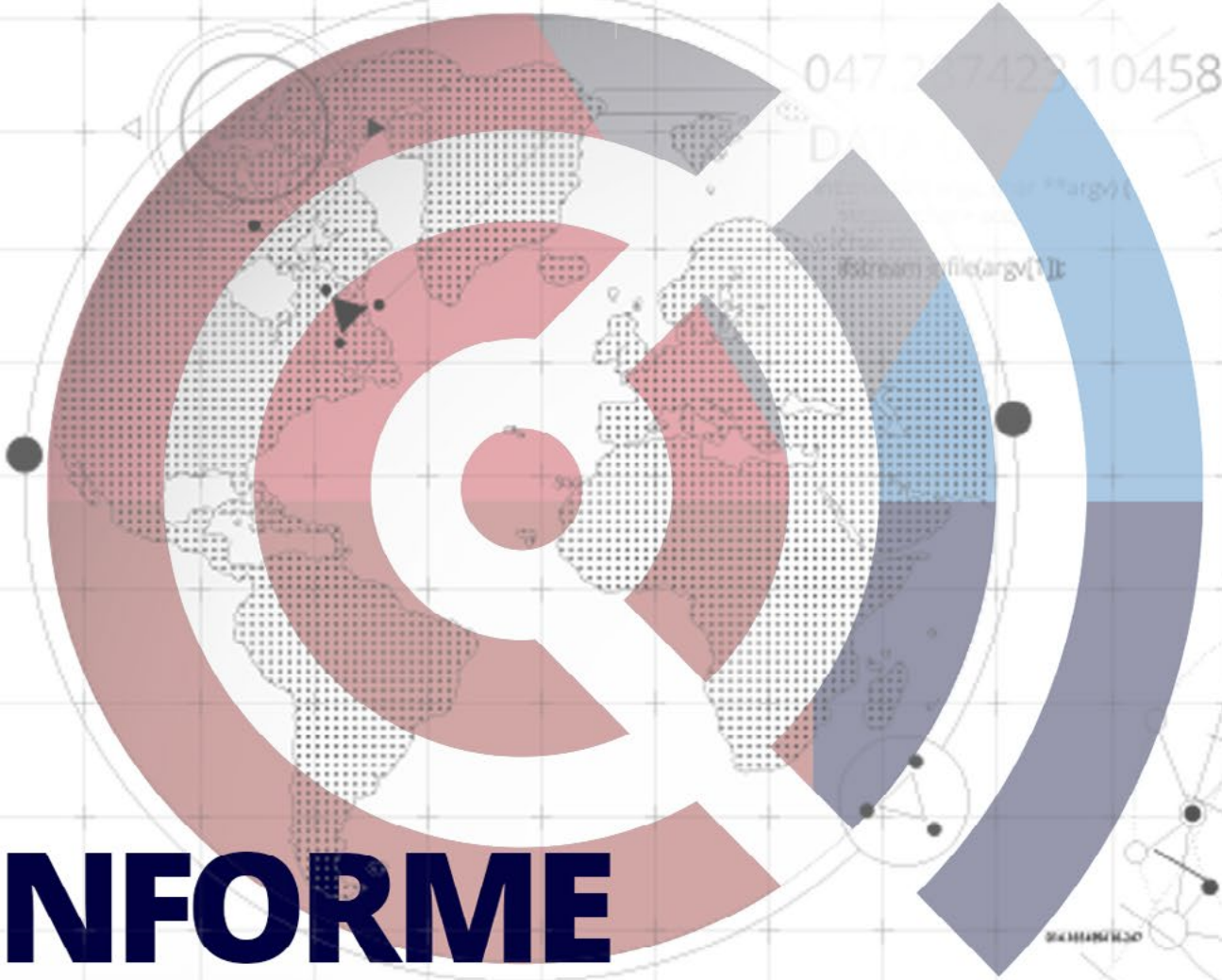
mimecast

RISK RADAR

DETECTION | ANALYSIS | ACTION



INFORME GLOBAL DE INTELIGENCIA SOBRE AMENAZAS

DE JULIO A DICIEMBRE DE 2024

INHALT.

INTRODUCCIÓN

Disponer de información fiable sobre amenazas se ha vuelto esencial para que empresas y organizaciones puedan hacer frente a la creciente sofisticación de los atacantes. Las organizaciones de todos los tamaños deben informarse sobre las últimas tendencias, hacer un seguimiento de las amenazas que afectan a su sector y a sus proveedores, y reforzar sus defensas y actualizar sus procesos para evitar que sus comunicaciones empresariales y sus empleados se utilicen en su contra.

En la segunda mitad de 2024, Mimecast procesó más de 90 000 millones de puntos de datos para sus casi 43 000 clientes, identificando más de 5000l millones de amenazas durante un período de seis meses. El número total de interacciones protegidas superó ampliamente esa cifra. El correo electrónico y las herramientas de colaboración continúan siendo los principales canales a través de los cuales la mayoría de los atacantes inician sus intentos de comprometer a las organizaciones objetivo, lo que permite a Mimecast detectar y analizar muchas amenazas antes de que se hagan de dominio público.

