Informe sobre el phishing de Zscaler ThreatLabz 2023

Índice

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.

Al analizar 280 000 millones de transacciones diarias y 8 000 millones de ataques bloqueados diarios en el transcurso de 2022, el equipo de Zscaler ThreatLabz observó un aumento del 47,2 % en los intentos de phishing con respecto a 2021, una tendencia al alza que se espera que continúe en 2023.

El aumento de la prevalencia de los kits de phishing provenientes de los mercados negros y las herramientas de IA de chatbot como ChatGPT ha hecho que los atacantes desarrollen rápidamente campañas de phishing más precisas. Esta mayor precisión a la hora de fijar objetivos de phishing ha simplificado el proceso de manipular a los usuarios para que realicen acciones que comprometan sus credenciales de seguridad, dejándolos a ellos y a sus organizaciones vulnerables.

Con el auge de las ofertas de IA y PaaS, es más fácil que nunca para los ciberdelincuentes comprometer instituciones y acceder a datos comerciales, personales y financieros confidenciales para usarlos para la extorsión. Si bien muchas de las organizaciones actuales tienen infraestructuras sólidas de ciberseguridad, deben volver a examinar esas infraestructuras a la luz de las tendencias actuales y considerar adoptar un enfoque de confianza cero.

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

Hallazgos clave en 2022

Los ataques de phishing aumentaron un 47,2 % en 2022 en comparación con 2021.

Las marcas de Microsoft, incluidas OneDrive y Sharepoint, junto con el intercambio de criptomonedas Binance y los servicios de streaming ilegales, 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, cayó un **67 %**.

Los ataques a marcas relacionadas con la COVID-19 representaron **el 7,2 %** de las estafas de phishing en 2021, mientras que 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 evolucionando y van más allá del phishing de SMS (SMiShing) para usar el phishing relacionado con el correo de voz (vishing) a fin de atraer a las víctimas para que abran archivos adjuntos maliciosos.

Los sofisticados ataques de adversario en el medio (AiTM) están ayudando a los atacantes a eludir las medidas de seguridad de autenticación multifactor (MFA).

Las estafas de contratación dirigidas a personas que buscan trabajo son cada vez más comunes.

Principales objetivos de phishing en 2022

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

Intentos de phishing en 2022 por país

Los diez principales países a los que se dirigieron las estafas de phishing en el último año fueron:

1. Estados Unidos
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 con el mayor número de ataques de phishing, una posición que siempre ha ocupado. Nuestra investigación indica que más del 65 % de todos los intentos de phishing ocurrieron en los EE. UU., un aumento del 60 % con respecto al año pasado. El Reino Unido experimentó un aumento del 269 % en los ataques de phishing.

Varios países vieron aumentar los intentos de phishing en 2022, incluido Canadá, que experimentó un asombroso aumento del 718 %. Algunos expertos de ThreatLabz atribuyen este aumento al aumento adyacente de objetivos en educación. Rusia experimentó un aumento de ataques del 198 % y Japón del 92 %. Sin embargo, Hungría fue testigo de una disminución significativa del 90 % en los ataques de phishing, y el total de objetivos de Singapur se redujo en casi un 48 %.

La reducción de los ataques de phishing dirigidos a Singapur puede deberse a los mayores esfuerzos de seguridad cibernética de su gobierno, incluidas las iniciativas de la Agencia de Seguridad Cibernética (CSA) del país. Esta agencia brinda pautas y consejos a individuos y empresas sobre cómo protegerse de las amenazas cibernéticas y, junto con la Comisión de Protección de Datos Personales (PDPC), hace cumplir las leyes y regulaciones de protección de datos.

Figura 1: Ataques de phishing por país en 2022

Intentos de phishing por sector en 2022

El sector de la educación experimentó un aumento del 576 % en los intentos de phishing en 2022, lo que hizo que pasase del octavo sector más atacado al primero, superando al sector que ocupó ese puesto el año pasado, la venta minorista/mayorista. Los autores del phishing probablemente aprovecharon los procesos para el pago de préstamos estudiantiles y las solicitudes de alivio de la deuda que se presentaron el año pasado, y explotaron las vulnerabilidades del aprendizaje remoto. Las finanzas y los seguros también vieron un aumento en los objetivos de phishing de un 273 % en 2022.

Los intentos de phishing en el sector de la salud también aumentaron exponencialmente y pasaron de poco menos de 31 millones a más de 114 millones. Los pacientes que postergaron sus revisiones médicas rutinarias durante el año inicial de la pandemia de COVID-19 reanudaron sus tratamientos de atención médica en 2022, iniciaron sesión en sus cuentas en línea y posiblemente interactuaron con atacantes de phishing que se hacen pasar por organizaciones de asistencia médica. Además, los atacantes de ransomware están aprovechando más tácticas de phishing para comprometer los datos de las organizaciones de asistencia médica.

Sin embargo, los ataques de phishing dieron un respiro en 2022, con una caída del 67 % en el comercio minorista y mayorista y del 38 % en los servicios. Es probable que la reducción de los ataques a minoristas y mayoristas se deba a un cambio a la baja en el comportamiento de los consumidores después de un periodo de grandes compras y gastos en bienes online en 2021.

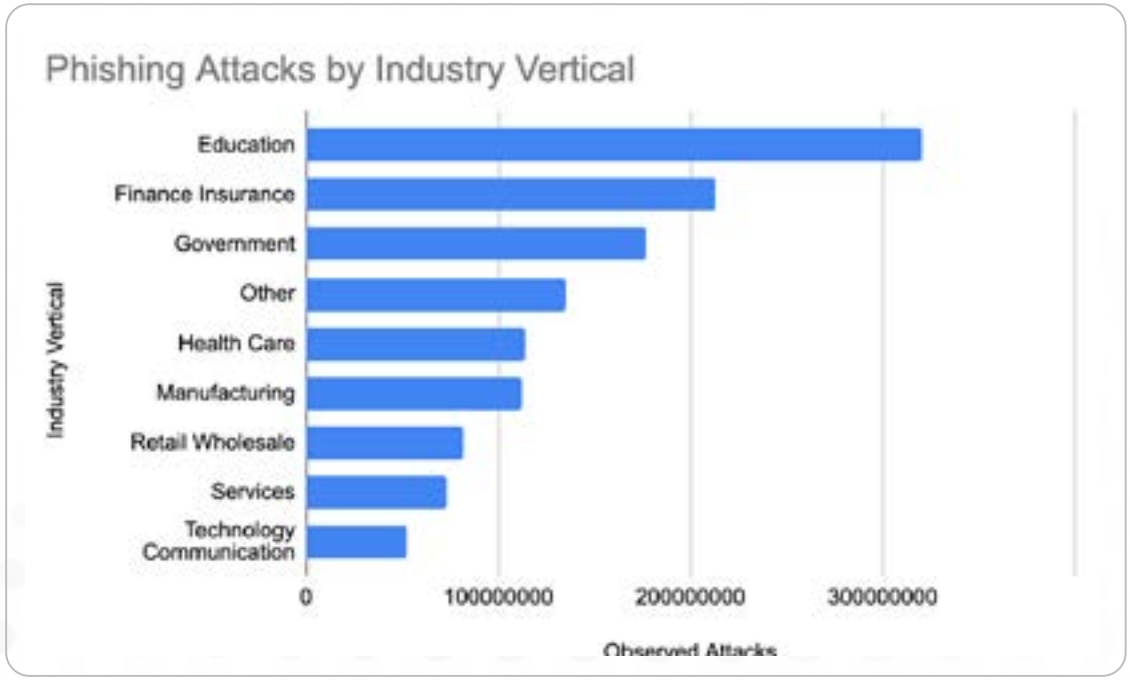
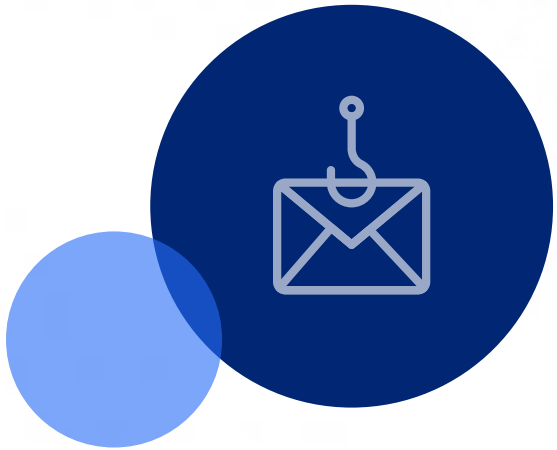


Figura 2: Ataques de phishing por sector en 2022



Marcas más imitadas en ataques de phishing en 2022

Los atacantes de phishing a menudo explotan las tendencias de los consumidores haciéndose pasar por marcas populares para engañar a los consumidores vulnerables. Las categorías de marcas que reciben ataques con más frecuencia incluyen herramientas de productividad, sitios de criptomonedas, sitios de streaming ilegales, plataformas de redes sociales y servicios de mensajería, instituciones financieras, sitios gubernamentales y servicios de logística.

Microsoft volvió a ser la marca más imitada del año, con algo menos del 31 % de los ataques. Su marca OneDrive representó otro 17 %, SharePoint casi el 4 % y Microsoft 365 otro 1,7 %. En 2022, Zscaler descubrió que los atacantes usaban cada vez más OneNote, que se puede integrar con OneDrive y otros productos de Microsoft, para enviar malware a través de correos electrónicos de phishing. Anteriormente, los autores de amenazas se dirigían a los usuarios con documentos maliciosos habilitados para macros, pero en julio de 2022, Microsoft desactivó las macros de forma predeterminada en todas las aplicaciones de Microsoft 365 (Office), lo que hizo que este modo fuera menos confiable para distribuir malware.

