Schtasks.exe registering binaries or scripts to run from a public directory

You might need to detect schtasks.exe registering a binary or script to run from a public directory 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 identifies schtasks.exe registering a binary or script to run from a public directory. These public directories include users\public, \programdata\, and \windows\temp. 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 information on process that include the name of the process responsible for the changes from your endpoints, and populating the Endpoint Process data model node.

Run the following search:

```
```
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>| tstats allow_old_summaries=true count, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE (&quot;Processes.process_name&quot;=schtasks.exe OR &quot;Processes.process&quot;=&quot;\users\public* OR &quot;Processes.process&quot;=&quot;\programdata* OR &quot;Processes.process&quot;=&quot;\windows\temp&quot;) OR &quot;Processes.process&quot;=&quot;/create&quot;) BY &quot;Processes.dest&quot;, &quot;Processes.user&quot;, &quot;Processes.parent_process&quot;, &quot;Processes.process_name&quot;, &quot;Processes.process&quot;, &quot;Processes.process_id&quot;, &quot;Processes.parent_process_id&quot;</td>
<td>Query the Endpoint.Processes data model object to search for schtasks.exe registering binaries or scripts to run from users\public, \programdata\ or \windows\ temp. Sort first by destination, then user, parent process, process name, process, process ID, and parent process ID.</td>
</tr>
<tr>
<td>| rename &quot;Processes.<em>&quot; AS &quot;</em>&quot;</td>
<td>Rename data model fields for better readability.</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

When examining your results, review the binary or script in the command line for legitimacy and assess whether it is an approved binary or script or not. You should also capture the binary or script in question and analyze it for further behaviors, as well as identify its source and containing the endpoint.

False positives from this search may be present. You should filter as needed by parent process or command line argument.

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 force a reboot**.