Registry activities

You might want to gather the latest registry values for a specific destination computer when doing the following:

- Monitoring for signs of Windows privilege escalation attacks
- Recognizing improper use of system administration tools

Prerequisites

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.

Example

The registry is a very common place to detect anomalous changes that might indicate compromise or signs of privilege escalation. A search that displays all the registry changes made by a user via reg.exe is a great way to monitor for anomalous changes to the registry.

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

1. Ensure that your deployment is ingesting information on registry changes that include the name of the process responsible for the changes from your endpoints into the Endpoint data model in the Processes and Registry nodes.

2. Run the following search:

```
|tstats summariesonly=true allow_old_summaries=true values(Registry.registry_path) AS registry_path
values(Registry.registry_key_name) AS registry_key_name count FROM datamodel=Endpoint.Registry
WHERE Registry.dest = "<dest>" BY Registry.process_id Registry.dest
|rename "Registry.*" as *
|join [| tstats summariesonly=true allow_old_summaries=true count values(Processes.user) AS user
values(Processes.process_name) AS process_name values(Processes.parent_process_name) AS
parent_process_name FROM datamodel=Endpoint.Processes WHERE Processes.process_name = reg.exe
BY Processes.process_id
|rename "Processes.*" as *]
```

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 summariesonly=true allow_old_summaries=true values(Registry.registry_path) AS registry_path values(Registry.registry_key_name) AS registry_key_name count FROM datamodel=Endpoint.Registry WHERE Registry.dest = &quot;&lt;dest&gt;&quot; BY Registry.process_id Registry.dest</td>
<td>Query the Endpoint.Registry data model object for the process_id and destination that performed the change. The required &lt;dest&gt; field is the IP address of the machine to investigate.</td>
</tr>
<tr>
<td>|rename &quot;Registry.<em>&quot; as &quot;</em>&quot;</td>
<td>Rename the data model object for better readability.</td>
</tr>
<tr>
<td>|join [|tstats summariesonly=true allow_old_summaries=true count values(Processes.user) AS user values(Processes.process_name) AS process_name values(Processes.parent_process_name) AS parent_process_name FROM datamodel=Endpoint.Processes WHERE Processes.process_name = reg.exe BY Processes.process_id |rename &quot;Processes.<em>&quot; as &quot;</em>&quot;]</td>
<td>Correlate registry changes with any process that used reg.exe to perform the changes.</td>
</tr>
</tbody>
</table>

**Result**

The results give the details of the latest registry values for a specific destination computer.

For additional information about this search, such as its applicability to common frameworks and standards, see [this project on GitHub](https://github.com).