High process termination frequency

You might need to detect a high frequency of process terminations when doing the following:

- Detecting a ransomware attack
- Detecting Clop ransomware

Prerequisites

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

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Search
- Data: System log data

Example

This search looks for a high frequency of process termination on a machine, which is a common behavior of ransomware malware before encrypting files. This technique is designed to avoid an exception error while accessing files in the infected machine for encryption.

- To optimize the search shown below, you should specify an index and a time range.
- If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

1. Ensure your deployment is ingesting logs with the image (process full path) of terminated process from your endpoints.
2. Run the following search:

```
| search (EventCode=5 (source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational))
| bin _time span=3s
| stats values(Image) AS proc_terminated min(_time) AS firstTime max(_time) AS lastTime count BY Computer EventCode ProcessID
| where (count >= 15)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```
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>search (EventCode=5 (source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational))</td>
<td>Search Sysmon Operational logs for event code 5, process termination events.</td>
</tr>
<tr>
<td>bin _time span=3s</td>
<td>Sort matching events into discrete sets, or bins, with time spans of 3 seconds.</td>
</tr>
<tr>
<td>stats values(Image) AS proc_terminated min(_time) AS firstTime max(_time) AS lastTime count BY Computer EventCode ProcessID</td>
<td>Return the values for the fields shown, sorting first by Computer and then by the rest of the fields shown.</td>
</tr>
<tr>
<td>where (count &gt;= 15)</td>
<td>Return instances where at least 15 processes are terminated at once.</td>
</tr>
<tr>
<td>convert timeformat=&quot;%Y-%m-\dT%H:%M:%S&quot; ctime(firstTime)</td>
<td>Convert these times into readable strings.</td>
</tr>
<tr>
<td>convert timeformat=&quot;%Y-%m-\dT%H:%M:%S&quot; ctime(lastTime)</td>
<td></td>
</tr>
</tbody>
</table>

Result

False positives from this search may occur as legitimate users may terminate multiple processes at once. You will need to create a baseline appropriate to your environment to ascertain what needs further investigation, and perform further searches to establish whether the behaviour is legitimate or anomalous.

If you receive clear positive results from this search, start your incident response process for dealing with a ransomware infection. You should check for recent backups for the systems affected by the infection.