Informe de phishing de Zscaler ThreatLabz de 2023

Contenido

Resumen ejecutivo 3
- Hallazgos clave 4

Principales objetivos de phishing en 2022 5

Evolución de las tendencias de phishing 9
- Ataques de vishing 9
- Estafas en la contratación 12
- Ataques de phishing de tipo Adversary-in-the-Middle (AiTM) 14
- Ataques de phishing tipo Browser-in-the-Browser (BiTB) 15
- Uso de servicios válidos para alojar sitios web de phishing 16
- Phishing mediante el sistema de archivos interplanetario (IPFS) 17
- Uso de WebSockets para exfiltrar datos de huellas digitales 18
- Uso de servicios de formularios basados en la web para obtener credenciales 20
- Phishing mediante contrabando de HTML y archivos SVG 21
- Herramientas y técnicas de phishing 22

Predicciones para 2024 25

Mejore su protección contra el phishing 26
- Mejores prácticas: Capacitación para aumentar el conocimiento en materia de seguridad 27
- Mejores prácticas: Controles de seguridad 28
- Mejores prácticas: Cómo identificar una página de phishing 29

Cómo Zscaler Zero Trust Exchange™ puede mitigar los ataques de phishing 31
- Productos de Zscaler relacionados 32

Acerca de ThreatLabz 33

Acerca de Zscaler 34

ANEXO

Categorización de los ataques de phishing 35
- Categorización de los ataques de phishing 35
- Principales estafas de phishing 38

Resumen ejecutivo

Las estafas de phishing son una amenaza creciente, y los métodos de los ciberdelincuentes son cada vez más sofisticados, lo que los hace más difíciles de detectar y bloquear.

Tras analizar 280,000 millones de transacciones diarias y 8,000 millones de ataques diarios bloqueados en el transcurso de 2022, el equipo de Zscaler ThreatLabz observó un aumento del 47.2% en los intentos de phishing en comparación con 2021, una tendencia al alza que se espera que continúe en 2023.

El aumento de la prevalencia de los kits de phishing procedentes de los mercados negros y de herramientas de IA de chatbot como ChatGPT ha permitido a los atacantes crear rápidamente campañas de phishing más selectivas. Esta focalización mejorada ha simplificado el proceso de manipulación de los usuarios para que realicen acciones que comprometan sus credenciales de seguridad, dejándolos a ellos y a sus organizaciones vulnerables.

Con el auge de la IA y las ofertas de PaaS, es más fácil que nunca para los ciberdelincuentes poner en peligro las instituciones y acceder a datos empresariales, personales y financieros sensibles con fines de extorsión. Aunque muchas de las organizaciones actuales cuentan con infraestructuras de ciberseguridad sólidas, deben revaluarlas en función de las tendencias actuales y plantearse adoptar un modelo de confianza cero.

Este informe le ayudará a reconocer las tácticas de ingeniería social y la sofisticada codificación utilizada en los ataques de phishing, para que pueda evitar filtraciones de datos costosas. Siga leyendo para conocer en detalle las últimas tendencias del phishing y las observaciones que el equipo de ThreatLabz recopiló durante el año pasado, y obtenga las mejores prácticas para salvaguardar su organización frente a las técnicas de phishing en constante evolución.

Principales hallazgos en 2022

Los ataques de phishing aumentaron un 47.2% en 2022 con respecto a 2021.

Las marcas de Microsoft, incluidas OneDrive y Sharepoint, junto con el intercambio de criptomonedas Binance y los servicios de transmisión ilegal, fueron las más atacadas.

Estados Unidos, el Reino Unido, los Países Bajos, Rusia y Canadá fueron los cinco países que sumaron más ataques.

La educación fue el sector más atacado, con un aumento de los ataques del **576 %**, mientras que el principal objetivo del año pasado, el comercio minorista y mayorista, se redujo en un **67 %**.

Los ataques a marcas relacionados con el covid representaron el **7.2 %** de las estafas de phishing en 2021, mientras que estas se redujeron a solo **el 3.7 %** en 2022.

Las herramientas de IA han contribuido significativamente al crecimiento del phishing, reduciendo las barreras técnicas de entrada para los delincuentes y ahorrándoles tiempo y recursos.

Los atacantes están dejando atrás el phishing por SMS (SMiShing) y recurriendo al phishing por buzón de voz (vishing) para conseguir que las víctimas abran archivos adjuntos maliciosos.

Los sofisticados ataques Adversary-in-Middle (AiTM) están ayudando a los atacantes a eludir las medidas de seguridad de autenticación multifactor (MFA).

Las estafas de contratación dirigidas a los solicitantes de empleo son cada vez más frecuentes.

Principales objetivos de phishing en 2022

Zscaler ThreatLabz analizó los datos de todos los países, sectores, marcas y plataformas para conocer los objetivos más frecuentes de los ataques de phishing en 2022.

Intentos de phising por país en 2022

Los diez países más afectados por estafas de phishing en el último año fueron:

1. EE. UU.
2. Reino Unido
3. Países Bajos
4. Rusia
5. Canadá
6. Singapur
7. Alemania
8. Francia
9. Japón
10. China

Estados Unidos vuelve a ser el país más atacado por los ataques de phishing, una posición que siempre ha ocupado. Nuestra investigación indica que más del 65 % de todos los intentos de phishing se produjeron en Estados Unidos, lo que supone un aumento con respecto al 60 % del año pasado. El Reino Unido sufrió un aumento del 269 % en los ataques de phishing.

Varios países vieron un aumento de los intentos de phishing en 2022, entre ellos Canadá, que registró un sorprendente incremento del 718 %. Algunos expertos de ThreatLabz atribuyen este repunte al aumento paralelo de objetivos en el ámbito de la educación. Rusia registró un aumento del 198 % y Japón del 92 %. Sin embargo, Hungría experimentó una disminución importante del 90 % en los ataques de phishing, y el total de ataques en Singapur se redujo en casi un 48 %.

La reducción de los ataques de phishing dirigidos a Singapur puede deberse al aumento de los esfuerzos de su gobierno en materia de ciberseguridad, incluidas las iniciativas de la Agencia de Ciberseguridad del país (CSA). Esta agencia ofrece directrices y asesoramiento a particulares y empresas sobre cómo protegerse de las ciberamenazas y, junto con la Comisión de Protección de Datos Personales (PDPC), hace cumplir las leyes y reglamentos sobre protección de datos.

Figura 1: Ataques de phishing por países en 2022

Intentos de phishing por industria en 2022

La industria de la educación experimentó un aumento del 576 % en los intentos de phishing en 2022, pasando del octavo sector más atacado al primero y superando a la industria más atacada del año pasado, el comercio minorista/mayorista. Es probable que los perpetradores del phishing hayan aprovechado los procesos de solicitud de reembolso de préstamos estudiantiles y de alivio de la deuda que se registraron el año pasado y hayan explotado las vulnerabilidades del aprendizaje a distancia. Las finanzas y los seguros también experimentaron un aumento de phishing de un 273 % en 2022.

Los intentos de phishing en el sector sanitario también aumentaron exponencialmente, pasando de algo menos de 31 millones a más de 114 millones. Los pacientes que aplazaron el tratamiento médico rutinario durante el año inicial de la pandemia de covid-19 reanudaron sus tratamientos en 2022, accediendo a sus cuentas en línea e interactuando potencialmente con atacantes de phishing que se hacían pasar por organizaciones de atención sanitaria. Además, los atacantes de ransomware están utilizando más tácticas de phishing para comprometer los datos de las organizaciones de atención sanitaria.

Sin embargo, en 2022 se produjo una pequeña pausa en los ataques de phishing, ya que el comercio minorista y mayorista experimentó un declive del 67 % y los servicios un desplome del 38 %. Es probable que el declive de los ataques contra el comercio minorista y mayorista se deba a una disminución de los hábitos de consumo tras las fuertes compras y gastos en bienes por Internet en 2021.

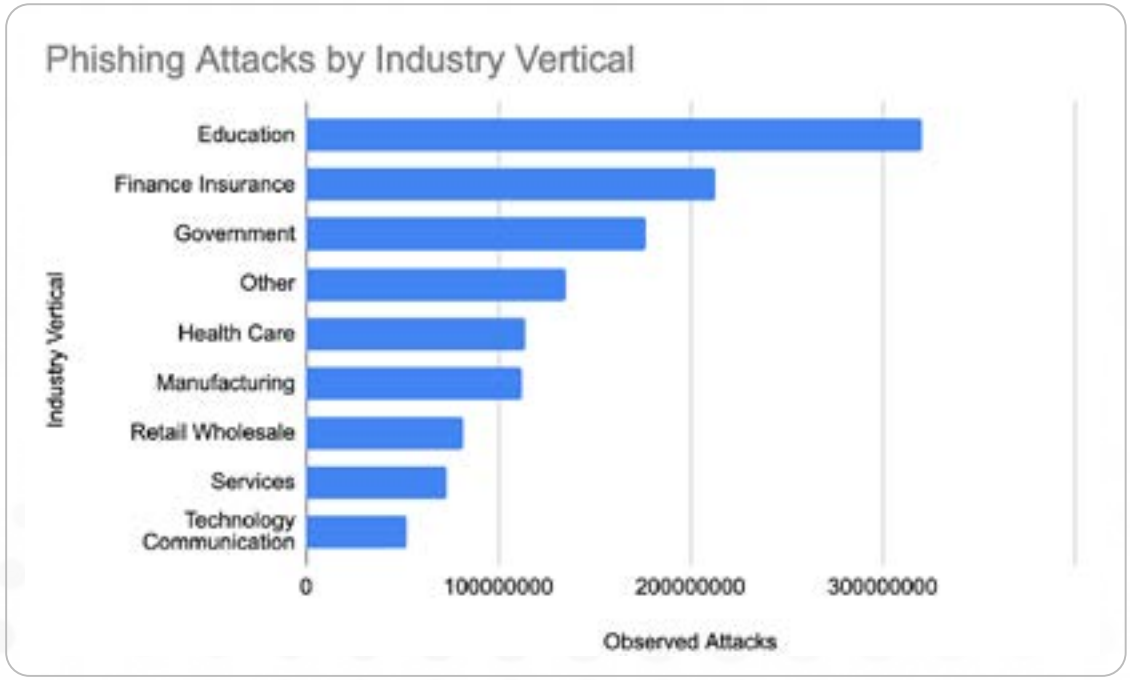
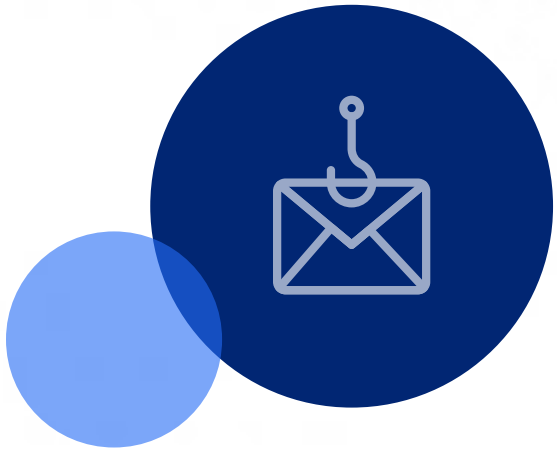


Figura 2: Ataques de phishing por industria en 2022



Las marcas más imitadas en los ataques de phishing de 2022

Los atacantes de phishing suelen aprovecharse de las tendencias de consumo haciéndose pasar por marcas populares para engañar a los consumidores vulnerables. Entre las categorías de marcas atacadas con mayor frecuencia se encuentran las herramientas de productividad, los sitios de criptomonedas, los sitios de streaming ilegal, las plataformas de medios sociales y los servicios de mensajería, las instituciones financieras, los sitios gubernamentales y los servicios logísticos.