En la segunda mitad de 2024, Mimecast procesó más de 90 000 millones de puntos de datos para sus casi 43 000 clientes, identificando más de 5000l millones de amenazas durante un período de seis meses.

En nuestro Informe global de inteligencia sobre amenazas del segundo semestre de 2024, Mimecast ha recopilado datos de nuestros sistemas que protegen a decenas de millones de usuarios, ha aportado información de nuestros analistas de inteligencia y ha incorporado inteligencia de fuentes abiertas sobre las amenazas más recientes. El informe incluye un análisis de la actividad de amenazas, estadísticas que revelan tendencias de ataque y una serie de recomendaciones para que las pequeñas y grandes empresas protejan a sus empleados y mitiguen el impacto de los usuarios de riesgo.

Le invitamos a explorar nuestro informe de inteligencia sobre amenazas del segundo semestre de 2024 y esperamos seguir compartiendo información en el futuro.

RESUMEN EJECUTIVO

EN LA SEGUNDA MITAD DE 2024, LOS ACTORES DE AMENAZAS UTILIZARON CON MAYOR FRECUENCIA SERVICIOS LEGÍTIMOS PARA DISFRAZAR SUS ATAQUES E INTENTAR SORTEAR LAS DEFENSAS.

La tendencia conocida como LOTS (Living Off Trusted Services), es decir, el uso de servicios legítimos para actividades maliciosas, obliga a las empresas a ir más allá de la reputación y la autenticación para protegerse de ataques a través de mensajes y estrategias de ingeniería social. Además, los ciberdelincuentes están utilizando proveedores externos, tanto de servicios como de software, para infiltrarse más fácilmente en una red específica.

02

LA GEOPOLÍTICA HA PROPORCIONADO A LOS ACTORES DE AMENAZAS TANTO EL INCENTIVO PARA MULTIPLICAR LOS INTENTOS DE VIOLACIÓN COMO UN TERRENO FÉRTIL DE CONTENIDO PARA DISEÑAR SUS ATAQUES.

Los actores estatales continuaron recurriendo a ciberataques y ciberespionaje para ejecutar acciones encubiertas contra sus rivales. China comprometió la infraestructura de EE. UU. y Canadá[1], Irán e Israel atacaron sus respectivas infraestructuras[2] y Rusia continuó atacando a organizaciones europeas y estadounidenses[3] tras el estancamiento de su invasión de Ucrania.

1. Tunney, Catharine. " China ataca las redes del gobierno canadiense y se hace con información de gran valor, según la inteligencia canadiense ". CBC. 30 de octubre de 2024. https://www.cbc.ca/news/politics/cse-cyber-threats-china-1.7367719.
2. Lemos, Robert. "A medida que aumentan las tensiones geopolíticas, crecen las operaciones cibernéticas de Irán". Dark Reading. Artículo de noticias. 18 de septiembre de 2024. https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow.
3. Eddy, Nathan. "Las batallas cibernéticas entre Ucrania y Rusia se trasladan al mundo real". Dark Reading. Artículo de noticias. 3 de octubre de 2024.

LAS TECNOLOGÍAS DE INTELIGENCIA ARTIFICIAL (IA) SIGUEN OFRECIENDO BENEFICIOS ÚNICOS TANTO A DEFENSORES COMO A ATACANTES.

Los analistas de ciberseguridad pueden evaluar con mayor rapidez posibles incidentes de seguridad con la ayuda de asistentes de IA, mientras que los equipos de respuesta a incidentes pueden usar la IA para bloquear y corregir un ataque de forma más rápida y eficaz. Los atacantes también sacan provecho: una investigación de Mimecast[4],basada en el análisis lingüístico, desveló que alrededor del 12 % de los correos electrónicos —incluidos los ataques de phishing— presentaban indicios de haber sido redactados mediante grandes modelos de lenguaje (LLM). Los deepfakes de audio y vídeo se han utilizado con éxito para suplantara directores ejecutivos y conseguir que empleados confiados realicen pagos fraudulentos a cuentas de ciberdelincuentes.

TODAS ESTAS TENDENCIAS CONTINUARÁN EN 2025.

Los ataques que hicieron uso de la nube, en mayor o menor medida, se dispararon en 2024, mientras la geopolítica sigue volviéndose más inestable: Francia y Alemania afrontan elecciones en Europa, Donald Trump asume un segundo mandato no consecutivo en EE. UU., y Rusia y China continúa exhibiendo su poder militar ante el mundo. Los investigadores de seguridad y los atacantes continúan desarrollando nuevas formas de explotar los sistemas de IA, ya sea detectando vulnerabilidades o perfeccionando sus estrategias de ataque.

4. Lee, Evonne. “Nueva inteligencia de amenazas de Mimecast: cómo ChatGPT revolucionó el correo electrónico”. Blog de inteligencia de amenazas de Mimecast. 30 de septiembre de 2024. https://www.mimecast.com/blog/how-chatgpt-upended-email/.

PRINCIPALES HALLAZGOS

Aunque la actividad de los actores de amenazas ha aumentado en casi todos los indicadores, algunas tendencias destacan sobre las demás.