El intercambio de criptomonedas Binance representó el 17 % de los ataques de marcas imitadas, con los atacantes haciéndose pasar por representantes de clientes falsos de bancos o empresas P2P. Los sitios de streaming ilegales representaron el 13,6 % de los ataques, con picos durante eventos deportivos importantes, como la Copa Mundial de la FIFA en noviembre y diciembre de 2022.

Si bien los ataques con motivo de la COVID siguen siendo frecuentes, están en declive. En 2021, los ataques relacionados con la 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. Relacionadas con la COVID-19
7. Gobierno
8. Netflix
9. Facebook
10. Microsoft 365
11. Google
12. Telegram
13. Adobe
14. DHL
15. Amazon
16. American Express
17. WhatsApp
18. Roblox
19. PayPal
20. Docusign

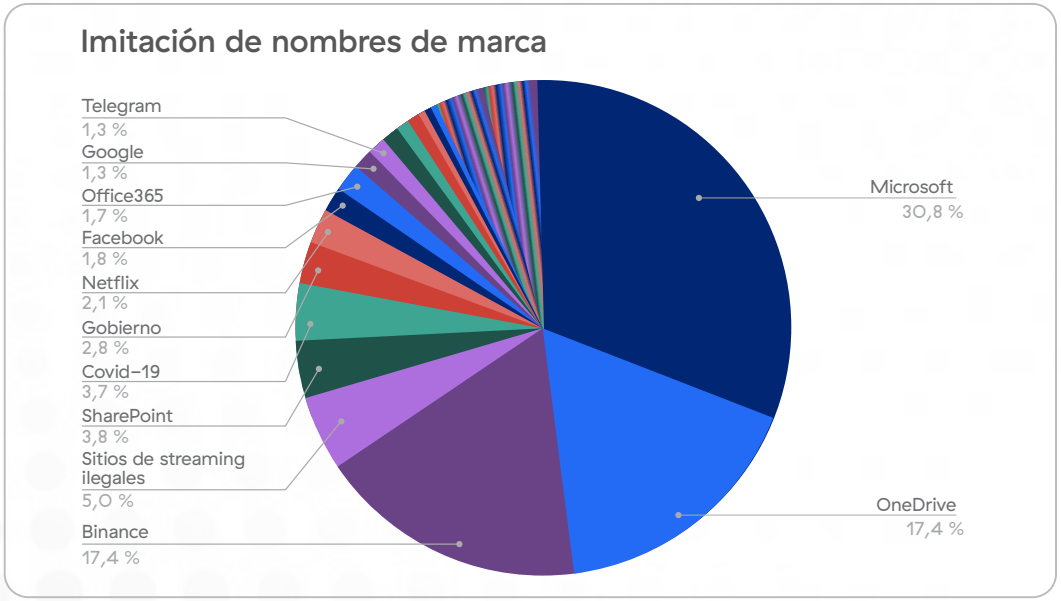


Figura 3: Marcas más imitadas en ataques de phishing

Principales dominios de referencia de 2022

Los atacantes suelen utilizar dominios de confianza para manipular a las víctimas y redirigirlas 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 como Evernote, Dropbox y GitHub.

Analizamos los dominios de referencia para determinar cuáles explotan más los atacantes. En 2022, estos incluyeron sitios de streaming de vídeo, intercambios de criptomoneda y otros sitios financieros, creadores de formularios y sitios web, sitios que alojan contenido generado por el usuario, 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 ataques de phishing

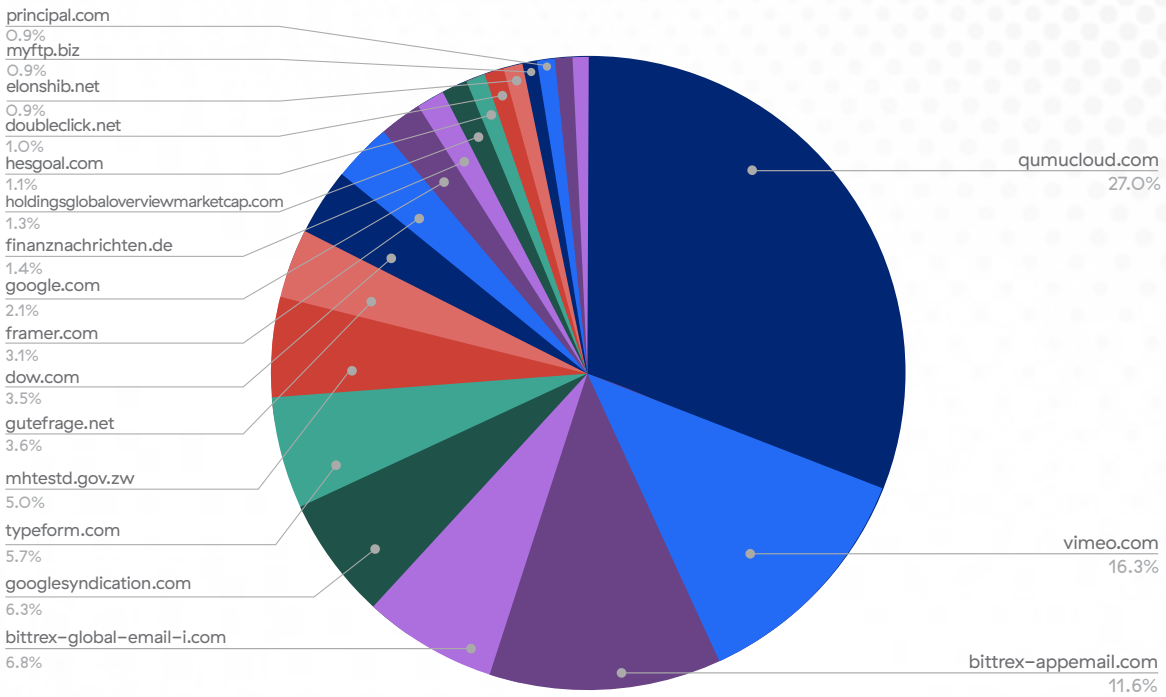


Figura 4: Dominios de referencia más comunes utilizados en los ataques de phishing de 2022

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 que eran responsables de alojar la infraestructura de phishing.

Nuestro análisis mostró que en 2022, el 39 % de los ataques de phishing se realizaron en sitios de alojamiento (frente al 50,6 % en 2021), el 53 % se encontraban en ISP (frente al 39,2 % en 2021) y el 8 % en dominios comerciales.

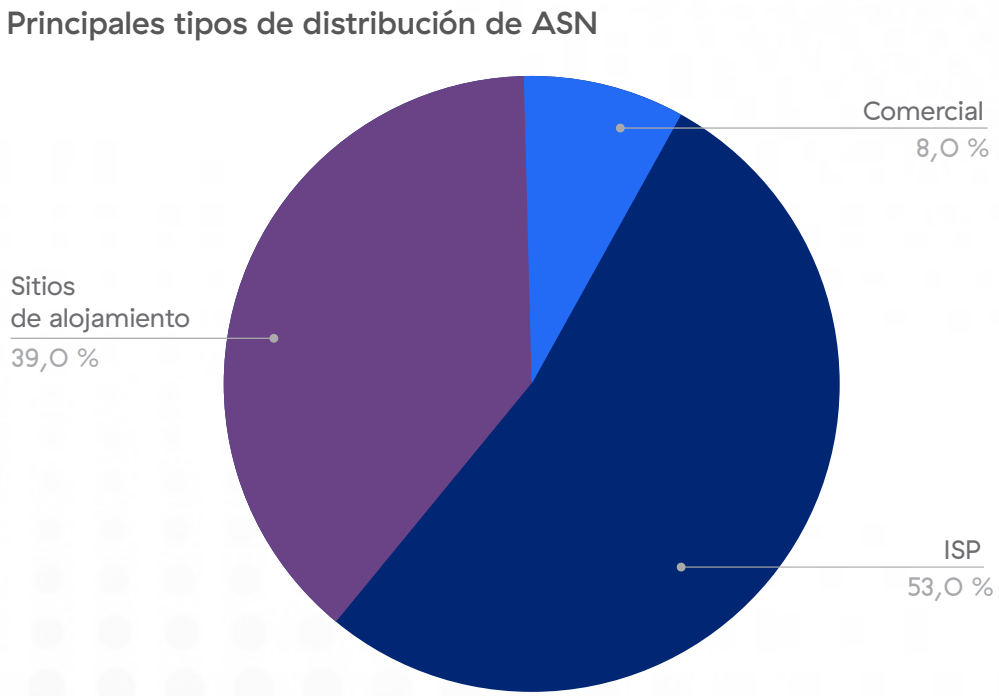


Figura 5: ASN para infraestructura de phishing

Tendencias de phishing en constante evolución

Cada año, los autores de amenazas emplean tácticas más sofisticadas y enfoques cada vez más avanzados para ejecutar sus estafas de phishing. Para garantizar que su organización esté preparada y que su equipo se mantenga a la vanguardia de los ataques, es esencial mantenerse informado sobre las últimas tendencias de amenazas. A continuación encontrará los puntos clave de las tendencias actualizadas de phishing observadas en 2022.

Ataques de vishing

Los ataques de vishing o campañas de phishing a través del correo de voz atraen a las víctimas para que abran archivos adjuntos maliciosos. A mediados de 2022, los autores de amenazas se dirigieron a usuarios de varias organizaciones con sede en EE. UU. con correos electrónicos maliciosos sobre notificaciones del correo de voz para robar sus credenciales de Microsoft 365 y Outlook.