Microsoft llegó a ser la marca más imitada del año, con algo menos del 31 % de los ataques. Su marca OneDrive representó otro 17 %, SharePoint casi un 4 % y Microsoft 365 otro 1.7 %. En 2022, Zscaler descubrió que los atacantes utilizaban cada vez más OneNote, que puede integrarse con OneDrive y otros productos de Microsoft, para distribuir malware a través de correos electrónicos de phishing. Anteriormente, atacantes se dirigían a los usuarios con documentos maliciosos habilitados para macros, pero en julio de 2022, Microsoft deshabilitó las macros por defecto en todas las aplicaciones de Microsoft 365 (Office), lo que hace que este modelo sea menos eficaz para la distribución de malware.

La plataforma de intercambio de criptomonedas Binance representó el 17% de los ataques de imitación de marcas, con phishers que se hacían pasar por falsos representantes de clientes de bancos o empresas P2P. Los sitios de streaming ilegales representaron el 13.6% de los ataques, registrando repuntes durante eventos deportivos destacados como la Copa Mundial de la FIFA en noviembre y diciembre de 2022.

Aunque los ataques relacionados con el covid siguen siendo frecuentes, están disminuyendo. En 2021, los ataques a marcas relacionados con el covid representaron el 7.2 % de las estafas de phishing, y se redujeron a solo el 3.7 % en 2022.

Las 20 marcas más imitadas en los ataques de phishing de 2022 son:

1. Microsoft
2. OneDrive
3. Binance
4. Sitios de streaming ilegales
5. Sharepoint
6. Atención relacionada con el covid-19
7. Gobierno
8. Netflix
9. Facebook
10. Microsoft 365
11. Google
12. Telegram
13. Adobe
14. DHL
15. Amazon, Amazon
16. American Express
17. WhatsApp
18. Roblox
19. PayPal
20. DocuSign

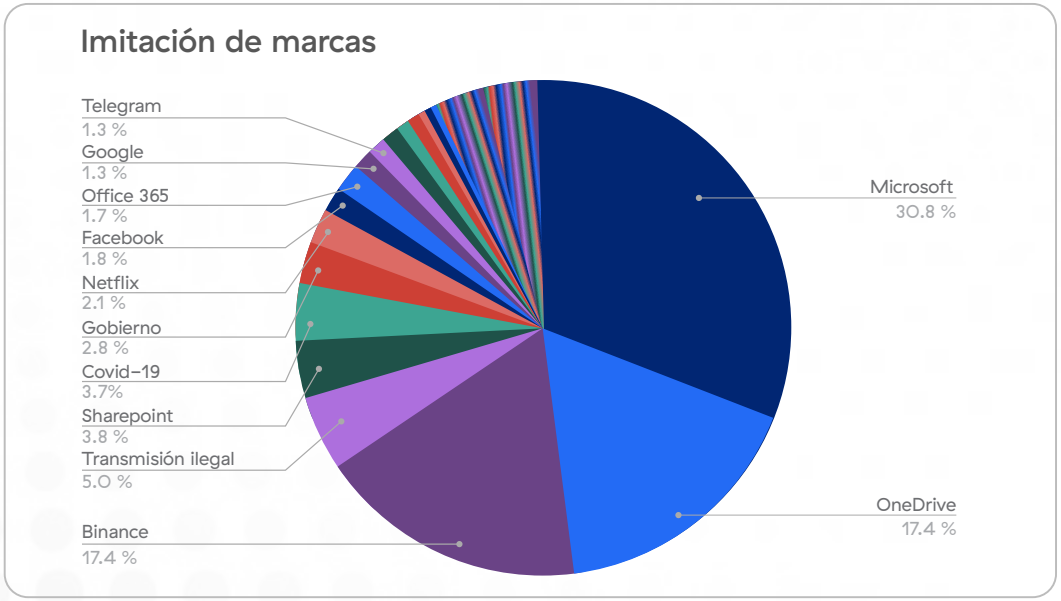


Figura 3: Marcas más imitadas en los ataques de phishing

Principales dominios de referencia en 2022

Los atacantes suelen utilizar dominios de confianza para manipular a las víctimas, redirigiéndolas a sitios web de phishing. Pueden comprar anuncios en medios de comunicación o plataformas de búsqueda como Google y Bing. También pueden publicar en foros corporativos y mercados como Walmart y Amazon o abusar de sitios/servicios para compartir información como Evernote, Dropbox y GitHub.

Analizamos los dominios de referencia para determinar cuáles son los más explotados por los atacantes. En 2022, estos incluían sitios de streaming de video, bolsas de criptomonedas y otros sitios financieros, páginas de creación de sitios web y formularios, sitios que alojan contenidos generados por los usuarios, motores de búsqueda y más.

Los 20 principales dominios de referencia en 2022 fueron:

1. qumucloud.com
2. vimeo.com
3. bittrex-appemail.com
4. bittrex-global-emaill-i.com
5. googlesyndication.com
6. typeform.com
7. mhtestd.gov.zw
8. gutefrage.net
9. dow.com
10. framer.com
11. google.com
12. finanznachrichten.de
13. holldingsglobaloverview marketcap.com
14. hesgoal.com
15. doubleclick.net
16. elonshib.net
17. myftp.biz
18. principal.com
19. marathonbet.ru
20. baidu.comDocuSign

Los 20 principales dominios de referencia utilizados en los ataques de phishing

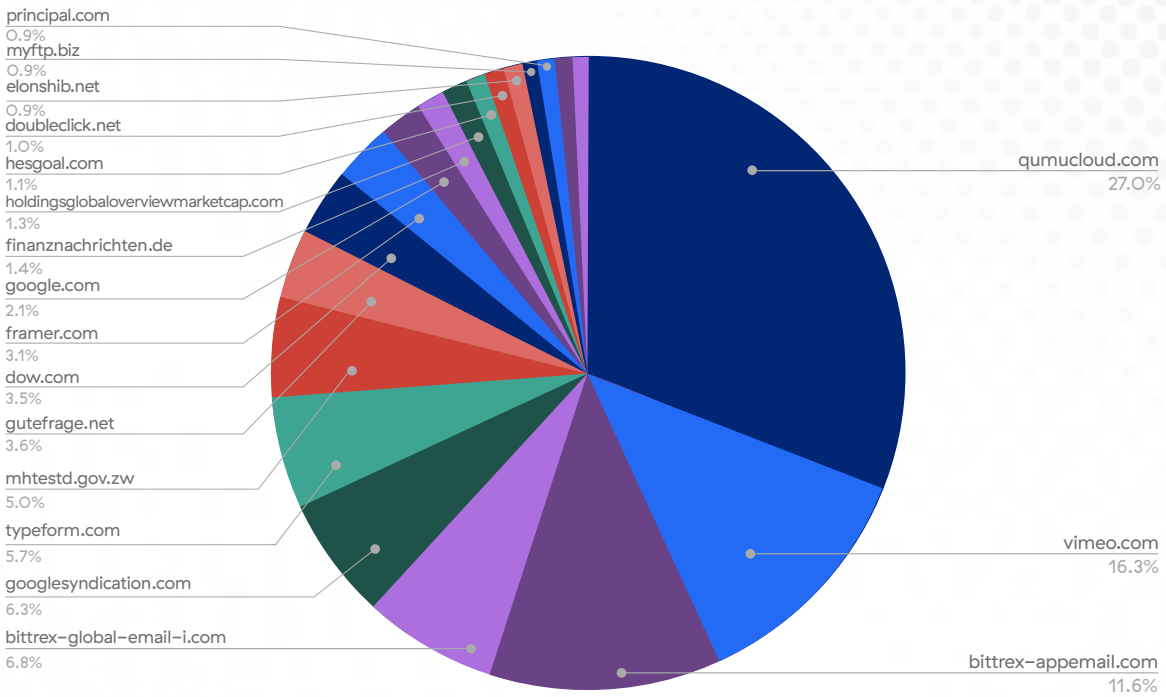


Figura 4: Dominios de referencia más utilizados en los ataques de phishing de 2022

Ataques a sistemas autónomos en 2022

Un sistema autónomo (AS) es una red o grupo de redes con una única política de enrutamiento. Cada AS tiene un identificador numérico único, conocido como ASN. Como parte de este análisis, el equipo de Zscaler ThreatLabz revisó los ASN responsables de alojar la infraestructura de phishing.

Nuestro análisis mostró que, en 2022, el 39 % de los ataques de phishing utilizaron sitios de alojamiento (una reducción con respecto al 50.6 % de 2021), el 53 % se produjeron en ISP (un aumento con respecto al 39.2 % de 2021) y el 8 % en dominios empresariales.

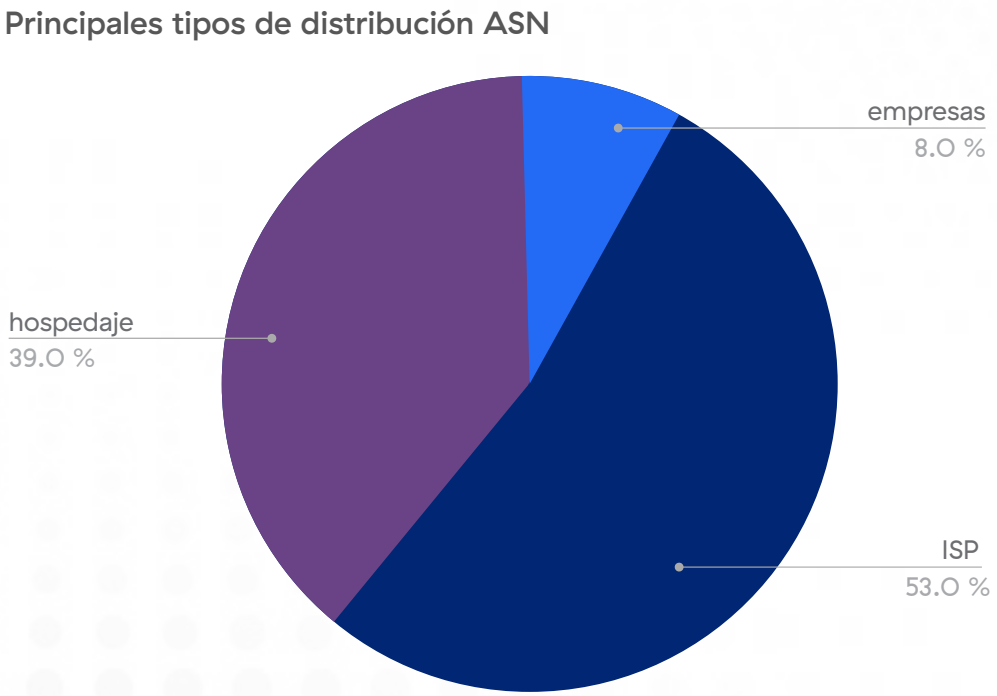


Figura 5: ASN para la infraestructura de phishing

Evolución de las tendencias de phishing

Cada año, los autores de las amenazas emplean tácticas más sofisticadas y enfoques cada vez más avanzados para llevar a cabo sus estafas de phishing. Para garantizar que su organización esté preparada y que su equipo se anticipe a los ataques, es esencial conocer las últimas tendencias en materia de amenazas. A continuación se detallan los principales aspectos de las nuevas tendencias de phishing observadas en 2022.

Ataques de vishing

Los ataques de vishing, o campañas de phishing con mensajes de voz, inducen a las víctimas a abrir archivos adjuntos maliciosos. A mediados de 2022, los delincuentes atacaron a usuarios de varias organizaciones con sede en Estados Unidos con correos electrónicos maliciosos en forma de notificaciones de voz para robar sus credenciales de Microsoft 365 y Outlook.

