Command-line parameters related to web browser credential dumpers

You might need to identify command-line parameters related to web browser credential dumpers when doing the following:

- Detecting indicators of Remcos RAT malware

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- People: Security analyst or Threat hunter
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Endpoint data

Example

This search detects a suspicious process that contains command-line parameters related to a web browser credential dumper. This technique is used by Remcos RAT malware, where it uses the Nirsoft webbrowserpassview.exe application to dump web browser credentials. Remcos use the "/stext" command line to dump the credential in text format. This search is a good indicator of hosts suffering from possible Remcos RAT infection.

- 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). This search requires the Endpoint data model. For information on installing and using the CIM, see the Common Information Model documentation.

Run the following search:

```
```

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>rename &quot;Processes.&quot; AS &quot;*&quot;</td>
<td>Query the Endpoint.Processes data model object to search for the /stext process and other associated processes dumping credentials. Sort first by destination, then by the rest of the fields shown.</td>
</tr>
<tr>
<td>rename &quot;Processes.<em>&quot; AS &quot;</em>&quot;</td>
<td>Rename data model fields for better readability.</td>
</tr>
<tr>
<td>convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(firstTime)</td>
<td>Convert these times into readable strings.</td>
</tr>
</tbody>
</table>
Result

Since this search is based on the parameter command and the possible path where it will save the text credential information, it may present false positives through catching normal tools that are using the same command and behavior.

During triage, isolate the endpoint and review for the source of the exploitation.

If your results indicate an attack has occurred, the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.