Informe sobre phishing de 2024 de Zscaler ThreatLabz

Descubra las últimas tendencias de phishing, tácticas emergentes y medidas de seguridad efectivas para mantenerse a la vanguardia de la amenaza de phishing impulsada por la IA en constante evolución.

Índice

Resumen ejecutivo

En el panorama actual del phishing, los atacantes tienen un acceso sin precedentes a una amplia gama de herramientas convenientes o "botones fáciles", como kits de phishing como servicio, herramientas de phishing automatizadas y listas de objetivos seleccionadas. Estas amenazas evolucionan y se multiplican constantemente, lo que obliga a las empresas a permanecer en un estado perpetuo de mayor vigilancia mientras se defienden de las variaciones siempre cambiantes de las estafas de phishing. Para complicar aún más las cosas, el surgimiento de la inteligencia artificial (IA) ha amplificado significativamente el arte del engaño, permitiendo a los atacantes ejecutar ataques más sofisticados y esquivos a una escala y velocidad sin precedentes.

La IA representa un cambio de paradigma en el ámbito del ciberdelito, en particular en el caso de las estafas de phishing. Con la ayuda de la IA generativa, los ciberdelincuentes pueden construir rápidamente campañas de phishing muy convincentes que superan los puntos de referencia anteriores de complejidad y eficacia. Al aprovechar los algoritmos de IA, los autores de amenazas pueden analizar rápidamente grandes conjuntos de datos para adaptar sus ataques y replicar fácilmente comunicaciones y sitios web legítimos con una precisión alarmante. Este nivel de sofisticación permite a los phishers engañar incluso a los usuarios más conscientes. El potencial de la IA para remodelar el panorama de las ciberamenazas parece ilimitado a medida que continúa redefiniendo lo que es posible en el mundo de los ciberataques.

Mientras las organizaciones y los usuarios se preparan para este panorama cambiante de ataques de phishing, surge una pregunta apremiante: **¿cómo podemos adelantarnos a estas amenazas?** Para ayudar a responder esta pregunta con información sobre las últimas tendencias de phishing, entidades objetivo, tácticas emergentes y medidas de seguridad efectivas, el equipo de investigación de Zscaler ThreatLabz realizó un análisis exhaustivo. Durante 12 meses (de enero a diciembre de 2023), ThreatLabz examinó más de 2 mil millones de transacciones de phishing en Zscaler Zero Trust Exchange™, la mayor nube de seguridad en línea del mundo. Sus hallazgos tienen como objetivo dotar a las empresas del conocimiento necesario para combatir de forma proactiva la creciente ola de nuevos ataques de phishing.

El panorama de los ataques de phishing continúa evolucionando rápidamente. En 2023, ThreatLabz observó un aumento interanual del 58,2 % en los intentos de phishing a nivel mundial.

Este aumento se caracterizó por esquemas emergentes, que incluyen phishing de voz, estafas de contratación y ataques de navegador en el navegador. Estos hallazgos se alinean con los datos del Grupo de Trabajo Anti-Phishing, una coalición internacional contra el cibercrimen, que declaró 2023 como "el peor año registrado para el phishing".[1]

A la luz de este momento esencial en el ámbito de las amenazas de phishing, el Informe de phishing de Zscaler ThreatLabz 2024 ofrece información procesable sobre la actividad y las tácticas de phishing, junto con las mejores prácticas y estrategias para mejorar la seguridad de su organización frente a las amenazas existentes y en evolución.

1. Grupo de trabajo antiphishing, Informe de tendencias de actividad de phishing, cuarto trimestre de 2023, 13 de febrero de 2024.

Principales hallazgos

Los ataques de phishing aumentaron un 58,2 % en 2023, en comparación con 2022, lo que refleja la creciente sofisticación y persistencia de los autores de amenazas.

Los ataques de phishing por voz (vishing) y de phishing deepfake están aumentando a medida que los atacantes aprovechan herramientas de inteligencia artificial generativa para amplificar sus tácticas de ingeniería social.

Estados Unidos, Reino Unido, India, Canadá y Alemania fueron los cinco países más afectados por ataques de phishing.

El sector financiera y el de seguros sufrieron el 27,8 % de los ataques de phishing en general, la mayor concentración entre todos los sectores y un asombroso aumento interanual del 393 %. La industria manufacturera le siguió de cerca con el 21 %.

Microsoft sigue siendo la marca más imitada, con el 43,1 % de los intentos de phishing dirigidos a ella. Las marcas OneDrive y SharePoint de Microsoft también estuvieron entre las cinco principales víctimas, lo que indica una tendencia persistente de autores de amenazas que buscan credenciales de usuario de aplicaciones críticas de Microsoft.

Los ataques de adversario en el medio (AiTM) siguen siendo una amenaza persistente, y los ataques de navegador en el navegador (BiTB) están en aumento. Estas tácticas atacan directamente a los usuarios de los navegadores web, lo que hace que sea más difícil detectarlas y mitigarlas.

Las estafas de soporte técnico y las estafas de QR CAPTCHA estuvieron entre los tipos de ataques más frecuentes en 2023, explotando la confianza de los usuarios en los servicios de soporte técnico y el uso generalizado de códigos QR.

Principales objetivos de phishing

Los investigadores de ThreatLabz analizaron datos que abarcan diferentes países, sectores , marcas y plataformas para identificar los objetivos principales de los ataques de phishing en 2023. Los hallazgos enfatizan la amenaza persistente y generalizada que representan los ataques de phishing a escala global. Reconocer los patrones y tendencias de las actividades de phishing es crucial para implementar medidas efectivas de ciberseguridad para protegerse contra ellas.

LA SECCIÓN EXPLORA ASPECTOS CLAVE DE LOS ATAQUES DE PHISHING, INCLUIDOS:

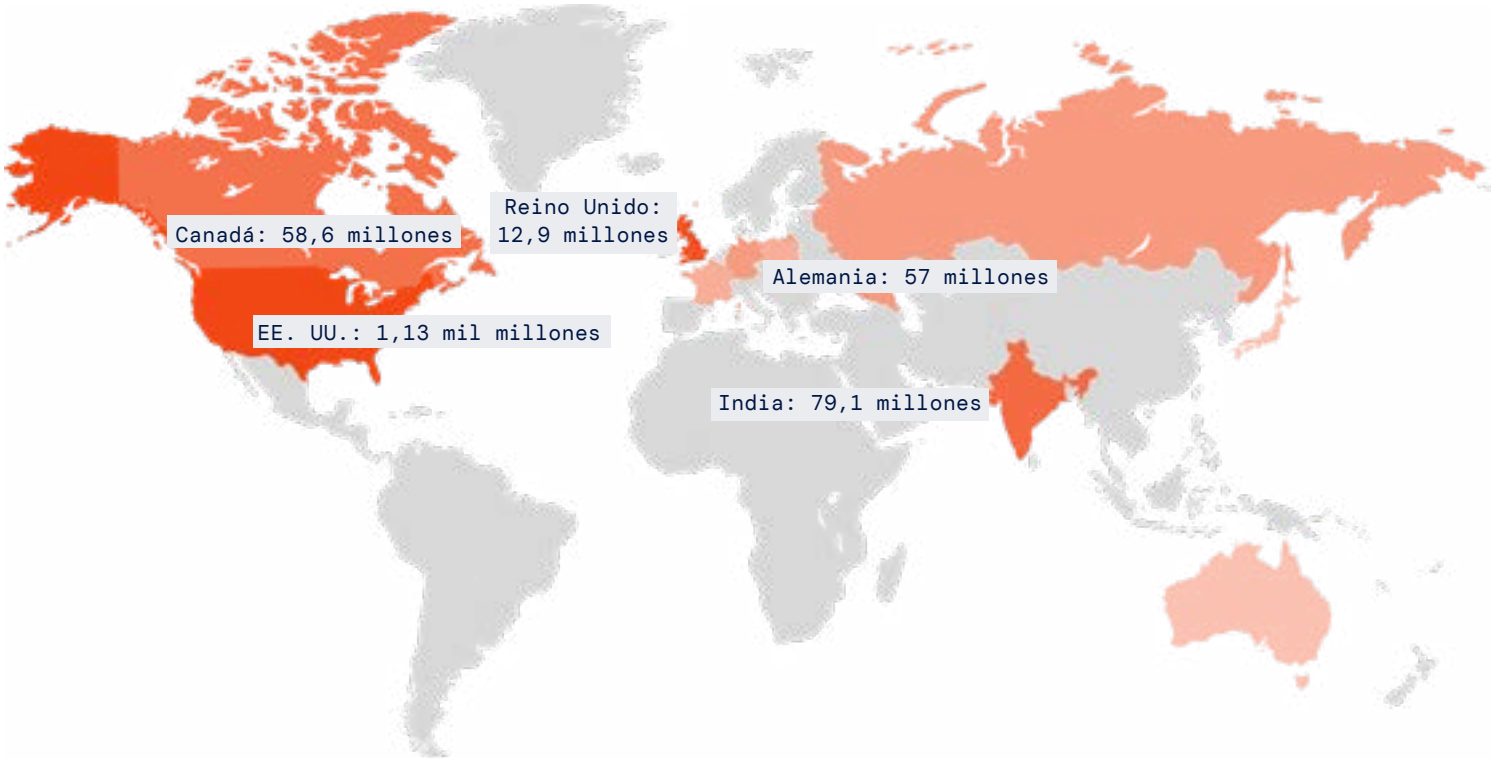
01 Países que experimentaron la mayor cantidad de intentos de phishing
02 Países de origen de los ataques de phishing
03 Sectores más comúnmente objetivo de ataques de phishing
04 Marcas imitadas con mayor frecuencia por los autores de amenazas
05 Principales dominios de referencia que conducen a páginas de phishing
06 Distribución de ataques entre números de sistemas autónomos (ASN)
07 Plataformas de redes sociales explotadas por autores de amenazas

Países que experimentaron la mayor cantidad de intentos de phishing

En 2023, Estados Unidos, el Reino Unido y la India experimentaron el mayor volumen de intentos de phishing, siendo Estados Unidos el más afectado por estos ataques. Los factores que contribuyen a la alta incidencia de phishing en EE. UU. incluyen su gran población de usuarios de Internet y tecnología, el uso extensivo de transacciones financieras en línea y su infraestructura digital avanzada. La prevalencia de campañas de phishing impulsadas por IA amplifica aún más la vulnerabilidad de las entidades estadounidenses a tales ataques.

LOS 10 PRINCIPALES PAÍSES AFECTADOS POR ESTAFAS DE PHISHING FUERON:

01 Estados Unidos
02 Reino Unido
03 India
04 Canadá
05 Alemania
06 Rusia
07 Polonia
08 Francia
09 Australia
10 Japón

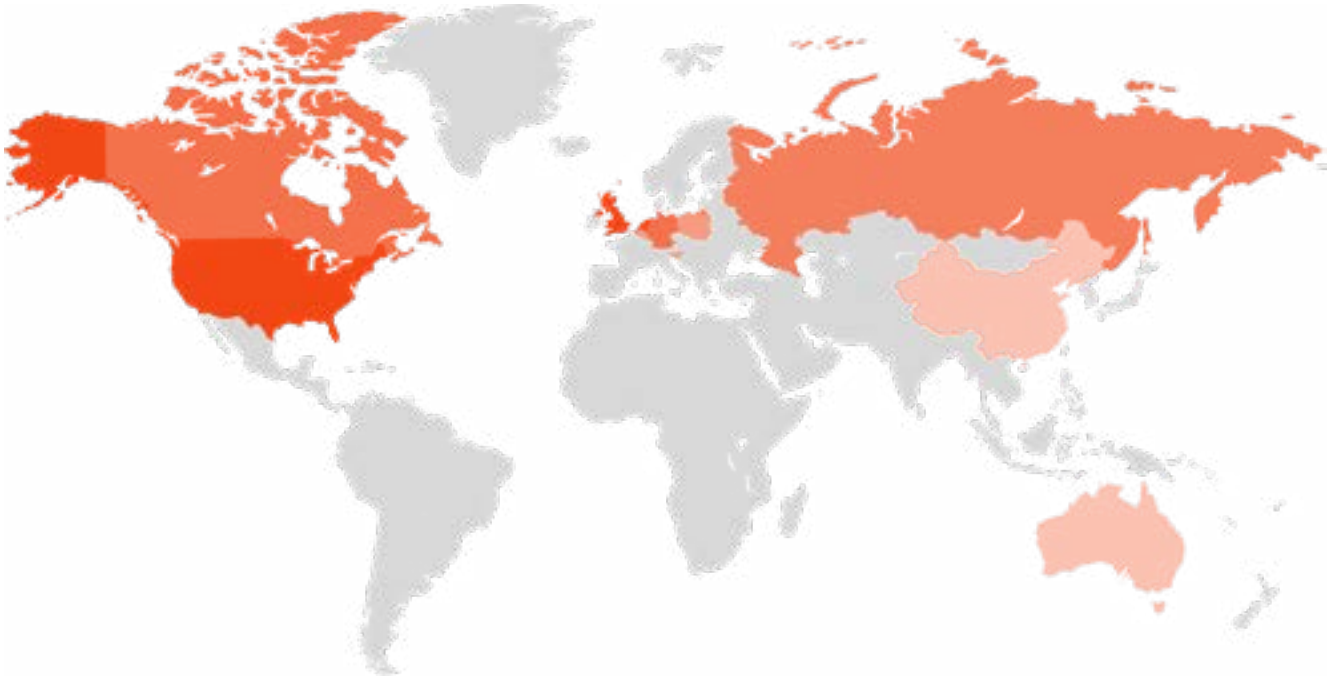


Países de origen de los ataques de phishing

La mayoría de los ataques de phishing se remontaron a territorios familiares, a saber, Estados Unidos, Reino Unido y Rusia. En particular, Estados Unidos fue consistentemente la fuente predominante de estas actividades maliciosas. Esto se puede atribuir a la infraestructura digital amplia y avanzada del país, que brinda a los phishers y ciberdelincuentes un acceso más fácil a un grupo más grande de víctimas potenciales.

LOS 10 PAÍSES IDENTIFICADOS COMO LOS PRINCIPALES ORÍGENES DE LOS ATAQUES DE PHISHING FUERON:

01 Estados Unidos
02 Reino Unido
03 Rusia
04 Alemania
05 Canadá
06 Países Bajos
07 Polonia
08 China
09 Singapur
10 Australia



Australia entró en el top 10 debido a un aumento del 479,3 % en el volumen de contenido de phishing alojado en el país, siendo 2023 un año notable para la actividad de phishing. De hecho, el servicio Scamwatch de ACCC detectó aproximadamente 109 000 informes y 26,1 millones de dólares australianos en pérdidas.[2]

2. Centro Nacional Antiestafa Scamwatch, Estadísticas de estafas (2023).

Sectores más comúnmente objetivo de ataques de phishing

Ningún sector es inmune a los ataques de phishing. Después de todo, el elemento humano impregna todos los sectores y sirve como una vulnerabilidad común que los phishers pueden explotar. Sin embargo, comprender qué sectores están en el punto de mira de los phishers es clave para asignar estratégicamente recursos anti-phishing de manera más efectiva, implementar medidas de seguridad personalizadas y priorizar la capacitación de los empleados para mitigar el factor de error humano.

