DLL loaded in a specific process

In the case of the Supernova and REvil malware infections, both use the same log and event code that can be used to load DLLs in specific processes. If your environment is ingesting Sysmon data, you can detect the activity of both infections using the following searches.

Required data

- Microsoft Sysmon
- Endpoint data

Procedure

Option 1 - Supernova web shell malware search

Your company uses SolarWinds Orion business software, which is vulnerable to the Supernova in-memory web shell attack. You know that because it runs in memory, detection and forensic analysis post-breach are difficult. You want to identify whether the Supernova trojanized DLL have been loaded to a specific process.

Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
| sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=7 |
| (file_name=*logoimagehandler.ashx* OR SHA256=C15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 OR SHA1=75af292f34789a1c782ea36c7127bf6106f595e8 OR MD5=56ceb6d0011d87b6e4d7023d7ef85676) |
| table _time Image ImageLoaded Computer |
```

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</td>
<td>Search only Sysmon operational data.</td>
</tr>
<tr>
<td>EventCode=7</td>
<td>Search for event code 7, which indicates an image was loaded.</td>
</tr>
</tbody>
</table>

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

(file_name=*logoimagehandler.ashx* OR SHA256=C15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 OR SHA1=75af292f34789a1c782ea36c7127bf6106f595e8 OR MD5=56ceb6d0011d87b6e4d7023d7ef85676)

| table _time Image ImageLoaded Computer |

Search for the file name shown or the hashes associated with the Supernova trojanized DLL.

Display the results in a table with columns in the order shown.

Result

If any results indicate the file or the hashes are detected, then 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 reimaging the system with a known good system build after investigation.

Option 2 - REvil ransomware search

REvil ransomware typically disables Windows Defender. As well as doing this, an older version (circa 2014) of msmpeng.exe (Defender) is being used to sideload REvil into the Kaseya agent software. If you have Sysmon EventCode 7, Image Loaded events, the following search could be helpful to detect this side-loading of malicious DLLs as well.

Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=7 Image="*MsMpEng.exe" ImageLoaded="*mpsvc.dll" SHA256 IN (e2a24ab94f865caeeacdf2c3ad015f3f23008ac6db8312c2cbf32e4a5466ea2, 8dd620d9ae2b35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd)
```

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

| source="WinEventLog:Microsoft-Windows-Sysmon/Operational" |

Search only Sysmon operational data.

EventCode=7

Search for event code 7, which indicates an image was loaded.

Image="*MsMpEng.exe" ImageLoaded="*mpsvc.dll"

Search for the image shown and the hashes associated
Splunk Search

<table>
<thead>
<tr>
<th>SHA256 IN (e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312 c2cbfb32e4a5466ea2, 8dd620d9aeb35960bb766458c8890ede987c33d239cf7 30f93fe49d90ae759dd)</th>
<th>with REvil ransomware.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>table _time Image ImageLoaded Computer</th>
<th>Display the results in a table with columns in the order shown.</th>
</tr>
</thead>
</table>

Results

If any results indicate the file or the hashes are detected, then 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.

Next steps

Finally, you might be interested in other processes associated with these use cases:

- Detecting Supernova web shell malware
- Detecting REvil ransomware infections

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.