Loading of Dynwrapx module

You might need to detect the loading of a Dynwrapx module 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: Microsoft Sysmon or Linux Sysmon

Example

DynamicWrapperX is an ActiveX component that can be used in a VBScript to call Windows API functions. It requires the dynwrapx.dll to be installed and registered. Registering or loading dynwrapx.dll to a host is an indicator of suspicious activity.

This detection returns instances of the DynamicWrapperX or dynwrapx.dll image loaded onto a host.

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

Run the following search:

```
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR source=Syslog:Linux-Sysmon/Operational EventCode=7 (ImageLoaded="*\dynwrapx.dll" OR OriginalFileName="dynwrapx.dll" OR Product="DynamicWrapperX") | stats count min(_time) AS firstTime max(_time) AS lastTime BY Image ImageLoaded OriginalFileName Product process_name Computer EventCode Signed ProcessId | 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>EventCode=7</td>
<td>Search for event code 7, when an image loaded event logs when a module is loaded in a specific process. Search within these logs for potentially suspicious dynwrapx.dll activities.</td>
</tr>
<tr>
<td>(ImageLoaded=&quot;\dynwrapx.dll&quot; OR OriginalFileName=&quot;dynwrapx.dll&quot; OR Product=&quot;DynamicWrapperX&quot;)</td>
<td>Return the values for the fields shown, sorting first by Image and then by the rest of the fields shown.</td>
</tr>
<tr>
<td></td>
<td>stats count min(_time) AS firstTime max(_time) AS lastTime BY Image QueryName QueryStatus process_name QueryResults Computer</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 timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(lastTime)</td>
</tr>
</tbody>
</table>

**Result**

You should treat activity that shows the registering or loading of dynwrapx.dll to a host as highly suspicious. In most instances when it is maliciously used, the best way to triage is to review parallel processes and pivot on the process_guid field.

During triage, isolate the endpoint and review for source of exploitation. Capture any additional file modification events.

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.