TOR traffic

You might need to detect TOR traffic 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: Network protocol data

Example

This search looks for network traffic that runs through The Onion Router (TOR). TOR is a benign anonymity network which can be abused during ransomware attacks to provide camouflage for attackers.

• To optimize the search shown below, you should specify an index and a time range.
• To run this search, you'll need to be ingesting data from firewalls or other network control devices that mediate the traffic allowed into an environment. This is necessary so that the search can identify an 'action' taken on the traffic of interest. The search also requires the Network Traffic data model to be populated. 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.

1. Run the following search:

```
| tstats allow_old_summaries=true count, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Network_Traffic WHERE ("All_Traffic.app"=tor "All_Traffic.action"=allowed) BY "All_Traffic.src_ip", "All_Traffic.dest_ip", "All_Traffic.dest_port", "All_Traffic.action"
| rename "All_Traffic." AS "*
| 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>[ tstats allow_old_summaries=true count, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Network_Traffic WHERE (&quot;All_Traffic.app&quot;=tor &quot;All_Traffic.action&quot;=allowed) BY &quot;All_Traffic.src_ip&quot;, &quot;All_Traffic.dest_ip&quot;, &quot;All_Traffic.dest_port&quot;, &quot;All_Traffic.action&quot; ]</td>
<td>Query the Network Traffic data model object to search for TOR traffic, and sort by source IP, destination IP, destination port and action.</td>
</tr>
<tr>
<td>[ rename &quot;All_Traffic.*&quot; AS *&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) ][ convert timeformat=&quot;%Y-%m-%dT%H:%M:%S&quot; ctime(lastTime) ]</td>
<td>Convert these times into readable strings.</td>
</tr>
</tbody>
</table>

Result

TOR has a number of legitimate uses, from allowing sensitive information to be protected and securely shared, to helping improve data privacy and security. You should check any results showing TOR usage against established policies and processes within your organization to assess whether legitimate usage is occurring.

If you see clear evidence of ransomware in these search results, you will want to start your incident response process for dealing with a ransomware infection. You should check for recent backups for the systems affected by the infection.