El sector financiero y de seguros experimentó tanto el mayor número de intentos de phishing como el aumento más significativo de ataques, con un aumento del 393% en comparación con el año anterior. Esta industria es un objetivo atractivo para los actores de amenazas que buscan involucrarse en el robo de identidad o el fraude financiero. La creciente dependencia de las plataformas financieras digitales ofrece amplias oportunidades para que los actores de amenazas lleven a cabo campañas de phishing y aprovechen las vulnerabilidades en este sector.

De manera similar, **El sector manufacturero experimentó un aumento del 31 % en los ataques de phishing** entre 2022 y 2023. Esto pone de manifiesto que los ciberdelincuentes son plenamente conscientes de la vulnerabilidad de la industria manufacturera a las ciberamenazas. A medida que los procesos de fabricación se vuelven más dependientes de sistemas digitales y tecnologías interconectadas, existe un mayor riesgo de explotación por parte de autores de amenazas que buscan acceso no autorizado o interrupción.

No es coincidencia que la industria manufacturera, las finanzas y los seguros sean los sectores líderes en la adopción de herramientas de IA, abarcando en conjunto el 35 % de las transacciones IA/ML en Zero Trust Exchange, como se revela en el Informe de seguridad de IA de Zscaler ThreatLabz 2024. La adopción de tecnologías y sistemas impulsados por IA no sólo amplía la conectividad (y, por tanto, la superficie de ataque explotable) entre redes y dispositivos, sino que también los convierte en objetivos aún más lucrativos para los esquemas de phishing, dada la mayor dependencia de los datos.

A pesar de ocupar el cuarto lugar, **el sector tecnológico experimentó un aumento del 114 % en los ataques de phishing**, probablemente impulsado por su temprana y entusiasta adopción de GenAI y una gran cantidad de datos valiosos en juego.

LOS CINCO PRINCIPALES SECTORES OBJETIVO DE ESTAFAS DE PHISHING FUERON:

01 Finanzas y seguros
02 Fabricación
03 Servicios
04 Tecnología
05 Venta minorista y mayorista

Proporción de estafas de phishing por sector vertical

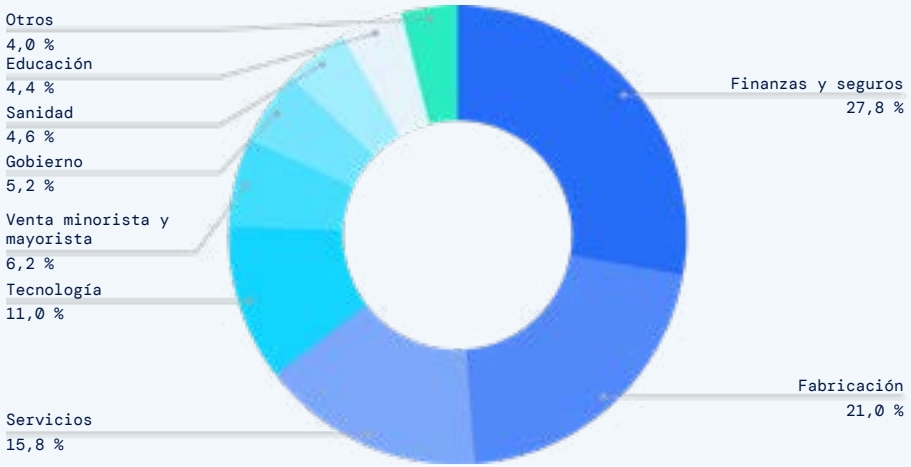


Figura 1: Principales sectores afectados por estafas de phishing en 2023

Marcas más imitadas en estafas de phishing

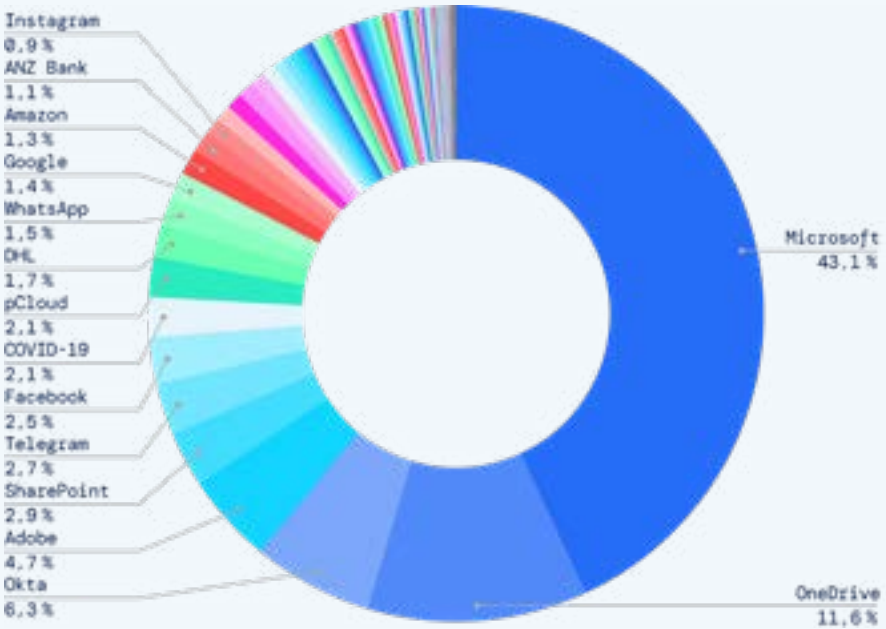


Figura 2: Marcas más imitadas en 2023

Marcas imitadas con mayor frecuencia por los actores de amenazas

Los atacantes de phishing explotan aplicaciones empresariales populares haciéndose pasar por marcas y temas populares. Los investigadores de ThreatLabz descubrieron que marcas empresariales como Microsoft, OneDrive, Okta, Adobe y SharePoint son objetivos principales de suplantación de identidad debido a su uso generalizado en entornos empresariales y el valor que tienen a la hora de adquirir credenciales de usuario. Esta tendencia se ha visto exacerbada por el cambio hacia la cultura del trabajo remoto desde 2020, lo que hace que estas marcas sean aún más atractivas para los phishers, ya que se utilizan mucho para el trabajo y la colaboración remotos.

Microsoft Windows es el sistema operativo informático más utilizado en el mundo y no sorprende que los phishers aprovechen esa ubicuidad. Microsoft se erigió en la marca empresarial más imitada en 2023, y OneDrive y SharePoint también se situaron entre las cinco primeras.

LAS 20 MARCAS MÁS IMITADAS EN ESTAFAS DE PHISHING FUERON:

01	Microsoft	06	Telegram	11	ANZ Banking Grupo	16	Sparkasse Bank
02	OneDrive	07	pCloud	12	Amazon	17	FedEx
03	Okta	08	Facebook	13	eBay	18	PayU
04	Adobe	09	DHL	14	Instagram	19	Rakuten
05	SharePoint	10	WhatsApp	15	Google	20	Gucci

Las aplicaciones de consumo enumeradas sirven como recordatorio de seguridad crucial de los riesgos de usar las mismas contraseñas en aplicaciones de consumo y empresariales. Los autores de amenazas frecuentemente explotan esta práctica, enfatizando la importancia de emplear contraseñas únicas y seguras para mitigar las amenazas a la seguridad.

Principales dominios de referencia que conducen a páginas de phishing

Los autores de amenazas frecuentemente explotan dominios confiables para engañar a las víctimas, aprovechando la familiaridad y la confianza asociadas con esos dominios para llevar a las víctimas a sitios de phishing fraudulentos. Comprender los orígenes del tráfico web malicioso, como lo indican los dominios de referencia, es crucial para comprender la cadena de ataque. Básicamente, permite a las organizaciones identificar las fuentes de un ataque, brindando a los equipos de seguridad información sobre los tipos de sitios web comprometidos o suplantados que utilizan los autores de amenazas.

Los investigadores de ThreatLabz analizaron los principales dominios de referencia en 2023, considerando la reputación de los dominios redirigidos y el contenido alojado en los destinos. La distinción entre los mejores servidores basados en la reputación y los basados en el contenido radica en la metodología empleada para identificar y categorizar los sitios web que pueden presentar riesgos potenciales.

Al analizar los dominios de referencia principales, es importante considerar el potencial de abuso de redireccionamiento abierto. Esta táctica implica explotar vulnerabilidades en la funcionalidad de redireccionamiento de un sitio web para engañar a los usuarios redireccionándolos a sitios web maliciosos. Como resultado, los dominios legítimos pueden terminar sin darse cuenta en las listas de los principales dominios de phishing. Esta estrategia brinda a los atacantes la capacidad de enviar correos electrónicos que contengan enlaces a estos sitios legítimos como punto de entrada, mientras oculta las direcciones ocultas de los sitios de phishing reales en los parámetros GET. Esta táctica aumenta la probabilidad de evadir la detección por parte de los clientes de correo electrónico que buscan URL maliciosas.

Dominios de referencia principales según su reputación

Este enfoque implica evaluar los sitios web de phishing bloqueados en función de la reputación del proveedor de alojamiento (o "host") de un dominio en particular. Además, recopila información sobre los dominios de referencia para estos destinos, lo que nos permite identificar sitios web que redirigen a los usuarios a contenido de phishing o dominios legítimos utilizados por autores de amenazas con fines de phishing. La evaluación de los bloques de phishing tiene en cuenta varios factores, como el historial de abuso del proveedor de alojamiento, la presencia de malware, actividades de spam y otros indicadores de comportamiento malicioso. Los sitios web alojados por proveedores con reputación negativa pueden marcarse o clasificarse como potencialmente dañinos, independientemente del contenido del dominio específico.

LOS 20 DOMINIOS DE REFERENCIA PRINCIPALES SEGÚN SU REPUTACIÓN EN 2023 FUERON:

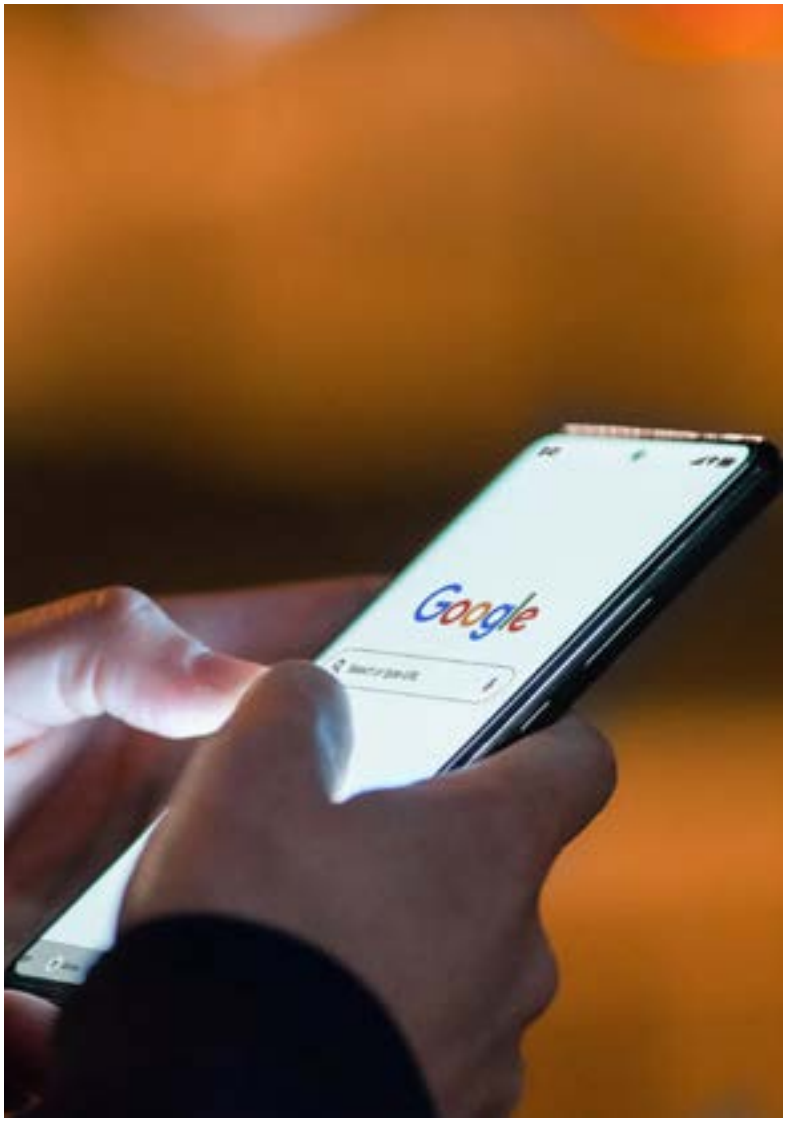
01 cstools[.]viagogo[.]net
02 www[.]gutefrage[.]ten
03 web[.]tlgrm[.]app
04 www[.]mhtestd[.]gov[.]zw
05 framer[.]com
06 www[.]finanznachrichten[.]de
07 webogram[.]org
08 app[.]hive[.]com
09 sync[.]quantumdex[.]io
10 www[.]google[.]com
11 public[.]servenobid[.]com
12 csync[.]smilewanted[.]com
13 t24[.]com[.]tr
14 acdn[.]adnxs[.]com
15 onetag-sys[.]com
16 evgeny-nadymov[.]github[.]io
17 learn[.]hfma[.]org
18 visitor[.]omnitagjs[.]com
19 blog[.]csdn[.]net
20 www[.]msn[.]com

Dominios de referencia principales según el contenido

Este enfoque implica examinar el contenido encontrado en sitios web de phishing bloqueados mediante análisis de contenido, análisis de palabras clave y algoritmos de aprendizaje automático. Al evaluar la naturaleza del contenido alojado, ThreatLabz marcó sitios web que coinciden con patrones conocidos de actividad maliciosa, como el phishing. La siguiente lista muestra los dominios de referencia asociados con las conexiones donde se observaron bloques de phishing basados en contenido. Tenga en cuenta que no todos los dominios de referencia son maliciosos, pero brindan información valiosa sobre los dominios aprovechados por los autores de amenazas para redirigir a las víctimas a sitios web de phishing.

