Windows accessibility binary modifications

Microsoft Windows contains accessibility features that can be launched with a key combination before a user has logged in. You might want to view all accessibility binaries that have been modified for each Windows host on your network when doing the following:

- Monitoring for signs of Windows privilege escalation attacks

Prerequisites

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Endpoint data model. For information on installing and using the CIM, see the Common Information Model documentation.

Example

You suspect that an adversary has modified or replaced accessibility programs so they can get a command prompt or backdoor without logging in to the system. You need to search for any such modifications.

To optimize the search shown below, you should specify an index and a time range.

1. Ensure that your deployment is ingesting data that records the file system activity from your hosts to populate the Endpoint file-system data model node.
2. If you are using Sysmon, ensure you have a Splunk Universal Forwarder on each endpoint from which you want to collect data.
3. Run the following search:

   ```search
   |tstats summariesonly=true allow_old_summaries=true count min(_time) AS firstTime max(_time) AS lastTime values(Filesystem.user) AS user values(Filesystem.dest) AS dest values(Filesystem.file_path) AS file_path FROM datamodel=Endpoint.Filesystem WHERE (Filesystem.file_path=\"\Windows\System32\sethc.exe\" OR Filesystem.file_path=\"\Windows\System32\utilman.exe\" OR Filesystem.file_path=\"\Windows\System32\osk.exe\" OR Filesystem.file_path=\"\Windows\System32\Magnify.exe\" OR Filesystem.file_path=\"\Windows\System32\Narrator.exe\" OR Filesystem.file_path=\"\Windows\System32\DisplaySwitch.exe\" OR Filesystem.file_path=\"\Windows\System32\AtBroker.exe\") BY Filesystem.file_name Filesystem.dest |rename "Filesystem.*" as "*" |convert timeformat="%m/%d/%Y %H:%M:%S" ctime(lastTime) |convert timeformat="%m/%d/%Y %H:%M:%S" ctime(firstTime)
   ```

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.
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 summariesonly=true allow_old_summaries=true count min(_time) AS firstTime max(_time) AS lastTime values(Filesystem.user) AS user values(Filesystem.dest) AS dest values(Filesystem.file_path) AS file_path FROM datamodel=Endpoint.Filesystem WHERE (Filesystem.file_path=&quot;\Windows\System32\sethc.exe&quot; OR Filesystem.file_path=&quot;\Windows\System32\utilman.exe&quot; OR Filesystem.file_path=&quot;\Windows\System32\osk.exe&quot; OR Filesystem.file_path=&quot;\Windows\System32\Magnify.exe&quot; OR Filesystem.file_path=&quot;\Windows\System32\Narrator.exe&quot; OR Filesystem.file_path=&quot;\Windows\System32\DisplaySwitch.exe&quot; OR Filesystem.file_path=&quot;\Windows\System32\AtBroker.exe&quot;) BY Filesystem.file_name Filesystem.dest ]</td>
<td>Query the Endpoint.Filesystem data model object for any common accessible files that are usually modified by attackers. We print the file's last modification time by the different host and user it was modified by.</td>
</tr>
<tr>
<td>[rename &quot;Filesystem.<em>&quot; as &quot;</em>&quot; ]</td>
<td>Rename the data model object for better readability.</td>
</tr>
<tr>
<td>[convert timeformat=&quot;%m/%d/%Y %H:%M:%S&quot; ctime(firstTime) ] [convert timeformat=&quot;%m/%d/%Y %H:%M:%S&quot; ctime(lastTime) ]</td>
<td>Convert these times into readable strings.</td>
</tr>
</tbody>
</table>

**Result**

Review if any unusual user has modified a windows accessibility binary. Note that Microsoft may provide updates to these binaries. Verify that these changes do not correspond with your normal software update cycle. If a binary has been modified, you might want to collect the hash and analyze it through common malware analysis tools like VirusTotal or Reversing Labs. If you have Splunk SOAR, this action can be automated via a playbook. The [Malware Hunt and Contain playbook](https://github.com/splunk/malware_hunt_contain) provides an example of how to do so.

For additional information about this search, such as its applicability to common frameworks and standards, see [this project on GitHub](https://github.com/splunk/malware_hunt_contain).