BOLETÍN DE ALERTA

Boletín Nro.: 2022-42
Fecha de publicación: 21/10/2022
Tema: Atacantes utilizan publicidad (Ads) de Google como medio para propagar *phishing*

Descripción:

Últimamente en nuestro país se ha notado un aumento en el abuso de anuncios publicitarios de Google (Ads) para la propagación de sitios de *phishing*, especialmente de sitios web que representan a entidades financieras locales.

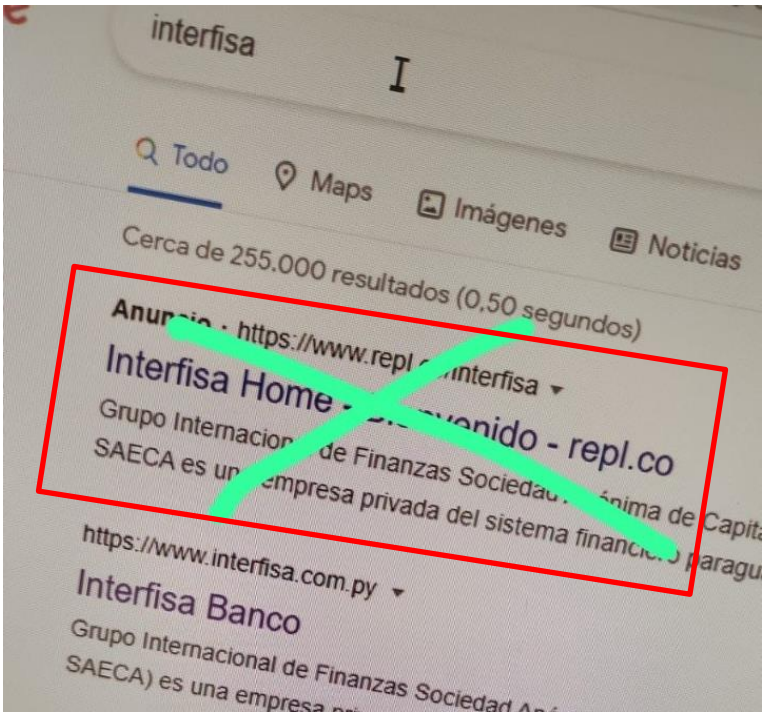
Modalidades de fraude más habituales a través de Google Ads:

- **Inicio de sesión al homebaking falsificado**

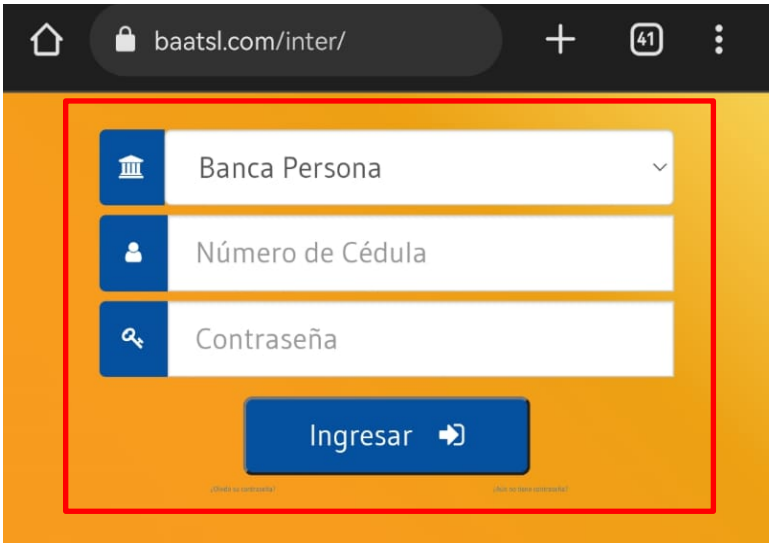
El estafador coloca un anuncio falso de Google Ads en las primeras posiciones de una búsqueda en el navegador, haciéndose pasar por un anuncio de la página de inicio de sesión oficial de un banco de plaza. Una vez ingresado a la página falsa igual o similar a la original, el usuario introduce su usuario y contraseña con confianza, sin notar que está entregando sus datos al atacante.

