AIRNITE

ZERO DAY

NUMERO 09/2026 · MARKETING E SEO

L'annuncio per gli annunci: come i truffatori si impossessano degli account Google Ads

Alcuni criminali pubblicano annunci Google che si spacciano per Google Ads e così rubano gli account pubblicitari delle aziende, budget compreso. Come funziona la truffa e come possono proteggersi gli inserzionisti.

Pubblicato: 21 novembre 2026 Tempo di lettura: 5 min Autore: Redazione Airnite

// LA SITUAZIONE IN CIFRE

sites.google.com
camuffamento della pagina di phishing
falsa home page di Google Ads su Google Sites (Malwarebytes)

+1 admin
nuovo amministratore nell'account
aggiunto tramite un altro indirizzo Gmail (Malwarebytes)

3
campagne osservate
gruppi dal Brasile e dall'Asia, un terzo forse dall'Europa orientale (Malwarebytes)

50+
annunci fraudolenti segnalati
segnalati a Google da Malwarebytes in pochi giorni

Chi fa pubblicità per un'azienda spesso cerca al volo “Google Ads” su Google e clicca sul primo risultato. È proprio su questo che hanno puntato i criminali descritti a gennaio 2025 dall'azienda di sicurezza Malwarebytes: hanno pubblicato annunci di ricerca a pagamento che si spacciavano per Google Ads, e con questi hanno rubato gli account pubblicitari delle aziende.

// Cosa è successo?

Secondo Malwarebytes, i falsi annunci “sponsorizzati” portavano a una pagina che sembrava la home page di Google Ads, ma era ospitata su **Google Sites** e rimandava a un kit di phishing. Lì le vittime inserivano le proprie credenziali. Malwarebytes definisce la campagna la peggiore operazione di malvertising che l'azienda abbia mai seguito e in pochi giorni ha segnalato a Google **oltre 50 annunci fraudolenti**.

Dietro la truffa ci sono, secondo Malwarebytes, almeno due gruppi principali: un gruppo di lingua portoghese dal Brasile, di gran lunga il più attivo secondo le osservazioni, e un gruppo dall'Asia che usava account pubblicitari di Hong Kong. Una terza campagna, forse dall'Europa orientale, sfruttava un falso CAPTCHA e un'esca a tema Google Authenticator.

// Come funziona l'attacco?

Il trucco sfrutta la fiducia due volte: nei risultati di ricerca di Google e nel dominio di Google. Poiché la pagina di phishing si trovava su sites.google.com, l'indirizzo mostrato nell'annuncio sembrava autentico. Secondo Malwarebytes, il kit di phishing raccoglieva nomi utente, password, cookie e un identificativo univoco.

Con i dati rubati i criminali accedevano e aggiungevano all'account pubblicitario, tramite un altro indirizzo Gmail, un **nuovo amministratore**. A quel punto potevano pubblicare annunci propri con il budget della vittima, spesso altri annunci truffa, e chiudere fuori il legittimo titolare. Secondo Malwarebytes, l'obiettivo dei gruppi è rivendere gli account. Un account pubblicitario con un metodo di pagamento registrato, per i criminali, vale denaro contante.

// Chi è colpito?

Sono colpiti aziende, agenzie e liberi professionisti che usano Google Ads, dal piccolo negozio online al grande gruppo. Il danno è doppio: il budget viene speso per annunci altrui e sotto il proprio nome potrebbero circolare truffe che danneggiano la reputazione. A questo si aggiunge l'onere di recuperare l'account.

Lo schema va oltre Google Ads. Ogni piattaforma la cui pagina di accesso si “cerca al volo su Google” è un bersaglio: account pubblicitari, home banking, servizi cloud, marketplace.

// Cosa fare adesso?

La regola più importante è semplice: non aprite mai le pagine di accesso tramite un annuncio di ricerca, ma da un segnalibro. A questo si aggiungono l'autenticazione a più fattori, il controllo regolare degli utenti nell'account e avvisi che non finiscano dimenticati nella casella di posta. Budget limitati fanno sì che un abuso emerga presto e resti contenuto. La checklist qui sotto riassume i passaggi.

// Come vi aiuta Airnite?

Airnite gestisce **campagne SEA** e mette in sicurezza gli account fin dall'inizio: ruoli, diritti, autenticazione a più fattori, avvisi e limiti di budget. Nella **formazione** i team marketing imparano a riconoscere il phishing tramite annunci e le false pagine di accesso. Con **penetration test** verifichiamo quanto bene i vostri account e accessi sono protetti dai tentativi di presa di controllo.

> Nota: la base è soprattutto il rapporto di Malwarebytes, che non contiene una presa di posizione di Google. Ricerca aggiornata al 21 novembre 2026.

Checklist: cosa fare adesso

[+] Aprite Google Ads solo da un segnalibro o digitando direttamente l'indirizzo, mai tramite un annuncio nei risultati di ricerca.

[+] Prima di ogni accesso controllate la barra degli indirizzi: i veri accessi a Google Ads non passano da sites.google.com.

[+] Attivate l'autenticazione a più fattori per tutti gli account con accesso, preferibilmente con chiavi di sicurezza.

[+] Controllate regolarmente utenti e amministratori dell'account e rimuovete subito gli accessi sconosciuti.

[+] Fate inviare a più responsabili le notifiche di accesso e di modifica dell'account, e prendetele sul serio.

[+] Limitate i budget giornalieri e dell'account e scegliete metodi di pagamento che facciano emergere rapidamente un abuso.

Come vi aiuta Airnite

- SEA – annunci a pagamento – Annunci su Google e Amazon che rendono.
- Formazione – Il vostro team impara i nostri strumenti e processi.
- Penetration test e sicurezza – Attacchi controllati con report chiaro e piano di interventi.

Il vostro account pubblicitario è sicuro quanto il vostro conto in banca?

Airnite gestisce le vostre campagne Google Ads e nel farlo mette in sicurezza l'account: autenticazione a più fattori, ruoli e diritti di accesso puliti, avvisi in caso di modifiche e limiti di budget. In caso di sospetto verifichiamo subito account e accessi.

Richiedete un primo colloquio · Scriveteci un'e-mail · Su WhatsApp

Contatti

Domande su questo articolo? Scriveteci su WhatsApp: +49 174 6834842

Leggi online: https://airnite.de/it/magazine/account-google-ads-violati-malvertising/

Fonti

Ogni fatto riportato in questo articolo si basa sulle fonti seguenti. Le fonti primarie sono contrassegnate.

1. **Malwarebytes · The great Google Ads heist: criminals ransack advertiser accounts via fake Google ads** · 15/01/2025 · FONTE PRIMARIA
   Ricerca sulla sicurezza (primo rapporto): svolgimento, phishing tramite Google Sites, nuovi amministratori, gruppi criminali
   https://www.malwarebytes.com/blog/news/2025/01/the-great-google-ads-heist-criminals-ransack-advertiser-accounts-via-fake-google-ads

2. **BleepingComputer · Hackers use Google Search ads to steal Google Ads accounts** · 2025
   Stampa specializzata: inquadramento della campagna
   https://www.bleepingcomputer.com/news/security/hackers-use-google-search-ads-to-steal-google-ads-accounts/

Informazione redazionale di carattere generale, non costituisce consulenza legale né una verifica specifica dei vostri sistemi. Aggiornato alla data di pubblicazione.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de