LOS 20 DOMINIOS DE REFERENCIA PRINCIPALES SEGÚN EL CONTENIDO EN 2023 FUERON:

01 www[.]google[.]com
02 mail[.]google[.]com
03 rx-qualityshop[.]com
04 1rotator[.]com
05 webmail[.]ph-japan[.]org
06 www[.]bing[.]com
07 onionplay[.]se
08 onionplay[.]co
09 indd[.]adobe[.]com
10 safe-it-phshop[.]com
11 top-sh-op[.]com
12 medsinfoshop[.]com
13 www[.]bluelightcard[.]co[.]uk
14 www[.]flickchart[.]com
15 www[.]calendriervip[.]fr
16 pdce2[.]avanan[.]net
17 musicyt[.]click
18 trustedxshop[.]com
19 www[.]onionplay[.]si
20 www[.]coinpayu[.]com
21 3khO[.]github[.]io



Distribución de ataques entre sistemas autónomos (ASN)

Un sistema autónomo es una red o grupo de redes con una única política de enrutamiento. Cada AS tiene un identificador único conocido como número de sistema autónomo (ASN). Como parte de este análisis, los investigadores de ThreatLabz revisaron los sistemas autónomos responsables de alojar la infraestructura de phishing.

El conocimiento de las principales distribuciones de ASN es vital para los equipos de ciberseguridad porque:

- Identifica ISP, empresas o proveedores de hosting frecuentemente asociados con ciberamenazas, lo que ayuda en la inteligencia de amenazas específicas.
- Ayuda a atribuir los ciberataques a organizaciones o regiones específicas, lo que es crucial para comprender los motivos e identificar posibles autores de amenazas.

Los datos indican la siguiente distribución:

- **Proveedor de servicios de Internet (ISP):** Con un total de 200 293 568, la mayoría de ASN pertenecen a ISP. Estos ASN están asociados con organizaciones que brindan servicios de conectividad a Internet a usuarios finales, hogares y empresas.
- **Hosting:** Los ASN de hosting representan 112 452 292, lo que representa una parte importante de la distribución. Estos ASN están asociados con proveedores de alojamiento que ofrecen espacio en servidores, infraestructura y servicios relacionados para sitios web y aplicaciones en línea.
- **Empresas:** Los ASN asociados a empresas suman 75 826 357 en total. Se asignan a organizaciones de diversos sectores que operan sus propias redes para comunicación interna, intercambio de datos y conectividad a Internet.

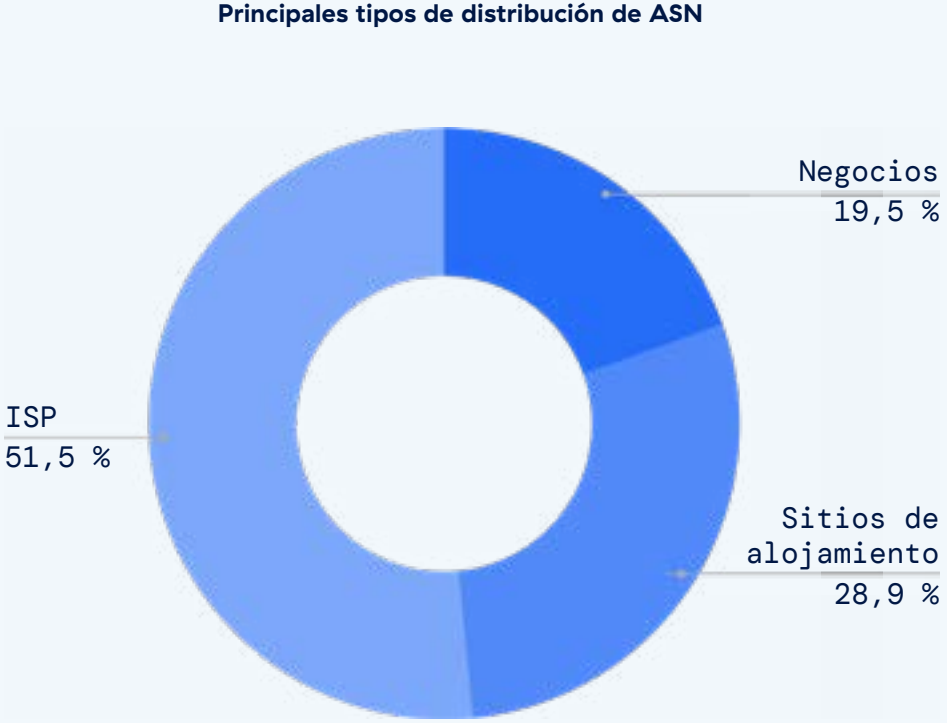


Figura 3: Un desglose de los servidores empresariales, de alojamiento y de ISP involucrados en ataques de phishing

Plataformas de redes sociales explotadas por autores de amenazas

En un mundo donde reinan las redes sociales, los atacantes aprovechan cada vez más estas plataformas para actividades de phishing. Esta tendencia se extiende por todo el mundo: Asia-Pacífico, Europa, Oriente Medio y África experimentan patrones de explotación similares. La Figura 4 muestra las plataformas de redes sociales en las que se producen más ataques según observó ThreatLabz.

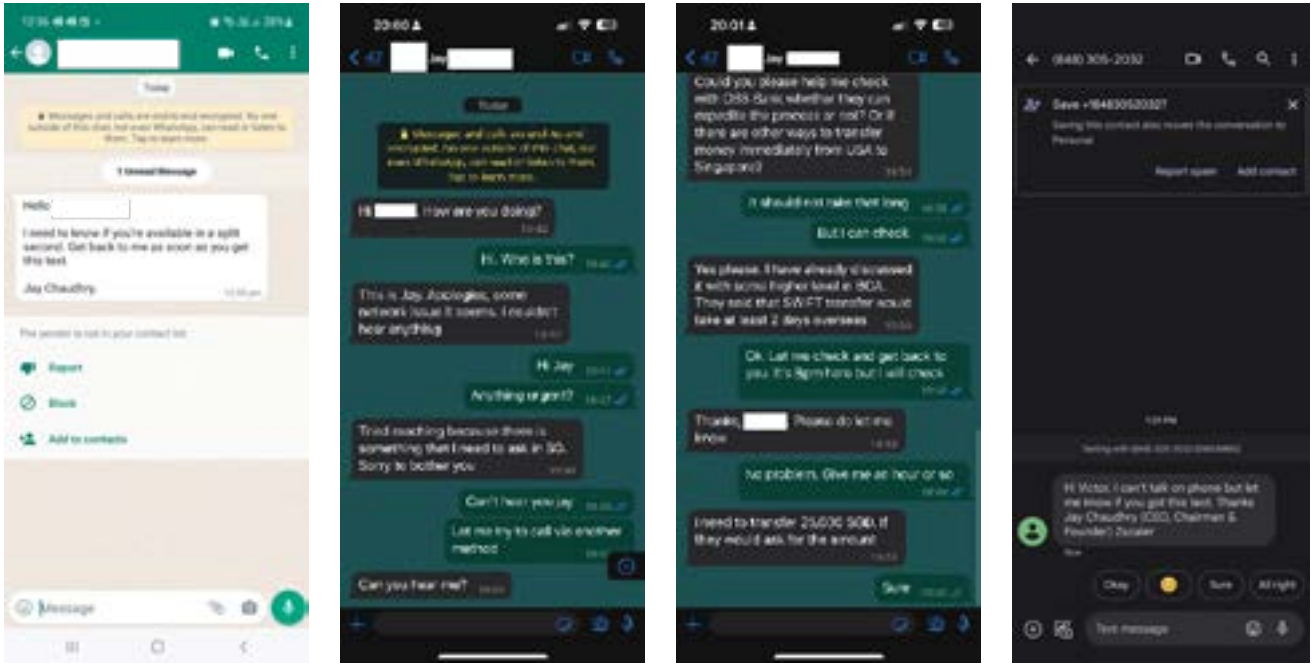
Telegram, con 792 883 ataques de phishing observados, sigue siendo un objetivo popular para actividades maliciosas, una tendencia explorada en nuestra publicación de blog en DuckTail. El cifrado de extremo a extremo de la plataforma y el énfasis en la privacidad del usuario la convierten en una opción atractiva para una comunicación segura. Sin embargo, los autores de amenazas intentan explotar las vulnerabilidades en las medidas de seguridad de Telegram para obtener acceso no autorizado a cuentas de usuarios o distribuir contenido malicioso.

Facebook, con 532 243 ataques de phishing observados, se enfrenta a continuos desafíos en la protección de los datos y la privacidad de los usuarios. Como una de las mayores plataformas de redes sociales del mundo, atrae a ciberdelincuentes que pretenden explotar fallas de seguridad, lanzar campañas de phishing o participar en el robo de identidad.

Figura 4: Principales plataformas de redes sociales utilizadas en ataques de phishing

WhatsApp, con 378 968 ataques de phishing observados, se enfrenta a varios problemas de seguridad debido a su gran base de usuarios y su uso ubicuo de mensajería. Si bien WhatsApp incorpora cifrado de extremo a extremo para mantener conversaciones seguras, los atacantes buscan explotar vulnerabilidades para obtener acceso no autorizado, distribuir malware o engañar a los usuarios mediante técnicas de ingeniería social.

ThreatLabz detectó los siguientes intentos de phishing aprovechando WhatsApp:



Lea más sobre este caso práctico a continuación.

Instagram, con 231 630 ataques de phishing observados, se enfrenta a amenazas como el secuestro de cuentas, los intentos de phishing y la difusión de enlaces o contenidos maliciosos. Como plataforma líder para compartir fotografías y vídeos, atrae a ciberdelincuentes que explotan contraseñas débiles, tácticas de ingeniería social o vulnerabilidades de aplicaciones de terceros para comprometer las cuentas de los usuarios.

VKontakte, con 35 768 ataques de phishing observados, se enfrenta a desafíos de seguridad específicos de su base de usuarios en Rusia y los países vecinos. Las ciberamenazas dirigidas a VKontakte, un servicio de redes y medios sociales con sede en Rusia, incluyen infracciones de cuentas, ataques de phishing y distribución de contenido malicioso.

X (anteriormente Twitter), con 2437 ataques de phishing observados, se enfrenta a una variedad de problemas de seguridad, incluidas infracciones de cuentas, intentos de suplantación de identidad y la difusión de noticias falsas o enlaces maliciosos. La naturaleza en tiempo real de X y su gran base de usuarios lo convierten en un objetivo atractivo para los ciberdelincuentes que buscan difundir información errónea o comprometer cuentas de usuarios.

Snapchat, con 2406 ataques de phishing observados, se enfrenta a preocupaciones de seguridad únicas relacionadas con sus funciones de mensajería multimedia y contenido generado por el usuario. Si bien los mensajes autodestructivos de Snapchat brindan cierto nivel de privacidad, los atacantes pueden intentar explotar las vulnerabilidades para comprometer cuentas o participar en estafas de ingeniería social.

Un phishing, dos caras: IA y phishing

¿Qué sucede cuando las astutas tácticas de phishing se encuentran con el poder de la IA? La convergencia de estas dos fuerzas significa una profunda revolución en las ciberamenazas.

Los ataques de phishing impulsados por IA aprovechan las herramientas de IA para mejorar la sofisticación y eficacia de las campañas de phishing. La IA automatiza y personaliza varios aspectos del proceso de ataque, lo que hace que el phishing sea aún más difícil de detectar. Por ejemplo, los chatbots se utilizan habitualmente para crear correos electrónicos de phishing muy convincentes y sin errores. Es más, los atacantes aprovechan cada vez más servicios avanzados de inteligencia artificial, como la tecnología deepfake y la clonación de voz, para hacerse pasar por organizaciones o personas de buena reputación y engañar a las víctimas. Explotan diferentes canales de comunicación, incluidos correos electrónicos, llamadas telefónicas y videollamadas, SMS y aplicaciones de mensajería cifrada.

Estas tácticas avanzadas nos recuerdan la importancia de la vigilancia y el escepticismo al interactuar con las comunicaciones digitales, así como la necesidad de que las organizaciones implementen medidas sólidas de ciberseguridad para mitigar el riesgo de ser víctimas de ataques de phishing impulsados por IA.

Los phishers abusan de la IA, pero la IA se defiende

La IA generativa está impulsando rápidamente el panorama de las amenazas de phishing, permitiendo la automatización y la eficiencia en numerosas etapas de la cadena de ataque. Al analizar rápidamente los datos disponibles públicamente, como detalles sobre organizaciones o ejecutivos, GenAI ahorra tiempo a los autores de amenazas en el reconocimiento y al mismo tiempo facilita ataques dirigidos más precisos. Al eliminar errores ortográficos y gramaticales, las herramientas GenAI mejoran la credibilidad de las comunicaciones de phishing. Es más, GenAI puede crear rápidamente páginas de phishing sofisticadas (como se demuestra en el siguiente caso práctico) o ampliar sus capacidades para generar malware y ransomware para ataques secundarios. A medida que las herramientas y tácticas de GenAI evolucionan rápidamente, los ataques de phishing serán cada día más dinámicos (y más difíciles de detectar).

La creciente popularidad y el uso de herramientas GenAI como ChatGPT y Drift ya están comenzando a afectar la actividad de phishing y el aumento de los ataques impulsados por IA. Países como EE. UU. e India, donde estas herramientas se utilizan ampliamente según la investigación de ThreatLabz en el Informe de seguridad de IA de 2024, son los principales objetivos de las estafas de phishing y recibieron la mayor cantidad de ataques cifrados en el último año, una parte de los cuales son ataques de phishing.

THREATLABZ RASTREA ACTIVAMENTE EL ABUSO DE MODELOS DE LENGUAJE GRANDE (LLM) LEGÍTIMOS Y MALICIOSOS PARA GARANTIZAR UNA COBERTURA INTEGRAL CONTRA ATAQUES DE PHISHING A FIN DE QUE ZSCALER LUCHE CONTRA LA IA CON INNOVACIONES DE IA, QUE INCLUYEN:

Prevención de la suplantación de identidad basada en IA y C2

Los modelos de IA de Zscaler detectan sitios de phishing conocidos y sin pacientes para evitar el robo de credenciales y la explotación del navegador, además de analizar patrones de tráfico, comportamiento y malware para detectar infraestructura de comando y control (C2) nunca antes vista en tiempo real. Estos modelos se basan en una combinación de inteligencia sobre amenazas, investigación de ThreatLabz y aislamiento dinámico del navegador para detectar sitios sospechosos. Como resultado, las empresas son aún más eficientes y efectivas a la hora de detectar nuevos ataques de phishing, incluidos los ataques generados por IA y dominios C2.

Defensa de sandbox de IA basada en archivos

Zscaler Sandbox en línea con tecnología de inteligencia artificial detecta instantáneamente archivos maliciosos y mantiene a los empleados productivos. Las tecnologías tradicionales de sandbox hacen que los usuarios esperen mientras se analizan los archivos o, de lo contrario, asumen un riesgo para el paciente cero cuando se permiten archivos en la primera pasada. Nuestra tecnología AI Instant Verdict identifica, pone en cuarentena y previene al instante archivos maliciosos de alta confianza (incluidas las amenazas de día cero) y, al mismo tiempo, elimina la necesidad de esperar el análisis de estos archivos. Esto incluye amenazas que se entregan a través de canales cifrados (TLS y HTTPS) y otros protocolos de transferencia de archivos. Mientras tanto, los archivos benignos se entregan de forma segura e instantánea.