También hemos observado campañas de phishing con archivos adjuntos de correo electrónico relacionados con mensajes de voz como el siguiente:

Figura 6: Correo electrónico de una campaña de vishing

El archivo .html contiene JavaScript ofuscado:

Figura 7: Código de correo electrónico de campaña de vishing con JavaScript oculto

Al desofuscar el código del correo electrónico, puede ver que si un usuario abriera el archivo, este lo redirigiría a un servidor controlado por el atacante:

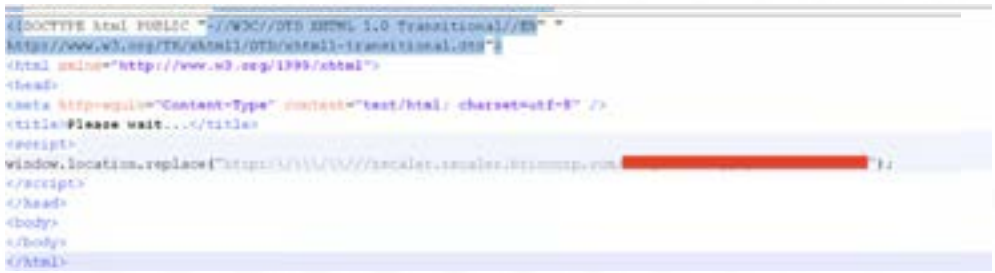


Figura 8: Código de correo electrónico de campaña de vishing con JavaScript oculto revelado

Esto conduce a una página de phishing de Microsoft:

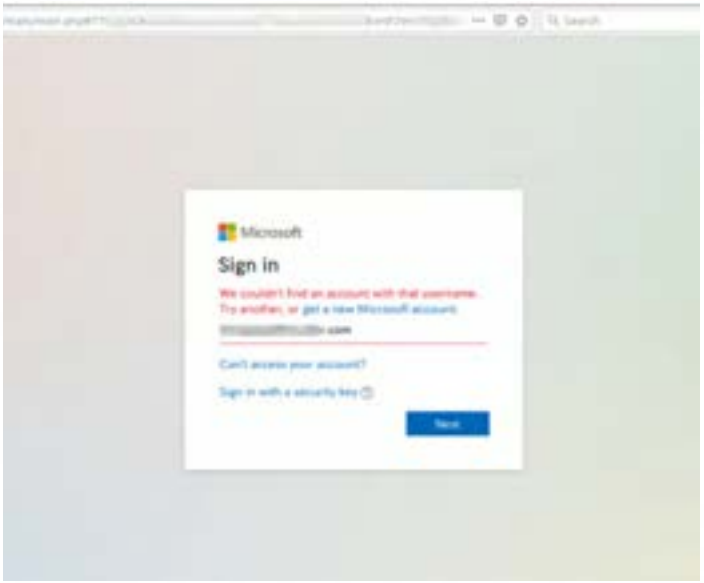


Figura 9: Página de destino de una campaña de Vishing

ThreatLabz también descubrió una estafa de llamada de voz en la que un actor de amenazas ataca a un empleado corporativo haciéndose pasar por un directivo. Primero, la víctima recibe una llamada telefónica suplantada con un mensaje con un "hola" pregrabado y, luego, la llamada finaliza. Posteriormente, la víctima recibe un mensaje del estafador indicándole que el directivo está teniendo problemas de conectividad con la red y solicitándole que continúe la comunicación por mensajería. A continuación, el estafador intenta convencer a la víctima de que divulgue información sobre la cuenta de la empresa o transfiera fondos.

Para evitar caer en las trampas de los atacantes, es crucial educar a los empleados para que se comuniquen entre sí solo a través de los canales oficiales y se mantengan alerta ante este tipo de estafas.

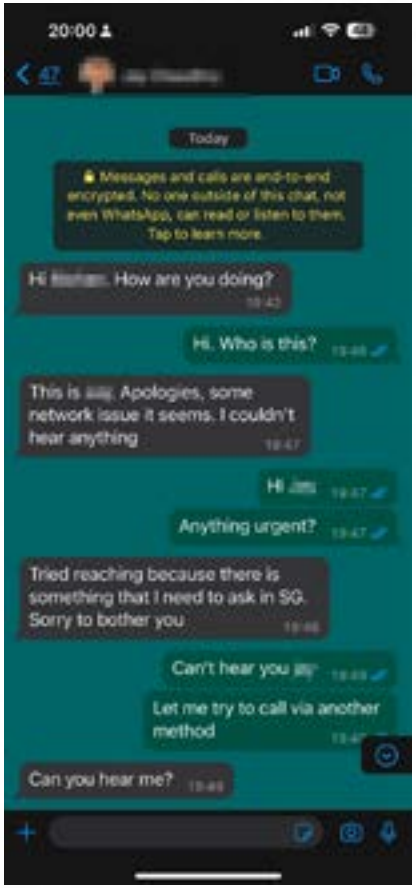


Figura 10: Mensajería de vishing

Estafas de contratación

Durante 2022, ThreatLabz presenció un aumento de los solicitantes de empleo atacados utilizando una serie de estafas de contratación. Estas estafas utilizaron anuncios de trabajo, sitios web o portales y formularios falsos para atraer a las personas que buscaban empleo.

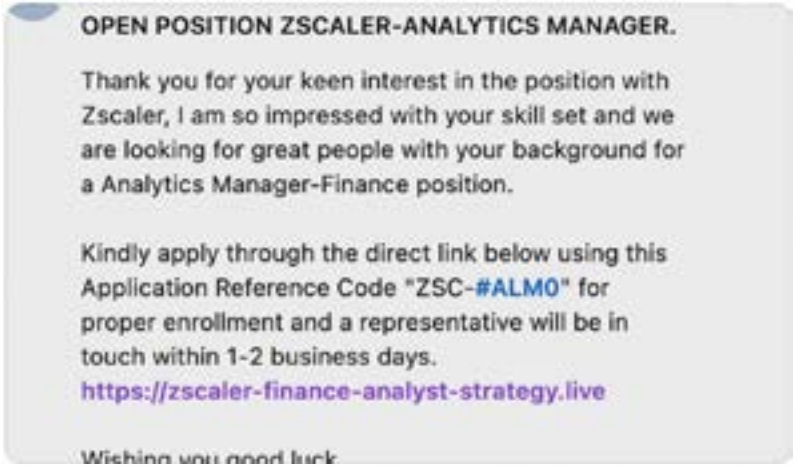


Figura 11: Anuncio falso de LinkedIn con una URL de phishing

En este caso, el atacante publicó un anuncio falso de LinkedIn con una URL de phishing. Al visitar la URL falsa, las víctimas potenciales se postularían para el trabajo.

Una vez que la víctima se postula, el atacante se comunica con ella y le solicita una entrevista por Skype en la que se hace pasar por un representante de Recursos Humanos.

Figura 12: Correo electrónico de contratación falso

Al examinar el código fuente, se puede ver el código utilizado para la exfiltración de datos de tarjetas de crédito.

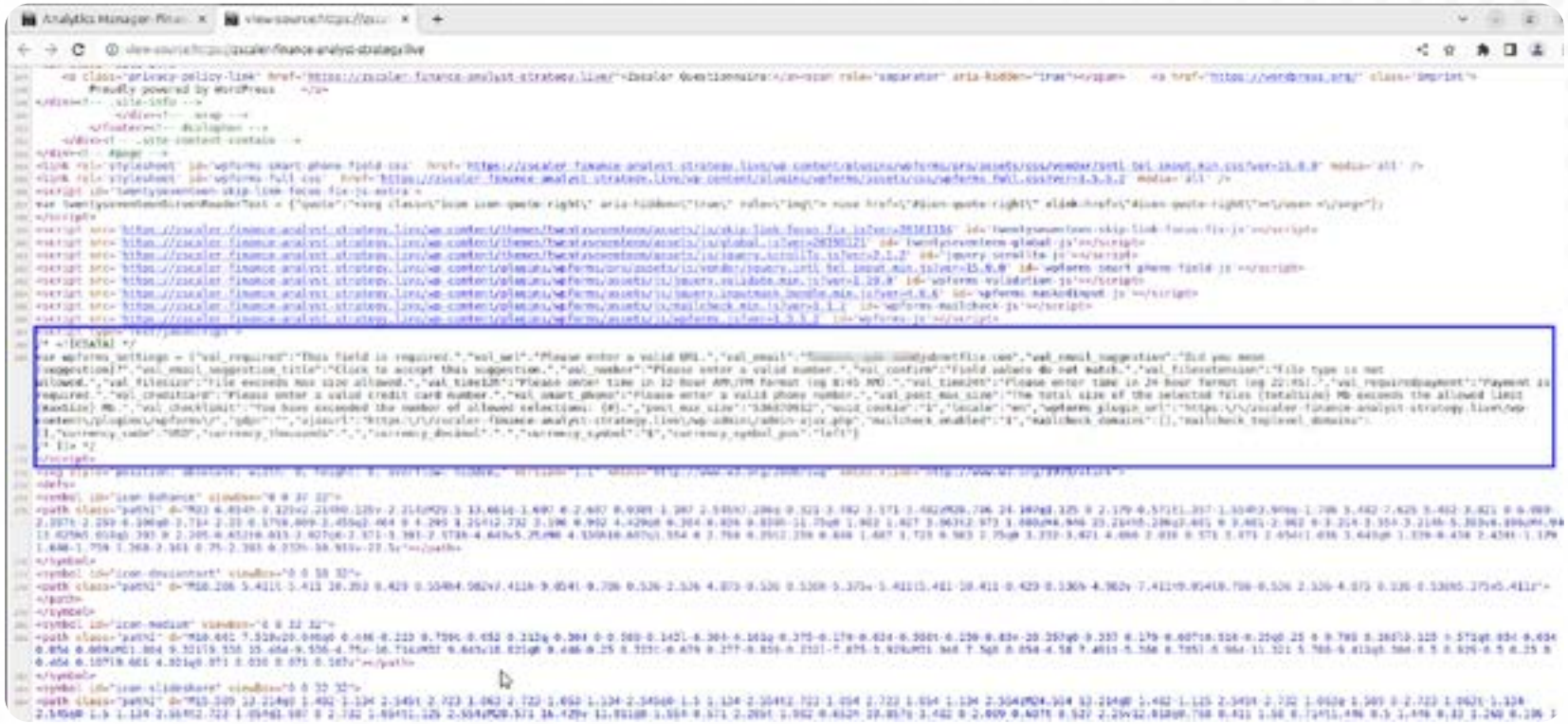


Figura 13: Código fuente del falso correo electrónico de reclutamiento

Ataques de phishing de tipo Adversary-in-the-Middle (AiTM)

Conozca más sobre los ataques de phishing de tipo Adversary-in-the-Middle (AiTM).

El equipo de ThreatLabz descubrió una nueva variedad de una campaña de phishing a gran escala que utiliza técnicas AiTM junto con varias tácticas de evasión. Los sitios web de phishing tradicionales que recopilan las credenciales de los usuarios nunca completan el proceso de autenticación con el servidor del proveedor de correo real. Si el usuario ha activado la MFA, impide que el atacante acceda a la cuenta únicamente con las credenciales robadas. Para eludir la MFA, los atacantes pueden utilizar ataques de phishing AiTM.

La figura 14 muestra un fragmento de código de una página de phishing de un servidor de phishing AiTM.

Figura 14: Código de la página de phishing del servidor de phishing AiTM

El servidor proxy malicioso AiTM modifica las URL de una página de destino legítima con URL controladas por el atacante (véase la figura 15) y actúa como relé entre la víctima y el servidor de destino.

Figura 15: URL controladas por el atacante y modificadas por el servidor proxy AiTM

El subdominio original (en verde), el nombre de dominio original (en azul, menos el TLD) y un ID único generado (en rosa) se unen con guiones y se convierten en un subdominio bajo el dominio del sitio de phishing (en naranja).

