Windows event log cleared

You might need to detect Windows events that indicate one of the Windows event logs has been purged 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: Windows event logs

Example

This search looks for Windows events that indicate Windows event logs have been purged. This action is typically used in ransomware attacks by attackers to cover up evidence of malicious activity. Several Windows events are targeted in this search - event code 1100, which indicates an event log service shutdown, as well as codes 104 or 1102, which indicate that the event log was cleared.

- To optimize the search shown below, you should specify an index and a time range.
- To successfully implement this search, your deployment needs to be ingesting Windows event logs from your hosts.

Run the following search:

```plaintext
| search ((EventCode=104 eventtype=wineventlog_system) OR 
(eventtype=wineventlog_security (EventCode=1100 OR EventCode=1102)))
| stats count min(_time) AS firstTime max(_time) AS lastTime BY EventCode dest 
| 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>search ((EventCode=104 eventtype=wineventlog_system) OR (eventtype=wineventlog_security (EventCode=1100 OR EventCode=1102)))</td>
</tr>
<tr>
<td></td>
<td>Search Windows event logs for event code codes 104 or 1102, which indicate that the event log was cleared, or event code 1100, which indicates an event log service shutdown.</td>
</tr>
<tr>
<td></td>
<td>stats count min(_time) AS firstTime max(_time) AS lastTime BY EventCode dest</td>
</tr>
<tr>
<td></td>
<td>Return the values for the fields shown, sorting first by event code, then by destination.</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 these times into readable strings.</td>
</tr>
<tr>
<td></td>
<td>convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(lastTime)</td>
</tr>
</tbody>
</table>

Result

False positives from this search may occur because administrators can clear event logs for legitimate reasons.

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.