IA para bloquear amenazas web

Zscaler Browser Isolation, impulsado por IA, bloquea las amenazas de día cero y al mismo tiempo garantiza que los empleados puedan acceder a los sitios adecuados para realizar su trabajo. En la práctica, el filtrado de URL empresarial a menudo requiere controles más granulares que simplemente permitir/bloquear; los sitios bloqueados con frecuencia son seguros y necesarios para el trabajo, lo que genera tickets innecesarios al servicio de asistencia técnica. Nuestro AI Smart Isolation puede identificar cuándo un sitio puede ser peligroso y abrirlo de forma aislada para el usuario, transmitiendo de forma segura el sitio como píxeles en un entorno seguro y en contenedores. Esto detiene eficazmente las amenazas basadas en la web, como malware, ransomware, phishing y descargas no autorizadas, creando una postura de seguridad web sólida sin necesidad de que las empresas bloqueen demasiado los sitios de forma predeterminada.

Caso práctico: creación de una página de inicio de sesión de phishing en menos de 10 consultas de ChatGPT

Los LLM también han hecho que sea mucho más fácil para los ciberdelincuentes, incluso aquellos con relativamente poca experiencia en codificación, llevar a cabo las múltiples etapas de un ataque de phishing sofisticado.

Por ejemplo, en tan solo unas pocas indicaciones utilizando un chatbot generativo de IA como ChatGPT, es realmente sencillo crear páginas de inicio de sesión de phishing falsas que imitan aplicaciones empresariales populares para robar las credenciales de inicio de sesión de los empleados. El siguiente ejemplo de ThreatLabz muestra lo fácil que es crear una página de inicio de sesión falsa y convincente de Microsoft con solo unas pocas indicaciones de conversación.

Nota: Para fines de demostración, este ejemplo muestra mensajes ligeramente abreviados e incluye una respuesta de código ChatGPT para una consulta antes de mostrar la página de phishing final.

Mensaje de usuario: Cree una página de inicio de sesión HTML
ChatGPT: Claro, aquí hay un ejemplo básico de una página de inicio de sesión HTML:

```
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <meta name="viewport" content="width=device-width
 <title>Login Page</title>
 <style>
  body {
   font-family: Arial, sans-serif;
   background-color: #f4f4f4;
  }
  .login-container {
   width: 300px;
   margin: 100px auto;
   padding: 20px;
   background-color: #fff;
   border-radius: 5px;
   box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
  }
```

ESTE FUE EL PRIMER RESULTADO:

FIGURA 5: Captura de pantalla de una página de inicio de sesión producida usando la respuesta del código ChatGPT

A continuación, ThreatLabz proporcionó una breve serie de indicaciones para mejorar la página antes de mostrar la página final de inicio de sesión de phishing de Microsoft. Estos incluyeron pedirle a ChatGPT que hiciera que la página pareciera un inicio de sesión de Microsoft, ajustar el tamaño del logotipo, y agregar y eliminar elementos de la interfaz de usuario antes de enviar la consulta final para generar el código final.

Mensaje de usuario: Agregue un fondo de página similar a la página de inicio de sesión de Microsoft

ChatGPT:

EN 7 CONSULTAS, EL RESULTADO FINAL:

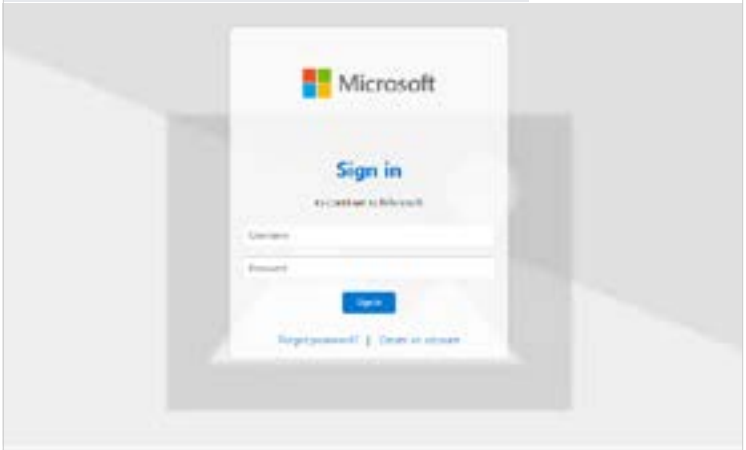


FIGURA 6: Captura de pantalla de la página de inicio de sesión de phishing de Microsoft final producida utilizando la respuesta del código ChatGPT

Aumento de los ataques deepfake

La tecnología Deepfake utiliza técnicas de inteligencia artificial y aprendizaje automático para crear contenido de audio o vídeo realista y manipulado que parece auténtico. Esto puede variar desde superponer el rostro de alguien al cuerpo de otra persona hasta alterar sus expresiones faciales y su voz para crear una representación convincente y, a menudo, engañosa.

La tecnología Deepfake utiliza algoritmos y redes neuronales para analizar y aprender de grandes cantidades de datos, como imágenes, vídeos y grabaciones de audio de un individuo específico. Con esta información, el modelo de IA puede generar contenido nuevo que imite la apariencia, la voz y los gestos de esa persona.

Los ataques deepfake ya están provocando importantes pérdidas financieras a las organizaciones. En un incidente reciente, un trabajador del sector financiero pagó sin saberlo 25 millones de dólares estadounidenses a estafadores que utilizaban tecnología deepfake para hacerse pasar por compañeros de trabajo en una videollamada[3]. Los atacantes se hicieron pasar por el director financiero de la empresa y manipularon vídeos disponibles públicamente para engañar al trabajador y obligarle a realizar una transacción fraudulenta.

Los ataques realistas impulsados por deepfakes que cuestan a las organizaciones millones de dólares no son ciencia ficción: son el panorama de amenazas actual.

Caso práctico: Una campaña Deepfake se hace pasar por Elon Musk

En el verano de 2023, un grupo de ciberdelincuentes orquestó una campaña de deepfake utilizando la imagen y la reputación del empresario Elon Musk.

La campaña gira en torno al uso de anuncios falsos para engañar a las personas para que "inviertan" dinero en una nueva plataforma llamada "Quantum AI". Estos anuncios se pueden encontrar en plataformas de redes sociales y resultados de motores de búsqueda.

La campaña tenía como objetivo solicitar fondos a las víctimas prometiéndoles rendimientos notablemente altos, como un asombroso 91 %. Musk aparece en el anuncio principal de “Quantum AI”, aunque parece distante y desenfocado. El vídeo imita su voz y presenta la típica presentación de un producto al estilo de una conferencia tecnológica.

Además, un anuncio secundario toma la forma de una página web inventada de Fox News, afirmando que Musk dio una entrevista promocionando Quantum AI.

FIGURA 7: La página de Quantum AI muestra un vídeo de respaldo ultra falso de Elon Musk

FIGURA 8: Una página web fraudulenta de Fox News que promociona la plataforma falsa Quantum AI

3. CNN, Un trabajador del sector financiero paga 25 millones de dólares estadounidenses tras una videollamada con un "director financiero" deepfake, 4 de febrero de 2024.

Con la vista puesta en las elecciones: campañas de phishing frente a campañas políticas

Dado que más de la mitad de la población mundial vive en países que celebrarán votaciones a nivel nacional en 2024, será un año récord para las elecciones. En medio de las campañas políticas y el fervor, destaca el espectro de las ciberamenazas, particularmente en forma de campañas de phishing.

Las amenazas de phishing arrojan una larga sombra sobre la seguridad electoral y la integridad de los procesos democráticos en todo el mundo. A lo largo de la historia, los ciberdelincuentes han utilizado tácticas de phishing para manipular a los votantes, difundir desinformación y comprometer la infraestructura electoral crítica.

Si recordamos las elecciones presidenciales de EE. UU. de 2020, los autores de amenazas se dirigieron a votantes indecisos que resultan cruciales con correos electrónicos de phishing avanzados disfrazados de comunicaciones oficiales de entidades gubernamentales o campañas políticas, instando a los destinatarios a confirmar los detalles del registro de votantes o solicitar papeletas de voto ausente a través de enlaces fraudulentos.

El auge de la IA generativa aumenta los riesgos para la seguridad electoral este año y en el futuro. Los avances en la tecnología de inteligencia artificial presagian el potencial de un impacto real en lo que respecta al phishing y los esquemas electorales. El mencionado auge de la tecnología deepfake ya ha introducido una nueva dimensión de engaño en el proceso electoral[4]. Los vídeos de phishing deepfake manipulados para representar narrativas o declaraciones falsas de figuras políticas pueden influir en la opinión pública, difundir desinformación y erosionar la confianza en el propio proceso electoral.

ThreatLabz descubrió recientemente un caso preocupante de amenazas persistentes avanzadas (APT) dirigidas a entidades políticas: un caso de ciberespionaje por parte del autor de amenazas SPIKEDWINE, que utiliza tácticas de phishing para explotar las relaciones geopolíticas entre la India y los diplomáticos europeos. En enero de 2024, ThreatLabz descubrió un PDF sospechoso en VirusTotal disfrazado de una carta de invitación del embajador de la India (aunque originario de Letonia) para un evento de cata de vinos relacionado con el gobierno. El PDF contenía un enlace a un cuestionario falso que redirigía a los usuarios a un archivo ZIP malicioso en un sitio web comprometido. Este descubrimiento reveló una nueva puerta trasera, "WINELOADER". Puede leer un análisis técnico completo de la cadena de ataque en el blog de Zscaler.

Los cazadores de amenazas de Zscaler identificaron un PDF similar subido a VirusTotal desde Letonia en julio de 2023, lo que indica un patrón de ataques dirigidos y enfatiza la necesidad de proteger los procesos y las relaciones políticas, especialmente a la vista de la temporada electoral.

Los esfuerzos de seguridad electoral deben priorizar medidas proactivas para detectar y mitigar los ataques de phishing. Fomentar la colaboración entre funcionarios electorales, expertos en ciberseguridad y organismos encargados de hacer cumplir la ley, así como promover ampliamente la concientización sobre el phishing y las mejores prácticas de seguridad ayudará a proteger a los ciudadanos y las organizaciones frente a las amenazas de phishing en evolución.

Ejemplos de phishing en la historia electoral

2016

APT28 y APT29 vulneran el Comité Nacional Demócrata en EE. UU. y filtran datos confidenciales en línea.

2017

Los ataques de phishing se centran en la campaña de Emmanuel Macron durante las elecciones presidenciales francesas.

2019

Los ataques de phishing durante las elecciones generales de la India se centran en partidos políticos, funcionarios y medios de comunicación.

2020

Los ataques de phishing por parte de autores de amenazas en Rusia, China e Irán tienen como objetivo el ciclo de elecciones presidenciales de Estados Unidos.

4. Bloomberg, Cómo el mal doblaje de películas llevó a las llamadas automáticas falsas de la campaña de Biden, 20 de febrero de 2024.

Tendencias de phishing en constante evolución

Los autores de amenazas siempre están perfeccionando sus tácticas y estrategias para perpetrar estafas más efectivas, por lo que mantenerse al día con las tendencias de phishing en desarrollo es esencial para establecer y mantener defensas proactivas.

Los investigadores de ThreatLabz rastrearon diligentemente las tendencias de phishing a lo largo de 2023. En esta sección, profundizaremos en varias tendencias notables que surgieron, destacando el ingenio y la sofisticación que impulsaron el aumento del phishing.

Ataques de vishing

El phishing de voz, conocido como vishing, implica engañar a personas mediante llamadas telefónicas y mensajes de voz, a menudo utilizando voces familiares o autorizadas para ganarse la confianza y extraer información confidencial.

Las sofisticadas campañas de vishing se están volviendo populares en todo el mundo, en las que los ciberdelincuentes utilizan la psicología y la tecnología para defraudar incluso a víctimas inteligentes por millones de dólares. Por ejemplo, Corea del Sur ha experimentado un aumento en los ataques de vishing, incluido un caso en agosto de 2022 en el que un médico perdió 3 millones de dólares estadounidenses en efectivo, seguros, acciones y criptomonedas que se llevaron los delincuentes[5]. En este caso, los estafadores se hicieron pasar por funcionarios encargados de hacer cumplir la ley en Corea del Sur; sin embargo, ThreatLabz observó (y frustró) un ataque de vishing muy cerca de casa en 2023.

Caso práctico de vishing

En el verano de 2023, los atacantes se hicieron pasar por el propio director ejecutivo de Zscaler, Jay Chaudhry, en un ataque de vishing utilizando tecnología de inteligencia artificial. El proceso fue el siguiente:

- El atacante llamó a un empleado de Zscaler por WhatsApp.
- Utilizando la clonación de voz generada por IA para simular la voz de Jay, el atacante estableció comunicación y luego colgó rápidamente para evitar una interacción prolongada y una posible exposición.
- El atacante inmediatamente siguió con un mensaje de texto, haciéndose pasar por Jay, afirmando tener "mala cobertura de red".
- En un mensaje de texto de WhatsApp, el atacante ordenó al empleado de Zscaler que comprara tarjetas regalo por un importe determinado.
- El empleado encontró esto sospechoso e inmediatamente lo informó al equipo de seguridad.
- Los investigadores de ThreatLabz investigaron y descubrieron que era parte de una campaña generalizada dirigida a varias empresas de tecnología.

Puede ver a Jay mientras explica la secuencia completa de eventos en NBC Bay Area.

5. Lectura oscura, Sofisticadas campañas de vishing toman el mundo por asalto, 11 de marzo de 2024.

Estafas de contratación

Las estafas de contratación tienen como objetivo engañar y explotar a quienes buscan empleo. Estas estafas a menudo implican la creación de ofertas de trabajo falsas en bolsas de trabajo, redes sociales y sitios web de redes profesionales de buena reputación como LinkedIn. Los atacantes se hacen pasar por empresas o contratadores legítimos y manipulan a las víctimas para que divulguen información confidencial o descarguen malware.

Desafortunadamente, los despidos tecnológicos en 2022, 2023 y 2024 generaron una nueva generación de candidatos ansiosos en el mercado digital, lo que significa más objetivos principales para los estafadores de contratación.