Detectamos esto cuando algunas de las solicitudes se pasaron con modificaciones incorrectas a la víctima, como se ve en la figura 16.

Figura 16: Modificaciones incorrectas pasadas a la víctima de phishing

Esto provocó una filtración de la dirección del servidor controlado por el atacante, como se muestra en la figura 17.

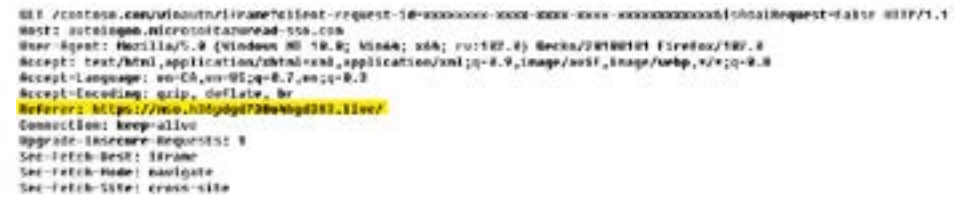


Figura 17: Se revela la dirección del servidor controlado por el atacante

Ataques de phishing Browser-in-the-Browser (BiTB)

Los ataques de phishing BiTB también experimentaron un aumento en 2022. Simulan una ventana de página de inicio de sesión dentro de una página principal de phishing que hace creer al blanco previsto que necesita introducir sus credenciales de inicio de sesión único (SSO) para seguir usando el sitio web.

Los atacantes utilizan una combinación de HTML/CSS básico y marco en línea (iframe) para crear una ventana emergente falsa que simula la típica ventana emergente de SSO del usuario. Puede resultar casi imposible para el usuario distinguir una ventana emergente auténtica de una falsa de phishing bien diseñada.

La figura 18 muestra un ejemplo de ataque BiTB que utiliza una ventana SSO falsa, generada mediante HTML, para atacar Steam, una popular plataforma digital de juegos.

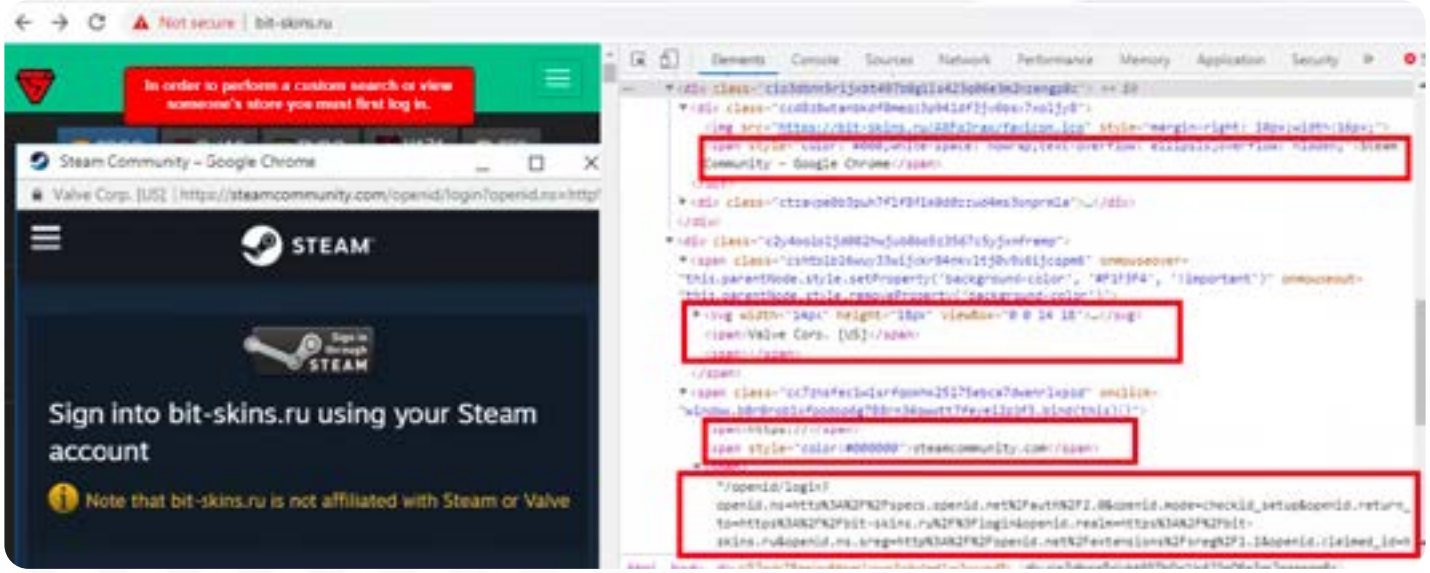


Figura 18: Ataque BiTB o "picture-in-picture"

Uso de servicios legítimos para alojar sitios web de phishing

El equipo de ThreatLabz también observó que los atacantes utilizaban servicios de alojamiento legítimos para alojar sitios de phishing. Algunos de estos sitios incluían proveedores de alojamiento gratuitos como OOwebhostapp.com, servicios de intercambio de archivos como transfer.sh, proveedores de servicios en la nube como amazonaws.com, y acortamiento de URL mediante servicios como linkedin.com.

En 2022, el equipo observó que los atacantes utilizaban servicios DNS dinámicos que permiten a los usuarios asignar un nombre de dominio a una dirección IP cambiante. Los usuarios aprovechan estos servicios principalmente para el acceso remoto o el alojamiento de sitios web en redes domésticas.

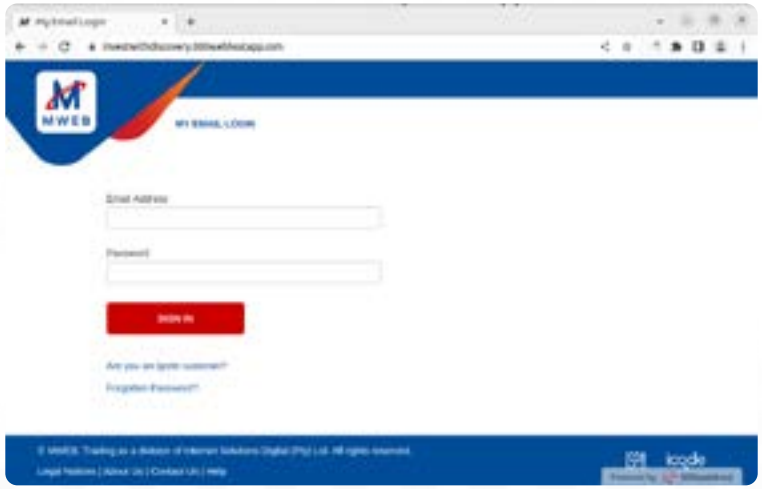


Figura 19: Subdominios DNS dinámicos para el alojamiento de páginas de phishing (ejemplo uno)

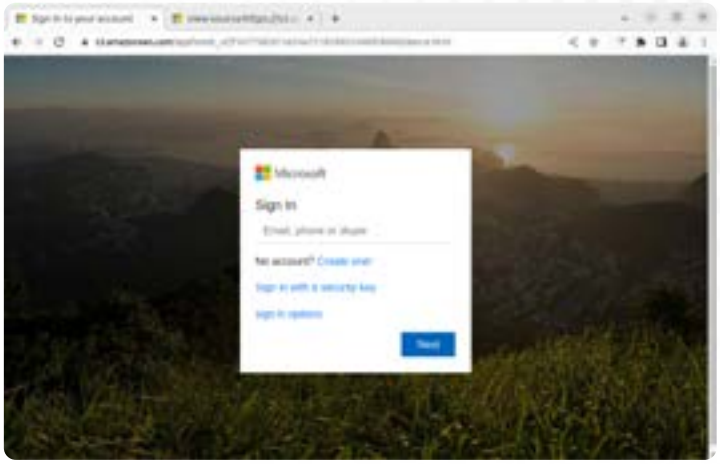


Figura 20: Subdominios DNS dinámicos para el alojamiento de páginas de phishing (ejemplo dos)

Los atacantes también pueden utilizar los servicios de DNS dinámico para alojar sitios web de phishing en equipos o servidores comprometidos sin direcciones IP fijas.

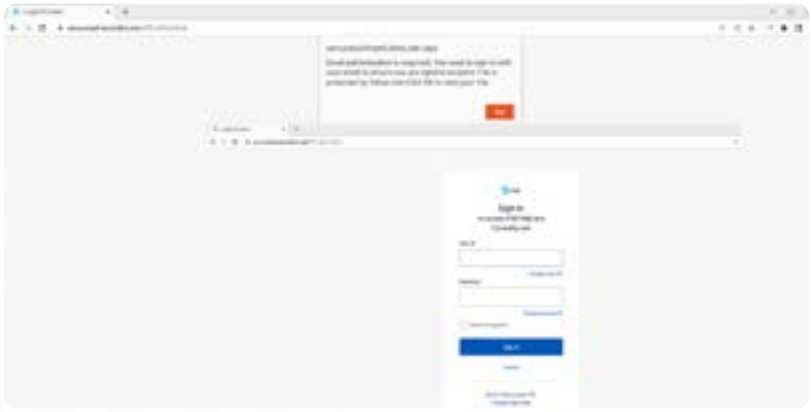


Figura 21: phishing de T&T alojado mediante DNS dinámico

Phishing mediante el sistema de archivos interplanetario (IPFS)

IPFS es un sistema de archivos distribuido de punto a punto que permite a los usuarios almacenar y compartir archivos en una red descentralizada de computadoras. En comparación con los sistemas de archivos centralizados tradicionales, ofrece una forma más segura, resistente y eficaz de almacenar y distribuir archivos.

En IPFS, los archivos se dividen en trozos más pequeños y se distribuyen por varios nodos de una red, lo que hace más difícil que un único punto de fallo comprometa todo el sistema. La figura 22 muestra cómo se ve el phishing con IPFS.

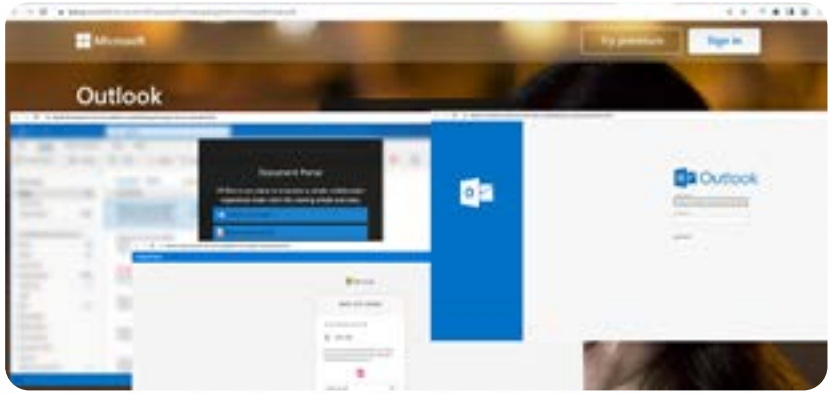


Figura 22: phishing con IPFS (ejemplo uno)

Debido a su estructura de punto a punto, es mucho más difícil eliminar una página de phishing alojada en IPFS que una alojada mediante un método más tradicional.

También observamos que los atacantes utilizaban Google Translate para hacer que sus URL parecieran auténticas.

Figura 23: Ejemplo de phishing de IPFS utilizando Google Translate

Como se muestra en la figura 23, los atacantes utilizaron Google Translate en un sitio de phishing alojado en IPFS y, a continuación, utilizaron la página para suplantar las credenciales de DocuSign.

Uso de WebSockets para filtrar datos individualizados (fingerprinting)

En el Informe sobre phishing 2022 de Zscaler ThreatLabz, hablamos de los kits de phishing y los marcos de phishing de código abierto. Estos kits y marcos agrupan y masifican las herramientas necesarias para lanzar rápidamente cientos o miles de páginas de phishing convincentes y eficaces, incluso si el atacante o los atacantes tienen pocos conocimientos técnicos.

