Print spooler adding a printer driver

You might need to search for a print spooler adding a printer driver 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 use the print spooler to load printer drivers by utilizing the Windows PrintService operational logs using event code 316. 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/Operational"
   EventCode=316 category = "Adding a printer driver" Message = "*\kernelbase.dll,*" Message = "*\UNIDRV.DLL,*"
   Message = "*.DLL.*"
   | 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/Operational&quot;</td>
<td>Search Windows PrintService operational data.</td>
</tr>
<tr>
<td>EventCode=316</td>
<td>Search for entries logged to the PrintService admin.</td>
</tr>
<tr>
<td>Splunk Search</td>
<td>Explanation</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>category = &quot;Adding a printer driver&quot; Message IN (&quot;*kernelbase.dll,*&quot;, &quot;*UNIDRV.DLL,*&quot;, &quot;*.DLL.*&quot;)</code></td>
<td>Search for message values that include the given strings.</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.