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 processes after
| 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", "taskkill.exe",
            "wmic.exe", "taskmgr.exe", "sc.exe", "findstr.exe", "curl.exe", "wget.
            "wevtutil.exe", "bcdedit.exe", "fsutil.exe", "cipher.exe", "schtasks.ex
// Processes with specific FPs removed
(FileName1 =~ "net.exe" and ProcessCommandLine !has "start") or
(FileName1 =~ "cmd.exe" and not(ProcessCommandLine has_any(".spl", "route add", "pr
(FileName1 =~ "netsh.exe" and not(ProcessCommandLine has_any("add portopening", "ru
(FileName1 =~ "powershell.exe" and ProcessCommandLine!has ".spl") or
(FileName1 =~ "rundll32.exe" and ProcessCommandLine != "" and ProcessCommandLine !(
```

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		
Discovery		
Lateral movement		
Collection		
Command and control		
Exfiltration		
Impact		
Vulnerability		

Exploit	v	
Misconfiguration		
Malware, component		
Ransomware		