Algunos de estos kits de phishing cuentan con una función denominada “cloaking", una técnica que permite a los phishers ocultar una página web de phishing real a los investigadores y escáneres de seguridad mientras la siguen mostrando a sus víctimas. El kit de phshing filtrará las conexiones de cada visitante en función de la dirección IP, las palabras clave del nombre de host, el agente de usuario, etc. En función de la coincidencia, mostrará una página inofensiva o una página de phishing, evitando ser detectada por los investigadores de seguridad y las herramientas antiphishing que examinan Internet en busca de contenidos maliciosos. Estos métodos tradicionales de cloaking pueden ser burlados por los atacantes utilizando diferentes técnicas.

Este año hemos observado novedades en el tema de fingerprinting (captación de huellas digitales) de clientes. Esto es lo que ocurre cuando un visitante entra en una página de phishing y se capta su huella digital:

1. El usuario navega por la página de phishing
2. El servidor envía un JavaScript para captar la huella digital del cliente, y el JavaScript la carga través de la conexión WebSocket.
3. El servidor genera una cookie basada en la huella digital y envía la cookie de vuelta a través de WebSocket
4. El código JavaScript actualiza automáticamente la página con la cookie
5. El usuario es redirigido a la página de phishing si las cookies pasan la comprobación

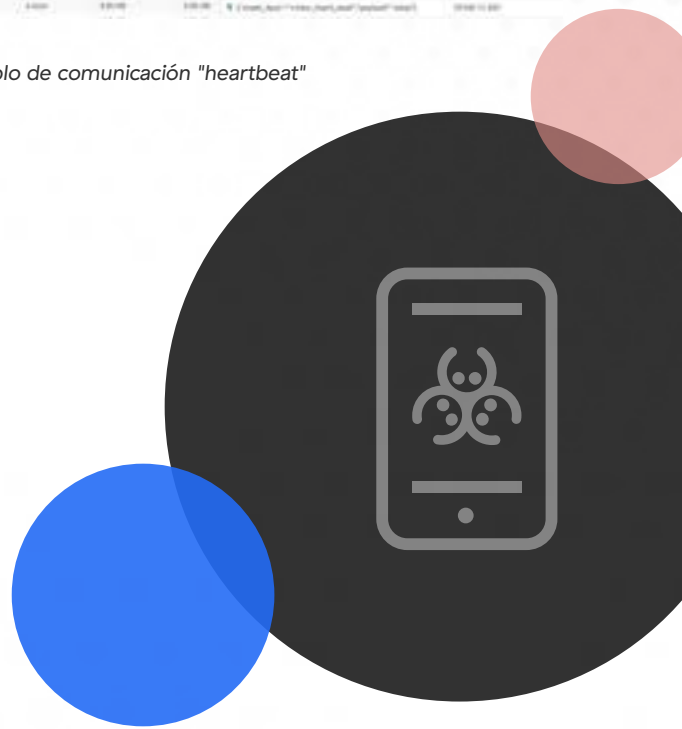
El JavaScript de fingerprinting se basa en este proyecto de código abierto en GitHub.

```
{
 "type": "vdata",
 "data": {
  "languages": [
   "en-US"
  ],
  "cookieEnabled": true,
  "serviceWorker": true,
  "hardwareConcurrency": 48,
  "javaEnabled": false,
  "referrer": "",
  "etsl": 33,
  "battery": true,
  "hasChrome": false,
  "webXR": true,
  "mediaSession": true,
  "webgl": "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver-5.0.0)",
  "timezone": "7",
  "platform": "Linux x86_64",
  "userAgent": "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0",
  "appCodeName": "Mozilla",
  "appName": "Netscape",
  "language": "en-US",
  "deviceMemory": 8,
  "vendor": "Google Inc.",
  "visitorId": "6b3a518d3ab6051e32ce5098f4fb411e",
  "permissions": {
   "accelerometer": "prompt",
   "ambient_light_sensor": "unknown",
   "background_fetch": "unknown",
   "background_sync": "unknown",
   "bluetooth": "unknown",
   "camera": "prompt",
   "clipboard_write": "unknown",
   "device_info": "unknown",
   "display_capture": "unknown",
   "geolocation": "prompt",
   "gyroscope": "prompt",
   "magnetometer": "prompt",
   "microphone": "prompt",
   "midi": "prompt",
   "nfc": "unknown",
   "notifications": "prompt",
   "persistent_storage": "unknown",
   "push": "prompt",
   "speaker_selection": "unknown",
   "speaker-selection": "unknown",
   "device-info": "unknown",
   "background-fetch": "prompt",
   "background-sync": "prompt",
   "persistent-storage": "prompt",
   "ambient-light-sensor": "unknown",
   "clipboard-write": "prompt",
   "display-capture": "prompt"
  },
```


Figura 24: Datos de la huella digital de una máquina

Esta técnica puede interrumpirse si se supervisa la comunicación WebSocket y se filtran los datos de las huellas dactilares. El kit de phishing puede establecer una comunicación de comando y control (C2) para recibir órdenes de los servidores de phishing a través de WebSocket mediante una técnica denominada comunicación "heartbeat", en la que el atacante envía y recibe datos de ida y vuelta desde el dispositivo de la víctima.

Figura 25: Ejemplo de comunicación "heartbeat"



Uso de servicios de formularios basados en la web para recopilar credenciales

También observamos que los atacantes se aprovechaban de los servicios que ayudan a los usuarios a recopilar información a través de formularios. Por ejemplo, FormSubmit es un servicio basado en la web que ofrece una forma sencilla de configurar y administrar formularios HTML para sitios web. Las organizaciones pueden utilizarlo para crear formularios personalizados con varios campos de entrada, como cuadros de texto, casillas de verificación, botones de opción, listas desplegables y cargas de archivos, y luego enviar los datos del formulario a una dirección de correo electrónico o URL de webhook especificada.

El ejemplo de la figura 26 demuestra cómo los atacantes pueden abusar de los servicios de creación de formularios para recopilar credenciales sin necesidad de instalar servidores.

Figura 26: Ejemplo de formulario

La "acción" del formulario es "https://submit-form[.]com/Qz1kGknr".

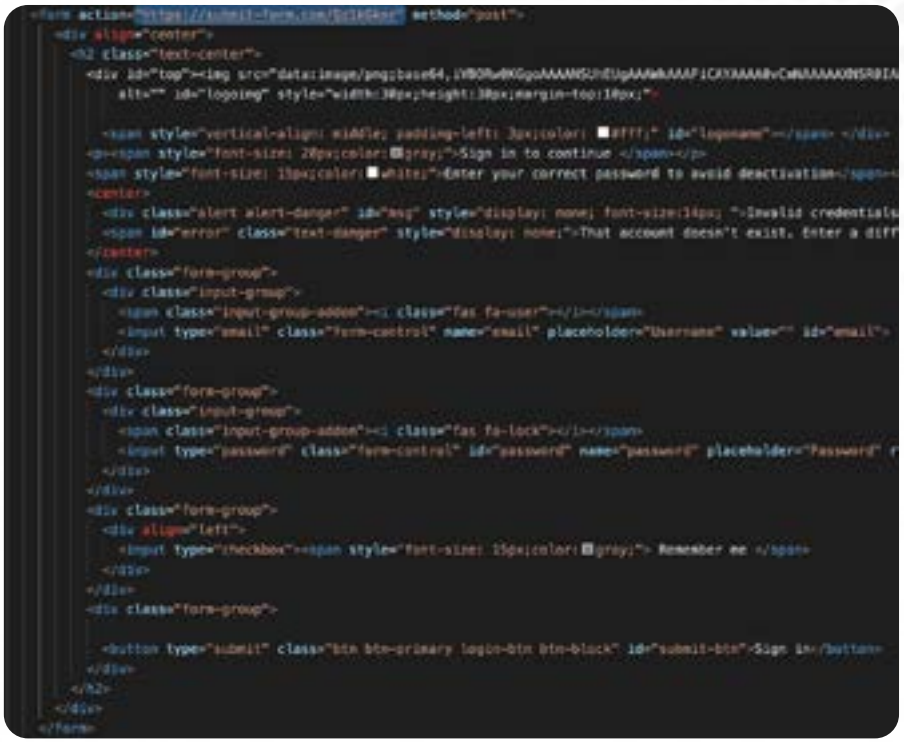


Figura 27: Cómo aprovecha el atacante el servicio de formularios para interceptar información

Phishing mediante contrabando de HTML y archivos SVG

El contrabando de HTML es una técnica que permite a los atacantes eludir los controles de seguridad de la red mediante la integración de código malicioso dentro de HTML aparentemente inofensivo yla posterior introducción de cargas útiles maliciosas en el sistema atacado. Los esquemas de detección suelen examinar y detectar JavaScript, por lo que los actores de amenazas recurren al contrabando de HTML para distribuir diversos tipos de malware.

Los atacantes suelen trasladar el código HTML de contrabando a Scalable Vector Graphics (SVG), un formato de gráficos vectoriales basado en XML que se utiliza para crear gráficos bidimensionales que pueden escalarse sin perder resolución. Pueden editar archivos SVG con editores de texto y software gráfico.

Los atacantes pueden utilizar JavaScript para manipular los elementos y atributos SVG para crear diferentes animaciones, como mover objetos, cambiar colores y crear transiciones. Con JavaScript, las animaciones SVG pueden ser interactivas, permitiendo a los usuarios interactuar con los gráficos y activar diferentes animaciones.

Las soluciones de detección no suelen comprobar JavaScript dentro de SVG, lo que las convierte en una opción atractiva para los atacantes.

Herramientas y técnicas de phishing

Existen varias aplicaciones independientes o extensiones de navegador disponibles en línea que los actores de amenazas utilizan para copiar un sitio web auténtico y modificar el código de exfiltración de datos para robarlos. Aquí hay algunos ejemplos:

- **HTTrack,** una aplicación independiente muy utilizada
- **singlefile,** una extensión de Google Chrome
- **Webscrapbook,** una extensión de navegador de código abierto
- **Save Page WE**, una extensión de Google Chrome

Phishing mediante iframes

Un iframe es un elemento HTML que permite a los desarrolladores web integrar otro documento HTML en la página web actual. Crea un "marco dentro de un marco" en el que el contenido del documento integrado se muestra en un recuadro rectangular en la página actual. Cuando los actores de amenazas integran contenidos de phishing en un iframe, pueden eludir la detección.

Un iframe puede utilizarse para el phishing de varias formas diferentes:

1. Iframe anidado
2. iframe como fondo
3. Iframe como fachada, como BiTB

Además, esperamos que también empiecen a aparecer "iframes como componentes". En este método, se pueden combinar varios iframes para generar una página de phishing, con un iframe como parte de la página.

Por ejemplo, el primer iframe se utiliza para obtener un nombre de usuario (figura 28):

Figura 28: iframe para obtener el nombre de usuario

El segundo iframe se utiliza para obtener una contraseña (figura 29):

Figura 29: iframe para obtener la contraseña

Por último, la página de phishing combina los dos iframes (figura 30):

Figura 30: Página de phishing con iframes combinados

Phishing de WebAssembly

WebAssembly es un formato de instrucciones binarias para una máquina virtual que se ejecuta en los navegadores web modernos. Ofrece un formato de código de bytes portátil y de bajo nivel que puede ejecutarse a una velocidad casi nativa, lo que lo hace idóneo para ejecutar aplicaciones de rendimiento crítico en la web.

WebAssembly aborda las limitaciones de JavaScript como lenguaje de rendimiento para aplicaciones web; su código puede escribirse en varios lenguajes, como C++, Rust y Go, y luego compilarse al formato de código de bytes WebAssembly.

