Processes running on a host

As part of a suspected privilege escalation attack, you have identified a suspicious host. You want to collect details about the processes running on this host, starting with the parent processes.

Required data

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Endpoint data model. For information on installing and using the CIM, see the Common Information Model documentation.

Procedure

1. Ensure that your deployment is ingesting endpoint data that tracks process activity, including parent-child relationships, to populate the Endpoint data model in the Processes node. The command-line arguments are mapped to the "process" field in the Endpoint data model.

2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   ```splunk
   |tstats summariesonly=true allow_old_summaries=true count values(Processes.process) AS process min(_time) AS firstTime max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE Processes.process_name = <process_name> Processes.dest = <dest> BY Processes.user Processes.parent_process_name Processes.process_name
   |rename "Processes.*" as "*
   |convert timeformat="%m/%d/%Y %H:%M:%S" ctime(firstTime)
   |convert timeformat="%m/%d/%Y %H:%M:%S" ctime(lastTime)
   ```

3. To investigate all processes, not just parent processes, change the first line of the search to the following and rerun it:

   ```splunk
   |tstats summariesonly=true allow_old_summaries=true count min(_time) max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE Processes.dest=<dest> BY Processes.parent_process
   ```

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>tstats summariesonly=true allow_old_summaries=true count values(Processes.process) AS process</td>
</tr>
</tbody>
</table>
**Splunk Search**

```
min(_time) AS firstTime max(_time) AS lastTime FROM
datamodel=Endpoint.Processes WHERE
Processes.process_name = <process_name>
Processes.dest = <dest> BY Processes.user
Processes.parent_process_name
Processes.process_name
```

**Explanation**

process, and process name on a target machine and
process. The required <dest> field is the host on which
the process is running. The required <process> field is
the process you want to investigate.

```
|rename "Processes.*" as "*"
```

Rename the data model object for better readability.

```
|convert timeformat="%m/%d/%Y %H:%M:%S"
ctime(firstTime)
```

Convert these times into readable strings.

```
|convert timeformat="%m/%d/%Y %H:%M:%S"
ctime(lastTime)
```

Query the Endpoint.Process object for the user, parent
process, and process name on a target machine and
process. The required <dest> field is the host on which
the process is running.

```
|tstats summariesonly=true allow_old_summaries=true
count min(_time) max(_time) AS lastTime FROM
datamodel=Endpoint.Processes WHERE
Processes.dest=<dest> BY Processes.parent_process
Processes.process_name Processes.user
Processes.dest
```

**Next steps**

The search returns all the processes running in a given machine, as well as the first and last time the process ran. This
is a great search to quickly inspect what is running on a system in a given time. This search is typically leveraged during
an investigation of a specific host when the offending process might not be known.

For additional information about this search, such as its applicability to common frameworks and standards, see these
projects on GitHub for parent processes and all processes.

Finally, you might be interested in other processes associated with these use cases:

- Monitoring for signs of Windows privilege escalation attacks
- Creating a timebound picture of network activity
- Detecting techniques in the Orangeworm attack group

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.