Gsuite calendar invite sharing detection

You might need to detect Gsuite calendar invite 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

Attackers may make phishing attempts via rogue calendar invites. In this use case, the attacker sends multiple invitations via Google Calendar, sometimes with a document attachment. In this case the bad actors often send the calendar invites out in large quantities. This search is designed to detect such scenarios.

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:calendar:json" email=[username] parameters.target_calendar_id > 1
   | stats count BY ip_address email parameters.api_kind parameters.organizer_calendar_id
   | parameters.target_calendar_id parameters.event.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.

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.
### Splunk Search

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype &quot;gsuite:calendar:json&quot; email=[username]</td>
<td>Search for invitations directed to specific users.</td>
</tr>
<tr>
<td></td>
<td>If you use [*] within username, you can find all users.</td>
</tr>
<tr>
<td>parameters.target_calendar_id &gt; 1</td>
<td>Search for the number of invitations sent.</td>
</tr>
<tr>
<td></td>
<td>stats count BY ip_address email parameters.api_kind event_title (parameters.event_title), parameters.target_calendar_id parameters.event.title</td>
</tr>
</tbody>
</table>

### Result

If this search returns a large number of invitations sent, this is potentially suspicious. Ensure you continue to troubleshoot other methods for detecting Gsuite phishing attacks.

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.