Forensic Poster for Google Workspace

Tools, logs, and guidance for investigating Google account compromise

Tools

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 months
Agenda : 6 months
Chat : 6 months
Chrome : 6 months
Cloud Search : 6 months
Accès contextuel : 6 months
Appareils : 6 months (sub)
Drive : 6 months
Gmail : 30 days
Groupes : 6 months
Keep : 6 months
Jamboard : 6 months

Meet : 6 months
Tokens Oauth : 6 months
Règles : 6 months
Utilisateurs : 6 months
Vault : Indefinitely
Voice : 6 months

List : Google Documentation

The Google Workspace logs cannot be deleted/altered by domain administrators.

Hunting

Initial Access

Search for events related to suspicious logins, login failures, or connection attempts on suspended accounts.

Related events :

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

Execution

Search for events related to the creation of "App Script" scripts or the authorization of suspicious third-party applications (OAuth tokens).

Related events :

create_script_trigger, authorize

It is also possible to detect the creation of "script" type files on Drive.

Persistence

Search for the creation of "App Script" scripts, suspicious third-party applications (OAuth tokens), addition of SSH keys, or account modifications.

Related events :

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

Search for traces of data export

Related events :

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

To adapt according to the observed legitimate volume.

Google Workspace Forensic

Forensic Poster for Google Workspace

Tools, logs, and guidance for investigating Google account compromise

OWN

Workspace Attack Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Phishing	Command & Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Internal Spearphishing	Data from Cloud Storage	Exfiltration over Alternative Protocol	Endpoint Denial of Service
Valid Accounts	Scheduled Task/Job	Create Account	Account Manipulation	Impersonation	Forge Web Credentials	Cloud Service Dashboard	Use Alternate Authentication Material	Data from Information Repositories	Exfiltration over Web Service	Financial Theft
		Modify Authentication Process	Valid Accounts	Indicator Removal	Modify Authentication Process	Cloud Service Discovery		Email Collection		Network Denial of Service
		Valid Accounts		Modify Authentication Process	Modify Authentication Process	Permission Groups Discovery				Account Acces Removal
		Scheduled Task/Job		Use Alternate Authentication Material	Multi-Factor Authentication Request Generation	Software Discovery				System Shutdown/ Reboot
				Valid Accounts	Steal Application Access Token					
					Steal Web Session Cookie					
					Unsecured Credentials					