Wbadmin delete backup files

You might need to detect flags passed to wbadmin.exe that delete backup files 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

Wbadmin.exe is a command line utility built into Windows to back up and restore operating systems, drive volumes, files, folders, and applications from a command-line interface (CLI). This search looks for flags related to backup file deletions passed to wbadmin.exe. This action is typically used in ransomware attacks to prevent file recovery.

- 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, including parent-child relationships from your endpoints, 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:

```splunk
| rename "Processes.*" AS "*"
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

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>\tstats allow_old_summaries=true count, min(_time) AS firstTime, max(_time) AS lastTime FROM</td>
<td>Query the Endpoint.Processes data model object to search for wbadmin.exe</td>
</tr>
<tr>
<td>datamodel=Endpoint.Processes WHERE</td>
<td>flags seen when backup files are deleted. Sort first by process name, then</td>
</tr>
<tr>
<td>\t rename &quot;Processes.*&quot; AS &quot;**&quot;</td>
<td>Rename data model fields for better readability.</td>
</tr>
<tr>
<td>\t convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(firstTime)</td>
<td>Convert these times into readable strings.</td>
</tr>
<tr>
<td>\t 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 from this search might occur because administrators can boot configuration settings 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.