También observamos campañas de phishing con archivos adjuntos de correo electrónico relativos al correo de voz como este:

Figura 6: Correo electrónico de la campaña de vishing

El archivo .html contiene JavaScript ofuscado:

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

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

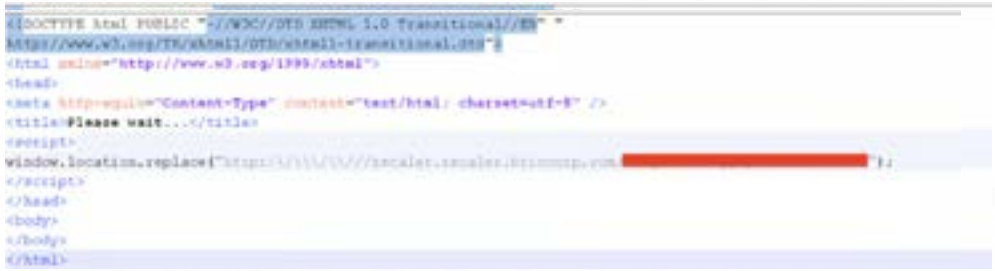


Figura 8: Código de correo electrónico de la campaña de vishing con JavaScript oculto revelado

Esto lleva a una página de phishing de Microsoft:

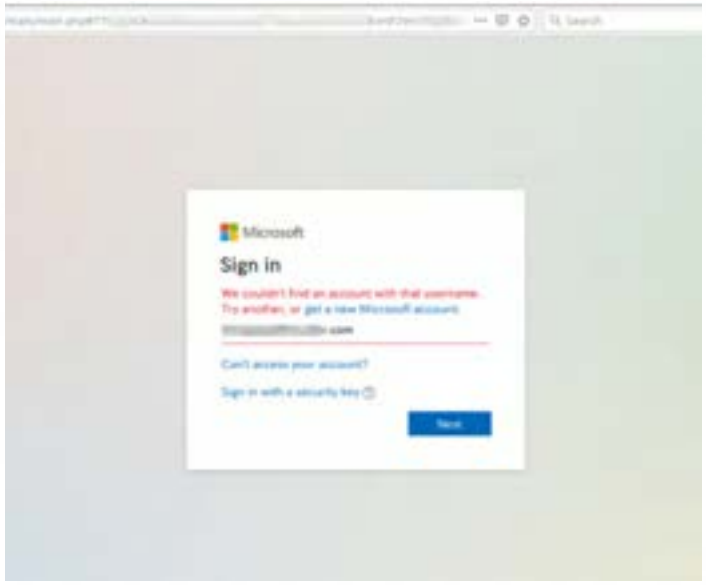


Figura 9: Página de destino de la campaña de vishing

ThreatLabz también descubrió una estafa a través de llamadas de voz en la que un autor de amenazas se dirige a un empleado corporativo haciéndose pasar por un gerente. Inicialmente, la víctima recibe una llamada telefónica suplantada con un mensaje de "hola" pregrabado y luego la llamada termina. Posteriormente, la víctima recibe un mensaje del estafador que indica que el gerente tiene problemas de conectividad de red y solicita que continúe la comunicación a través de mensajes. Luego, el estafador intenta persuadir a la víctima para que divulgue información de la cuenta corporativa 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 estén atentos a este tipo de estafas.

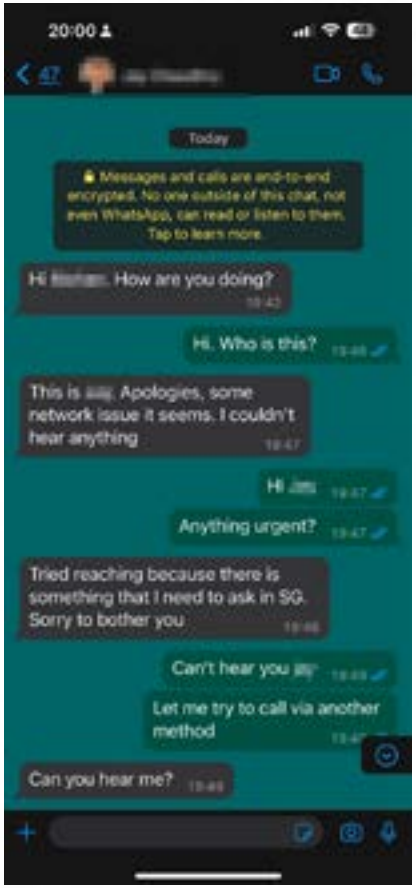


Figura 10: Mensajes de vishing

Estafas de contratación

Durante 2022, ThreatLabz fue testigo de un aumento en los ataques a quienes buscan empleo mediante una variedad de estafas de empleo. Estas estafas utilizaban anuncios de trabajo, sitios web o portales y formularios prefabricados para atraer a personas que buscaban empleo.

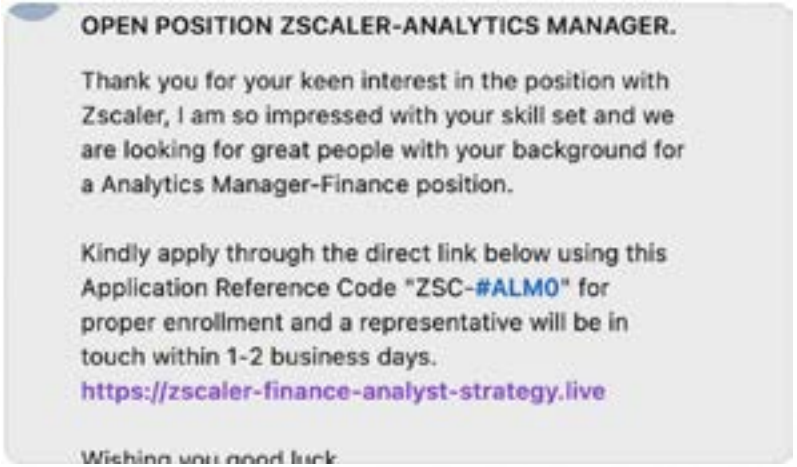


Figura 11: Anuncio falso de LinkedIn con una URL de phishing

Como se puede ver aquí, el atacante publicó un anuncio falso de LinkedIn con una URL de phishing. Visitar la URL falsa permitiría a las posibles víctimas solicitar el trabajo.

Una vez que la víctima solicitara el trabajo, el atacante se comunicaría con ellos y pediría una entrevista por Skype en la que el atacante se haría 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 filtrar datos de tarjetas de crédito.

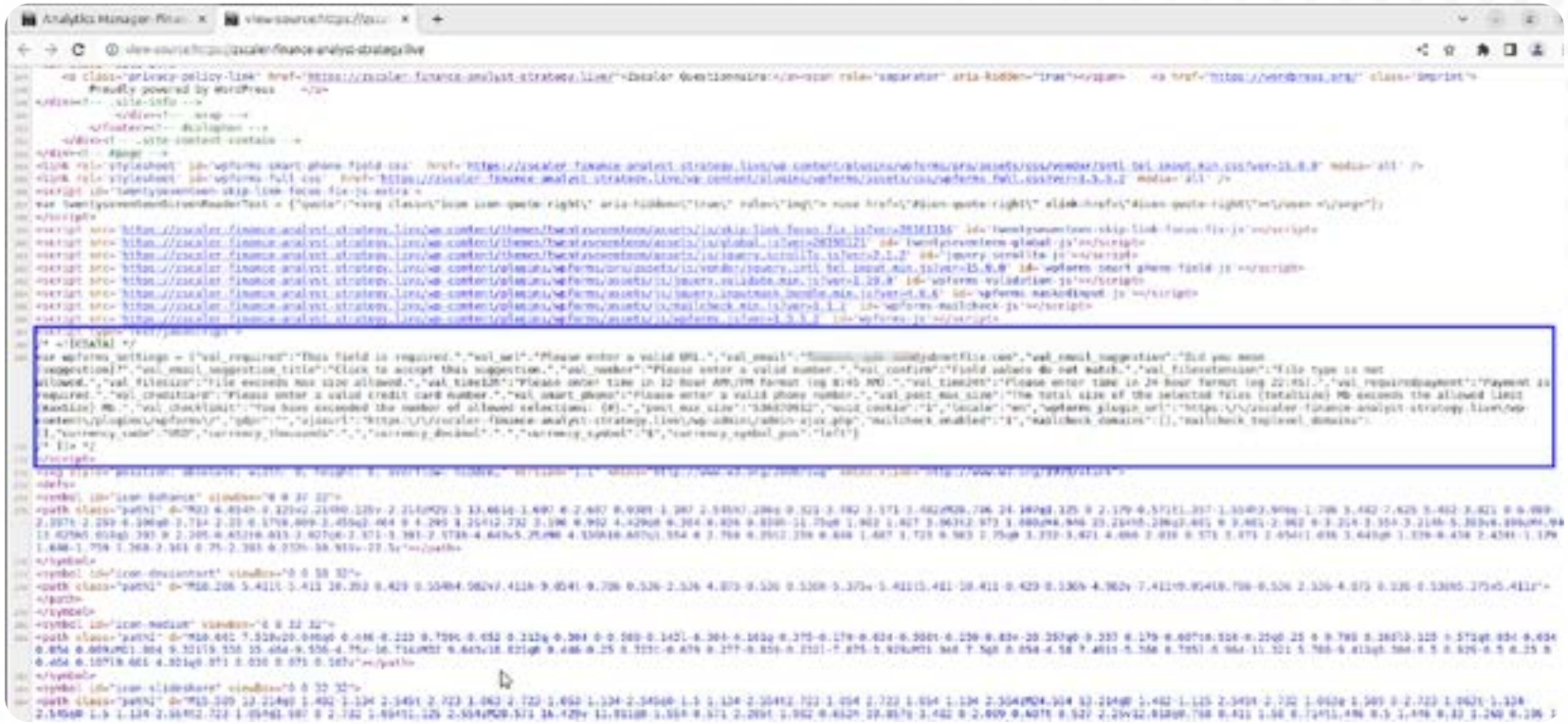


Figura 13: Código fuente de correo electrónico de contratación falso

Ataques de phishing de adversario en el medio (AiTM)

Obtenga más información sobre los ataques de phishing de adversario en el medio (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 tradicionales de phishing que recopilan las credenciales de los usuarios nunca completan el proceso de autenticación con el servidor del proveedor de correo electrónico real. Si el usuario ha habilitado MFA, esta evita que el atacante inicie sesión en la cuenta solo con las credenciales robadas. Para eludir MFA, los atacantes pueden usar ataques de phishing AiTM.

