Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

microsoft / Microsoft-365-Defender-Hunting-Queries Public archive
Notifications Fork 539 Star 1.9k
Code Issues 12 Pull requests 34 Actions Projects Wiki Security Insights

Files
efa17a6
Go to file
Campaigns
Collection
Command and Control
Credential Access
Defense evasion
Delivery
Discovery
Email Queries
Execution
Exfiltration
Exploits
Print Spooler RCE
Spoolsv Spawning Rundll32.md
Suspicious DLLs in spool folder...
Suspicious Spoolsv Child Proce...
Suspicious files in spool folder....
AcroRd-Exploits.txt
CVE-2021-36934 usage detecti...
Electron-CVE-2018-1000006.txt
Flash-CVE-2018-4848.txt
Linux-DynoRoot-CVE-2018-11...
MosaicLoader.md
SolarWinds -CVE-2021-35211....
printnightmare-cve-2021-1675...
winrar-cve-2018-20250-ace-file...
winrar-cve-2018-20250-file-cre...
Fun
General queries
Impact
Initial access
Lateral Movement
M365-PowerBi Dashboard
Network
Notebooks
Persistence

Microsoft-365-Defender-Hunting-Queries / Exploits / Print Spooler RCE / Suspicious Spoolsv Child Process.md

dreadphones Update Suspicious Spoolsv Child Process.md da699dc · 3 years ago History

Preview Code Blame 50 lines (48 loc) · 2.18 KB Raw

Suspicious Spoolsv Child Process

Surfaces suspicious spoolsv.exe behavior likely related to CVE-2021-1675

Query

```
// Look for file load events for spoolsv
DeviceImageLoadEvents
| where Timestamp > ago(7d)
| where InitiatingProcessFileName =~ "spoolsv.exe"
| where FolderPath has @"spool\drivers"
| extend LoadFileTime = Timestamp
| distinct DeviceId, LoadFileTime, FileName, SHA256
// Join process data associated with spoolsv launching suspicious proces
| join DeviceProcessEvents on $left.DeviceId == $right.DeviceId
| where Timestamp > ago(7d)
| where Timestamp < LoadFileTime +5m
| where InitiatingProcessFileName =~ "spoolsv.exe"
| where ProcessIntegrityLevel =~ 'SYSTEM'
| where (FileName1 in~("gpupdate.exe", "whoami.exe", "nltest.exe", "task
            "wmic.exe", "taskmgr.exe", "sc.exe", "findstr.exe", "curl.ex
            "wevtutil.exe", "bcdedit.exe", "fsutil.exe", "cipher.exe", "
// Processes with specific FPs removed
(FileName1 =~ "net.exe" and ProcessCommandLine !has "start") or
(FileName1 =~ "cmd.exe" and not(ProcessCommandLine has_any(".spl", "rout
(FileName1 =~ "netsh.exe" and not(ProcessCommandLine has_any("add portop
(FileName1 =~ "powershell.exe" and ProcessCommandLine!has ".spl") or
(FileName1 =~ "rundll32.exe" and ProcessCommandLine != "" and ProcessCom
```

Category

This query can be used to detect the following attack techniques and tactics (see MITRE ATT&CK framework) or security configuration states.

Technique, tactic, or state	Covered? (v=yes)	Notes
Initial access		
Execution		
Persistence		
Privilege escalation	v	
Defense evasion		
Credential Access		

› Privilege escalation
› Protection events
› Ransomware
› TVM
› Troubleshooting
› Webcasts
.gitignore

Discovery		
Lateral movement		
Collection		
Command and control		
Exfiltration		
Impact		
Vulnerability		
Exploit	v	
Misconfiguration		
Malware, component		
Ransomware		