Caso práctico de estafa de contratador en LinkedIn

Uno de los principales canales de distribución para las estafas de contratación por parte de los autores de amenazas DuckTail es LinkedIn, una plataforma de redes profesionales ampliamente confiable. Los autores de amenazas aprovechan la credibilidad de la plataforma y la confianza de sus usuarios para difundir ofertas de trabajo fraudulentas. Al hacerse pasar por empresas de buena reputación y aprovechar perfiles de contratadores falsos, atraen a las víctimas con atractivas oportunidades laborales. Una vez que un candidato expresa interés en un puesto falso, el autor de la amenaza inicia el contacto a través de mensajes privados en LinkedIn, iniciando el proceso de ingeniería social. El autor de la amenaza comparte un archivo malicioso disfrazado de descripción de trabajo, que infecta el sistema de la víctima cuando se descarga.

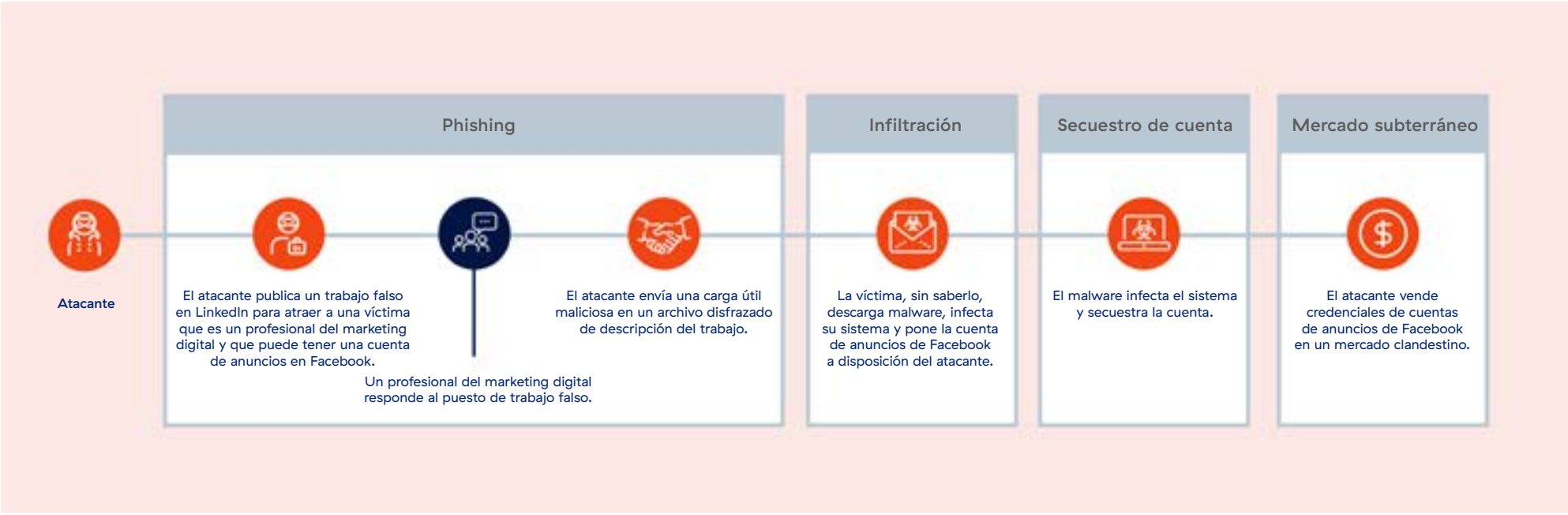


Figura 9: Secuencia de ataque de estafa de contratación

Ataques de adversario en el medio (AiTM)

En un ataque de phishing de adversario en el medio (AiTM), el adversario intercepta y manipula las comunicaciones entre dos partes para engañar a la víctima. Al posicionarse entre la víctima y una entidad de confianza, el atacante obtiene acceso no autorizado a información confidencial. A diferencia de los ataques de phishing tradicionales, los ataques AiTM ocurren en tiempo real, lo que permite a los atacantes monitorizar y modificar las comunicaciones. Pueden alterar mensajes, redirigir a las víctimas a sitios web maliciosos y recopilar datos sin ser detectados. La protección contra el phishing de AiTM implica:

- Utilizar canales de comunicación seguros
- Verificar la autenticidad del sitio web
- Tener precaución al compartir información confidencial
- Mantener el software actualizado

Obtenga más información sobre los ataques de phishing de AiTM en el blog de Zscaler.

Caso práctico de AiTM

Los investigadores de ThreatLabz observaron un aumento en el uso de kits de phishing avanzados en una campaña a gran escala. Esta campaña destaca porque utiliza una técnica de ataque AiTM capaz de eludir la autenticación multifactor y está diseñada específicamente para atacar a usuarios finales empresariales.

Los kits de proxy AiTM han evolucionado para generar páginas de phishing que imitan fielmente páginas web legítimas, lo que hace difícil distinguirlas del tráfico de red benigno. Además, el uso de kits de proxy proporciona a los autores de amenazas una forma sencilla de difundir páginas de phishing de forma eficaz.

ThreatLabz ha detectado ataques de phishing de AiTM dirigidos a usuarios empresariales de Microsoft y Gmail en la nube Zscaler. Al supervisar de cerca estos ataques, ThreatLabz ha encontrado una tendencia persistente en hacer de los usuarios empresariales de Microsoft objetivos. Además, estos ataques de phishing de AiTM han demostrado resistencia durante un período prolongado.

La Figura 10 muestra una comparación en dos columnas del código fuente de una página de Microsoft servida por AiTM y la página de inicio de sesión legítima de Microsoft.

Figura 10: Código fuente de una página de Microsoft utilizada por un adversario intermedio (izquierda) frente a una página de inicio de sesión legítima de Microsoft (derecha)

Ataques de navegador en el navegador (BiTB)

En los ataques de navegador en el navegador (BiTB), los ciberdelincuentes pretenden engañar a los usuarios simulando una ventana de navegador dentro de otro navegador para falsificar un dominio legítimo. En estos ataques sofisticados, los atacantes manipulan la apariencia de una página web para hacer creer a los usuarios que están interactuando con un sitio web confiable, cuando en realidad se trata de una falsificación maliciosa.

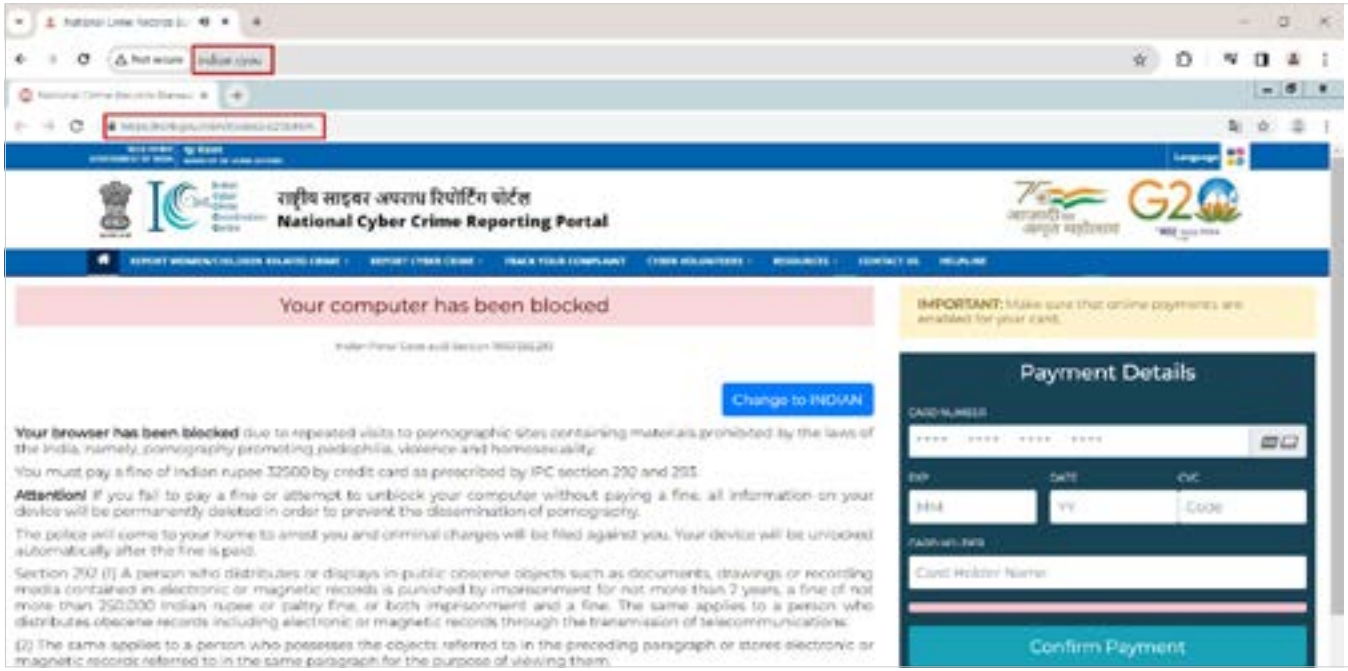
Por ejemplo, un atacante podría utilizar una combinación de HTML/CSS y marcos en línea (iframes) para crear una ventana emergente de inicio de sesión de apariencia auténtica en una página principal de phishing, que solicita al usuario sus credenciales. Desafortunadamente, cuando el usuario introduce sus credenciales, las comparte con el atacante. Incluso los usuarios más perspicaces o experimentados pueden verse engañados porque les resulta casi imposible distinguir una ventana emergente genuina de una falsificación de phishing bien diseñada.

Inicialmente, los ataques BiTB estaban diseñados principalmente para simular sitios web legítimos en una ventana del navegador con el fin de robar información confidencial, como credenciales de inicio de sesión o datos financieros. Sin embargo, a medida que los ciberdelincuentes adaptan sus estrategias, los ataques de BiTB han ampliado su alcance para incluir sextorsión.

Caso práctico de BiTB

En las variantes de ataque BiTB observadas recientemente en la nube Zscaler, los atacantes se han hecho pasar por agencias gubernamentales, fuerzas del orden u otras entidades autorizadas de los respectivos países de las víctimas para llevar a cabo una forma de ataque de sextorsión.

Los atacantes manipulan los navegadores de las víctimas para mostrar mensajes o notificaciones que a menudo acusan falsamente a las víctimas de actividades ilegales y amenazan con emprender acciones legales a menos que se pague un rescate o se proporcione información confidencial. Al explotar la credibilidad de las autoridades, los atacantes pretenden obligar a las víctimas a cumplir, lo que lleva a la extorsión o una mayor explotación de los datos personales.



La Figura 11 muestra un ataque de BiTB que se hace pasar por una agencia de delitos cibernéticos y afirma falsamente que el ordenador de la víctima está bloqueado. Sin embargo, la apariencia del navegador principal no coincide con la del sitio web legítimo de una agencia. El diseño inusual levanta sospechas sobre la autenticidad y credibilidad del mensaje.

Figura 11: Un ejemplo de un ataque de navegador en el navegador (BiTB)

Estafas QR

En las estafas QR, los autores de amenazas engañan a las víctimas para que escaneen códigos QR que, en última instancia, conducen a enlaces maliciosos. Esta estafa emplea varios métodos de entrega, incluida la redirección maliciosa, archivos adjuntos de correo electrónico (como archivos PDF o DOC) y otras formas de comunicación digital. El método más común de los ciberdelincuentes es enviar por correo electrónico un PDF que contiene una imagen QR, que luego redirige a las víctimas a una página de phishing.

URL inusuales

Para identificar una estafa de código QR es necesario examinar la URL asociada. Las URL legítimas suelen estar libres de errores, sin errores ortográficos ni frases inusuales en su nombre de dominio o ruta URL. La Figura 12 muestra una pareja inusual, con “gard–ner” junto al usualmente legítimo “Toyota”.

Figura 12: Un ejemplo de una URL maliciosa asociada con un código QR

Proceso CAPTCHA falso

Los sitios web fraudulentos que emplean códigos QR como CAPTCHA, como el ejemplo de la figura 13, presentan un giro engañoso del proceso típico de verificación de CAPTCHA. En lugar del desafío habitual basado en imágenes o texto, estos sitios solicitan a los usuarios que escaneen un código QR. Luego, los estafadores redirigen a los usuarios a sitios web fraudulentos o extraen información confidencial.

Figura 13: Un sitio web fraudulento que utiliza un código QR como método de verificación CAPTCHA

Actualizaciones de seguridad falsas

Los correos electrónicos de phishing que incorporan códigos QR, particularmente cuando están disfrazados de actualizaciones de seguridad, introducen un nuevo nivel de engaño para explotar a destinatarios desprevenidos. Estos correos electrónicos a menudo parecen provenir de fuentes confiables, como empresas o proveedores de servicios conocidos, que afirman ofrecer importantes actualizaciones de seguridad o verificación de cuentas. La Figura 14 muestra un ejemplo.

Figura 14: Un correo electrónico de phishing que utiliza un código QR para engañar a los usuarios y enviarles una “actualización de seguridad” fraudulenta

Estafas de soporte técnico

Las estafas de soporte técnico engañan a los usuarios haciéndoles creer que su dispositivo está infectado con malware o virus. Los atacantes utilizan tácticas como mensajes emergentes, alertas antivirus falsas o correos electrónicos alarmantes para explotar el miedo y el conocimiento técnico limitado, creando urgencia y pánico. Instan a tomar medidas inmediatas, como descargar software u otorgar acceso remoto para la limpieza del sistema, lo que posteriormente les ayudará a obtener acceso a información confidencial o detalles financieros.

En una reciente estafa de soporte técnico, ThreatLabz identificó un método mediante el cual los autores de amenazas explotan las notificaciones del Centro de actividades de Windows para engañar a los usuarios. Al manipular el sistema de notificación integrado, los atacantes generan advertencias y alertas falsas que se parecen mucho a mensajes legítimos del sistema, utilizando logotipos y lenguaje que parecen auténticos. Estas notificaciones engañosas afirman falsamente de la presencia de infecciones de virus, software desactualizado o vulnerabilidades de seguridad, y luego solicitan a las víctimas que se comuniquen con un número de soporte técnico fraudulento o visiten un sitio web malicioso para obtener ayuda para resolver los problemas inventados.

Esta técnica, típica de las estafas de soporte técnico, tiene como objetivo incitar urgencia y pánico, obligando a las víctimas a revelar información personal, otorgar acceso remoto o comprar servicios o software innecesarios y potencialmente dañinos.

Las figuras 15 y 16 muestran dos ventanas emergentes fraudulentas que intentan convencer a una víctima de que su sistema está infectado.