La Figura 14 muestra un fragmento del código de una página de phishing atendida por un servidor de phishing AiTM.

Figura 14: Código de página de phishing atendida por el servidor de phishing AiTM.

El servidor proxy malicioso AiTM modifica las URL en una página de destino legítima con URL que controla el atacante (consulte la figura 15) y actúa como un relé entre la víctima y el servidor de destino.

Figura 15: URL controladas por atacantes modificadas por el servidor proxy AiTM

El subdominio original (en verde), el nombre del dominio original (en azul, menos el TLD) y una ID única generada (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 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 resultó en una fuga de la dirección del servidor controlado por el atacante, como se muestra en la figura 17.

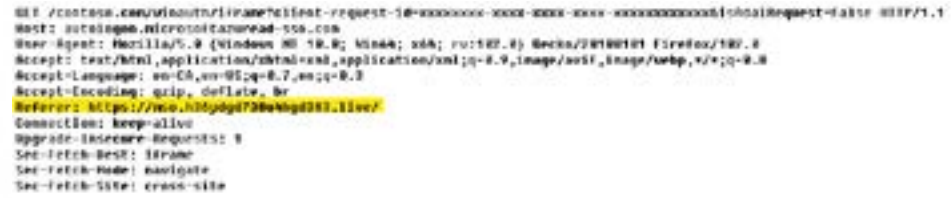


Figura 17: Revelación de la dirección del servidor controlado por el atacante

Ataques de phishing de navegador en el navegador (BiTB)

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

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

La Figura 18 muestra un ejemplo de un ataque de BiTB usando una ventana SSO falsa, generada usando HTML, que tiene como objetivo a Steam, una popular plataforma de juegos digitales.

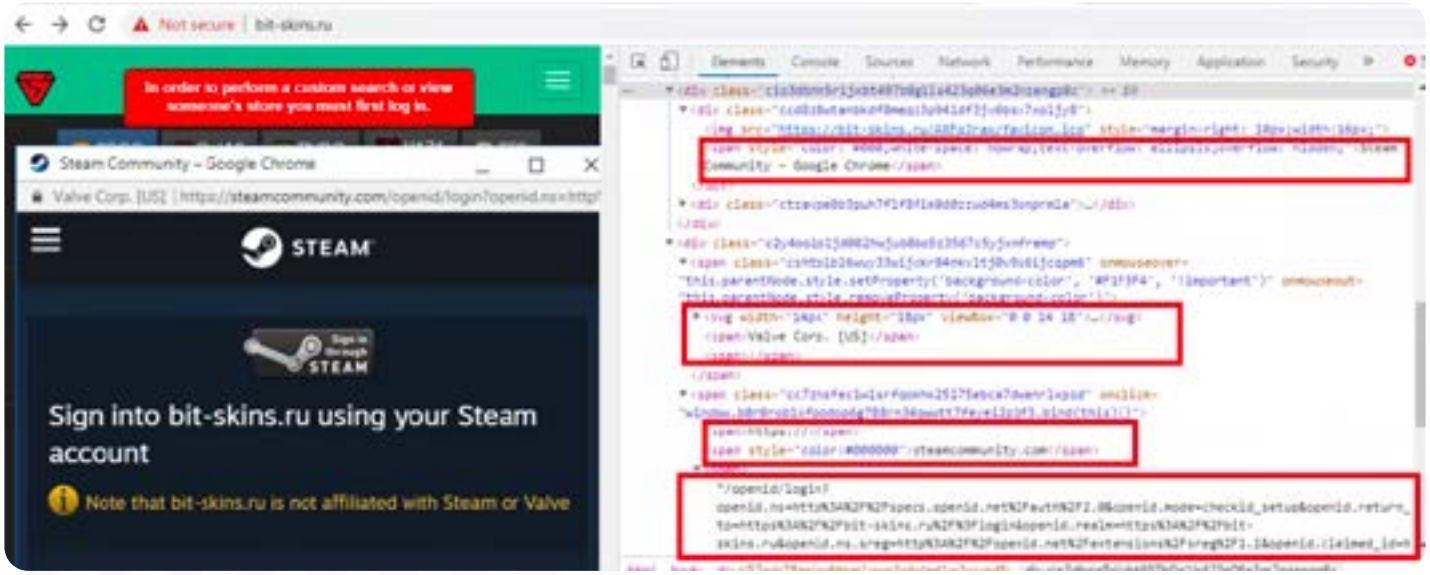


Figura 18: Ataque BiTB o "imagen en imagen"

Uso de servicios legítimos para alojar sitios web de phishing

El equipo de ThreatLabz también observó atacantes que usaban 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 utilizando servicios como linkedin.com.

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

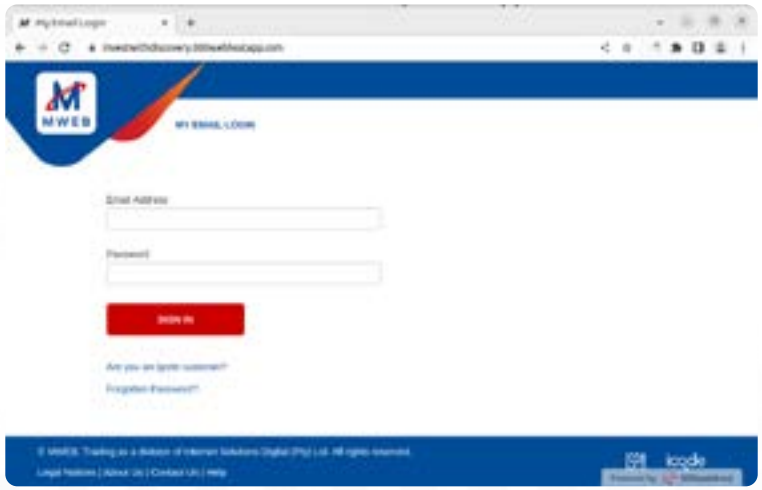


Figura 19: Subdominios DNS dinámicos para alojamiento de páginas de phishing (ejemplo uno)

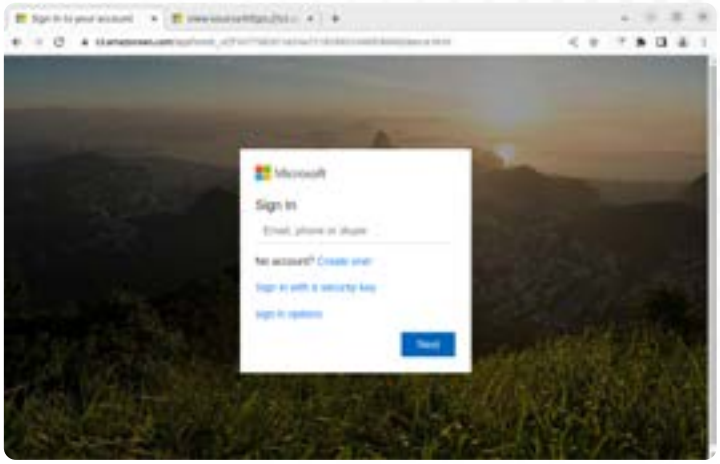


Figura 20: Subdominios DNS dinámicos para alojamiento de páginas de phishing (ejemplo dos)

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

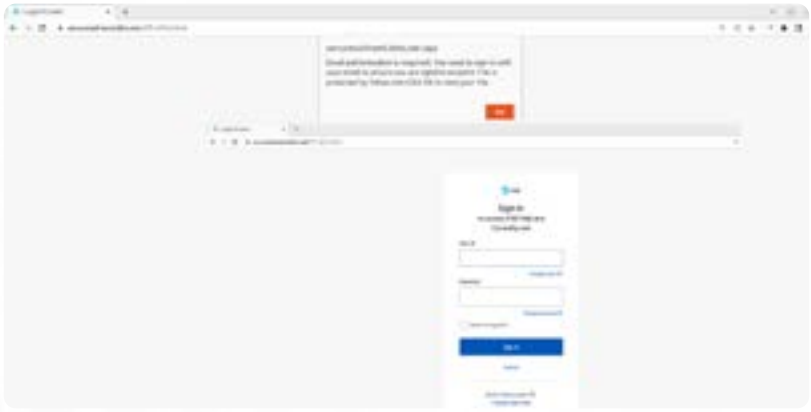


Figura 21: Phishing de T&T alojado mediante DNS dinámico

Phishing mediante el sistema de archivos interplanetario (IPFS)

IPFS es un sistema de archivos peer-to-peer distribuido que permite a los usuarios almacenar y compartir archivos en una red descentralizada de ordenadores. En comparación con los sistemas de archivos centralizados tradicionales, proporciona una forma más segura, resistente y eficiente de almacenar y distribuir archivos.

