Executable uploaded to a web server

You might need to investigate whether files or executables were uploaded to a web server when doing the following:

- Reconstructing a website defacement
- 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
- Web server data

Example

Your web server has been breached by an attacker and you suspect the attacker has uploaded an executable in order to continue the attack. You want to find the executable.

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

1. Run the following search:

   ```plaintext
   sourcetype=stream:http dest=<IP address of infected server> *.exe
   ```

2. In the field sections on the left, find and click `part_filename()`. Then review the values for any suspicious .exe files.

Stream requires special configuration. If you do not see the fields referenced in this procedure, see the Splunk Stream Installation and Configuration Manual on the Splunk documentation site.

3. When you have identified a suspicious file .exe, verify your findings using other sourcetypes. For example, if you found the suspicious executable example.exe, you might search:

   ```plaintext
   sourcetype=suricata dest_ip=<IP address of infected server> http_method=POST .exe
   ```

4. In the field sections on the left, find and click `fileinfo.filename`. Then review the values for the same example.exe executable.

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.
# 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:http</td>
<td>Search only web traffic data from Splunk Stream logs.</td>
</tr>
<tr>
<td>dest=&lt;IP address of infected server&gt;</td>
<td>Search only the affected server.</td>
</tr>
<tr>
<td></td>
<td>Logs vary in the information they contain. Not all logs have hostnames or IP addresses. Sometimes the dest 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>(dest=&quot;192.0.2.0&quot; OR dest_ip=&quot;192.0.2.0&quot;)</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>(dest=&quot;192.0.2.0&quot; OR dest=&quot;example.com&quot;)</td>
</tr>
<tr>
<td>*.exe</td>
<td>Search for executables.</td>
</tr>
<tr>
<td>http_method=POST</td>
<td>Search for a request pushed to the server. In this case, the request is an upload of an executable.</td>
</tr>
</tbody>
</table>

## Result

The result of this search is an executable that you will likely want to investigate further. Clicking on the name of an executable in the results to add it to the search allows you to get other potentially useful information, such as its source IP address. You can use that to corroborate other findings in your investigation.

---

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.