Web activity to and from a host

You might want to gather details about all web activity to and from a host when doing the following:

- Monitoring for signs of Windows privilege escalation attacks
- Detecting techniques in the Orangeworm attack group

Prerequisites

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Web data model. For information on installing and using the CIM, see the Common Information Model documentation.

Example

As part of an insider threat investigation, you want to profile web activity to characterize some specific host activity.

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

1. Ensure that your deployment is ingesting your web traffic and populating the Web data model.
2. Run the following search:

```
|from datamodel Web.Web
|search src=<dest>
```

3. Update the second line of the search to reflect the source, rather than the destination, to gather more information and rerun the search:

```
|search src=<src_ip>
```

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>search src=&lt;dest&gt;`</td>
</tr>
<tr>
<td>Splunk Search</td>
<td>Explanation</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>`</td>
<td>search src=&lt;dest&gt;`</td>
</tr>
</tbody>
</table>

**Result**

This search returns all web traffic for the specific IP addresses. The results show URIs you can investigate to verify maliciousness.

For additional information about this search, such as its applicability to common frameworks and standards, see [this project on GitHub](https://github.com).

---

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.