En IPFS, los archivos se dividen en fragmentos más pequeños y se distribuyen a través de múltiples nodos en una red, lo que dificulta que un único punto de falla comprometa todo el sistema. La Figura 22 muestra el aspecto del phishing de IPFS.

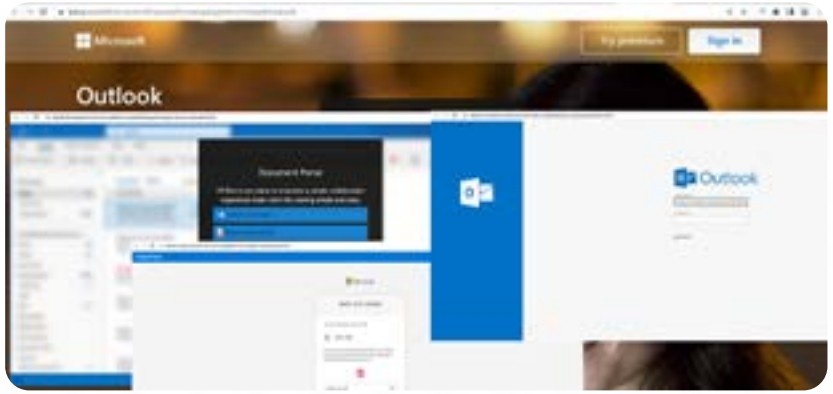


Figura 22: Phishing de IPFS (ejemplo uno)

Debido a su construcción peer-to-peer, es mucho más difícil eliminar una página de phishing alojada en IPFS que una alojada con un método más tradicional.

También observamos atacantes que usaban Google Translate para hacer que sus URL parecieran legítimas.

Figura 23: Ejemplo de phishing de IPFS aprovechando Google Translate

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

Uso de WebSockets para extraer datos de huellas digitales

En el Informe de phishing de Zscaler ThreatLabz 2022, analizamos los kits de phishing y los marcos de phishing de código abierto. Estos kits y marcos empaquetan y comercializan las herramientas necesarias para lanzar rápidamente cientos o miles de páginas de phishing convincentes y efectivas, incluso si el atacante o los atacantes tienen pocas habilidades técnicas.

Algunos de estos kits de phishing tienen una característica llamada "encubrimiento", una técnica que permite a los autores del phishing ocultar una página web de phishing real de los investigadores y análisis de seguridad mientras se la siguen entregando a sus víctimas. El kit de phishing filtra las conexiones de cada visitante según la dirección IP, las palabras clave del nombre de host, el agente de usuario y más. En función de la coincidencia, se definirá como una página benigna o una página de phishing, evitando que los investigadores de seguridad y las herramientas antiphishing que analizan Internet en busca de contenido malicioso la detecten. Los autores de amenazas que utilizan diferentes técnicas de encubrimiento pueden eludir estos métodos de descubrimiento tradicionales.

Este año, observamos una nueva característica en la toma de huellas digitales de los clientes. Esto es lo que sucede cuando un visitante llega a una página de phishing y se toman sus huellas digitales:

1. El usuario navega por la página de phishing
2. El servidor devuelve un JavaScript para tomar la huella digital del cliente y JavaScript carga la huella digital a través de una conexión WebSocket.
3. El servidor genera una cookie basada en la huella digital y la envía de vuelta a través de WebSocket.
4. El código JavaScript actualiza automáticamente la página con la cookie.
5. Si las cookies pasan el proceso de verificación, se redirige al usuario a la página de phishing.

El JavaScript de huellas digitales 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": "6b3a518d3ab6051e32ce5098746b411e",
  "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 huellas digitales de una máquina

Esta técnica se puede interrumpir supervisando la comunicación de WebSocket y filtrando los datos de huellas digitales. El kit de phishing puede configurar una comunicación de comando y control (C2) para recibir comandos de servidores de phishing a través de WebSocket mediante una técnica conocida como comunicación de latidos, donde el atacante envía y recibe datos del dispositivo de la víctima.

Figura 25: Ejemplo de comunicación de latidos

Uso de servicios de formularios basados en web para recopilar credenciales

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

El ejemplo de la figura 26 demuestra cómo los autores de amenazas pueden abusar de los servicios de creación de formularios para recopilar credenciales sin configurar servidores.

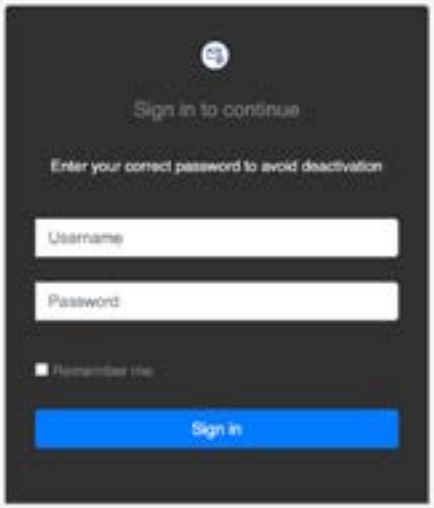


Figura 26: Ejemplo de formulario

La "acción" en el formulario es “https://submit-form[.]com/Qz1kGknr”.

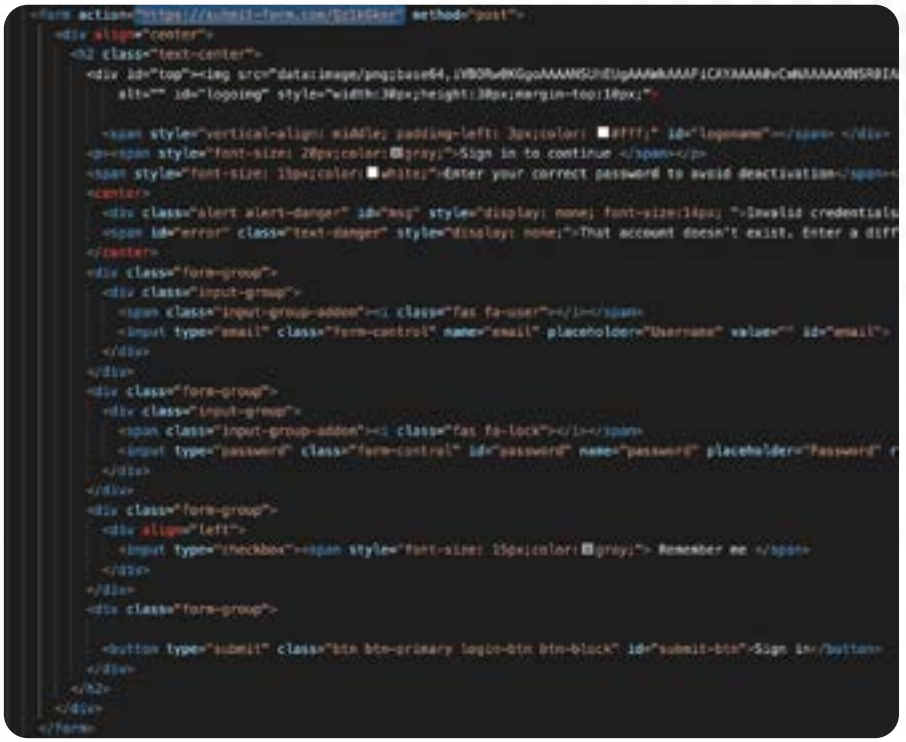


Figura 27: Cómo aprovecha el atacante el servicio de formularios para interceptar información

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 inserción de código malicioso dentro de HTML aparentemente benigno y la entrega posterior de cargas maliciosas a un sistema de destino. Los esquemas de detección a menudo analizan y detectan JavaScript, por lo que los autores de amenazas recurren al contrabando de HTML para entregar varios tipos de malware.

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

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

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

Herramientas y técnicas de phishing

Hay varias aplicaciones independientes o extensiones de navegador disponibles en línea que los autores de amenazas utilizan para copiar un sitio web legítimo y modificar el código de exfiltración de datos para robar datos. He aquí algunos ejemplos:

- **HTTrack,** una aplicación independiente ampliamente 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 incrustar otro documento HTML dentro de la página web actual. Crea un "marco dentro de un marco" en el que el contenido del documento incrustado se muestra en un cuadro rectangular en la página actual. Cuando los autores de amenazas incrustan contenido de phishing en un iframe, pueden evadir la detección.

Un iframe se puede usar para phishing de diferentes maneras:

1. Iframe anidado
2. Iframe como fondo
3. Iframe como frente, como BiTB

Además de estos, esperamos que pronto comiencen a aparecer también "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 usa para recoger un nombre de usuario (figura 28):

Figura 28: iframe para recogida de nombres de usuario

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

Figura 29: iframe para la recogida de contraseñas

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

Figura 30: Página de phishing con iframes combinados

Phishing WebAssembly

WebAssembly es un formato de instrucción binaria para una máquina virtual que se ejecuta en navegadores web modernos. Proporciona un formato de código de bytes de bajo nivel portátil que se puede ejecutar a una velocidad casi nativa, lo que lo hace ideal para ejecutar aplicaciones críticas para el rendimiento 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 en el formato de código de bytes de WebAssembly.

Phishing basado en la región geográfica

Los autores de amenazas que desean atacar a usuarios que se encuentran en regiones específicas o que hablan idiomas específicos pueden recurrir a API de terceros y servicios específicos para identificar esas audiencias.

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 de la pantalla, pueden crear reglas personalizadas basadas en factores como las direcciones IP, la configuración de idioma y las zonas horarias.

