Schtasks.exe used to force a reboot

You might need to detect schtasks.exe being used to force a reboot when doing the following:

- Detecting a ransomware attack

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: Endpoint data

Example

Schtasks.exe is Windows' Scheduled Tasks tool. This search looks for flags passed to schtasks.exe on the command line that indicate that a forced reboot of system is scheduled. Ransomware authors have been seen to use schtasks.exe to achieve persistence in compromised environments.

- To optimize the search shown below, you should specify an index and a time range.
- Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation. To run this search, your deployment needs to be ingesting logs with both the process name and command-line from your endpoints to populate the Endpoint data model in the Processes node. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

Run the following search:

```
| rename "Processes.*" AS "*
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

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.
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 allow_old_summaries=true values(&quot;Processes.process&quot;) AS process, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE (&quot;Processes.process_name&quot;=&quot;schtasks.exe&quot; &quot;Processes.process&quot;=&quot;<em>shutdown</em>&quot; &quot;Processes.process&quot;=&quot;*/create *&quot;) BY &quot;Processes.process_name&quot;, &quot;Processes.parent_process_name&quot;, &quot;Processes.dest&quot;, &quot;Processes.user&quot;</td>
</tr>
<tr>
<td></td>
<td>rename &quot;Processes.<em>&quot; AS &quot;</em>&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Result

False positives from this search may occur because administrators may create jobs on systems, forcing reboots to perform upgrades or maintenance for legitimate reasons.

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.

Another tactic you may want to search for is attackers using `schtasks.exe to register binaries or scripts to run from a public directory`. 

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.