Ejemplos de anuncios de Google fraudulentos contra Entidades Bancarias paraguayas:


Google
atlas
Todos
Maps
Imágenes
Noticias
Videos
Libros
Patrocinado
catlas.cosmepro.repl.co
https://catlas.cosmepro.repl.co
Banco - Atlas
Con las mejores promociones que tenemos para ti. Estamos para ayudarte a ti y a tu familia.
bancoatlas.com.py
https://www.bancoatlas.com.py
Banco Atlas
Bienvenido a Banco Atlas S.A.Somos el banco paraguayo, con más de 27 años de experiencia en el rubro financieroque se ha consolidado con un crecimiento ...


interfisa
Todo
Maps
Imágenes
Noticias
Cerca de 255.000 resultados (0,50 segundos)
Interfisa Home
repl.co
https://www.interfisa.com.py
Interfisa Banco
Grupo Internacional de Finanzas Sociedad

Se puede visualizar que el inicio de sesión desplegado en el sitio web del atacante es muy similar al de la entidad víctima:



A continuación, compartimos otra página de homebanking falsificada utilizada en anuncios publicitarios:

Impacto:

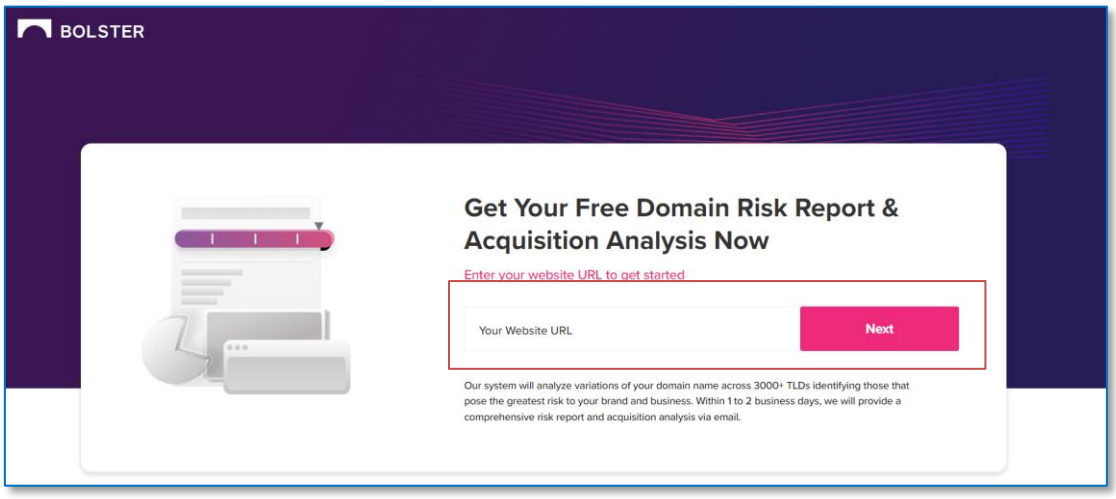
La explotación de este método permitiría a un atacante robar contraseñas o datos bancarios, a través del servicio de anuncios de Google Ads.

Detección y Protección:

Si bien la utilización de Ads o anuncios publicitarios de Google es frecuente como estrategia de marketing, también se trata de un tipo de propagación de *phishing* poco conocido y por ello es importante ser consciente de su existencia para evitar ser víctima del mismo. Los estafadores se están volviendo cada vez más sofisticados a la hora de lograr que sus sitios web parezcan legítimos. Es difícil estar seguro de que le han dirigido a un sitio web de *phishing*. Sin embargo, hay algunos signos que se podrían tener en cuenta para identificar el *phishing* a través de Google Ads.

- **Recomendaciones para empresas/marcas:**
    - Verificar regularmente las palabras que estén relacionadas con la marca de la entidad en los resultados de búsquedas del navegador.
    - Monitorear constantemente los resultados de los registros de dominios similares al del sitio web oficial de la entidad, teniendo en cuenta que estos dominios podrían ser utilizados para realizar anuncios publicitarios fraudulentos.