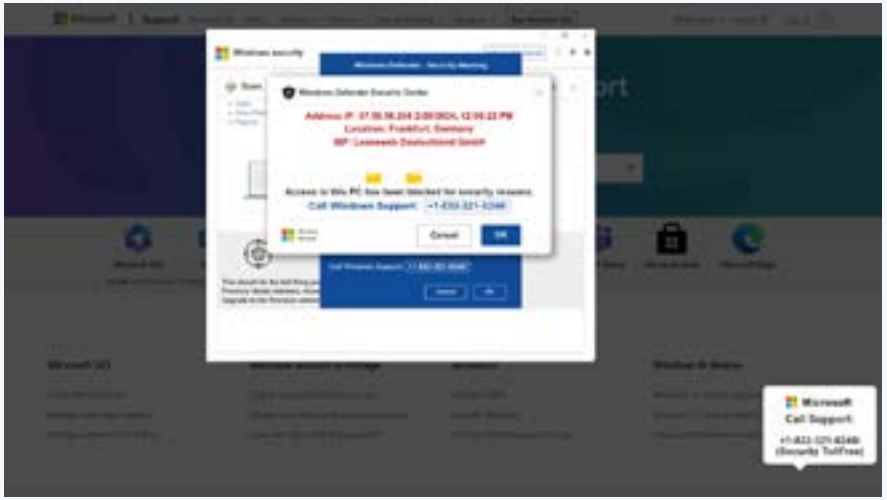


Figura 15: Una captura de pantalla de una ventana emergente falsa del Centro de seguridad de Windows Defender

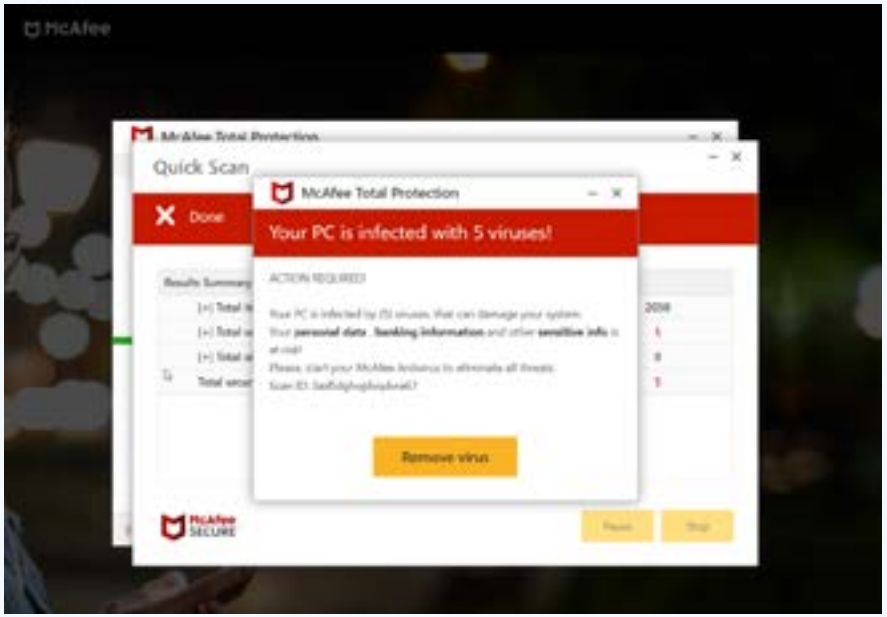


Figura 16: Una ventana emergente alarmante disfrazada de notificación de McAfee

Predicciones 2024–2025

1 La IA contra la IA será un desafío duradero.

En 2025, anticipamos una transformación significativa en las estrategias de ciberataque y defensa con la adopción generalizada de la IA generativa. Los autores de amenazas adoptarán ampliamente la IA para diseñar esquemas de phishing más sofisticados y técnicas avanzadas. Al mismo tiempo, los proveedores de seguridad integrarán la IA generativa en sus kits de herramientas para mejorar las capacidades de detección y respuesta a amenazas. Esta era introduce una realidad ineludible: la IA será un arma de doble filo, ya que tanto los autores de amenazas como los defensores utilizan su poder. Se necesitarán medidas de seguridad impulsadas por la IA para contrarrestar eficazmente los ataques impulsados por la IA.

Aunque la intervención dirigida ha detenido algunos de estos ataques, las empresas deberían prepararse para la persistencia de iniciativas de IA respaldadas por el Estado. Estas abarcan el despliegue de herramientas de inteligencia artificial populares, la creación de LLM patentados y la aparición de variantes sin restricciones inspiradas en ChatGPT, como los bien llamados FraudGPT o WormGPT. El panorama en evolución presenta un panorama complicado en el que los ciberdelincuentes patrocinados por el Estado continúan aprovechando la IA de formas novedosas para crear nuevas ciberamenazas complejas.

2 El phishing como servicio intensificará su enfoque en la explotación de MFA y AiTM.

Durante el año pasado, surgió una tendencia preocupante en la que los adversarios eluden con éxito la autenticación multifactor empresarial (MFA) mediante ataques de phishing basados en proxy de adversario en el medio (AiTM). En el próximo año, esperamos que los kits de phishing incluyan cada vez más técnicas sofisticadas de AiTM, contenido de phishing localizado y huellas dactilares de objetivos, por supuesto habilitadas por IA. Estos avances permitirán a los atacantes realizar campañas de phishing de gran volumen destinadas a evadir las protecciones de MFA a escala empresarial.

3 Los ataques de vishing encabezados por grupos de malware aumentarán significativamente.

Espere un aumento en las campañas de phishing de voz y vídeo con objetivos específicos llevadas a cabo por grupos como Scattered Spider, reconocido por utilizar tácticas y técnicas sofisticadas. Estas campañas se centrarán en obtener credenciales de inicio de sesión de los empleados para obtener acceso no autorizado a sistemas seguros, lo que podría conducir a una mayor explotación, persistencia, exfiltración de datos e incluso infracciones en toda la organización. Sumado a la prevalencia de herramientas de voz y vídeo impulsadas por IA, esto puede hacer que sea aún más fácil para los autores de amenazas hacerse pasar por personal corporativo, planteando nuevos desafíos para los empleados a la hora de identificar estos ataques de phishing.

4 Los atacantes se centrarán en las vulnerabilidades inherentes a los dispositivos y plataformas móviles.

Esta tendencia se verá subrayada por un cambio en las tácticas de phishing para explotar la clave de acceso y la biometría como métodos de autenticación a través de tácticas como solicitudes de autenticación falsas e ingeniería social promovida por IA dirigida a usuarios móviles. Es de esperar que los atacantes también utilicen cada vez más la inserción falsa de notificaciones que imitan las de aplicaciones legítimas y conducen a sitios web de phishing relacionados, explotando la confianza de los usuarios móviles en un canal de comunicación de uso común.

5 Espere un aumento del phishing diseñado para perturbar los procesos electorales.

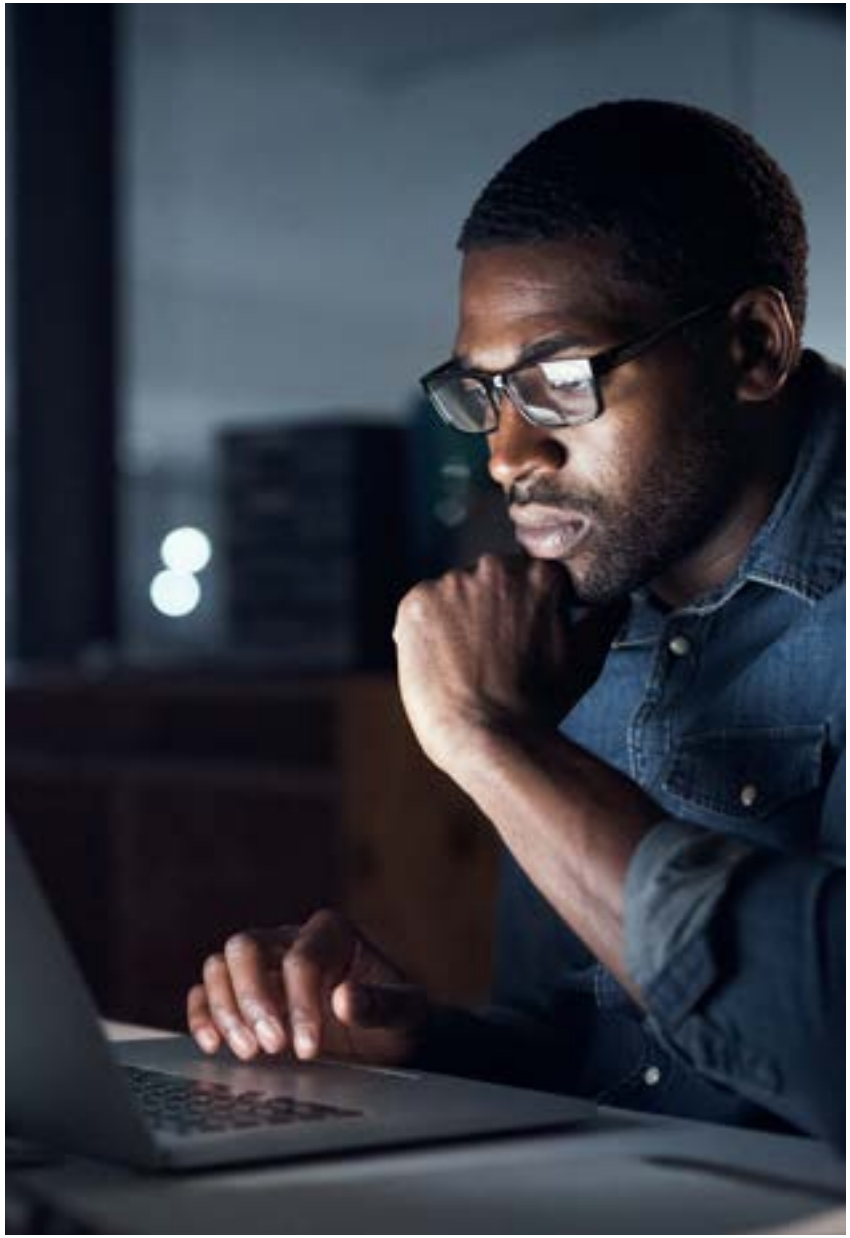
Estas estafas abarcarán todos los aspectos, desde la manipulación del registro de votantes hasta la difusión de desinformación destinada a influir en la opinión pública. Más allá del alcance del phishing tradicional con fines de lucro, estas campañas girarán hacia un objetivo más malicioso: captar la mentalidad e influir en los resultados políticos. Los atacantes explotarán las vulnerabilidades inherentes al panorama digital para manipular la confianza de los usuarios y difundir narrativas engañosas, gracias a tácticas de phishing impulsadas por IA, como la creación de mensajes altamente personalizados y persuasivos. Este cambio supondrá una grave amenaza a la integridad fundamental de los sistemas democráticos, socavando la percepción pública y erosionando la confianza en los procesos electorales.

6 Las plataformas de mensajería cifrada se convertirán en caldo de cultivo para ataques de phishing.

Estas plataformas presentarán oportunidades atractivas para los aspirantes a phishers y brindarán un espacio para que los autores de amenazas operen libremente. Utilizando bots, por ejemplo, los atacantes podrán automatizar actividades ilegales, desde generar páginas de phishing hasta recopilar datos confidenciales de los usuarios. Los canales operados por estafadores surgirán como centros de esquemas fraudulentos, atrayendo a los usuarios con ofertas aparentemente generosas, como kits de phishing listos para usar y diseñados para atacar a marcas globales y locales.

7 Los ataques de phishing desde el navegador dentro del navegador aumentarán.

Al explotar la confianza que los usuarios depositan en los navegadores abiertos y los sitios web legítimos, estos ataques llevarán a los usuarios confiados a interactuar con sitios fraudulentos convincentes. Los atacantes utilizarán cada vez más la personalización impulsada por la IA en los ataques a los navegadores a fin de, por ejemplo, adaptar las páginas web de phishing para imitar los entornos de los navegadores de manera más convincente o analizar las interacciones de los usuarios y ajustar el contenido de phishing en función de los comportamientos observados.



Cómo puede Zscaler Zero Trust Exchange mitigar los ataques de phishing

Proteger su organización para evitar que los usuarios se vean comprometidos es un desafío importante, especialmente con el aumento de los ataques de phishing impulsados por IA. Para defenderse eficazmente ante este panorama de amenazas en evolución, las organizaciones deben integrar controles avanzados de prevención de phishing en estrategias de confianza cero. A la vanguardia de esta estrategia de defensa se encuentra Zscaler Zero Trust Exchange™, construido sobre una sólida arquitectura de confianza cero.

Adoptando un enfoque integral de la ciberseguridad, Zero Trust Exchange frustra eficazmente los ataques de phishing tanto convencionales como impulsados por IA en múltiples etapas de la cadena de ataque al:

01 Impedir que nadie se vea comprometido

02 Eliminar el movimiento lateral

03 Bloquear a usuarios comprometidos y amenazas internas

04 Detener la pérdida de datos

Impedir que nadie se vea comprometido

Aprovechar la inspección a escala TLS/SSL total, el aislamiento del navegador y el control de acceso basado en políticas para evitar el acceso a sitios web sospechosos.

Zscaler utiliza técnicas de análisis avanzadas para identificar y bloquear URL de phishing sospechosas mientras descifra e inspecciona el tráfico cifrado con TLS/SSL en tiempo real para prevenir intentos de phishing antes de que lleguen a los usuarios. Esto implica analizar los sitios y dominios de destino en busca de varios indicadores de phishing mientras los motores de IA de Zscaler evalúan las características del dominio, la información del certificado, el parecido con la marca y más en busca de anomalías. Es más, al ejecutar sesiones de navegación web en un entorno aislado, Zscaler garantiza que cualquier amenaza potencial que se origine en la web no pueda llegar al dispositivo del usuario.

El control de acceso basado en políticas frena el acceso no autorizado, particularmente en casos de credenciales robadas o compromiso de MFA. Incluso si los atacantes logran superar las defensas iniciales, deben autenticarse correctamente a través de Zero Trust Exchange para acceder a los recursos. Zscaler incorpora conciencia contextual en sus procesos de autenticación, examinando factores como la identidad del dispositivo y la ubicación geográfica. Las desviaciones de las normas establecidas desencadenan medidas de seguridad adicionales: bloquear el acceso a sitios web sospechosos y mantener segura su organización.

En caso de que se produzca una infección inicial exitosa, Zscaler continúa interrumpiendo activamente las campañas de los atacantes al interceptar las comunicaciones con dominios de comando y control (C2) conocidos, impidiendo futuras actividades maliciosas y sirviendo como una barrera crucial contra el movimiento lateral.

Eliminar el movimiento lateral

Conecte a los usuarios directamente a las aplicaciones, no a la red, para limitar el radio de explosión de un posible incidente.

Con la conectividad directa a la aplicación a través de Zscaler, los empleados (o los atacantes detrás de una campaña de phishing) tienen acceso a recursos limitados. Esta restricción previene efectivamente el movimiento lateral dentro de la red, impidiendo el acceso no autorizado a datos confidenciales u otras aplicaciones. Segmentando el acceso de esta manera, Zscaler minimiza el radio de explosión de un posible incidente y elimina el riesgo de daños generalizados.

