Spoolsv suspicious process access

You might need to search for spoolsv.exe suspicious process access when doing the following:

- Detecting print spooler attacks

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data:
  - Windows event logs
  - Microsoft Sysmon

Example

Some attacks such as PrintNightmare take advantage of a critical Windows Print Spooler Vulnerability to gain privilege escalation on the vulnerable machine. This search looks for suspicious process access made by the spoolsv.exe that may be related to the attack.

To optimize the search shown below, you should specify an index and a time range.

1. Ensure you have at least version 6.0.4 of the Sysmon TA. Tune and filter known instances of spoolsv.exe.
2. Run the following search:

```bash
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational EventCode=10 SourceImage = "*\spoolsv.exe" CallTrace = "*\Windows\system32\spool\DRIVERS\x64\*" TargetImage IN ("*\rundll32.exe", "*\spoolsv.exe") GrantedAccess = 0x1fffff | stats count min(_time) AS firstTime max(_time) AS lastTime BY Computer SourceImage TargetImage GrantedAccess CallTrace EventCode
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
Splunk Search

sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

EventCode=10

SourceImage = "**\spoolsv.exe"

CallTrace = "**\Windows\system32\spool\Drivers\x64\*"
TargetImage IN ("**\rundll32.exe", "**\spoolsv.exe")
GrantedAccess = 0x1fffff

| stats count min(_time) AS firstTime max(_time) AS lastTime BY Computer SourceImage TargetImage GrantedAccess CallTrace EventCode

Explanation

Search Sysmon operational data.

Search for a process opening another process.

Search for the spoolsv.exe source image.

Search for CallTrace = AND Target image matches either one OR the other strings IN between the (), AND GrantedAccess = 0x1fffff

Return the first and last times this process occurred and rename those fields as shown. Then, sort first by Computer and then by rest of the fields shown.

Result

Ensure you filter for false positives on this search.

During triage, isolate the endpoint and review for source of exploitation. Capture any additional file modification events.

If your results indicate an attack has occurred, the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.