Malware transfer via Google Chrome

You might need to check for malware transfer via Google Chrome when doing the following:

- Improving Google Chrome security

Prerequisites

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

- People: Security analyst
- Technologies: Splunk Cloud Platform or Splunk Enterprise
- App: Google Chrome Add-on for Splunk

Example

You need to search for scenarios where a user has accessed content considered dangerous, malicious or banned unwanted content. URL to content is configured based on the content path mask, including options to use regular expressions.

Within Google Chrome, this is indicated by the event type `malwareTransferEvent`.

1. Ensure you are using the recommended Splunk Common Information Model (CIM) `Malware` data model with the `Malware_Attacks` dataset. Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the CIM. For information on installing and using the CIM, see the [Common Information Model](#) documentation.

2. Use field mapping to correlate the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>CIM Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>device_user</td>
<td>user</td>
</tr>
<tr>
<td></td>
<td>user_name</td>
</tr>
<tr>
<td></td>
<td>src_user</td>
</tr>
<tr>
<td></td>
<td>src_user_name</td>
</tr>
<tr>
<td>event</td>
<td>change_type</td>
</tr>
</tbody>
</table>
3. Look for examples of activity, for example:

```json
{
  "device_user": "test_user_6",
  "event": "malwareTransferEvent",
  "device_name": "chrome-tests-MacBook-Pro",
  "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4400.10 Safari/537.36",
  "result": "WARNED",
  "url": "https://storage.server.com/malware_file.zip",
  "content_hash": "58BDD769D335053BDF66AB4D4A0EC7541C38FABF00F85EA34542481B887E485F",
  "content_type": "application/zip",
  "content_size": "9973",
  "reason": "DANGEROUS",
  "os_platform": "Mac OS X 10.14",
  "browser_version": "90.0.4400.10",
  "profile_user": "test_user_12@gmail.com",
  "device_id": "C02T45R8GTFL",
  "client_type": "CHROME_BROWSER",
  "time": "1612061495",
  "content_name": "/Users/test_user_6/Downloads/malware_file (38).zip",
  "trigger_type": "FILE_DOWNLOAD"
}
```
Result

Since this event is triggered when the content uploaded or downloaded by the user is considered to be malicious, dangerous, or unwanted, events that appear should be investigated further and assessed against your existing organizational policies.