Google Drive sharing with multiple users

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 returns whether or not a specific user is sharing documents with a single person or multiple people. In many observed Gsuite phishing campaigns, bad actors share malicious documents in significant numbers sometimes to many users at a time, so identifying high amounts of sharing can be an indicator of this type of attack.

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 > 1 | stats count BY email action ip_address parameters.owner parameters.target_user parameters.doc_type parameters.doc_title
```

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.
**Splunk Search**

```
sourcetype="gsuite:drive:json"
"parameters.target_user"="[username]"
name=change_user_access parameters.target_user > 1
```

**Explanation**

Search Gsuite data to find file sharing by a specific person, to single or multiple users.

```
| stats count BY email action ip_address
| parameters.owner parameters.target_user
| parameters.doc_type parameters.doc_title
```

Return count of events grouped by specified fields.

**Result**

If you are experiencing a case of spear or targeted phishing, this search can help you, however further analysis and compensating detections are required in order to narrow the search for the source of the attack.

If your search returns potentially suspicious results, ensure you continue to troubleshoot other methods for detecting Gsuite phishing attacks.