Bcdedit boot recovery modifications

You might need to detect modifications to bcdedit.exe 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

This search looks for flags that ransomware passes to bcdedit.exe, a command-line tool for managing boot configuration data (BCD) stores. Ransomware can use this tool to modify Windows error recovery boot configurations on a target machine. This tactic is typically used by ransomware to prevent recovery of encrypted files.

- 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.

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>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

You can tune your search results based on parent process names. False positives in this search may occur because administrators can modify boot configurations 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.