Spoolsv.exe writing a DLL

You might need to search for spoolsv.exe writing a DLL 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 write a DLL (Dynamic-Link Library). This is not normal behavior for spoolsv.exe. This search detects the loaded module made by spoolsv.exe after the exploitation by checking for the suspicious DLL written to disk within a path of `\spool\drivers\x64`.

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

1. Run the following search:

```
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational EventID=11 process_name=spoolsv.exe file_path="*\spool\drivers\x64\*" file_name=*.dll | stats count min(_time) AS firstTime max(_time) AS lastTime BY dest, UserID, process_name, file_path, file_name, TargetFilename
```

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.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR</td>
<td>Search Sysmon operational data.</td>
</tr>
<tr>
<td>Splunk Search</td>
<td>Explanation</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</td>
<td>Searches for when a file has been overwritten.</td>
</tr>
<tr>
<td>EventID=11</td>
<td>Searches for spoolsv.exe writing a .dll within a path of \spool\drivers\x64.</td>
</tr>
<tr>
<td>process_name=spoolsv.exe file_path=&quot;**\spool\drivers\x64** file_name=*.dll</td>
<td>Return the first and last times this process occurred and rename those fields as shown. Then, sort first by destination and then by the rest of the fields shown.</td>
</tr>
<tr>
<td></td>
<td>stats count min(_time) AS firstTime max(_time) AS lastTime BY dest, UserID, process_name, file_path, file_name, TargetFilename</td>
</tr>
</tbody>
</table>

**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.