Time elapsed between two related events

The time elapsed between two events on a network or device can be useful when working on the following use cases:

- Investigating a ransomware attack
- Reconstructing a website defacement
- Monitoring command line interface actions

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Microsoft Sysmon

Example

A command line process executed on your network might have exposed the network to a virus. You want to know how much time has passed between the potential exposure and now.

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

1. Run the following search:

```
| sourcetype=“XmlWinEventLog:Microsoft-Windows-Sysmon/Operational” CommandLine=* 
| table _time host CommandLine 
| eval cl_length=len(CommandLine) 
| eval daydiff=round((now()-_time) / 86400, 0)
```

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>Splunk Search</td>
<td>Explanation</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>CommandLine=*</td>
<td>Return logs with a value in the command line field.</td>
</tr>
<tr>
<td></td>
<td>table _time host CommandLine</td>
</tr>
<tr>
<td></td>
<td>eval cl_length=len(CommandLine)</td>
</tr>
<tr>
<td></td>
<td>eval daydiff=round((now()-_time) / 86400, 0)</td>
</tr>
</tbody>
</table>

**Result**

The difference in time can help you determine what other machines and files on your network have been exposed to the virus if they were connected to the network during the same time. You might also need this time difference for reporting purposes.