BOLETÍN DE ALERTA

Boletín Nro.: 2022-25
Fecha de publicación: 08/06/2022
Tema: Phishing a través de tunelización inversa y acortadores

Descripción:

Se ha reportado un aumento significativo de casos de utilización de técnicas que involucran acortadores de URL y servicios de tunelización inversa, en campañas de phishing a una gran escala, volviéndose más difícil de detectar. Esta práctica se ha encontrado en más de 500 sitios. Además, últimamente hemos detectado la utilización de esta técnica ampliamente en correos de phishing para atacar a clientes de bancos paraguayos.

Las páginas se enrutan desde las computadoras de los delincuentes a través de servicios de túnel inverso como *Ngrok, Cloudflare Argo y LocalhostRun*, que ocultan las conexiones y permiten el acceso remoto a las páginas locales. Luego, los enlaces se integran en servicios de acortadores de URL como *Bit.ly, is.gd y cutt.ly*, generalmente con caracteres aleatorios y resultados generados automáticamente.

Los servicios de túnel inverso protegen el sitio de phishing al manejar todas las conexiones al servidor local en el que está alojado. De esta forma, cualquier conexión entrante es resuelta por el servicio de túnel y reenviada a la máquina local del delincuente. Las víctimas que interactúan con estos sitios de phishing terminan con sus datos confidenciales almacenados directamente en la computadora del atacante.

Mediante el uso de acortadores de URL, el actor de amenazas enmascara el nombre de la URL, que suele ser una cadena de caracteres aleatorios. Así, un nombre de dominio que levantaría sospechas se oculta en una URL corta.

Impacto:

La explotación de este método permitiría a un atacante robar contraseñas o datos bancarios, mediante servicios de túnel inverso con URL acortadas. Estos acortadores se actualizan constantemente para no ser bloqueados ni detectados.

Detección y Protección:

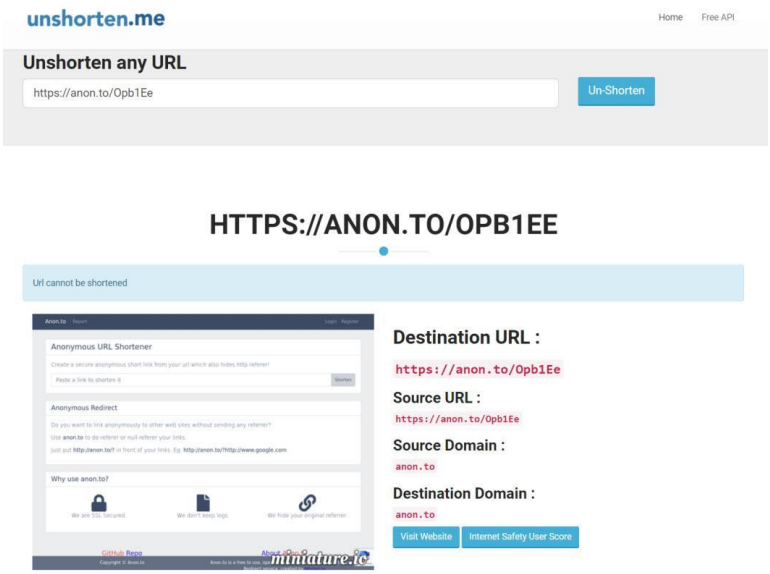
Los delincuentes están distribuyendo enlaces falsos a través de canales de comunicación populares como WhatsApp, Telegram, correos electrónicos, mensajes de texto o páginas de redes sociales falsas. Evitar hacer clic en enlaces que lleguen por estos medios de desconocidos y no descargar archivos adjuntos sin verificar. Lo mismo ocurre con los

mensajes directos, incluso si provienen de contactos conocidos. Así también, evitar iniciar sesión a través de fuentes que no sean fiables.

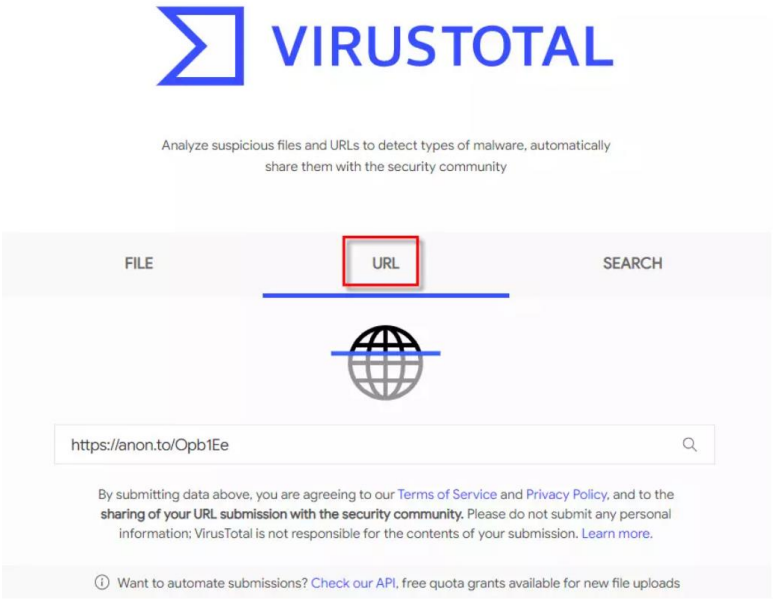
Verificar que los enlaces estén alojados en dominios legítimos y pertenezcan a la organización que dice enviar. En lo posible, siempre utilizar páginas web oficiales y/o aplicaciones legítimas para el envío de datos personales, información bancaria o para realizar compras y/o algún tipo de transacción.

Mitigación:

- Utilizar herramientas que comprueben si la URL acortada es real, algunas de las mismas son:
  - ***Unshorten.me*:** Es un sitio web bastante sencillo, que nos muestra que hay detrás de cada enlace acortado, indicando el enlace original, una vista previa:



  - ***VirusTotal*:** es un servicio bastante útil para trabajar con enlaces acortadores, se debe seleccionar la pestaña URL para comprobar si es un enlace seguro, al final del análisis se obtendrá un resultado distintos motores mostrarán si han visto algo malo en nuestro link:



Nota: Puede visualizar la lista completa de todas las herramientas que pueden ser utilizadas para la comprobación de URL en el siguiente enlace.

- Utilizar extensiones de navegadores para bloquear la publicidad en los enlaces acortados:
  - *Ads Link Skiper*, disponible para Chrome.
  - *Adfly Skipper*, disponible para Firefox.
  - *Universal Bypass*, disponible para Mozilla Firefox y Microsoft Edge.
- Desarrolladores/dueños de plataformas digitales:
  - Evaluar la posibilidad de implementar autenticación de 2 factores (2FA) basado en TOTP u otros para el inicio de sesión de sus usuarios.

Información adicional:

- https://www.tecnobreak.com/las-nuevas-estafas-de-phishing-utilizan-tacticas-para-ocultar-las-url-de-las-aplicaciones-de-seguridad/
- https://blog.segu-info.com.ar/2022/06/phishing-traves-de-tunelizacion-inversa.html
- https://www.redeszone.net/noticias/seguridad/nueva-estrategia-phishing-robar/
- https://www.redeszone.net/tutoriales/seguridad/direccion-url-real-enlaces-acortados/