Un ejemplo de herramienta que se encarga de realizar monitoreos para los registros de dominios es Bolster.



- **Recomendaciones generales:**

  - Comprobar siempre la URL del sitio web que se desee visitar. Por lo general, la URL de un sitio de *phishing* aparenta ser correcta, pero a menudo contiene fallos en la ortografía o tiene un carácter/símbolo diferente al nombre auténtico dentro de la misma. Por ejemplo, *www.1uno.com* en lugar de *www.luno.com*.
  - Leer atentamente los anuncios de Google antes de hacer clic, observando con atención que el nombre de la empresa en la URL debajo del encabezado del anuncio sea correcto.
  - En caso de ingresar a un sitio web de un anuncio, en el que se despliega inmediatamente una ventana emergente que solicita que ingreses tus datos de inicio de sesión o información personal, es probable que se trate de un sitio web de *phishing*.
  - Tener en cuenta que el icono de un candado cerrado a la izquierda de la URL no es necesariamente un signo fiable de un sitio web, sino solamente indica que el sitio web posee un certificado de confianza.
  - Verificar el contenido del sitio web ingresado, ya que a menudo es posible que contengan errores tipográficos y errores gramaticales, que pudieran ser indicios de *phishing*.
  - En caso de sospechar del sitio web, comprobar ingresando una contraseña falsa en el formulario proveído. Si esta funciona e inicia sesión, es probable que estés en un sitio de *phishing*.
  - Utilizar un navegador con una extensión de detección *anti-phishing,* que pueda ayudar a detectar sitios de *phishing*. Sobre todo, si hay sospechas de *phishing* en Google Ads, algunos ejemplos son:
    - Ads Link Skiper, disponible para Chrome.
    - Adfly Skipper, disponible para Firefox.
    - Universal Bypass, disponible para Mozilla Firefox y Microsoft Edge.
  - En caso de serios indicios o de haber sido víctima de un ataque de *phishing* a través de un anuncio de Google, puede realizar las siguientes acciones:
    - Bloquear el anuncio como indica Google aquí.
    - Denunciar el anuncio a través del formulario indicado por Google.
    - Reportar a abuse@cert.gov.py.

Adicionalmente, para detectar y prevenir ataques de *phishing* en general, recomendamos seguir la siguiente guía que hemos elaborado con relación a este tipo de ataques:

- https://www.cert.gov.py/wp-content/uploads/2022/07/Guia_de_Seguridad_de_prevencion_de_phishing.pdf

Información adicional:

- https://www.cert.gov.py/noticias/campana-de-phishing-contra-clientes-de-bancos-paraguayos/
- https://www.cert.gov.py/noticias/phishing-a-traves-de-tunelizacion-inversa-y-acortadores/
- https://www.cert.gov.py/wp-content/uploads/2022/07/Guia_de_Seguridad_de_prevencion_de_phishing.pdf
- https://www.bluecaribu.com/phishing-en-adwords
- https://www.mcafee.com/blogs/es-es/internet-security/ejemplos-de-phishing-como-detectar-un-correo-de-phishing/#:~:text=El%20phishing%20siempre%20se%20basa,de%20las%20pistas%20m%C3%A1s%20frecuentes.
- https://twitter.com/InterfisaPY/status/1582844107327692815?s=20&t=XKGUM5FcKgi_C-IUOEtx-A
- https://securityboulevard.com/2022/05/how-scammers-use-google-ads-to-target-brands-customers/
- https://support.google.com/google-ads/answer/7660847?hl=es-419#:~:text=Complete%20el%20formulario%20Informar%20un,medidas%20necesarias%20respecto%20del%20anuncio.
- https://www.antevenio.com/blog/2019/04/phishing-en-google-ads/
- https://bolster.ai/domain-risk-report?utm_source=blog&utm_medium=web&utm_campaign=&utm_content=google-ads-scam