Phishing según la región geográfica

Los actores de amenazas que pretendan dirigirse a usuarios que se encuentren en regiones concretas o hablen idiomas específicos pueden recurrir a API de terceros y a servicios específicos para identificar a esos sectores.

Geo Targetly es un servicio que permite a los usuarios personalizar el contenido de su sitio web en función de la ubicación geográfica de sus visitantes. Para determinar el contenido que se muestra, pueden crear reglas personalizadas basadas en factores como las direcciones IP, la configuración del idioma y las zonas horarias.

Lógicamente, los atacantes utilizan este servicio como técnica de cloaking cuando practican el phishing.

Uso de Punycode o de una dirección IP no estándar en las URL para evitar la detección

Una dirección IP es simplemente un número de 32 bits que puede representarse utilizando diferentes cantidades de dígitos. La cantidad estándar es de cuatro dígitos, pero también existen direcciones IP de uno, dos o tres dígitos, y cada dígito puede representarse utilizando una base diferente (binaria, octal, decimal, hexadecimal). Cuando los atacantes de phishing representan una dirección IP de forma no normalizada, pueden eludir la detección, pero esto puede mitigarse normalizando las direcciones IP.

Phishing mediante "Hash en URL"

El "hash" en una URL se refiere a la parte de la URL que viene después del símbolo "#". También conocido como identificador de fragmento, identifica una sección específica en una página web, como el encabezado de una sección o un párrafo, y permite al usuario navegar directamente a esa sección haciendo clic en un enlace o marcador.

El contenido después del símbolo "#" no se envía al servidor, por lo que los cambios en el hash no provocan una actualización de la página. Esta función se utiliza a menudo en aplicaciones de una sola página y contenidos web dinámicos.

Los atacantes de phishing han encontrado dos nuevas formas de aprovecharse de esto:

1. Representando la información del usuario con el hash.
    - Las direcciones de correo electrónico son las más comunes. Cuando se muestra la página de inicio de sesión, la dirección de correo electrónico del usuario se rellena automáticamente para engañarlo.
2. Generando páginas de phishing específicas basadas en el hash, que pueden distinguir a los usuarios.

IA y phishing

Los recientes avances de la tecnología de IA, como ChatGPT, facilitan a los actores de amenazas el desarrollo de código malicioso, la generación de ataques Business Email Compromise (BEC), la creación de malware polimórfico, etc. Intentamos generar una página de inicio de sesión de phishing con ChatGPT y, con solo tres interacciones sencillas, la herramienta generó esta página web:

Figura 31: Página de phishing generada por ChatGPT

Con un poco más de esfuerzo, un atacante podría añadir el fondo y modificarlo para que pareciera una página de inicio de sesión auténtica.

Predicciones para el 2024

1. **Los ataques con IA se utilizarán con más frecuencia a medida que los** actores de las amenazas descubran nuevas aplicaciones para estos servicios. Prepárese para ver estafas más sofisticadas en diferentes canales de comunicación, como los correos electrónicos, los SMS y los sitios web. Además, prepárese para un aumento de los intentos de phishing a medida que los atacantes aprovechen la IA para lanzar ataques más coordinados y eficaces contra grupos más grandes de personas.

2. **Las ofertas de phishing como servicio seguirán evolucionando,** y los proveedores ofrecerán plantillas de phishing personalizadas, acceso a bases de datos más amplias de víctimas potenciales y técnicas de ingeniería social más avanzadas. Los proveedores también pueden ofrecer servicios adicionales como la instalación de malware, alojamiento y análisis. Es más, estos proveedores competirán por ofrecer el mejor valor con modelos de precios asequibles y atención al cliente 24 horas al día, 7 días a la semana. Esto puede provocar un aumento de los ataques de phishing a pequeña escala, por lo que es crucial mantenerse informado sobre las últimas amenazas y tendencias del phishing.

3. **Los ataques a celulares serán más frecuentes,** ya que los atacantes se centran en explotar nuestra dependencia de estos dispositivos. Los atacantes desarrollarán contenidos más adaptados a los teléfonos móviles, como aplicaciones optimizadas, sitios web y programas maliciosos, incluidos programas espía y troyanos de acceso remoto. También encontrarán nuevas formas de extorsionar a las víctimas para obtener beneficios financieros.

4. **Los bombardeos MFA y los ataques AitM aumentarán** a medida que los atacantes encuentren formas de eludir las medidas de seguridad MFA. Las "bombas" MFA atosigan a las víctimas con solicitudes de autenticación, mientras que los ataques AitM interceptan la sesión de la víctima después de que se haya autenticado con éxito mediante MFA. Los atacantes utilizarán técnicas avanzadas, incluida la IA, para predecir y generar códigos de verificación o identificar patrones en el comportamiento de los usuarios para aprovecharse de ellos y obtener acceso. Para protegerse contra estos ataques, es importante utilizar contraseñas seguras, activar la autenticación de dos factores y supervisar las cuentas en busca de actividad sospechosa.

5. **Los ataques personalizados serán más difíciles de detectar** a medida que los atacantes desarrollen técnicas avanzadas de reconocimiento para recopilar información sobre las víctimas potenciales. Esta información se utilizará para generar correos electrónicos de phishing personalizados que parezcan más auténticos y convincentes, lo que aumentará sus probabilidades de éxito. A medida que los atacantes se vuelvan más sofisticados en su uso de la personalización, será cada vez más difícil para los usuarios identificar y evitar los ataques de phishing.

Mejore sus defensas contra el phishing

Las estadísticas del sector revelan que la organización promedio recibe docenas de correos electrónicos de phishing a diario, con pérdidas financieras que crecen exponencialmente al tiempo que las pérdidas causadas por malware y ataques de ransomware aumentan los costos promedio de los ataques efectivos de phishing de un año al otro.

Enfrentarse a todas las amenazas descritas en este informe es una tarea difícil y, aunque no es posible eliminar por completo el riesgo de las amenazas de phishing, sí se pueden reducir las posibilidades de que su organización sea víctima de ellas.

Conceptos básicos para mitigar el riesgo de los ataques de phishing

Mejores prácticas: capacitación para la concientización sobre seguridad

Las campañas de phishing tienen altas tasas de éxito porque atacan a los usuarios y solo hace falta que un empleado distraído cometa un error y muerda el anzuelo. Un estudio realizado en 2020 por la Universidad de Stanford informó que casi el 88 % de las filtraciones de datos fueron causadas por un error humano. El informe también reveló que los empleados jóvenes varones son más vulnerables a estafas de phishing y que la distracción es la causa principal de error, cualquiera sea la demografía. Es por eso que la capacitación de los usuarios finales sobre la seguridad es fundamental para prevenir las filtraciones de la seguridad. Una vez al año no es suficiente. Todos los miembros de su organización deben recibir información sobre cómo las víctimas son presas de las amenazas de phishing y deben tener cuidado de proporcionar información o de hacer clic en enlaces cuando reciban correos electrónicos o tengan acceso a sitios web, mensajes de texto, aplicaciones y llamadas telefónicas no confiables.

Es fundamental implementar una capacitación continua sobre la seguridad y realizar simulacros de phishing con regularidad para desarrollar una cultura de vigilancia que esté mucho más atenta al phishing. Estas actividades le permiten impartir una formación oportuna a las personas que necesitan un apoyo adicional para identificar los intentos de phishing y modificar su comportamiento de riesgo. Otra forma de reducir el número de incidentes de phishing es mejorar la notificación por parte de los usuarios de los correos electrónicos sospechosos de phishing, lo que puede disminuir el tiempo que tardan los equipos de seguridad en eliminar las amenazas relacionadas de otras bandejas de entrada. Esto puede hacerse mediante un botón de "Informar phishing" directamente desde la bandeja de entrada.

ThreatLabz recomienda además que su capacitación sobre la seguridad siga las pautas de la Agencia de Seguridad e Infraestructura de la Ciberseguridad (CISA) de los EE. UU. que aconseja a los usuarios finales estar atentos a los siguientes indicadores:

- **Direcciones de remitentes sospechosas**. La dirección de correo electrónico de un remitente puede imitar a la de una empresa auténtica. Los ciberdelincuentes suelen utilizar direcciones que se asemejan mucho a las de empresas de buena reputación alterando u omitiendo algunos caracteres.
- **Saludos y firmas genéricas.** Tanto un saludo genérico, como "Estimado cliente" o "Señor/Señora", como la falta de información de contacto en el bloque de la firma son fuertes indicadores de un correo electrónico de phishing. Una organización de confianza normalmente se dirigirá a usted por su nombre y proporcionará su información de contacto.
- **Hipervínculos y sitios web falsificados.** Si pasa el cursor por encima de cualquier enlace del cuerpo del correo electrónico y el texto que aparece al pasar el ratón no coincide, es posible que el enlace sea falso. Los sitios web maliciosos pueden parecer idénticos a los auténticos, pero la URL puede tener una variación ortográfica o un dominio diferente (por ejemplo, ".com" en vez de ".net"). Además, los ciberdelincuentes pueden utilizar un servicio de acortamiento de URL para ocultar el verdadero destino del enlace.
- **Ortografía y diseño.** Una mala estructura gramatical y de oraciones, errores ortográficos y un formato incongruente son otros indicadores de un posible intento de phishing. Las instituciones confiables tienen personal dedicado que produce, verifica y revisa la correspondencia con los clientes.
- **Archivos adjuntos sospechosos.** Un correo electrónico no solicitado en el que se pide al usuario que descargue y abra un archivo adjunto es un mecanismo de entrega habitual de malware. Un ciberdelincuente puede utilizar una falsa sensación de urgencia o importancia para ayudar a persuadir a un usuario a descargar o abrir un archivo adjunto sin examinarlo primero.

Mejores prácticas: controles de seguridad

Dado que los empleados y otros usuarios finales serán invariablemente víctimas de intentos de phishing, los equipos de seguridad deben disponer de protecciones para detectar y mitigar los daños. Algunas protecciones importantes:

- **Escaneo del correo electrónico.** El correo electrónico es, por mucho, el vector de phishing más común, por lo que es fundamental contar con un servicio de escaneo de correo electrónico basado en la nube que inspeccione los correos electrónicos antes de que lleguen a su perímetro, con protección en tiempo real contra enlaces maliciosos y falsificación de nombres de dominio.
- **Informar**. Los ataques de phishing suelen dirigirse a muchos usuarios finales de una organización para aumentar las posibilidades de éxito. Permita que los usuarios finales informen los intentos de phishing para bloquear los remitentes y enlaces maliciosos lo antes posible, idealmente con un botón de notificación de phishing integrado en los correos electrónicos de los clientes y usuarios. Implemente un manual de procedimientos para investigar y responder a los incidentes de phishing, incluida la presentación de informes por parte de las agencias para ayudar al gobierno a luchar contra los estafadores y detener los ataques contra otras organizaciones.
- **Autenticación multifactor**. La MFA sigue siendo una de las defensas más efectivas contra el phishing. Con la MFA en funcionamiento, se necesita más que una contraseña para comprometer una cuenta. Las aplicaciones de autenticación como Okta Verify o Google Authenticator son especialmente eficaces y proporcionan una defensa adicional contra las tácticas de MiTM que pueden interceptar mensajes SMS.
- **Inspección del tráfico cifrado.** Más del 95 % de los ataques utilizan canales cifrados, que a menudo no se inspeccionan, lo que facilita que incluso atacantes no muy sofisticados eludan los controles de seguridad. Las organizaciones deben inspeccionar todo el tráfico, cifrado o no, para evitar que los atacantes pongan en peligro sus sistemas.
- **Software antivirus**. Los puntos finales deben protegerse con antivirus actualizados periódicamente para identificar archivos maliciosos y evitar que se descarguen.
- **Protección avanzada contra amenazas**. Los antivirus pueden detener las amenazas conocidas, pero los adversarios son capaces de crear nuevas variantes de malware desconocidas que pueden eludir las herramientas de detección por firmas. Implemente un sistema de aislamiento en línea que pueda poner en cuarentena y analizar archivos sospechosos, y un sistema de aislamiento del navegador que restrinja el contenido web potencialmente malicioso sin interrumpir los flujos de trabajo del usuario final.
- **Filtrado de URL.** Limite el riesgo de phishing con el filtrado de URL que utiliza políticas para administrar el acceso a las categorías más peligrosas de contenido web, como los dominios recién registrados.
- **Parches regulares.** Mantenga actualizadas las aplicaciones, los sistemas operativos y las herramientas de seguridad con los parches más recientes para reducir las vulnerabilidades y garantizar que estén instaladas las protecciones más recientes.
- **Arquitectura de confianza cero**. Si bien es importante contar con controles para evitar el phishing, también lo es disponer de otros controles que limiten los daños de un ataque exitoso. Emplee una segmentación granular, imponga el acceso con menos privilegios y supervise continuamente el tráfico para detectar a los atacantes que puedan haber comprometido su infraestructura.
- **Fuentes de inteligencia sobre amenazas.** Las fuentes de inteligencia sobre amenazas se integran con las herramientas de seguridad existentes para proporcionar un enriquecimiento automático del contexto con el fin de mejorar la detección y acelerar la resolución de las amenazas de phishing. Las fuentes de inteligencia sobre amenazas proporcionan un contexto actualizado sobre las URL denunciadas, los indicadores de peligro (IOC) extraídos y las tácticas, técnicas y procedimientos (TTP) para la toma de decisiones y el establecimiento de prioridades.

