IP address sending repeated requests to a web server

You might want to investigate repeated requests to your web server when doing the following.

- Reconstructing a website defacement

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- Web server data

Example

An advanced persistent threat (APT) group has taken over your website and plastered their logo all over your homepage. You want to find the IP address of the machine that scanned your website for the vulnerability that allowed them to attack.

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

1. Run the following search:

   "<URL of affected website>"

2. In the field sections on the left, find and click sourcetype.
3. Click the value with the highest count to add it to the search.
4. Make a note of the other source types.
5. Add the following to the search:

   |stats count(src_ip) AS Requests BY src_ip
   |sort - Requests

6. Make a note of the src_ip with the highest number of requests.
7. Change the sourcetype to one of the others you previously noted and run the search again. Repeat this step with the remaining source types to see if they all indicate the same src_ip with the highest number of requests.

Different data sets provide different perspectives to the same question, so validating findings by using multiple data sets is important.
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>&quot;&lt;URL of affected website&gt;&quot;</td>
<td>Search any log your website name appears in.</td>
</tr>
<tr>
<td></td>
<td>Use wildcards so you don't miss a result. For example, <em>splunk.com</em></td>
</tr>
<tr>
<td>stats count(src_ip) AS Requests BY src_ip</td>
<td>Count the number of times each source IP address appears and rename the count column &quot;Results&quot;.</td>
</tr>
<tr>
<td>sort - Requests</td>
<td>Sort the results with the most common source IP address first</td>
</tr>
</tbody>
</table>

Result

The IP address that originated the most requests is likely to be the one that conducted the scan. Looking at its source header information can help you determine if the IP address is associated with a web vulnerability scanner. Depending on the source type you used in your search, you might also be able to use IDS signatures to further validate your findings. To do so:

1. In the results table, click the source IP address with the most requests.
2. Scroll down the left column of the results page and select the <X> more fields option.
3. If a signature field exists, expand it and look for signatures of known web application vulnerabilities.

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.