Suspicious domains visited by a user

You might need to sift through a large number of websites that a user visited if you suspect that one of them caused a problem on your network when doing the following:

- Investigating a ransomware attack

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- Deep packet inspection data

Example

A user has reported ransomware on her machine. You think that it might have been downloaded from a malicious website.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Stream DNS data. You can replace this source with any other deep packet inspection data used in your organization.

1. Run the following search:

   sourcetype=stream:DNS src=<IP address of infected machine> record_type=A |table _time query{} src dest |reverse

2. In the field sections on the left, find and click query.

3. Examine the websites the user visited.

4. Decide what domains or other results you can eliminate from your search to make your investigation more efficient. For example, Google and Microsoft websites are probably safe. A Whois search can help you decide what domains to whitelist.

5. Update the record_type parameter of your search as necessary. For example, to eliminate all microsoft.com and live.com sites, use:

   record_type=A NOT(query{}=*microsoft.com OR query{}=*live.com)
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>sourcetype=stream:DNS</td>
<td>Search only DNS data from Splunk Stream logs.</td>
</tr>
<tr>
<td>src=&lt;IP address of infected machine&gt;</td>
<td>Search logs coming from the infected machine.</td>
</tr>
<tr>
<td></td>
<td>Logs vary in the information they contain. Not all logs have hostnames or IP addresses. Sometimes the src field will have a hostname in it but sometimes it will have an IP address. Parentheses and OR statements will broaden your search so you don’t miss anything.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>(src=&quot;192.0.2.0&quot; OR src_ip=&quot;192.0.2.0&quot;)</td>
</tr>
<tr>
<td>record_type=A</td>
<td>Search only DNS A records, which return IPv4 addresses.</td>
</tr>
<tr>
<td></td>
<td>table _time query{src dest}</td>
</tr>
<tr>
<td></td>
<td>reverse</td>
</tr>
</tbody>
</table>

Result

The table shows the websites the user visited that might have been the source of the ransomware. Next, you might want to ask the user about the purpose of the suspicious websites and what kind of content they include. If the websites are safe, investigate other possible origins of the problem:

- Removable devices connected to a machine
- File added to the system through external media
- Suspicious script in the command line
- Signature-based threat investigation