Spoolsv spawning Rundll32

You might need to search for spoolsv.exe spawning Rundll32 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 use spoolsv.exe to spawn processes, such as rundll32.exe. It is not normal behavior for spoolsv.exe to spawn a process, so this can be an indicator that a print spooler vulnerability has been exploited.

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

1. Ensure you are ingesting information on process that includes the name of the process responsible for the changes from your endpoints into the Endpoint datamodel in the Processes node.
2. Run the following search:

   sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational EventID=1 parent_process_name=spoolsv.exe process_name=rundll32.exe | stats count min(_time) AS firstTime max(_time) AS lastTime BY Computer, User, parent_process_name, process_name, OriginalFileName, process_path, CommandLine

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.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Splunk Search

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

EventID=1

parent_process_name=spoolsv.exe
process_name=rundll32.exe

| stats count min(_time) AS firstTime max(_time) AS lastTime BY Computer, User, parent_process_name, process_name, OriginalFileName, process_path, CommandLine

Explanation

Search Sysmon operational data.

Search for a process creation event.

Search for process rundll32.exe running from spoolsv.exe.

Return the first and last times these processes ran, renaming the fields as shown. Then, sort first by computer and then by the rest of the fields shown.

Result

Be aware that there are limited instances where rundll32.exe may be spawned by a legitimate print driver.

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.