Como era de esperar, los atacantes utilizan este servicio como técnica de encubrimiento cuando realizan phishing.

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

Una dirección IP es simplemente un número de 32 bits que se puede representar usando 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 se puede representar usando una base diferente (binaria, octal, decimal, hexadecimal). Cuando los atacantes de phishing representan una dirección IP de una manera no estándar, pueden evadir la detección, pero esto se puede mitigar normalizando las direcciones IP.

Phishing utilizando "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 dentro de una página web, como un encabezado de sección o un párrafo, y permite al usuario llegar 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 activan una actualización de la página. Esta característica se usa a menudo en aplicaciones de una sola página y contenido web dinámico.

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

1. Representando la información del usuario con el hash.
    - Lo más común es que se usen las direcciones de correo electrónico. Cuando se muestra la página de inicio de sesión, la dirección de correo electrónico del usuario se completa automáticamente para engañar al usuario.
2. Generando páginas de phishing específicas basadas en el hash, que pueden distinguir a los usuarios.

IA y phishing

Los recientes avances tecnológicos de IA, como ChatGPT, facilitan que los autores de amenazas desarrollen código malicioso, generen ataques de Business Email Compromise (BEC), creen malware polimórfico y más. Intentamos generar una página de inicio de sesión de phishing usando ChatGPT y, tras solo tres interacciones simples, la herramienta generó esta página web:

Figura 31: Página de phishing generada por ChatGPT

Con un poco más de esfuerzo, un atacante podría agregar un fondo y modificarlo para que parezca una página de inicio de sesión genuina.

Previsiones para 2024

1. **Los ataques de IA serán más frecuentes** a medida que los autores de amenazas descubran nuevas aplicaciones para estos servicios. Cabe esperar ver estafas más sofisticadas a través de diferentes canales de comunicación, como correo electrónico, SMS y sitios web. Además, prepárese para un aumento en los intentos de phishing a medida que los atacantes aprovechen la IA para lanzar ataques más coordinados y efectivos en 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 grandes de posibles víctimas y técnicas de ingeniería social más avanzadas. Los proveedores también podrían ofrecer servicios adicionales, como instalación, alojamiento y análisis de malware. Además, estos proveedores competirán para ofrecer el mejor valor con modelos de precios asequibles y atención al cliente las 24 horas del día, los 7 días de la semana. Esto puede dar lugar a un aumento de los ataques de phishing a pequeña escala, por lo que es crucial mantenerse informado sobre las amenazas y tendencias de phishing más recientes.

3. **Los ataques móviles serán más frecuentes** a medida que los atacantes se centren en explotar nuestra dependencia de estos dispositivos. Los atacantes desarrollarán más contenido compatible con dispositivos móviles, como aplicaciones, sitios web y malware optimizados, incluidos spyware y troyanos de acceso remoto. También encontrarán nuevas formas de extorsionar a las víctimas para obtener ganancias financieras.

4. **Aumentarán los bombardeos de MFA y los ataques de AitM** a medida que los atacantes encuentren formas de eludir las medidas de seguridad MFA. Las bombas MFA abruman a las víctimas con solicitudes de autenticación, mientras que los ataques de AitM interceptan la sesión de la víctima después de que se hayan autenticado con éxito con MFA. Los atacantes utilizarán técnicas avanzadas, incluida la IA, para predecir y generar códigos de verificación o identificar patrones en el comportamiento del usuario para explotar el acceso. Para protegerse contra estos ataques, es importante usar contraseñas seguras, habilitar 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 de reconocimiento avanzadas para recopilar información sobre posibles víctimas. Esta información se utilizará para crear correos electrónicos de phishing personalizados que parezcan más legítimos y convincentes, lo que aumentará su probabilidad de éxito. A medida que los atacantes se vuelvan más sofisticados en el 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 una organización promedio recibe docenas de correos electrónicos de phishing a diario, con un impacto financiero que se multiplica a medida que las pérdidas producidas como consecuencia de ataques de malware y ransomware aumentan los costes promedio de los ataques de phishing recibidos año tras año. Enfrentarse a todas las amenazas descritas en este informe es una tarea difícil y, a pesar de que no puede eliminar por completo el riesgo de las amenazas de phishing, puede reducir las posibilidades de que su organización sea víctima de ellas.

Lo básico para mitigar el riesgo de ataques de phishing:

Mejores prácticas: formación en concienciación sobre seguridad

Las campañas de phishing tienen un alto índice 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 de que casi el 88 % de las filtraciones de datos se produjeron como consecuencia de un error humano. El informe también reveló que los empleados jóvenes de sexo masculino son los más vulnerables a las estafas de phishing y que la distracción es la principal causa de error en todos los grupos demográficos. Por ello, la formación para concienciar a los usuarios finales es fundamental para prevenir las brechas de seguridad y una vez al año no es suficiente. Todos los miembros de su organización deben recibir formación sobre cómo las víctimas son susceptibles a las amenazas de phishing y deben tener cuidado a la hora de proporcionar información o de hacer clic en los enlaces cuando se encuentren con correos electrónicos, sitios web, mensajes de texto, aplicaciones y llamadas telefónicas no confiables.

Implementar una formación continua para concienciar sobre la seguridad y realizar simulaciones de phishing regulares es clave para desarrollar una cultura vigilante con un sólido conocimiento sobre phishing. Estas actividades le permiten brindar formación puntual a las personas que necesitan apoyo adicional para identificar intentos de phishing y modificar su comportamiento de riesgo. Otra forma de reducir la cantidad de incidentes de phishing es mejorar los informes de los usuarios sobre correos electrónicos sospechosos de phishing, lo que puede reducir el tiempo que tardan los equipos de seguridad en eliminar las amenazas relacionadas de otras bandejas de entrada. Esto se puede hacer mediante la creación de un botón para informar de phishing directamente desde la bandeja de entrada.

Además, ThreatLabz recomienda que su formación de concienciación siga las directrices de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA), 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 legítima. Los ciberdelincuentes suelen utilizar direcciones que se asemejan mucho a las de empresas de renombre 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 sólidos 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 sobre cualquier enlace que haya el cuerpo del correo electrónico y el texto que aparece al hacerlo no coincide, es posible que el enlace esté falsificado. Los sitios web maliciosos pueden parecer idénticos a los sitios legítimos, pero la URL puede usar una variación ortográfica o un dominio diferente (por ejemplo, ".com" en lugar de ".net"). Además, los ciberdelincuentes pueden utilizar un servicio de acortamiento de URL para ocultar el verdadero destino del enlace.
- **Ortografía y diseño**. La mala gramática y estructura de las frases, las faltas de ortografía y el formato incoherente son otros indicadores de un posible intento de phishing. Las instituciones de prestigio cuentan con personal especializado que crea, verifica y corrige la correspondencia dirigida a los clientes.
- **Adjuntos sospechosos.** Un correo electrónico no solicitado que le pide a un usuario que descargue y abra un archivo adjunto es un mecanismo de entrega común de malware. Un ciberdelincuente puede recurrir a una falsa sensación de urgencia o importancia para ayudar a persuadir a un usuario para que descargue o abra un archivo adjunto sin examinarlo primero.

Mejores prácticas: controles de seguridad

Para contrarrestar el hecho de que los empleados y otros usuarios finales invariablemente serán víctimas de intentos de phishing, los equipos de seguridad deben contar con protecciones para detectar y mitigar los daños. Las protecciones principales incluyen:

- **Análisis del correo electrónico.** El correo electrónico es, con mucha diferencia, el vector de phishing más común, por lo que es crucial contar con un servicio de análisis 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.
- **Informes.** Los ataques de phishing a menudo se dirigen a muchos usuarios finales de una organización para aumentar las posibilidades de éxito. Permita que los usuarios finales informen de los intentos de phishing para bloquear remitentes y enlaces maliciosos lo más rápido posible, idealmente con un botón de informe de phishing integrado en los clientes de correo electrónico de los usuarios. Implemente un manual de estrategias para investigar y responder a incidentes de phishing, incluidos los informes a las agencias para ayudar al gobierno a combatir a los estafadores y detener los ataques contra otras organizaciones.
- **Autenticación multifactor (MFA).** La MFA sigue siendo una de las defensas más críticas contra el phishing. Cuando la MFA está implementada, una contraseña por sí sola no es suficiente para comprometer una cuenta. Las aplicaciones de autenticación como Okta Verify o Google Authenticator son particularmente efectivas y brindan una defensa adicional contra las tácticas MiTM que pueden interceptar mensajes SMS.
- **Inspección de tráfico cifrado.** Más del 95 % de los ataques utilizan canales cifrados, que a menudo no se inspeccionan, lo que facilita que incluso los atacantes moderadamente sofisticados eludan los controles de seguridad. Las organizaciones deben inspeccionar todo el tráfico, esté o no cifrado, para evitar que los atacantes pongan en peligro sus sistemas.
- **Software antivirus.** Los puntos finales deben protegerse con un antivirus actualizado regularmente para identificar archivos maliciosos y evitar que se descarguen.
- **Protección contra amenazas avanzadas.** El antivirus puede detener las amenazas conocidas, pero los adversarios son capaces de generar nuevas variantes de malware desconocidas que pueden evadir las herramientas de detección basadas en firmas. Implemente un sandbox en línea que pueda poner en cuarentena y analizar archivos sospechosos, y un aislamiento del navegador que extraiga contenido web potencialmente malicioso sin interrumpir los flujos de trabajo de los usuarios finales.
- **Filtrado de URL.** Limite su riesgo de phishing con el filtrado de URL que utiliza la política para gestionar 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 dispone de las protecciones más recientes.
- **Arquitectura de confianza cero.** Tan importante como tener controles para prevenir el phishing es contar con controles que limiten el daño de un ataque exitoso. Emplee la segmentación granular, imponga el acceso con privilegios mínimos y supervise continuamente el tráfico para encontrar autores de amenazas que puedan haber comprometido su infraestructura.
- **Fuentes de información sobre amenazas.** Estas fuentes se integran con sus herramientas de seguridad existentes para proporcionar un enriquecimiento automático del contexto y mejorar así la detección y acelerar la resolución de las amenazas de phishing. Asimismo, proporcionan un contexto actualizado sobre URL notificadas, indicadores de peligro (IOC) extraídos y tácticas, técnicas y procedimientos (TTP) para la toma de decisiones y el establecimiento de prioridades.