Mejores prácticas: cómo identificar un intento de phishing

Las páginas de phishing se pueden identificar por indicadores de tácticas comunes que los malintencionados utilizan para engañar a los usuarios y a los motores de seguridad, así como por atajos que los malintencionados suelen tomar al generar nuevas páginas de phishing. La creación de nuevos sitios de phishing aumenta en la época de las fiestas y durante otros eventos aislados. Por ejemplo, durante la pandemia, el sector de la seguridad vio cómo los atacantes publicaban una cantidad de sitios web falsos relacionados con COVID-19 que se aprovechaban de las víctimas haciéndose pasar por organizaciones sanitarias y sitios de pedidos de kits de pruebas y suministros médicos. Para detectar las últimas amenazas de phishing, es importante estar al tanto de las últimas investigaciones y recoger información procesable con indicadores actualizados para utilizarlos en sus reglas de detección y flujos de trabajo de respuesta.

A continuación le ofrecemos una visión general de varios indicadores que usted (y sus herramientas antiphishing) deberían tener en cuenta:

Toda la página se basa en una sola imagen. Los atacantes aprovechan el phishing basado en imágenes en el que toda la página se basa en una imagen de fondo que es una copia de una página web legítima. El único componente distinto de la página es un formulario web para recoger las credenciales robadas. Esta es una técnica muy común utilizada para atacar especialmente a los bancos.

La página no tiene título.

La página tiene un anclaje vacío para enlaces críticos. Las páginas de phishing suelen usar anclajes vacíos para páginas importantes como ayuda, preguntas frecuentes, etc., cuando copian contenido de páginas legítimas.

La página tiene un certificado autofirmado.

La página parece ser un cliente de correo electrónico web genérico. Los actores de phishing a menudo utilizan páginas de correo electrónico web genérico para hacer phishing de credenciales de correo electrónico, imitando sitios como Webmail, Zimbra, etc.

La página no está cifrada. Una solicitud de inicio de sesión en una página "http" es sospechosa y debe ser marcada.

La página tiene múltiples redireccionamientos antes de llegar a un aviso de inicio de sesión.

La página contiene contrabando de HTML. Con el contrabando de HTML, los atacantes ocultan un blob de JavaScript malicioso codificado dentro de un archivo adjunto de correo electrónico, que es luego ensamblado por el navegador. Esto les permite eludir los filtros de correo electrónico. El contrabando de HTML junto con una solicitud de inicio de sesión es un comportamiento muy sospechoso.

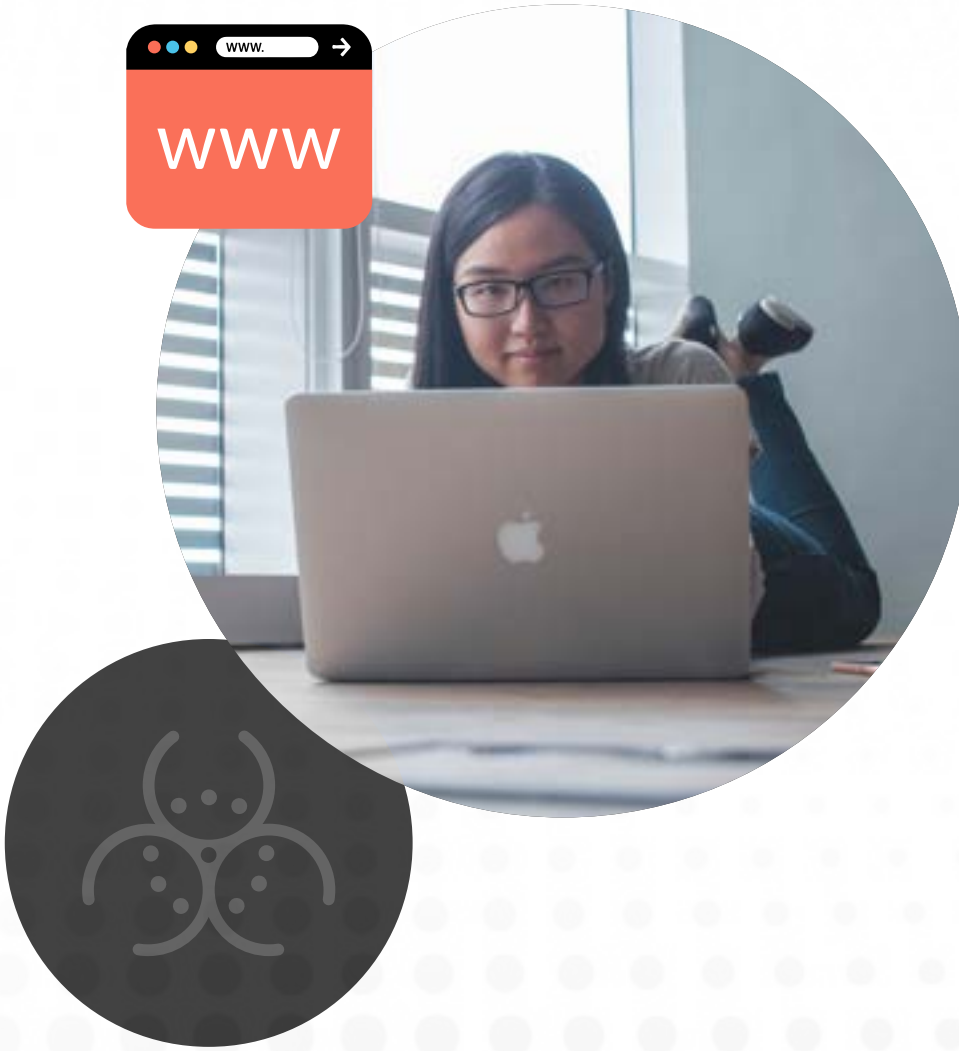
La página contiene etiquetas encubiertas. Los operadores de phishing pueden encubrir campos como el título, el copyright, etc.

La página reemplaza los caracteres clave por "homoglifos". Las páginas de phishing abusan de los homoglifos (caracteres que parecen similares a otros caracteres) para evitar la detección. Esta técnica aprovecha las similitudes en caracteres que pertenecen a diferentes secuencias de caracteres para engañar a los usuarios, así como a los motores de seguridad que buscan coincidencias con los patrones ASCII.

Cómo Zscaler Zero Trust Exchange puede mitigar los ataques de phishing

El usuario afectado es uno de los problemas de seguridad más difíciles de defender. Su organización debe implementar controles de prevención de phishing como parte de una estrategia más amplia de Zero Trust que le permita detectar las filtraciones activas y minimizar los daños causados por las filtraciones exitosas. El Zscaler Zero Trust Exchange™ está construido sobre una arquitectura holística de confianza cero que ayuda a detener el phishing de las siguientes maneras:

- **Evitando el compromiso:** inspección SSL completa a escala, aislamiento del navegador y control de acceso basado en políticas para evitar el acceso a sitios web sospechosos.
- **Eliminando el movimiento lateral:** conecta a los usuarios directamente con las aplicaciones, no con la red, para limitar el radio de alcance de un posible incidente.
- **Bloqueando a los usuarios comprometidos y las amenazas internas:** si un atacante obtiene acceso a su sistema de identidad, podemos evitar intentos de utilización de las aplicaciones privadas mediante la inspección en línea y detectar a los atacantes más sofisticados con el servicio de engaño integrado.
- **Evitando la pérdida de datos:** Inspeccione los datos en movimiento y en reposo para evitar posibles robos por parte de un atacante activo.



Productos Zscaler relacionados:

Zscaler Internet Access™: el acceso a Internet de Zscaler ayuda a identificar y detener la actividad maliciosa al enrutar e inspeccionar todo el tráfico de Internet a través de Zero Trust Exchange. Zscaler bloquea:

- **Las URL e IP** observadas en la nube de Zscaler y de fuentes de información de amenazas comerciales y de código abierto integradas de manera nativa. Esto incluye las categorías de URL de alto riesgo definidas por la política y utilizadas habitualmente para el phishing, como los dominios recién observados y los recién activados.
- **Firmas IPS** desarrolladas a partir del análisis de ThreatLabz de kits y páginas de phishing.
- **Sitios de phishing nuevos** que se identifican por análisis de contenido utilizando la detección de IA/aprendizaje automático.

Advanced Threat Protection bloquea todos los dominios C2 conocidos.

Advanced Firewall amplía la protección C2 a todos los puertos y protocolos, incluidos los destinos C2 emergentes.

Browser Isolation: el aislamiento del navegador en la nube crea un espacio seguro entre los usuarios y las categorías web maliciosas, presentando el contenido como un flujo de imágenes perfectas para eliminar la fuga de datos y la distribución de amenazas activas.

Advanced Cloud Sandbox: el sandbox avanzado en la nube evita la distribución de malware desconocido en cargas útiles de segunda etapa.

Zscaler Private Access™: el acceso privado de Zscaler protege las aplicaciones al limitar el movimiento lateral mediante la segmentación usuario–a–aplicación de acceso con privilegios mínimos y la inspección completa en línea del tráfico de aplicaciones privadas.

Zscaler Deception™ el servicio de engaño de Zscaler detecta y contiene a los atacantes que intentan moverse lateralmente o escalar privilegios atrayéndolos con servidores, aplicaciones, directorios y cuentas de usuario señuelo.

Los próximos pasos

Descubra los riesgos críticos en todo su entorno de nube pública con Zscaler Security Risk Assessment. Disponga de un inventario completo de activos en la nube, una visión clara de los riesgos de seguridad en su nube pública, una visión general de cómo está cumpliendo con los puntos de referencia de cumplimiento y una guía de corrección práctica.

Acerca de ThreatLabZ

ThreatLabz es el brazo de investigación de seguridad de Zscaler. Este equipo de primer nivel es responsable de la búsqueda de nuevas amenazas y de garantizar que las miles de organizaciones que utilizan la plataforma global de Zscaler estén siempre protegidas. Además de la investigación de malware y el análisis conductual, los miembros del equipo están involucrados en la investigación y el desarrollo de nuevos módulos de prototipo para la protección avanzada contra amenazas en la plataforma Zscaler, y realizan auditorías de seguridad internas regularmente para garantizar que los productos e infraestructura de Zscaler cumplan con los estándares de seguridad. ThreatLabz publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal, research.zscaler.com.

