Shadow copies deleted

You might need to detect when shadow copies are deleted when doing the following:

- Detect 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

The vssadmin.exe utility is used to interact with the Volume Shadow Copy Service. WMIC is a software utility that allows users to perform Windows Management Instrumentation operations with a command prompt. This search looks for either of these tools being used to delete shadow copies, which are backups of your files and volumes.

- 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 tracks process activity, including parent-child relationships, from your endpoints 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.

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)
```
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 count, values(&quot;Processes.process&quot;) AS process, values(&quot;Processes.parent_process&quot;) AS parent_process, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Processes WHERE ((&quot;Processes.process_name&quot;=vssadmin.exe OR &quot;Processes.process_name&quot;=wmic.exe) &quot;Processes.process&quot;=&quot;delete&quot; &quot;Processes.process&quot;=&quot;shadow&quot;) BY &quot;Processes.user&quot;, &quot;Processes.process_name&quot;, &quot;Processes.parent_process_name&quot;, &quot;Processes.dest&quot;</td>
</tr>
<tr>
<td></td>
<td>rename &quot;Processes.<em>&quot; AS &quot;</em>&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Result

False positives in this search may occur since vssadmin.exe and wmic.exe are standard applications shipped with modern versions of Windows and may be used by administrators to legitimately delete old backup copies, although this is typically rare.

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 ransomware tactic you may want to search for is attackers using wmic.exe to launch processes on remote systems.