Registry key modifications

You might need to identify modifications to registry keys 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

Ransomware can use changes in startup registry keys to launch a program every time the targeted system is started. This tactic can be used, for example, to start a keylogger program that steals a user's passwords, allowing the ransomware attack to take place. This search looks for modifications to registry keys that can be used to launch an application or service at system startup.

- 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 endpoint data that records registry activity from your hosts to populate the Endpoint data model in the Processes node. This is typically populated via endpoint detection-and-response product, such as Carbon Black or endpoint data sources, such as Sysmon. The data used for this search is typically generated via logs that report reads and writes to the registry.

Run the following search:

```bash
| tstats allow_old_summaries=true count, values("Registry.registry_key_name") AS registry_key_name, values("Registry.registry_path") AS registry_path, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Registry WHERE ("Registry.registry_path"=*currentversion\run* OR "Registry.registry_path"=*currentVersion\Windows\AppInit_DLLs* OR "Registry.registry_path"=*CurrentVersion\Winlogon\Shell* OR "Registry.registry_path"=*CurrentVersion\Winlogon\Userinit* OR "Registry.registry_path"=*CurrentVersion\Winlogon\VmApplet* OR "Registry.registry_path"=*CurrentVersion\policies\Explorer\run* OR "Registry.registry_path"=*CurrentVersion\runservices* OR "Registry.registry_path"
```

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.
path"=*\CurrentControlSet\Control\Lsa\* OR "Registry.registry_path"="*Microsoft\Windows NT\CurrentVersion\Image File Execution Options*" OR "Registry.registry_path"=HKLM\SOFTWARE\Microsoft\Netsh\*) BY "Registry.dest", "Registry.user"
| rename "Registry.*" AS "*"
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)

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, values(&quot;Registry.registry_key_name&quot;) AS registry_key_name, values(&quot;Registry.registry_path&quot;) AS registry_path, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Registry WHERE (&quot;Registry.registry_path&quot;=<em>currentversion\run</em> OR &quot;Registry.registry_path&quot;=<em>currentVersion\Windows\Appinit_Dlls</em> OR &quot;Registry.registry_path&quot;=CurrentVersion\Winlogon\Shell* OR &quot;Registry.registry_path&quot;=<em>CurrentVersion\Winlogon\Userinit</em> OR &quot;Registry.registry_path&quot;=<em>CurrentVersion\Winlogon\VmApplet</em> OR &quot;Registry.registry_path&quot;=<em>currentversion\policies\explorer\run</em> OR &quot;Registry.registry_path&quot;=<em>currentversion\runservices</em> OR &quot;Registry.registry_path&quot;=\CurrentControlSet\Control\Lsa* OR &quot;Registry.registry_path&quot;=&quot;<em>Microsoft\Windows NT\CurrentVersion\Image File Execution Options</em>&quot; OR &quot;Registry.registry_path&quot;=HKLM\SOFTWARE\Microsoft\Netsh*)</td>
<td>Query the Endpoint.Registry data model object to search for registry key modifications, and sort by destination then user.</td>
</tr>
<tr>
<td>rename &quot;Registry.<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(lastTime)</td>
<td>Convert these times into readable strings.</td>
</tr>
<tr>
<td>convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(firstTime)</td>
<td></td>
</tr>
</tbody>
</table>

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.
Result

False positives from this search may occur because there are many legitimate applications that must execute on system startup and will use these registry keys to accomplish that task.

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.