Monitoring DNS queries

Applicability

- Product: Splunk Enterprise or Splunk Cloud Platform
- Data type: Microsoft Sysmon
- Function: Endpoint monitoring

Configuration needs to be performed to get the most out of your Sysmon events. You can access templates to help you get started, for example the Swift on Security configuration. You'll also need to install the Splunk Add-On for Microsoft Sysmon.

Problem

You are a security analyst looking to improve threat detection on your endpoints. You already use Sysmon, particularly event code 1, process creation, to gain fidelity into programs starting on your systems, but you know there are other Sysmon events that you may want to utilize during your hunts. You're especially interested in digging more into the detail of DNS queries, which could complement your existing hunt techniques and potentially also help you drive more automation.

Solution

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

1. Run the following search:

   ```
   source="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=22
   EventDescription="DNS Query" host="<hostname>"
   Image="[C:\Program Files(x86)\Microsoft\Edge\Application\msedge.exe]"
   QueryName="<URL>"
   ```

Explanation

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=&quot;xmlwineventlog:microsoft-windows-sysmon/operational&quot;</td>
<td>Search only Sysmon operational data.</td>
</tr>
<tr>
<td>EventCode=22 EventDescription=&quot;DNS Query&quot;</td>
<td>Search for event code 22, DNS queries being executed,</td>
</tr>
</tbody>
</table>
Splunk Search

host="<hostname>"
Image="[C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe]"
QueryName="<URL>"

Explanation

by a specific path on a specific host.

Search for the URL specified.

Result

Here is an example result, showing host bstoll-1 using Microsoft Edge to lookup www.blogger.com and getting an IP address back in response:

![Example Result](image)

In this example, the result is benign, but this search could return both benign and suspicious results. Modifying the image on a suspect host could yield greater insight on domain queries.

Additional resources

The content in this guide comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. In addition, these Splunk resources might help you understand and implement this use case:

- Lantern: Visualizing processes and their parent/child relationships
- Lantern: Monitoring a network for DNS exfiltration
- Blog: A salacious solliloquy on Sysmon
- Blog: Process hunting with a process

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.