Server Message Block (SMB) traffic connection spikes

You might need to detect spikes in the number of Server Message Block (SMB) traffic connections 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

Server Message Block (SMB) is a network file sharing and data fabric protocol. Ransomware authors can use SMB to trick a target machine into contacting a malicious server running inside a trusted network, or to any server outside of the network. This search looks for spikes in the number of Server Message Block (SMB) traffic connections, which can be indicative of ransomware attacks.

- 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). For information on installing and using the CIM, see the Common Information Model documentation. To run this search, your deployment needs to be ingesting your network traffic logs and populating the Network Traffic data model.

Run the following search:

```
| tstats allow_old_summaries=true count FROM datamodel=Network_Traffic WHERE ("All_Traffic.dest_port"=139 OR "All_Traffic.dest_port"=445 OR "All_Traffic.app"=smb) BY _time span=1h, "All_Traffic.src"
| rename "All_Traffic.*" AS "*"
| eventstats max(_time) AS maxtime
| stats count AS num_data_samples max(evaluation(_time => relative_time(maxtime, "-70m@m"), count, null))) AS count avg(evaluation(_time<relative_time(maxtime, "-70m@m"), count, null))) AS avg stdev(evaluation(_time<relative_time(maxtime, "-70m@m"), count, null))) AS stdev BY src
```
eval upperBound=(avg + (stdev * 2)), isOutlier=if(((count > upperBound) AND (num_data_samples >= 50)),1,0)
| where (isOutlier == 1)
| table src, count

**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></td>
<td>tstats allow_old_summaries=true count FROM datamodel=Network_Traffic WHERE (&quot;All_Traffic.dest_port&quot;=139 OR &quot;All_Traffic.dest_port&quot;=445 OR &quot;All_Traffic.app&quot;=smb) BY _time span=1h, &quot;All_Traffic.src&quot;</td>
</tr>
<tr>
<td></td>
<td>rename &quot;All_Traffic.<em>&quot; AS &quot;</em>&quot;</td>
</tr>
<tr>
<td></td>
<td>eventstats max(_time) AS maxtime</td>
</tr>
<tr>
<td></td>
<td>stats count AS num_data_samples max(eval(if(_time &gt;= relative_time(maxtime, &quot;-70m@m&quot;), count, null))) AS count avg(eval(if(_time&lt;relative_time(maxtime, &quot;+70m@m&quot;), count, null)))AS avg stdev(eval(if(_time&lt;relative_time(maxtime, &quot;+70m@m&quot;), count, null))) AS stdev BY src</td>
</tr>
<tr>
<td></td>
<td>eval upperBound=(avg + (stdev * 2)), isOutlier=if(((count &gt; upperBound) AND (num_data_samples &gt;= 50)),1,0)</td>
</tr>
<tr>
<td></td>
<td>where (isOutlier == 1)</td>
</tr>
<tr>
<td></td>
<td>table src, count</td>
</tr>
</tbody>
</table>

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.
False positives from this search may occur because a legitimate file server may experience high-demand loads that could cause this search to trigger.

If you receive clear positive results from this search, start your incident response process for dealing with a ransomware infection. You should check for recent backups for the systems affected by the infection.