Print spooler failing to load a plug-in

You might need to search for a print spooler failing to load a plug-in 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

Example

Some attacks such as PrintNightmare cause driver load errors utilizing the Windows PrintService Admin logs. This search detects instances of this taking place.

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

1. Ensure PrintService Admin and operational logs are being logged to Splunk from critical or all systems.
2. Run the following search:

```
source="WinEventLog:Microsoft-Windows-PrintService/Admin"
((ErrorCode="0x45A" (EventCode="808" OR EventCode="4909")) OR ("The print spooler failed to load a plug-in module" OR "\drivers\x64\")
| stats count min(_time) AS firstTime max(_time) AS lastTime BY OpCode EventCode ComputerName Message
```

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>source=&quot;WinEventLog:Microsoft-Windows-PrintService/Admin&quot;</td>
<td>Search Windows PrintService administrative data.</td>
</tr>
<tr>
<td>((ErrorCode=&quot;0x45A&quot; (EventCode=&quot;808&quot; OR EventCode=&quot;4909&quot;)) OR (&quot;The print spooler failed to load a plug-in module&quot;) OR &quot;\drivers\x64&quot;)</td>
<td>Search for events with ErrorCode AND one of two possible EventCodes, and if not found look for events</td>
</tr>
<tr>
<td>Splunk Search</td>
<td>Explanation</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>load a plug-in module&quot; OR &quot;\drivers\x64&quot;)))</td>
<td>with one OR both of two possible strings as shown.</td>
</tr>
<tr>
<td></td>
<td>stats count min(_time) AS firstTime max(_time) AS lastTime BY OpCode EventCode ComputerName Message</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.