Mejores prácticas: cómo identificar una página de phishing

Las páginas de phishing se pueden identificar por indicadores de tácticas comunes que los autores de amenazas utilizan para engañar a los usuarios y a los motores de seguridad, así como por atajos que suelen tomar al generar nuevas páginas de phishing. La creación de nuevos sitios de phishing se dispara en torno a las fiestas y otros acontecimientos aislados. Por ejemplo, durante la pandemia, el sector de la seguridad fue testigo de cómo los atacantes lanzaban un conjunto de sitios web falsos relacionados con la COVID-19 que se aprovechaban de las víctimas haciéndose pasar por organizaciones sanitarias y sitios en los que se podían pedir kits de prueba y suministros médicos. Para detectar las amenazas de phishing más recientes, es importante mantenerse al tanto de las últimas investigaciones y disponer de información procesable con indicadores actualizados para usar en sus reglas de detección y flujos de trabajo de respuesta.

A continuación encontrará una descripción general de varios indicadores que usted (y sus herramientas anti-phishing) deben 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 otro componente de la página es un formulario web para recopilar credenciales robadas. Esta es una técnica muy común utilizada para atacar a los bancos en particular.

La página no tiene título.

La página tiene un ancla vacía para enlaces importantes. Las páginas de phishing suelen utilizar anclas vacías para páginas importantes como Ayuda, Preguntas frecuentes, etc., cuando copian el contenido de páginas legítimas.

La página tiene un certificado autofirmado.

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

La página no está cifrada. Una indicación de inicio de sesión en una página "http" es sospechosa y debe ser algo que nos llame la atención.

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 luego ensambla 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.

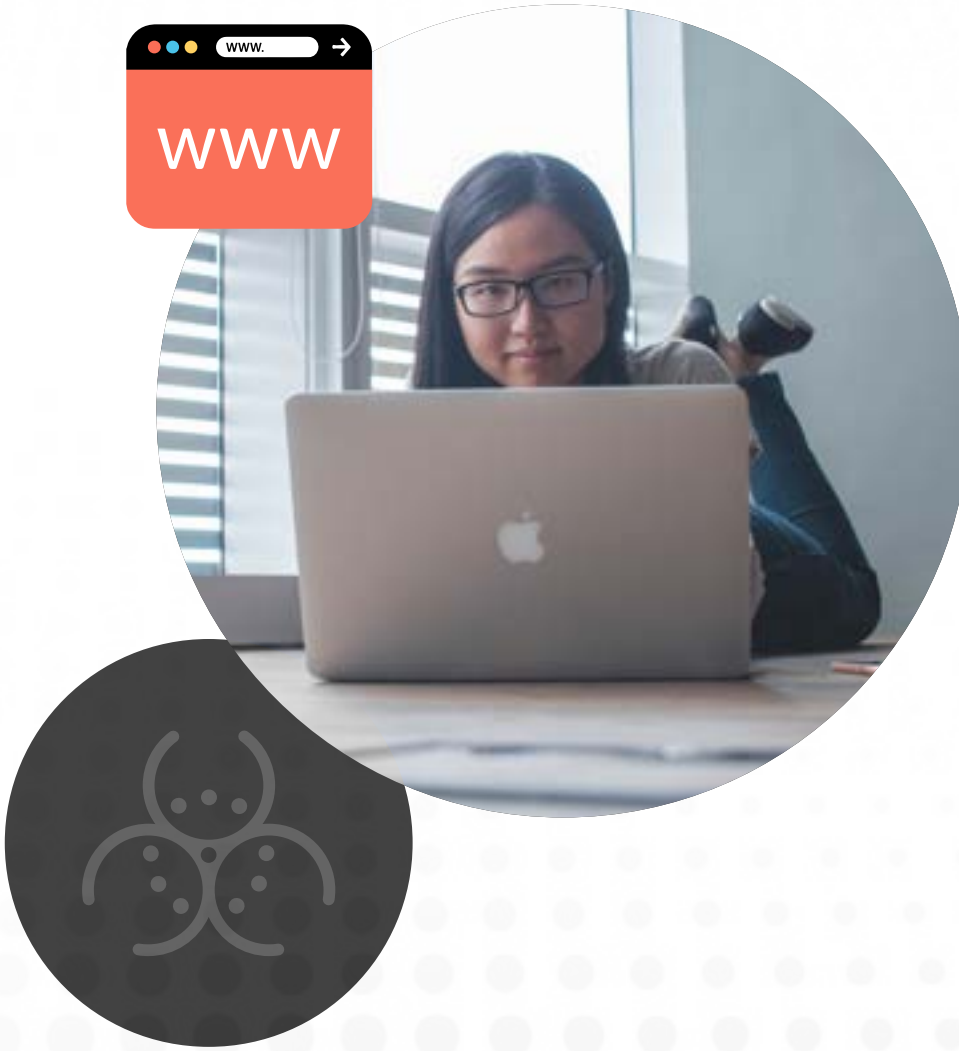
La página contiene etiquetas ofuscadas. Los operadores de phishing pueden ofuscar campos como título, derechos de autor, etc.

La página reemplaza los caracteres clave por homóglifos. Hay un abuso de homóglifos (caracteres que se asimilan a otros caracteres) en las páginas de phishing para evitar la detección. Esta técnica aprovecha las similitudes entre los caracteres que pertenecen a diferentes tipos de escritura de caracteres para engañar a los usuarios, así como a los motores de seguridad que buscan la coincidencia con los patrones ASCII.

Cómo puede Zscaler Zero Trust Exchange mitigar los ataques de phishing

Que el usuario no se vea comprometido es uno de los retos de seguridad más difíciles de defender. Su organización debe implementar controles de prevención de phishing como parte de una estrategia más amplia de confianza cero que le permita detectar las infracciones activas y minimizar los daños que causan las infracciones exitosas. Zscaler Zero Trust Exchange™ se basa en una arquitectura global de confianza cero que ayuda a detener el phishing de las siguientes maneras:

- **Evita la vulneración:** inspección TLS/SSL completa a escala, aislamiento del navegador y control de acceso basado en políticas para evitar el acceso a sitios web sospechosos.
- **Elimina el movimiento lateral:** conecta a los usuarios directamente a las aplicaciones, no a la red, para limitar el radio de explosión de un incidente potencial.
- **Bloquea a los usuarios comprometidos y las amenazas internas:** si un atacante obtiene acceso a su sistema de identidad, Zero Trust Exchange evita intentos de explotación de aplicaciones privadas con inspección en línea y detecta a los atacantes más sofisticados con engaño integrado.
- **Detiene la pérdida de datos:** inspeccione los datos en movimiento y en reposo para evitar que un atacante activo lleve a cabo posibles robos.



Productos Zscaler relacionados

Zscaler Internet Access™ ayuda a identificar y detener la actividad maliciosa mediante el enrutamiento y la inspección de 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 forma 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 mediante los análisis de contenido impulsados por la detección de IA/ML.

Advanced Threat Protection bloquea todos los dominios C2 conocidos.

Advanced Firewalll extiende la protección C2 a todos los puertos y protocolos, incluidos los destinos C2 emergentes.

Browser Isolation crea un espacio seguro entre los usuarios y las categorías web maliciosas, lo que genera contenido como un flujo de imágenes perfectas para eliminar la fuga de datos y la entrega de amenazas activas.

Advanced Cloud Sandbox previene el malware desconocido entregado en las cargas útiles de segunda etapa.

Zscaler Private Access™ protege las aplicaciones limitando el movimiento lateral con el acceso menos privilegiado, la segmentación de usuario a aplicación y la inspección completa en línea del tráfico de aplicaciones privadas.

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

Sus próximos pasos

Descubra riesgos esenciales en todo su entorno de nube pública con Zscaler Security Risk Assessment. Obtenga un inventario completo de activos en la nube, una imagen clara de sus riesgos de seguridad en la nube pública, una descripción general de cómo está cumpliendo con los puntos de referencia de cumplimiento y una guía de pautas de corrección accionables.

Acerca de ThreatLabz

ThreatLabZ es la división de investigación de seguridad de Zscaler. Este equipo de primera clase es responsable de buscar nuevas amenazas y garantizar que las miles de organizaciones que usan la plataforma global Zscaler estén siempre protegidas. Además de investigar el malware y de analizar los comportamientos, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección avanzada contra las amenazas en la plataforma Zscaler. Asimismo, realizan habitualmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler cumplen con los estándares de cumplimiento de seguridad. ThreatLabZ publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal research.zscaler.com.

Manténgase informado sobre las investigaciones 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, sólidos y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en línea en la nube del mundo.

Obtenga más información en zscaler.es o síganos en Twitter @zscaler.

