Checking for files created on a system

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 situations where files have been created on a system, 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=11 host=<hostname> process_name=<processname> | table file_create_time file_path process_name host | sort _time
```

Explanation

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>source=&quot;xmlwineventlog:microsoft-windows-sysmon/operational&quot;</code></td>
<td>Search only for Sysmon operational data.</td>
</tr>
</tbody>
</table>
### Splunk Search

**EventCode=11**

Search for event code 11, files created on a system.

**host=<hostname>**

Search on a host you specify.

**process_name=<processname>**

Search for a process name you specify.

| table file_create_time file_path process_name host |
| sort _time |

Display the results in a table with columns in the order shown, sorted by time.

### Result

Here is an example result, showing host ghoppy-1 running a process called setup.exe, with the resulting files created and their associated paths:

This event code can return an excessive number of false positives, depending on which directories and file types it monitors, so you'll need to investigate further to exclude benign results.

### 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](#)