Connections between network devices and an individual machine

You might need to identify what network devices an individual user machine connected to when doing the following:

- Reconstructing 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
- System log data

Example

A user on your network reports that his machine has been infected with malware. You need to know the user’s machine connected to a file server during the infection to understand the possible scope of the infection.

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

Option 1

1. Run the following search:

   ```
   src=<path to the user's workstation> sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
   ```

2. In the field sections on the left, click EventDescription.
3. Look for a value that indicates a connection to the network, then click it to add it to the search.
4. Add the following command to the search and rerun it:

   ```
   |stats count BY dest_ip
   |sort - count
   ```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the

---

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.
specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>src=&lt;path to the user’s workstation&gt;</td>
<td>Search only connections coming from this user’s workstation.</td>
</tr>
<tr>
<td></td>
<td>If you don’t know the whole path, you can search on the host name first, then examine the src field values to find the path.</td>
</tr>
<tr>
<td>sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</td>
<td>Search only Windows Sysmon operational logs.</td>
</tr>
<tr>
<td></td>
<td>stats count BY dest_ip</td>
</tr>
<tr>
<td></td>
<td>sort - count</td>
</tr>
</tbody>
</table>

**Result**

The table shows all network destinations that the individual connected to during the time range you set.

**Option 2**

1. Set the search time range to the time the infection began, if known.
2. Enter the following search command into the search bar:

```shell
index=<indexname> host=<hostname> sourcetype=winregistry fileshare
```

**Search explanation**

Here is 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>host=&lt;hostname&gt;</td>
<td>Restrict your search to the known infected host.</td>
</tr>
<tr>
<td>sourcetype=winregistry</td>
<td>Search only Windows Registry logs.</td>
</tr>
<tr>
<td>fileshare</td>
<td>Search for results with the “fileshare” string.</td>
</tr>
<tr>
<td></td>
<td>The string “explorer” can also provide relevant results for this scenario.</td>
</tr>
</tbody>
</table>

**Result**

The results include a key_path field that provides the IP address of the fileshare on the network.

You can use this IP address to identify the devices the user connected to and any processes that occurred. This information is useful in determining the scope of the infection.