.NET assemblies being compiled

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 determine if .NET assemblies are being compiled.

Required data

- Microsoft Sysmon
- Endpoint data

Option 1 - Normalized data

1. Ensure that your deployment is ingesting endpoint logs from your various systems and populating the Endpoint data model.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
| tstats count FROM datamodel=Endpoint.Processes WHERE
  Processes.process_exec=cvtres.exe Processes.parent_process_exec=csc.exe
  groupby Processes.process_exec Processes.process_id Processes.process
  Processes.parent_process_exec Processes.parent_process
  Processes.parent_process_id Processes.dest Processes.user
  Processes.vendor_product _time span=1s
```

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></td>
<td>Query the Endpoint data model for the creation of CSC.exe and CVTRES.exe as child processes during execution of .NET apps.</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.
Option 2 - Microsoft Sysmon

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

1. Ensure that your deployment is ingesting Microsoft Sysmon data.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=1 CommandLine=*cvtres.exe* ParentCommandLine=*csc.exe*
| table _time CommandLine ParentCommandLine User host ProcessId ParentProcessId
```

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=1</td>
<td>Search for event code 1, which indicates process creation.</td>
</tr>
<tr>
<td>CommandLine=<em>cvtres.exe</em> ParentCommandLine=<em>csc.exe</em></td>
<td>Search for the text shown in the command line data and in the parent command line data.</td>
</tr>
<tr>
<td></td>
<td>table _time CommandLine ParentCommandLine User host ProcessId ParentProcessId</td>
</tr>
</tbody>
</table>

Next steps

Because many .NET apps can create CSC.exe and CVTRES.exe as child processes during execution, this is a tactic to hunt, not to deploy as a signature with your SIEM. This is not an indicator of compromise but, it may be worth the time to run this search and then hunt for additional actions occurring immediately after this behavior on vulnerable systems.

Finally, you might be interested in other processes associated with the Detecting Supernova web shell malware use case.