 23:52:28.803 ProcessGuid: {2bd4fb04-64bc-614e-be00-000000006200} ProcessId: 1368 Image: C:\Windows\System32\rundll32.exe FileVersion: 10.0.17763.1 (WinBuild.160101.0800) Description: Windows host process (Rundll32) Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: RUNDLL32.EXE CommandLine: rundll32.exe CurrentDirectory: C:\Windows\System32\User: NT AUTHORITY\SYSTEM LogonGuid: {2bd4fb04-6211-614e-e703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5-C73BA51880F5A7FB20C84185A23212EFSHA256-01B407AF020B066A34D9B1FA6D9EAAB758FEFA36A36BB99B554384F59F8690B1AJMPHASH=F27A7FC3A53E74F45BE370131953896A ParentProcessGuid: {2bd4fb04-622d-614e-3d00-000000006200} ParentProcessId: 3136 ParentImage: C:\Windows\System32\spoolsv.exe ParentCommandLine: C:\Windows\System32\spoolsv.exe targetfilename = sourceprocessid = sysmoneventdesc = INFO destinationip = threadid = 4416 destinationport = originalfilename = RUNDLL32.EXE providerguid = {5770385F-C22A-43E0-BF4C-06F5698FBBD9} processid = 3372 sourcethreadid = srccode = category = Process Create (rule:ProcessCreate) parentimage = C:\Windows\System32\spoolsv.exe user = NT AUTHORITY\SYSTEM

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