Wmic.exe launching processes on a remote system

You might need to detect wmic.exe being used to launch processes on a remote system 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

WMIC is a software utility that allows users to perform Windows Management Instrumentation operations with a command prompt. Ransomware authors have been seen to use wmic.exe to gain access to remote systems and then perform processes on it to prepare for or execute the ransomware attack. This search looks for wmic.exe launched with parameters to spawn a process on a remote system to find evidence of the attack.

- 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 records registry 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:

```
```
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></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Result

False positives from this search may occur since the wmic.exe utility is a benign Windows application. It may be used legitimately by administrators with these parameters for remote system administration, but it’s relatively uncommon.

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 tactic you may want to search for is attackers using wmic.exe to delete shadow copies.