Manténgase informado acerca de la investigación de ThreatLabz suscribiéndose a nuestro boletín Trust Issues hoy mismo.

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zero Trust Exchange™ protege a miles de clientes contra ciberataques y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange, basado en SASE, es la plataforma de seguridad en la nube en línea más grande del mundo.

Obtenga más información en zscaler.com.mx o síganos en Twitter @zscaler.

Anexo

Categorización de los ataques de phishing

Los ataques de phishing pueden clasificarse de diversas maneras y pueden englobar diversas técnicas. Sin embargo, los atacantes están adaptando sus métodos para engañar a los usuarios que son cada vez más astutos y eludir las herramientas de defensa. A continuación, describimos las definiciones y características más comunes de los ataques de phishing.

Estas listas incluyen varias descripciones de métodos de ataque físico y la amenaza que suponen para las organizaciones. La mayor parte de este informe se centra en las amenazas de phishing virtual que requieren una conexión a Internet para llevarse a cabo. Una característica reveladora de las estafas de phishing en línea es que suelen pedir a los usuarios que envíen información o descarguen programas maliciosos a través de uno de los siguientes métodos:

- **Enlace:** Un usuario hace clic en un enlace malicioso a un sitio de phishing, un archivo alojado o malware.
- **Indicación:** Se solicita a un usuario que envíe información sensible, lo que resulta en el robo de datos.
- **Archivo adjunto:** Un usuario abre un archivo adjunto que contiene software malicioso.

Cuando piense en qué invertir para reducir los incidentes de phishing este año, tenga en cuenta los siguientes tipos de ataques de phishing.

Todos los tipos más comunes de ataques de phishing

1. **Bombardeo MFA:** Los atacantes engañan a los usuarios con credenciales comprometidas para que verifiquen una solicitud MFA no auténtica realizada por el actor de la amenaza. Estos ataques se caracterizan normalmente por un flujo continuo de solicitudes de MFA, a veces acompañadas de una llamada, un mensaje de texto o un correo electrónico falsos que engañan al usuario para que, sin saberlo o por accidente, verifique una de las solicitudes.
2. **Phishing Adversary-in-the-Middle (AitM):** Los atacantes imitan las acciones de una víctima desprevenida para obtener sus credenciales de inicio de sesión y las cookies de sesión.
3. **Phishing Angler:** Los atacantes se hacen pasar por un servicio de atención al cliente y ofrecen ayuda para responder a comentarios negativos sobre una empresa publicados en las redes sociales, con el objetivo de captar clientes insatisfechos, sobre todo de bancos.
4. **Phishing Baiting:** Los atacantes utilizan ofertas tentadoras, nombres de archivos o dispositivos para atraer a los curiosos a una trampa, de forma similar a un ataque con troyanos.
5. **Phishing Browser-in-the-Browser (BitB):** Los atacantes despliegan una ventana maliciosa dentro de una ventana del navegador para imitar un dominio auténtico y replicar ventanas emergentes de inicio de sesión que parecen proceder de proveedores de autenticación de terceros.
6. **Phishing con seguimiento:** los atacantes obtienen acceso físico a un área restringida siguiendo a una persona autorizada que tiene acceso al interior. Esta forma de ataque se clasifica como phishing cuando alguien muerde el anzuelo de ingeniería social (por ejemplo, llevando muchas cajas grandes) presentado por el atacante y le permite entrar sin verificación.

7. **Phishing de clones:** Los atacantes crean mensajes de correo electrónico duplicados que parecen proceder de fuentes de confianza, con ligeras modificaciones y archivos adjuntos o enlaces maliciosos.

8. **Phishing de código QR:** Los atacantes utilizan códigos QR que, al ser escaneados por el smartphone de la víctima, conducen a sitios web maliciosos o descargan malware en el dispositivo.

9. **Phishing de correo electrónico:** Los atacantes envían mensajes de correo electrónico con ingeniería social haciéndose pasar por marcas conocidas, con enlaces URL maliciosos o activos adjuntos diseñados para robar información o distribuir programas maliciosos.

10. **Phishing de Doc Clouding:** Los atacantes envían documentos maliciosos desde fuentes comunes en la nube como Google Drive, Box o OneDrive para eludir las herramientas de seguridad tradicionales y hacer que su detección resulte difícil para la mayoría de los equipos de seguridad.

11. **Phishing de fraude de CEO o de correo electrónico empresarial comprometido (BEC):** los atacantes se dirigen a los empleados de la empresa utilizando cuentas de ejecutivos comprometidas para enviar facturas falsas o solicitudes de pago por transferencia bancaria u otras formas.

12. **Phishing de HTTPS:** Los atacantes utilizan el "protocolo de transferencia de hipertexto seguro" cifrado para engañar a los usuarios que confían en él y lograr que hagan clic en enlaces URL maliciosos.

13. **Phishing de malvertising:** Los atacantes utilizan secuencias de comandos en los anuncios para enviar contenido no deseado directamente a los equipos de las víctimas.

14. **Phishing de motor de búsqueda**: los atacantes apuntan a los consumidores con sitios de compras en línea falsos indexados por los motores de búsqueda. Al ofrecer descuentos significativos en productos destacados, estos sitios que aparecen en los resultados pueden aparecer como elementos emergentes de temporada o contener comentarios falsos con fechas retroactivas. Sin saberlo, las víctimas pueden compartir datos personales, información bancaria, números de tarjeta de crédito o incluso pagar por productos falsos. Los estafadores han llegado a ofrecer información falsa de envío y seguimiento e incluso "artículos de muestra baratos" para extender el ciclo de vida de estos sitios.

15. **Phishing de obtención de credenciales:** los atacantes crean páginas de inicio de sesión falsas o envían correos electrónicos de phishing que imitan las solicitudes de inicio de sesión auténticas para robar nombres de usuario y contraseñas a víctimas desprevenidas.

16. **Phishing de Pharming o DNS Cache:** Los atacantes redirigen a los visitantes a un sitio malicioso alterando la dirección IP de un sitio web legítimo en los servidores del sistema de nombres de dominio (DNS) comprometidos, o enviando un correo electrónico de phishing con un código malicioso que redirige a la víctima al sitio cuando introduce cualquier URL desde su computadora.

17. **Phishing de ransomware:** Los atacantes envían correos electrónicos con archivos adjuntos o enlaces maliciosos que, al hacer clic, descargan el ransomware en la computadora de la víctima y exigen un pago a cambio de una clave de descifrado de recuperación.

18. **Phishing de túnel inverso:** Los atacantes utilizan un servidor remoto para crear un túnel SSH inverso al equipo de la víctima, lo que les permite explotar la máquina para diversos fines, como la instalación de malware o el robo de datos confidenciales, permaneciendo ocultos para evitar ser detectados por la víctima.

19. **Phishing Evil Twin:** Los atacantes imitan una red Wi-Fi pública de confianza para observar la actividad en línea de las víctimas y robar los datos que pasan por el punto de acceso malicioso.

20. **Phishing Man-in-the-Middle (MiTM):** Los atacantes se centran en los usuarios de un servidor o sistema específico, capturando datos en tránsito como credenciales, cookies o información de cuentas bancarias, imitando servicios en línea a través de servidores proxy.

21. **Phishing por chat o mensajería instantánea:** Los atacantes utilizan los mensajes instantáneos para enviar estafas dentro de las aplicaciones, normalmente con enlaces a URL maliciosas.

22. **Phishing selectivo**: los atacantes organizan campañas utilizando información disponible públicamente que está orientada a personas que trabajan para organizaciones específicas. Estos correos electrónicos engañosos pueden contener información real y parecen solicitudes internas legítimas para engañar a los destinatarios para que realicen la acción deseada.

23. **Phishing Watering Hole:** los atacantes apuntan a los miembros de grupos específicos con probabilidades de visitar un sitio específico que ha sido afectado por el atacante o creado con este fin.

24. **Smishing**: los atacantes utilizan mensajes de texto (comunicación por SMS) para distribuir estafas, normalmente con enlaces de URL maliciosos. El remitente del mensaje parece ser una marca conocida o un conocido del destinatario.

25. **USB:** los atacantes plantan físicamente dispositivos USB cargados con ejecutables maliciosos que se cargan cuando se conectan a cualquier punto final vulnerable o envían a las víctimas a ellos.

26. **Vishing** o ataques de phishing de voz: los atacantes hacen llamadas telefónicas maliciosas que utilizan la ingeniería social para presionar a los destinatarios a realizar una acción como transferir dinero o revelar información personal.

27. **Whaling:** Los atacantes apuntan a ejecutivos y personas de alto perfil utilizando información disponible públicamente. Utilizarán ingeniería social para que el blanco revele secretos comerciales confidenciales que puedan utilizarse con fines fraudulentos o lo engañarán para que realice otra acción que el actor de la amenaza pueda utilizar para lograr sus objetivos.

El phishing no puede eliminarse únicamente a través de la tecnología. Las organizaciones deben seguir la evolución de las estafas de phishing para observar cómo los cambios en el conocimiento cultural mitigan las técnicas específicas con el paso del tiempo. Conocer los diferentes tipos de estafas puede ayudar a los profesionales de la seguridad a educar a los empleados sobre cómo adoptar una perspectiva de confianza cero cuando se encuentren con lo que pueda parecer una oportunidad real, una solicitud de verificación o una notificación push. Cuando desarrolle su propia estrategia para reducir los incidentes de phishing, considere incluir los siguientes tipos de estafas comunes:

Principales categorías de estafas de phishing

Las estafas en la nube se hacen pasar por servicios de intercambio de archivos o de almacenamiento en la nube con señuelos como falsas solicitudes de acceso y notificaciones de cuentas.

Las estafas al consumidor se hacen pasar por marcas de comercio electrónico con señuelos como notificaciones de cuentas falsas y declaraciones de afiliación o beneficios.

Las estafas comerciales se hacen pasar por servicios generales como FedEx con señuelos como notificaciones de seguimiento y solicitudes de pago.

Las estafas corporativas se hacen pasar por empresas específicas con señuelos como falsas notificaciones de cuentas, actualizaciones de la empresa, tareas de recursos humanos y solicitudes de pago de facturas.

Las estafas de citas se hacen pasar por personas que buscan citas utilizando una plataforma en línea con señuelos como perfiles falsos, mensajes, me gusta y seguidores.

Las estafas de servicios financieros se hacen pasar por instituciones financieras conocidas y apuntan a personas con señuelos como notificaciones de cuentas falsas o alertas de seguridad.

Las estafas de gobierno se hacen pasar por organismos federales como el IRS con señuelos como reclamos de beneficios, préstamos de ayuda y solicitudes de pago atrasado falsos.

Las estafas de oferta de trabajo se hacen pasar por empresas falsas y reales que buscan contratar empleados nuevos con señuelos como publicaciones, solicitudes y ofertas de empleo falsas.

Las estafas de notificaciones push o por navegador se hacen pasar por notificaciones del navegador web con señuelos como recordatorios falsos para instalar actualizaciones, alertas de mensajes y anuncios de productos.

Las estafas de redes sociales se hacen pasar por plataformas sociales o usuarios con señuelos como cuentas falsas o falsificadas, mensajes privados, avisos o notificaciones de cuentas y alertas de seguridad.

Las estafas técnicas se hacen pasar por servicios generales o marcas conocidas con señuelos como notificaciones de cuenta, mensajes de error y actualizaciones de software.

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de los ciberataques y la pérdida de datos al conectar a los usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos a nivel mundial, Zero Trust Exchange en SASE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en www.zscaler.com.mx.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com.mx