Los expertos en ciberseguridad han emitido una alerta sobre una nueva campaña de publicidad maliciosa (malvertising) que apunta a usuarios y empresas que utilizan Google Ads. Esta operación busca robar credenciales mediante anuncios fraudulentos que se hacen pasar por legítimos dentro de la plataforma de Google.

> *«El objetivo del esquema es comprometer la mayor cantidad posible de cuentas de anunciantes, haciéndose pasar por Google Ads y redirigiendo a las víctimas a páginas falsas de inicio de sesión»,* explicó Jérôme Segura, director senior de inteligencia de amenazas en Malwarebytes, en un informe.

Se cree que la intención detrás de este ataque es reutilizar las credenciales robadas para llevar a cabo nuevas campañas fraudulentas, además de vender esta información a otros actores delictivos en foros clandestinos. Según reportes en plataformas como Reddit, Bluesky y los foros de soporte de Google, esta amenaza ha estado activa desde al menos mediados de noviembre de 2024.

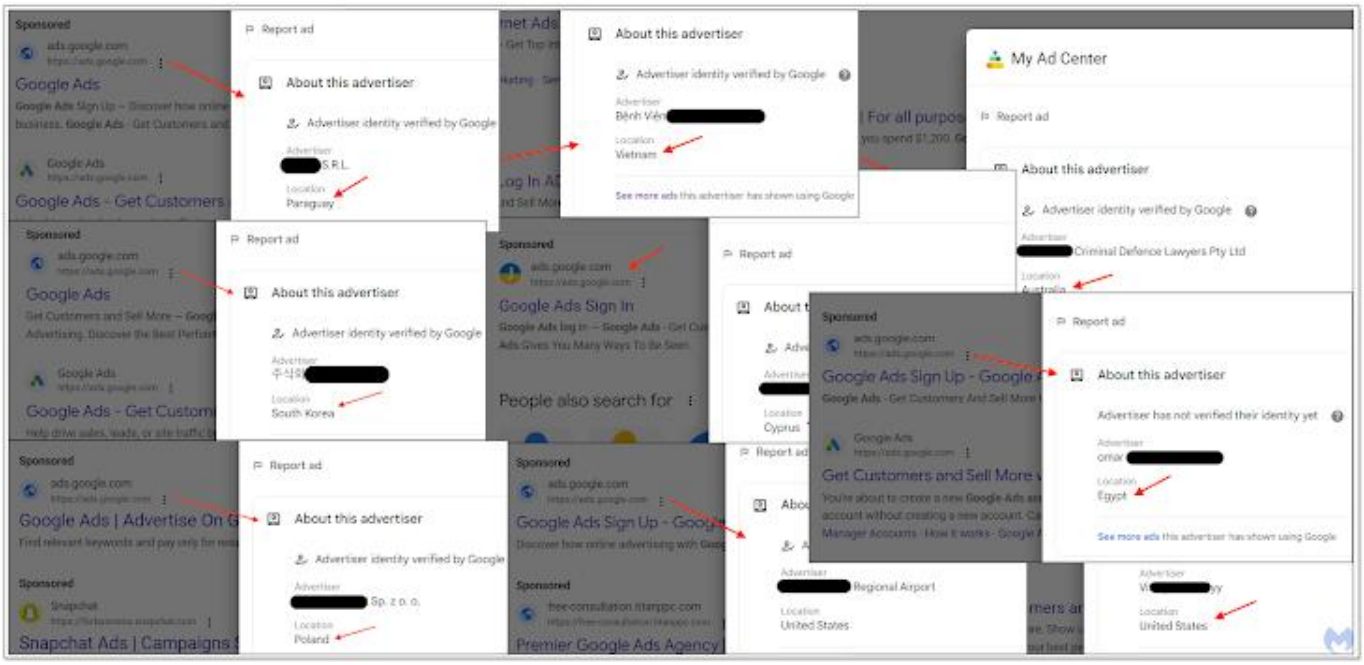
El método utilizado recuerda a otras campañas que emplean malware tipo «stealer» para obtener acceso a cuentas de publicidad y negocios en Facebook. Estas cuentas secuestradas luego se usan para lanzar campañas de malvertising que ayudan a propagar más malware.

Cómo funciona esta campaña

El ataque está dirigido a personas que buscan «Google Ads» en el motor de búsqueda de Google. Los atacantes colocan anuncios falsos que, al hacer clic en ellos, redirigen a los usuarios a sitios fraudulentos alojados en Google Sites.

Estos sitios fraudulentos actúan como páginas de entrada para guiar a los usuarios hacia sitios externos diseñados para robar credenciales y códigos de autenticación en dos pasos (2FA). Los datos capturados son enviados a servidores remotos controlados por los atacantes mediante WebSocket.

> *«Los anuncios falsos para Google Ads son creados por diversos individuos y negocios (incluyendo incluso un aeropuerto regional) ubicados en distintas regiones. Algunas de estas cuentas ya estaban operando cientos de anuncios legítimos»*, mencionó Segura.



Un aspecto particularmente astuto de esta campaña es que explota una característica de Google Ads que permite que la URL visible del anuncio no coincida completamente con la URL final, siempre que pertenezcan al mismo dominio. Esto permite a los atacantes alojar páginas intermediarias en sites.google[.]com mientras muestran URLs visibles como ads.google[.]com. Además, utilizan técnicas avanzadas como huellas digitales, detección de bots, señuelos tipo CAPTCHA, y métodos de ocultación para disfrazar su infraestructura de phishing.

Uso de las credenciales comprometidas

Según Malwarebytes, las credenciales robadas son empleadas para acceder a las cuentas de

Google Ads de las víctimas, añadir nuevos administradores y aprovechar sus presupuestos publicitarios para promocionar anuncios falsos.

En resumen, los atacantes están tomando el control de cuentas de Google Ads para publicar sus propios anuncios fraudulentos, lo que aumenta el número de víctimas en un ciclo continuo de hackeo de cuentas utilizadas para perpetuar la estafa.

> *«Hay varios grupos o individuos involucrados en estas campañas. La mayoría de ellos hablan portugués y probablemente operan desde Brasil. La infraestructura de phishing utiliza dominios intermediarios con la extensión .pt, lo que sugiere una conexión con Portugal»,* señaló Segura.

Falta de acción de Google y nuevas amenazas

> *«Esta actividad maliciosa no infringe las normas publicitarias de Google, ya que se permite mostrar URLs engañosas en los anuncios, haciéndolos prácticamente indistinguibles de sitios legítimos. Hasta ahora, Google no ha tomado medidas contundentes para suspender estas cuentas comprometidas hasta que se solucione el problema de seguridad»,* añadió Segura.

Paralelamente, Trend Micro ha informado sobre el uso de plataformas como YouTube y SoundCloud para distribuir enlaces a instaladores falsos de software pirateado. Estos instaladores conducen a la instalación de malware como Amadey, Lumma Stealer, Mars Stealer, Penguish, PrivateLoader y Vidar Stealer.

> *«Los atacantes suelen aprovechar servicios de almacenamiento de archivos confiables como Mediafire y Mega.nz para ocultar el origen del malware y dificultar su detección. Muchas descargas maliciosas están protegidas con contraseñas y codificadas, lo que complica su análisis en entornos de seguridad como sandboxes*

> *y permite que evadan la detección inicial»,* explicó la empresa.