Google Drive sharing detection

You might need to detect Google Drive sharing when doing the following:

- Detecting Gsuite phishing attacks

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security Analyst, Threat Hunter
- Technologies: Splunk Cloud Platform or Splunk Enterprise
- Technologies: Splunk Add-on for Google Workspace
- Data: GSuite

This type of attack vector requires a logging infrastructure in place configured to ingest Gsuite logs, specifically configured to look at different elements including visibility, owner, and target user parameters. You can view the range of parameters used in these searches [here](#).

Example

This search investigates when someone shares a Google Drive, who shared it, and what was shared in the Google Drive within the company’s domain.

A malicious actor can obfuscate the origin of communication by creating a generic Gsuite account to send emails or share documents. This is why many times significant numbers of file shares, especially containing [phishing related terms](#), may indicate malicious intent.

To optimize the search shown below, you should specify an index and a time range. In addition, many of these searches have to be adjusted per specific environments and specific findings behind a detection, hunt policy which can be customized per timeframe, subdomains, or organizational units.

1. Run the following search:

   ```
   sourcetype="gsuite:drive:json" "parameters.target_user"="[username]" name=change_user_access parameters.target_user
   | spath "parameters_owner"
   | search "parameters_owner"="*"
   | stats count dc(parameters.target_user) as distinct_target BY src_ip parameters.owner parameters.target_user
   parameters.doc_type parameters.doc_title
   | where distinct_target > 50
   ```

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=&quot;gsuite:drive:json&quot; parameters.target_user=[username] name=change_user_access</td>
<td>Using the gsuite drive sourcetype, filter for the username you are investigating. Filter further for the events that have change_user_access set to the name field in the event.</td>
</tr>
<tr>
<td></td>
<td>spath &quot;parameters_owner&quot;</td>
</tr>
<tr>
<td></td>
<td>search &quot;parameters_owner&quot;=&quot;*&quot;</td>
</tr>
<tr>
<td></td>
<td>stats count dc(parameters.target_user) as distinct_target BY src_ip parameters.owner parameters.target_user parameters.doc_type parameters.doc_title</td>
</tr>
<tr>
<td></td>
<td>where distinct_target &gt; 50</td>
</tr>
</tbody>
</table>

### Result

This search may help investigate compromise of accounts by looking at, for example, source ip addresses, document titles and abnormal number of shares and shared target users.

Explore your results by looking at parameters.target_user (users that were shared the document), the type of document (parameters.doc_type), or the title of the document (parameters.doc_title).

If your search returns potentially suspicious results, continue to troubleshoot other methods for [detecting Gsuite phishing attacks](https://example.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.