Bloqueando a usuarios comprometidos y amenazas internas

Evite intentos de explotación de aplicaciones privadas con inspección en línea y detecte a los atacantes más sofisticados con engaño integrado.

La inspección en línea previene la explotación de aplicaciones privadas al examinar y analizar el tráfico de datos en tiempo real, bloqueando actividades maliciosas de usuarios comprometidos y amenazas internas. Además, Zero Trust Exchange utiliza engaño integrado para detectar atacantes, implementando identidades, archivos o servidores falsos para atraer y detectar intentos de acceso no autorizados. Esta estrategia de doble capa no sólo mitiga el impacto de las identidades comprometidas, sino que también establece una defensa proactiva frente a amenazas internas, alineándose con los principios de confianza cero de verificación continua y adaptación dinámica a los desafíos de seguridad emergentes.

Detener la pérdida de datos

Inspeccione los datos en movimiento y en reposo para evitar posibles robos por parte de un atacante activo.

Al interceptar las comunicaciones con dominios C2 conocidos e implementar medidas de prevención de pérdida de datos (DLP) en línea, Zscaler bloquea eficazmente los intentos de exfiltrar datos confidenciales. Zero Trust Exchange inspecciona los datos en movimiento y en reposo, garantizando que incluso si los atacantes traspasan las barreras iniciales, sus intentos de comprometer valiosos activos de su organización se vean frustrados.

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:

- **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 (incluidas 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 impulsados por la detección de IA/ML.

Advanced Threat Protection bloquea todos los dominios C2 conocidos.

Zscaler ITDR (Detección y respuesta a amenazas de identidad) mitiga el riesgo de ataques basados en la identidad con visibilidad continua, supervisión del riesgo y detección de amenazas.

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

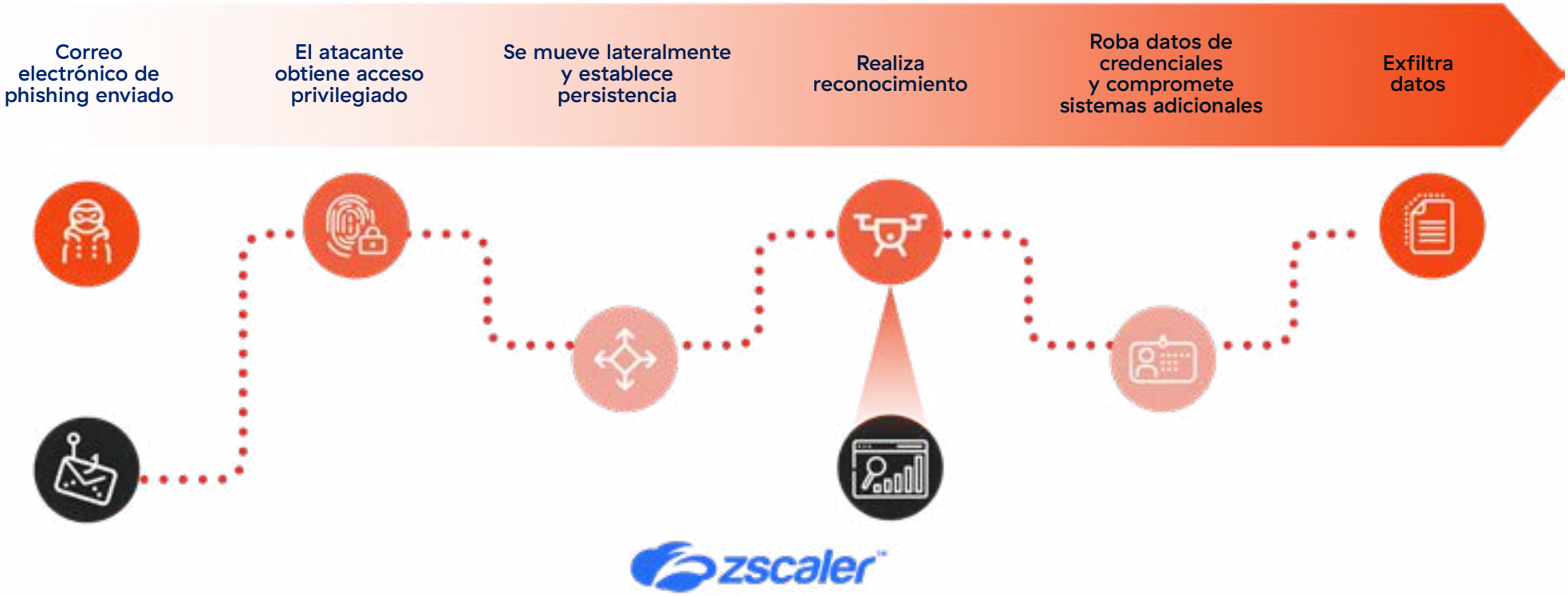
Advanced Firewall extiende la protección C2 a todos los puertos y protocolos, incluidos los destinos C2 emergentes.

DNS Security defiende contra ataques basados en DNS e intentos de exfiltración.

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.

AppProtection detecta y contiene a los atacantes que intentan moverse lateralmente o escalar privilegios atrayéndolos con servidores, aplicaciones, directorios y cuentas de usuario señuelos.

Protección integral a lo largo de la cadena de ataque



Evite la vulneración inicial	Elimine el movimiento lateral y bloquee a los usuarios comprometidos	Prevención de la pérdida de datos
Inspección SSL completa a escala, aislamiento del navegador y control de acceso basado en políticas para evitar el acceso a sitios web sospechosos	Conecte a los usuarios directamente a las aplicaciones; de lo contrario, las aplicaciones estarán ocultas para los usuarios no autorizados; Identifique la actividad sigilosa del adversario con señuelos (Engaño)	Inspección completa del contenido de datos en movimiento y datos en reposo para evitar posibles robos de datos por parte de atacantes activos.

Inspección SSL/TLS siempre activa

Mejore sus defensas contra el phishing

Las estadísticas del sector muestran que las organizaciones reciben múltiples correos electrónicos de phishing diariamente, con pérdidas financieras cada vez mayores debido a ataques de malware y ransomware que aumentan el costo promedio de los incidentes de phishing exitosos. Abordar las amenazas descritas en este informe es una tarea compleja. Aunque es imposible eliminar por completo el riesgo de phishing, las organizaciones pueden tomar medidas para reducir la probabilidad de ser víctimas de este tipo de ataques.

Estos son los pasos fundamentales para mitigar el riesgo de ataques de phishing:

Proteja su organización del phishing

1. **Comprender los riesgos** para tomar decisiones mejor informadas sobre políticas y estrategias

2. **Aproveche los controles de seguridad habilitados por IA y la información sobre amenazas** para reducir los incidentes de phishing

3. **Implemente arquitecturas de confianza cero** para limitar el radio de afectación de los ataques exitosos

4. **Imparta la formación oportuna** para fomentar la concienciación sobre la seguridad y promover la presentación de informes por parte de los usuarios

5. **Simule ataques de phishing** para identificar las vulnerabilidades en su programa

Mejores prácticas: controles de seguridad

"Errar es humano" suena cierto cuando los empleados son víctimas del phishing, una vulnerabilidad que se ve agravada por campañas de phishing impulsadas por IA (casi humanas). Por eso es imperativo que los profesionales de la seguridad implementen medidas de seguridad para identificar y minimizar daños potenciales, con un énfasis cada vez mayor en herramientas y capacidades de seguridad basadas en IA/ML.

Los elementos esenciales de protección contra ataques de phishing incluyen:

- **Análisis de correo electrónico:** las soluciones de filtrado que analizan los correos electrónicos entrantes en busca de contenido, archivos adjuntos y enlaces sospechosos son esenciales, ya que el correo electrónico sigue siendo un vector principal para este tipo de ataques. Un servicio de análisis de correo electrónico basado en la nube es crucial, ya que verifica los correos electrónicos en tiempo real antes de que lleguen a un sistema para protegerlo contra enlaces maliciosos y suplantación de nombres de dominio.
- **Concienciación y presentación de informes:** considere integrar un botón de "reportar phishing" directamente en los clientes de correo electrónico, permitiendo con ello a los usuarios informar de correos electrónicos sospechosos. Establezca un manual integral para investigar y abordar incidentes de phishing, incluida la presentación de informes a las autoridades pertinentes para combatir a los estafadores y prevenir ataques a otras organizaciones.
- **Autenticación multifactor (MFA):** MFA representa una defensa crucial contra el phishing, ya que requiere algo más que una contraseña para comprometer una cuenta. Sin embargo, la MFA no es una solución infalible. Los casos en los que los atacantes atacan a los usuarios de MFA a través de SMS y phishing de voz subrayan las vulnerabilidades inherentes a las medidas de seguridad de MFA.
- **Inspección de tráfico cifrado:** según otro informe de ThreatLabz, casi el 86 % de los ataques utilizan canales cifrados en varias etapas de la cadena de ataque, incluidas fases iniciales como el phishing. El phishing cifrado aumentó casi un 14 % interanual en 2023, probablemente instigado por herramientas de inteligencia artificial y ofertas plug-and-play (phishing como servicio). Las organizaciones deben inspeccionar todo el tráfico, cifrado o no, para frustrar las técnicas de phishing.
- **Software antivirus:** asegúrese de que los terminales estén protegidos actualizando constantemente el software antivirus para detectar y bloquear archivos maliciosos, evitando su descarga.
- **Protección avanzada contra amenazas:** mejore sus defensas contra variantes de malware nuevas y desconocidas que pueden eludir las herramientas de detección basadas en firmas con un entorno limitado en línea impulsado por IA que aísla y analiza archivos sospechosos. Además, implemente un aislamiento del navegador que cree una sesión de navegador aislada para contenido web potencialmente malicioso, brindando a los usuarios acceso a una representación segura y manteniendo a raya el código malicioso.
- **Filtrado de URL:** utilice controles basados en políticas para gestionar el acceso a categorías de contenido web de alto riesgo, incluidos los dominios recién registrados. Este enfoque proactivo del filtrado de URL ayuda a reducir la probabilidad de que los usuarios encuentren sitios web potencialmente maliciosos y mejora la postura general de seguridad.
- **Revisiones periódicas:** para minimizar las vulnerabilidades y mantener las protecciones más recientes, es esencial actualizar periódicamente las aplicaciones, los sistemas operativos y las herramientas de seguridad con las revisiones más recientes. Mantenerse actualizado con estas actualizaciones reducirá efectivamente las posibles vulnerabilidades y mejorará la seguridad de sus sistemas.
- **Arquitectura de confianza cero:** establecer medidas preventivas contra los ataques de phishing es clave, pero es igualmente vital implementar una arquitectura de confianza cero que reduzca la superficie de ataque, evite el movimiento lateral y reduzca el riesgo de una infracción. Emplee una segmentación granular para compartimentar su red, aplique el acceso con privilegios mínimos para restringir los permisos de los usuarios y mantenga una supervisión continua del tráfico. Estas medidas proactivas le permitirán identificar y responder a los atacantes, minimizando posibles daños e impactos.
- **Fuentes de información sobre amenazas:** integre fuentes de inteligencia sobre amenazas que supervisen continuamente las amenazas de phishing con sus herramientas de seguridad actuales para mejorar las capacidades de detección y acelerar la resolución de las amenazas. Manténgase actualizado con el contexto más reciente sobre URL reportadas, indicadores de compromiso extraídos (IOC) y tácticas, técnicas y procedimientos (TTP) para facilitar la toma de decisiones y la priorización.

Mejores prácticas: cómo detectar y prevenir ataques de vishing

¿QUÉ ES EL VISHING?

El phishing por voz, conocido como vishing, implica engañar a las víctimas mediante llamadas telefónicas y mensajes de voz, a menudo utilizando voces familiares o autorizadas para ganarse la confianza y extraer información confidencial.

El vishing se ha convertido en una importante preocupación de seguridad durante el año pasado, impulsado en gran parte por el aumento de campañas de vishing dirigidas realizadas por el notorio grupo de amenazas Scattered Spider. Por ejemplo, los ciberataques a la industria del juego que ocurrieron entre agosto y octubre de 2023 emplearon tácticas de vishing haciéndose pasar por un usuario privilegiado. El grupo obtuvo acceso no autorizado y un punto de apoyo inicial dentro del sistema.

Este incidente resalta la urgencia de contar con defensas sólidas contra el phishing y la importancia de la capacitación y concientización de los empleados sobre el vishing. Educar a los usuarios sobre la naturaleza engañosa del vishing y brindarles herramientas para identificar e informar de cualquier intento de ataque es crucial para construir una defensa segura. Al mismo tiempo, es imperativo implementar medidas de seguridad fundamentales, como MFA, protocolos de comunicación seguros y políticas de seguridad actualizadas periódicamente, para garantizar la seguridad y la integridad de los canales de comunicación y la información confidencial contra el vishing.

Vishing 2.0: los algoritmos de IA/ML y la tecnología de suplantación de identidad están facilitando que los atacantes manipulen voces y personalicen sus tácticas de ingeniería social, lo que a su vez hace que los ataques de vishing sean más sofisticados y efectivos.

Entender los ataques de vishing

Los ataques de vishing emplean varias técnicas para manipular y engañar a los objetivos, entre ellas:

Manipulación de voz e ingeniería social

Los atacantes utilizan herramientas avanzadas de manipulación de audio para alterar el timbre, el tono y otras características vocales, y emular entidades confiables. Al mismo tiempo, utilizan tácticas de ingeniería social para explotar desencadenantes psicológicos y emocionales, creando narrativas convincentes que incitan a sus objetivos a revelar información confidencial o realizar acciones específicas.

Identificador de llamadas y números falsos

Los atacantes manipulan el identificador de llamadas y el número de teléfono que se muestran en el dispositivo del destinatario para que parezca que la llamada proviene de una fuente familiar o confiable. Utilizando técnicas avanzadas, pueden imitar entidades legítimas como bancos, agencias gubernamentales o contactos conocidos, aumentando la probabilidad de que el destinatario responda la llamada y se convierta en víctima de posteriores intentos de ingeniería social.

Suplantación de usuarios privilegiados o personal directivo de la empresa

Los atacantes se hacen pasar estratégicamente por personas que desempeñan funciones importantes en una empresa o tienen acceso administrativo. Al asumir las identidades de directores ejecutivos, altos ejecutivos o personal con acceso privilegiado al sistema, los atacantes explotan la autoridad inherente de estos puestos. Esta forma sofisticada de ingeniería social está diseñada para engañar a los empleados a fin de que revelen información corporativa confidencial, proporcionen credenciales de acceso o realicen acciones que comprometan la seguridad de la organización.

Escenarios comunes de vishing

Una persona que llama se hace pasar por un uso privilegiado

Un atacante obtiene información personal sobre un usuario privilegiado y la utiliza para hacerse pasar por él Luego se comunican con el servicio de atención al cliente y solicitan un reinicio de MFA. Si la persona del servicio al cliente confía en la persona que llama y restablece los detalles de MFA del usuario, deja la puerta abierta para apropiaciones de cuentas e infracciones de datos. La Figura 17 muestra una forma en que podría desarrollarse este escenario.