Apéndice

Clasificación de los ataques de phishing

Los ataques de phishing se pueden clasificar de varias maneras y pueden incluir múltiples técnicas. Sin embargo, los atacantes están adaptando sus enfoques para engañar a los usuarios cada vez más inteligentes y evadir las herramientas de defensa. En esta sección, damos las definiciones y características comunes de los ataques de phishing.

Esta lista incluye varias descripciones de métodos de ataque físico y la amenaza que representan 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 delatora de las estafas de phishing en línea es que normalmente solicitan a los usuarios que envíen información o descarguen malware a través de uno de los siguientes métodos:

- **Enlace:** un usuario hace clic en un enlace malicioso que lleva a un sitio de phishing, archivo alojado o malware.
- **Solicitud:** se solicita a un usuario que envíe información confidencial, lo que resulta en el robo de datos.
- **Archivo adjunto:** un usuario abre un archivo adjunto que entrega software malicioso.

Mientras planifica en qué invertir para reducir los incidentes de phishing este año, considere los siguientes tipos de ataques de phishing.

De la A a la Z: tipos comunes de ataques de phishing

1. **Baiting:** los atacantes usan ofertas, nombres de archivos o dispositivos tentadores para atraer a personas curiosas a una trampa. Es similar a un ataque de caballo de Troya.
2. **Bombardeo de MFA:** los atacantes engañan a los usuarios con credenciales comprometidas para que verifiquen una solicitud de MFA ilegítima que realiza el autor de amenazas. Estos ataques suelen caracterizarse 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 accidentalmente, verifique una de las solicitudes.
3. **Fraude del CEO o ataque al correo electrónico empresarial (BEC):** los atacantes se dirigen a los empleados de la empresa que utilizan cuentas ejecutivas comprometidas para enviar facturas falsas o solicitudes de pago mediante transferencia bancaria u otras formas.
4. **Pharming o phishing de caché de DNS:** 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 código malicioso que redirige a la víctima al sitio cuando ingresan cualquier URL desde su ordenador.
5. **Phishing Angler:** los atacantes se hacen pasar por personal de atención al cliente y se ofrecen para ayudar a resolver los comentarios negativos sobre una empresa publicados en las redes sociales. Tienen como objetivo los clientes insatisfechos, en particular los de los bancos.
6. **Phishing con memorias USB:** los atacantes colocan físicamente o envían dispositivos USB al objetivo que contienen ejecutables maliciosos que se cargan cuando se conectan a cualquier punto final vulnerable.

7. **Phishing con publicidad maliciosa:** los atacantes utilizan secuencias de comandos en anuncios para enviar contenido no deseado directamente a los ordenadores de las víctimas.
8. **Phishing de adversario en el medio (AitM):** los atacantes imitan las acciones de una víctima desprevenida para obtener sus credenciales de inicio de sesión y cookies de sesión.
9. **Phishing de chat o de mensajería instantánea:** los atacantes usan mensajes instantáneos para enviar estafas dentro de las aplicaciones, generalmente con enlaces URL maliciosos.
10. **Phishing de clonación:** los atacantes crean mensajes de correo electrónico duplicados que parecen provenir de fuentes confiables, con ligeras modificaciones y archivos adjuntos o enlaces maliciosos.
11. **Phishing de código QR:** los atacantes usan códigos QR que, cuando se escanean con el teléfono inteligente de la víctima, conducen a sitios web maliciosos o descargan malware en el dispositivo.
12. **Phishing de intermediario (MiTM):** los atacantes se dirigen a 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.
13. **Phishing de navegador en el navegador (BitB):** los atacantes muestran una ventana de navegador maliciosa dentro de una ventana de navegador para imitar un dominio legítimo y replicar ventanas de inicio de sesión emergentes que parecen ser de proveedores de autenticación de terceros.
14. **Phishing de ransomware:** los atacantes envían correos electrónicos con archivos adjuntos o enlaces maliciosos. Al hacer clic en ellos, descargan ransomware en el ordenador de la víctima y exigen el pago a cambio de una clave de descifrado de recuperación.
15. **Phishing de recolección 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 legítimas para robar nombres de usuario y contraseñas de víctimas desprevenidas.
16. **Phishing de túnel inverso:** los atacantes usan un servidor remoto para crear un túnel SSH inverso al ordenador de la víctima, lo que les permite explotar la máquina para varios propósitos, como la instalación de malware o el robo de datos confidenciales, mientras permanecen ocultos para evitar que la víctima los detecte.
17. **Phishing Doc Clouding:** los atacantes entregan documentos maliciosos desde fuentes comunes en la nube como Google Drive, Box o OneDrive para eludir las herramientas de seguridad tradicionales y dificultar su detección para la mayoría de los equipos de seguridad.
18. **Phishing en motores de búsqueda:** los atacantes acometen a los consumidores mediante la creación de sitios web de compras en línea falsos indexados por los motores de búsqueda. Ofrecen grandes descuentos en productos destacados y pueden parecer ventanas emergentes de temporada o contener reseñas retroactivas falsas. Las víctimas pueden, sin saberlo, compartir datos personales, información bancaria, números de tarjetas de crédito o incluso pagar productos falsos. Los estafadores han llegado incluso a proporcionar información falsa de envío y seguimiento, "productos simbólicos baratos" inclusive, para ampliar el ciclo de vida de estos sitios.
19. **Phishing Evil Twin:** los atacantes imitan una red wifi pública confiable para observar la actividad en línea de las víctimas y robar datos que pasan por el punto de acceso malicioso.
20. **Phishing HTTPS:** los atacantes utilizan el protocolo seguro de transferencia de hipertexto encriptado para engañar a los usuarios de confianza para que hagan clic en enlaces URL maliciosos.

21. **Phishing por correo electrónico:** los atacantes envían mensajes de correo electrónico de ingeniería social que se hacen pasar por marcas conocidas, con enlaces URL maliciosos o activos adjuntos diseñados para robar información o entregar malware.
22. **Phishing Watering Hole o ataques de abrevadero:** los atacantes se dirigen a miembros de grupos específicos que probablemente visiten un sitio específico que el atacante comprometió o creó con el propósito de llevar a cabo el ataque.
23. **Smishing:** los atacantes usan mensajes de texto (comunicaciones SMS) para enviar estafas, generalmente con enlaces URL maliciosos. El remitente del mensaje parece ser una marca conocida o un conocido del destinatario.
24. **Spear phishing:** los atacantes organizan campañas que utilizan información disponible públicamente para dirigirse a personas que trabajan para organizaciones específicas. Estos correos electrónicos engañosos pueden contener información real y parecer solicitudes internas legítimas para engañar a los destinatarios para que realicen una acción deseada.
25. **Tailgating:** los atacantes logran acceso físico a un área restringida siguiendo a una persona autorizada con acceso al interior. Esta forma de ataque se considera phishing cuando alguien muerde el anzuelo de ingeniería social (como llevar varias cajas grandes) que presenta el atacante y le permite ingresar sin verificación.
26. **Vishing:** los atacantes hacen llamadas telefónicas maliciosas que usan ingeniería social para presionar a los destinatarios a realizar una acción, como transferir dinero o revelar información personal.
27. **Whaling:** los ataques se dirigen a ejecutivos y cargos de alto perfil utilizando información disponible públicamente. Tratan de sonsacar al objetivo secretos comerciales confidenciales que pueden usarse con fines fraudulentos o los engañan para que realicen otra acción que el autor de la amenaza pueda usar para lograr sus objetivos.

El phishing no se puede eliminar solo con tecnología. Las organizaciones deben realizar un seguimiento de la evolución de las estafas de phishing para observar cómo los cambios en la conciencia cultural van aplacando técnicas específicas a lo largo del tiempo. Comprender los diferentes tipos de estafas puede ayudar a los profesionales de seguridad a educar a los empleados sobre cómo aplicar una perspectiva escéptica de confianza cero cuando se encuentran con lo que puede parecer una oportunidad legítima, una solicitud de verificación o una notificación automática. Cuando desarrolle su propia estrategia para reducir los incidentes de phishing, plantéese incluir los siguientes tipos de estafas comunes:

Principales categorías de estafas de phishing

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

Las estafas de **consumidor** suplantan marcas de comercio electrónico con señuelos como notificaciones de cuentas falsas y reclamaciones de afiliación o beneficios.

Las estafas **comerciales** suplantan servicios generales como FedEx con señuelos como notificaciones de seguimiento y solicitudes de pago.

Las estafas **corporativas** suplantan a empresas específicas con señuelos como notificaciones de cuentas falsas, actualizaciones de la empresa, tareas de RR. HH. y solicitudes de pago de facturas.

Las estafas de **citas** suplantan a las personas que buscan una cita a través de 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 se dirigen a los particulares con señuelos como falsas notificaciones de cuentas o alertas de seguridad.

Las estafas de **gobierno** se hacen pasar por agencias federales como el IRS con señuelos como reclamaciones falsas de beneficios, préstamos de ayuda y solicitudes de pagos atrasados.

Las estafas de **ofertas de trabajo** suplantan a empresas falsas y reales que buscan contratar nuevos empleados con engaños como anuncios de empleo, solicitudes y ofertas de empleo falsos.

Las estafas de **notificaciones push** o de navegador suplantan las notificaciones del navegador web con engaños como recordatorios falsos para instalar actualizaciones, alertas de mensajes y anuncios de productos.

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

Las estafas **técnicas** suplantan servicios generales o marcas conocidas con señuelos como notificaciones de cuenta, mensajes de error y actualizaciones de software.

Experience your world, secured.™

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 ataques cibernéticos y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de forma segura en cualquier ubicación. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Para obtener más información, visite www.zscaler.es.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.es