AIRNITE

ZERO DAY

NUMÉRO 09/2026 · MARKETING & SEO

La pub pour la pub : comment des escrocs détournent des comptes Google Ads

Des criminels diffusent des annonces Google se faisant passer pour Google Ads et volent ainsi les comptes publicitaires d'entreprises – budget compris. Comment fonctionne l'arnaque et comment les annonceurs se protègent.

Publié le: 21 novembre 2026 Temps de lecture: 5 min Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

sites.google.com
camouflage de la page de phishing
fausse page d'accueil Google Ads sur Google Sites (Malwarebytes)

+1 admin
nouvel administrateur dans le compte
ajouté via une autre adresse Gmail (Malwarebytes)

3
campagnes observées
groupes du Brésil et d'Asie, un troisième peut-être d'Europe de l'Est (Malwarebytes)

50+
annonces frauduleuses signalées
signalées à Google par Malwarebytes en quelques jours

Quiconque fait de la publicité pour son entreprise tape souvent vite « Google Ads » dans Google et clique sur le premier résultat. C'est précisément sur ce réflexe qu'ont misé les criminels décrits par la société de sécurité Malwarebytes en janvier 2025 : ils diffusaient des annonces de recherche payantes se faisant passer pour Google Ads – et volaient ainsi les comptes publicitaires d'entreprises.

// Que s'est-il passé ?

Selon Malwarebytes, les fausses annonces « sponsorisées » menaient à une page ressemblant à l'accueil de Google Ads, mais hébergée sur **Google Sites** et redirigeant vers un kit de phishing. Les victimes y saisissaient leurs identifiants. Malwarebytes qualifie cette campagne d'opération de malvertising la plus flagrante qu'elle ait jamais suivie et a signalé **plus de 50 annonces frauduleuses** à Google en quelques jours.

Selon Malwarebytes, au moins deux groupes principaux sont derrière l'arnaque : un groupe lusophone du Brésil, de loin le plus actif selon ses observations, et un groupe d'Asie utilisant des comptes publicitaires de Hong Kong. Une troisième campagne, peut-être d'Europe de l'Est, utilisait un faux CAPTCHA et un leurre Google Authenticator.

// Comment fonctionne l'attaque ?

L'astuce exploite deux fois la confiance : dans les résultats de Google et dans le domaine Google. Comme la page de phishing se trouvait sur sites.google.com, l'adresse affichée dans l'annonce semblait authentique. Selon Malwarebytes, le kit collectait noms d'utilisateur, mots de passe, cookies et un identifiant unique.

Avec ces données, les auteurs se connectaient et ajoutaient au compte publicitaire un **nouvel administrateur** via une autre adresse Gmail. Ils pouvaient alors diffuser leurs propres annonces avec le budget de la victime – souvent d'autres annonces frauduleuses – et bloquer le titulaire légitime. Selon Malwarebytes, les groupes visent à revendre les comptes. Un compte publicitaire avec un moyen de paiement enregistré vaut de l'argent comptant pour des criminels.

// Qui est concerné ?

Sont concernés les entreprises, agences et indépendants utilisant Google Ads – de la petite boutique en ligne au grand groupe. Le préjudice est double : le budget finance les annonces d'autrui, et une fraude peut circuler sous votre nom, au détriment de votre réputation. S'y ajoute l'effort pour récupérer le compte.

Le schéma dépasse Google Ads. Toute plateforme dont on « cherche vite » la page de connexion est une cible : comptes publicitaires, banque en ligne, services cloud, places de marché.

// Que faire maintenant ?

La règle essentielle est simple : ne jamais ouvrir une page de connexion via une annonce, toujours via un favori. Ajoutez l'authentification multifacteur, un contrôle régulier des utilisateurs du compte et des alertes qui ne se perdent pas dans la boîte de réception. Des budgets plafonnés font qu'un abus se remarque vite et reste limité. La check-list ci-dessous résume les étapes.

// Comment Airnite vous aide-t-il ?

Airnite gère des **campagnes SEA** et sécurise les comptes dès le départ : rôles, droits, authentification multifacteur, alertes et plafonds de budget. En **formation**, les équipes marketing apprennent à reconnaître le phishing par annonces et les fausses pages de connexion. Avec des **tests d'intrusion**, nous vérifions la protection de vos comptes et accès contre les tentatives de prise de contrôle.

> Remarque : la base est principalement le rapport de Malwarebytes ; il ne contient pas de déclaration de Google. État de la recherche : 21 novembre 2026.

Check-list : ce qu'il faut faire maintenant

[+] N'ouvrir Google Ads que via un favori ou en saisissant l'adresse – jamais via une annonce dans les résultats de recherche.

[+] Vérifier la barre d'adresse avant chaque connexion : les vraies connexions Google Ads ne passent pas par sites.google.com.

[+] Activer l'authentification multifacteur pour tous les comptes ayant accès, idéalement avec des clés de sécurité.

[+] Contrôler régulièrement les utilisateurs et administrateurs du compte et supprimer immédiatement tout accès inconnu.

[+] Faire envoyer les alertes de connexion et de modification à plusieurs responsables – et les prendre au sérieux.

[+] Plafonner les budgets quotidiens et du compte et choisir des moyens de paiement qui révèlent vite un abus.

Comment Airnite vous aide

- SEA – publicité payante – Des annonces Google et Amazon rentables.
- Formations – Votre équipe apprend nos outils et méthodes.
- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.

Votre compte publicitaire est-il aussi sûr que votre compte bancaire ?

Airnite gère vos campagnes Google Ads et sécurise le compte en même temps : authentification multifacteur, rôles et droits d'accès propres, alertes en cas de modification et plafonds de budget. Au moindre soupçon, nous vérifions immédiatement le compte et les accès.

Demander un premier échange · Écrire un e-mail · Par WhatsApp

Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/comptes-google-ads-pirates-malvertising/

Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.

1. **Malwarebytes · The great Google Ads heist: criminals ransack advertiser accounts via fake Google ads** · 15/01/2025 · SOURCE PRIMAIRE
   Recherche en sécurité (rapport initial) : déroulé, phishing via Google Sites, nouveaux administrateurs, groupes
   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
   Presse spécialisée : contexte de la campagne
   https://www.bleepingcomputer.com/news/security/hackers-use-google-search-ads-to-steal-google-ads-accounts/

Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.

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