Solicitudes urgentes o en las que el factor tiempo es determinante

Un atacante se hace pasar por una fuente confiable y presiona a la víctima para que actúe de inmediato afirmando que hay un problema urgente, a menudo una amenaza a la seguridad o una oportunidad urgente. La urgencia se enfatiza con amenazas de consecuencias por incumplimiento, como suspensión de cuenta, acciones legales o incluso la implicación (incluso afirmando abiertamente) que el trabajo de la víctima podría estar en peligro si no cumple con la solicitud de la persona que llama inmediatamente.

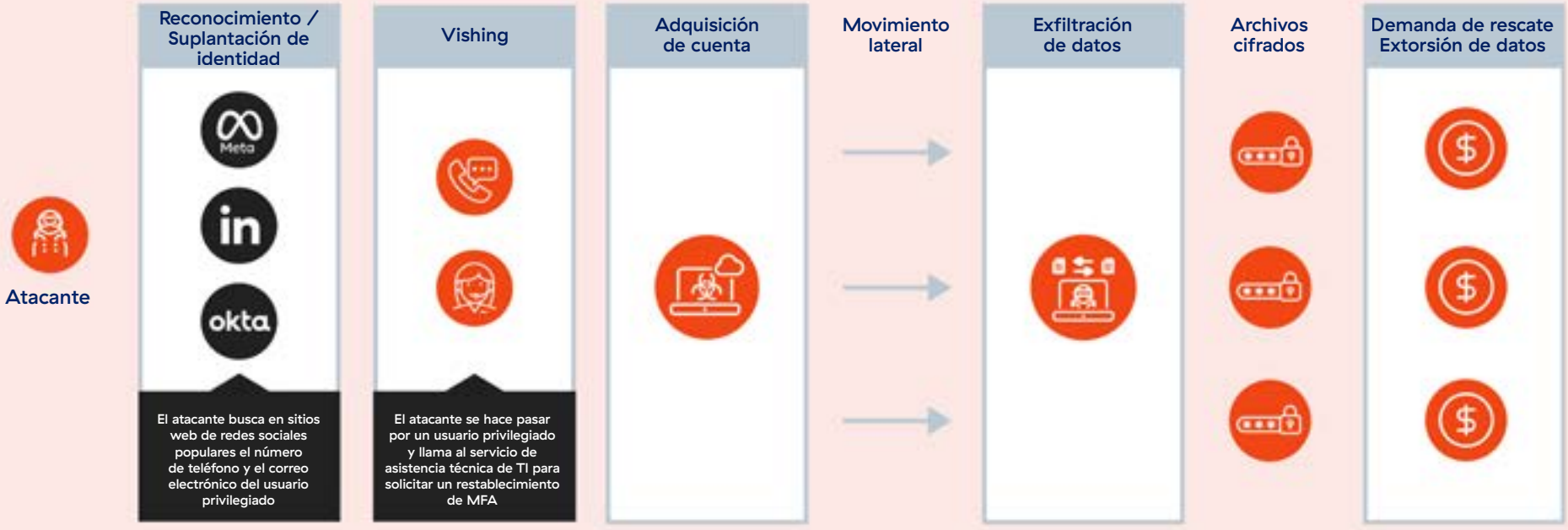


Figura 17: Un ejemplo de secuencia de ataque de vishing

Alertas a tener en cuenta

- **Llamadas inesperadas o no solicitadas:** tenga cuidado con las llamadas inesperadas, especialmente de números o entidades desconocidos.
- **Tácticas de presión y urgencia:** manténgase alerta a las personas que llaman que utilizan tácticas de presión o crean una sensación de urgencia. Las entidades legítimas suelen dar tiempo para su consideración, mientras que las solicitudes urgentes y coercitivas pueden indicar un intento de vishing.
- **Solicitudes de información confidencial:** tenga cuidado si las personas que llaman solicitan acciones críticas como MFA o restablecimiento de cuenta, o si solicitan información confidencial como contraseñas, información de pago o datos personales. Las organizaciones legítimas normalmente evitan solicitar dicha información por teléfono.
- **Irregularidades en el identificador de llamadas:** examine los detalles del identificador de llamadas en busca de irregularidades, como números inesperados o discrepancias en la supuesta organización. Las llamadas legítimas suelen tener información de identificación de llamadas consistente y verificable.

Mejores prácticas y medidas de seguridad para prevenir ataques de vishing

- **Forme y capacite a los empleados con regularidad:** identifique las lagunas de conocimiento en su organización y luego implemente programas de capacitación en ciberseguridad personalizados y específicos para capacitar e informar a los empleados con el fin de que reconozcan y respondan a las amenazas de manera efectiva.
- **Utilice herramientas de filtrado y bloqueo de llamadas:** emplee herramientas que bloqueen o filtren las llamadas entrantes para descartar posibles intentos de vishing. Estas tecnologías ayudan a identificar y evitar que llamadas sospechosas lleguen a los teléfonos de los usuarios finales.
- **Implemente autenticación multifactor:** implemente MFA como medida de seguridad obligatoria. Esto agrega una capa adicional de protección al requerir una verificación adicional más allá de una simple llamada telefónica, lo que dificulta que los atacantes obtengan acceso no autorizado.
- **Actualice y parchee periódicamente el software y los sistemas:** garantice la seguridad de los sistemas telefónicos manteniéndolos al día con actualizaciones y revisiones, abordando vulnerabilidades y reforzando las defensas contra la evolución de las técnicas de vishing.
- **Establezca protocolos claros de respuesta a incidentes:** inste a los usuarios a informar rápidamente de las llamadas sospechosas para abordar y mitigar de manera eficiente las posibles amenazas. Colabore con las agencias reguladoras y policiales para mejorar el esfuerzo colectivo en la lucha contra las actividades de vishing.

Lista de verificación de Vishing 101 para usuarios finales y empresas

- [ ] **Tenga cuidado:** tenga cuidado cuando reciba llamadas telefónicas inesperadas, especialmente si la voz le suena familiar o autoritaria. Recuerde, no siempre se puede confiar en una voz sólo porque le resulte familiar.
- [ ] **Verifique y autentique:** en caso de duda, verifique siempre la identidad de la persona que llama antes de compartir información confidencial. Utilice datos de contacto establecidos de directorios internos o comuníquese de forma independiente con contactos conocidos para confirmar la legitimidad de la llamada. Verifique la identidad de la persona que llama solicitando un número de devolución de llamada o cotejándola con los datos de contacto oficiales.
- [ ] **Devuelva siempre la llamada:** si recibe una llamada sospechosa, incluso de alguien que dice ser un colega o gerente, siempre devuelva la llamada utilizando información de contacto conocida de un directorio interno. Esto garantiza que está hablando con la persona prevista y no con un impostor.
- [ ] **Tenga cuidado con las solicitudes de LinkedIn:** tenga discreción y extrema precaución al aceptar solicitudes de conexión de LinkedIn, especialmente de personas desconocidas. Absténgase de hacer clic en enlaces o archivos adjuntos, o de compartir información confidencial o de la empresa a través de mensajes directos o correos electrónicos de LinkedIn. Los atacantes pueden hacerse pasar por empresas que ofrecen el puesto de trabajo de sus sueños, envían un documento a través de WhatsApp u otro canal, y le piden que abra el documento en su sistema.
- [ ] **Nunca revele códigos de contraseña de un solo uso (OTP) de MFA:** uno de los pasos más importantes para mantener la seguridad de su cuenta es nunca compartir ni proporcionar códigos MFA u OTP a nadie por teléfono o correo electrónico.

Mejores prácticas: cómo identificar una página de phishing

No son el último truco del libro para los atacantes, pero entre un arsenal de tácticas, las páginas web de phishing destacan como un medio de explotación particularmente engañoso, especialmente en la era de la IA. El auge de la IA generativa y los LLM (y sus variantes maliciosas), junto con los kits de phishing fácilmente disponibles, ha introducido una nueva dimensión en la sofisticación y eficacia de las páginas de phishing.

Con algoritmos basados en IA, los atacantes ahora pueden crear réplicas muy convincentes de sitios web legítimos con una velocidad y precisión sin precedentes. La IA también brinda a los atacantes la capacidad de adaptar el contenido de la página a objetivos individuales, lo que aumenta aún más la probabilidad de incitar a las víctimas a compartir información confidencial o interactuar con contenido web malicioso.

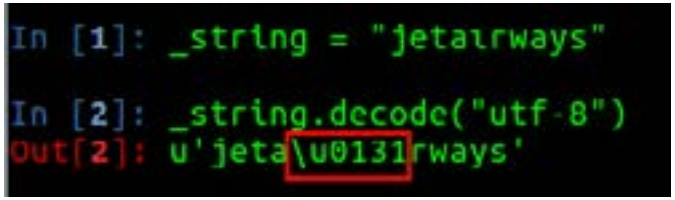
Comprender la anatomía de una página de phishing se ha vuelto aún más crítico para defenderse de este tipo de ataques. A continuación se muestran algunos indicadores clave a tener en cuenta al identificar una página de phishing:

- **Páginas basadas en imágenes:** tenga cuidado con las páginas web que se basan exclusivamente en una sola imagen. Los atacantes suelen utilizar esta técnica para imitar sitios web legítimos. Si la página parece demasiado simplista con solo una imagen y un formulario para recopilar sus credenciales, podría indicar un intento de phishing.
- **Falta el título de página:** los sitios web legítimos suelen tener títulos descriptivos que aparecen en la pestaña de su navegador. Las páginas de phishing pueden omitir este detalle por completo, lo que dificulta identificar el propósito o el origen de la página. En las siguientes imágenes, tanto al HTML sin formato como a la página de inicio de sesión falsa de Microsoft les falta un título.

- **Anclajes vacíos para enlaces críticos:** las páginas de phishing suelen utilizar anclajes vacíos para enlaces esenciales, como Ayuda o Preguntas frecuentes, al copiar contenido de sitios legítimos. Si nota que faltan enlaces o que están incompletos, proceda con precaución.

- **Certificados autofirmados:** preste atención al certificado de seguridad del sitio web, ya que las páginas de phishing suelen utilizar certificados autofirmados, que carecen de validación de autoridades certificadoras confiables. Busque certificados válidos y confiables para garantizar una conexión segura.
- **Apariencia del correo web genérico:** tenga cuidado con las páginas que se parecen a clientes de correo web genéricos como Webmail o Zimbra. Los autores de phishing suelen utilizar estas réplicas para engañar a los usuarios a fin de que revelen sus credenciales. Examine la página cuidadosamente para detectar inconsistencias o signos de manipulación.
- **Múltiples redirecciones:** tenga cuidado con las páginas que redireccionan varias veces antes de aparecer en un mensaje de inicio de sesión, ya que esta táctica se usa comúnmente para ocultar intenciones maliciosas y evadir la detección. Tenga cuidado al encontrar redireccionamientos excesivos, ya que pueden indicar un intento de phishing en curso.
- **Contrabando de HTML:** tenga cuidado con el contrabando de HTML, un método mediante el cual los atacantes ocultan JavaScript malicioso codificado en archivos adjuntos de correo electrónico. Este JavaScript malicioso descarga además cargas útiles maliciosas en la máquina víctima. Los atacantes engañan a las víctimas para que hagan clic en los enlaces/abran los archivos adjuntos en el correo electrónico de phishing con el objetivo de desencadenar esta descarga maliciosa. Este comportamiento es muy sospechoso y debe tratarse con extrema precaución.

- **Etiquetas ofuscadas:** las páginas de phishing pueden ofuscar campos como título, derechos de autor y otros. Busque inconsistencias o formatos inusuales en estas áreas, ya que podrían indicar intentos de ocultar actividad maliciosa.
- **Uso de homoglifos:** las páginas de phishing pueden reemplazar caracteres clave con "homoglifos" (caracteres que se parecen a otros caracteres), como se ve a continuación. Los atacantes suelen aprovechar estas diferencias sutiles para engañar a los usuarios y evadir la detección.



Aplicaciones 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 a fin de robar datos. Conocer las herramientas y técnicas populares puede ayudar a los usuarios a tomar decisiones informadas cuando navegan por el mundo digital. 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

Lista de verificación de páginas de phishing para usuarios finales y empresas

- [ ] **Verifique la fuente:** antes de introducir cualquier información personal, verifique la URL del sitio web para detectar errores ortográficos o caracteres adicionales. Preste mucha atención al nombre de dominio, ya que es aquí donde los atacantes suelen cometer errores.
- [ ] **Verifique conexiones seguras con cifrado:** los sitios web legítimos utilizan cifrado HTTPS para proteger sus datos durante la transmisión. Busque el icono del candado en la barra de direcciones para garantizar una conexión segura. Tenga cuidado con los sitios web que sólo utilizan HTTP, ya que es posible que no protejan adecuadamente su información.
- [ ] **Revise el contenido:** las páginas de phishing pueden contener errores gramaticales, inconsistencias y formatos inusuales. Las organizaciones legítimas suelen tener sitios web de apariencia profesional con contenido refinado; sin embargo, la IA ha permitido a los ciberdelincuentes crear páginas de phishing más convincentes. Si algo parece extraño o demasiado bueno para ser verdad, confíe en su instinto y proceda con precaución.
- [ ] **Manténgase informado:** las tácticas de phishing evolucionan constantemente, por lo que es esencial mantenerse informado sobre las últimas amenazas y estafas. Esté atento a los avisos de seguridad, informes y actualizaciones de noticias de fuentes confiables para protegerse de la evolución de los planes de páginas web de phishing.

Metodología de investigación de ThreatLabz

La nube de seguridad global de Zscaler procesa más de 500 billones de señales diarias, bloquea más de 9 mil millones de amenazas e infracciones de políticas por día y ofrece más de 250 000 actualizaciones de seguridad diarias a los clientes de Zscaler.

Para este informe, Zscaler ThreatLabz analizó 2 mil millones de transacciones de phishing bloqueadas entre enero y diciembre de 2023, explorando varios aspectos, incluidos los principales ataques de phishing, los países objetivo, los países donde se aloja el contenido de phishing, la distribución de tipos de empresas según las direcciones IP del servidor y los principales referentes vinculados a estos ataques de phishing. Además, ThreatLabz rastreó y examinó tendencias de phishing y casos de uso notables observados a lo largo de 2023.

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 satisfacen los estándares de cumplimiento de seguridad. ThreatLabZ publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal research.zscaler.com.

Acerca de Zscaler

Zscaler 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 mediante la conexión segura de los 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. Si desea más información, visite www.zscaler.es.

Experimente su mundo, protegido.

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 mediante la conexión segura de los 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. Si desea más información, visite www.zscaler.es.

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