USN journal deletion

You might need to detect deletions of the USN journal 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

The fsutil.exe application is a legitimate Windows utility used to perform tasks related to the file allocation table (FAT) and NTFS file systems. The update sequence number (USN) change journal provides a log of all changes made to the files on the disk. This search looks for fsutil.exe deleting the USN journal, a technique used by attackers to eliminate evidence of files created during post-exploitation activities.

- 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 data that records process activity from your hosts to populate the Endpoint data model in the Processes node. You must also be ingesting logs with both the process name and command line from your endpoints. The command-line arguments are mapped to the Process field in the Endpoint data model.

Run the following search:

```bash
```

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.
**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>rename &quot;Processes.<em>&quot; AS &quot;</em>&quot;</td>
</tr>
<tr>
<td></td>
<td>search (process=&quot;<em>deletejournal</em>&quot; process=&quot;<em>usn</em>&quot;)</td>
</tr>
<tr>
<td></td>
<td>convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(firstTime)</td>
</tr>
<tr>
<td></td>
<td>convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(lastTime)</td>
</tr>
</tbody>
</table>

**Result**

If you find evidence of a ransomware infection 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.

---

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.