K-1 UNO

LOS ATACANTES RECURREN CADA VEZ MÁS DE LOS SERVICIOS DE CONFIANZA (LOTS).

Los servicios en la nube de Microsoft, Google y Evernote suelen alojar las cargas útiles y páginas de destino de los ciberdelincuentes. Sin embargo, otros servicios en la nube se utilizan con frecuencia para componentes específicos de la infraestructura de ataque: los CAPTCHA Turnstyle de Cloudflare se utilizan con frecuencia para impedir el análisis de amenazas; DocuSign, TeamViewer y Wave Compliance alojan inadvertidamente el contenido de los atacantes; y Gmail de Google y Microsoft Outlook (antes Hotmail) se utilizan para enviar ataques de phishing.

03

PULPO

ESPECIES

Maestros del **análisis** con un sistema nervioso altamente desarrollado y un cerebro grande. Sobresalen en adaptarse a su entorno y superar desafíos, lo que les hace destacar en la inteligencia de amenazas.

K-2 DOS

LA SITUACIÓN GEOPOLÍTICA AUMENTA LA PROBABILIDAD DE CIBERATAQUES.

Las elecciones francesas y alemanas y la continua incertidumbre de la guerra entre Rusia y Ucrania elevarán la tensión de la política de la Unión Europea. El alejamiento del gobierno estadounidense de las normas establecidas también podría dar lugar a una mayor actividad en el ámbito cibernético. Expertos en negocios, política y ciberseguridad advierten cada vez con más frecuencia de que las tensiones geopolíticas y los riesgos de ciberseguridad están interrelacionados.
Los dos principales riesgos identificados para 2025 en la encuesta anual del barómetro de riesgos sistémicos, realizada por la Depository Trust and Clearing Corporation, fueron los asociados a la geopolítica y a la ciberseguridad.[5]

K-3 TRES

LAS TECNOLOGÍAS DE AUTENTICACIÓN DEL CORREO ELECTRÓNICO HAN INCREMENTADO LAS DIFICULTADES PARA LOS ATACANTES, MIENTRAS QUE LA IA HA ALLANADO EL CAMINO PARA LA CIBERDELINCUENCIA.

Al utilizar servicios de confianza, los atacantes logran cumplir con los estrictos requisitos de autenticación de tecnologías de correo electrónico como SPF, DKIM y DMARC, y hacerse pasar por fuentes fiables. Aunque las tecnologías complican sus ataques, los atacantes siguen encontrando servicios que les permiten sortear las verificaciones de autenticación y homologación. Además, la proliferación de bots de chat con IA permite incluso a los aspirantes a ciberdelincuentes adquirir las habilidades necesarias para hackear.

5."Los riesgos geopolíticos y de ciberseguridad siguen siendo las principales amenazas para el sector de los servicios financieros en 2025". DTCC. 4 de diciembre de 2024. https://www.dtcc.com/news/2024/december/04/geopolitical-and-cyber-risks-remain-top-threats-to-the-financial-services-sector-in-2025.

K-4 CUATRO

LOS SECTORES DE MEDIOS DE COMUNICACIÓN Y PUBLICACIONES, ARTES, OCIO Y Y SERVICIOS LEGALES REGISTRARON LA MAYOR CANTIDAD DE AMENAZAS POR USUARIO EN EL SEGUNDO SEMESTRE DE 2024.

La mayoría de los sectores presentaron un perfil de amenazas característico, incluyendo una mayor proporción de archivos maliciosos dirigidos a los sectores de las Artes, Ocio y Entretenimiento, mientras que los trabajadores del sector de Medios de comunicación y Publicaciones registraron un mayor número de enlaces maliciosos. Los ataques de suplantación de identidad fueron los más comunes en el sector de software y SaaS.

K-5 CINCO

LAS PERSONAS CONTINÚAN SIENDO EL PRINCIPAL PUNTO DÉBIL EN LA MAYORÍA DE LOS INCIDENTES.

La mayoría de las brechas de seguridad se producen porque un usuarios interno realiza una acción que permite a los atacantes acceder a recursos sensibles o protegidos. La versión 2024 del informe anual sobre investigaciones de fugas de datos (DBIR, Data Breach Investigations Report) desveló que más de dos tercios (68 %) de los incidentes que ocurrieron en 2023[6] tenían "un elemento humano no malicioso". Una encuesta de 2024 realizada entre 1000 empleados reveló que un tercio (34 %) temía ser el eslabón débil aprovechado por los atacantes, a pesar de que la gran mayoría (86 %) se consideraba conocedora de la ciberseguridad[7]. Más de la mitad de los encuestados teme perder su trabajo si expone su organización a un ciberataque.

6. Data Breach Investigations Report 2024, Verizonhttps://www.verizon.com/business/resources/reports/dbir/#takeaways
7. Por qué la IA aumenta la preocupación por la ciberseguridad, en particular entre los empleados más jóvenes https://www.ey.com/en_us/consulting/human-risk-in-cybersecurity

04

EL PANORAMA DE AMENAZAS

MURCIÉLAGO

ESPECIES

Detectar amenazas es su especialidad. Mediante la ecolocalización, emiten sonidos de alta frecuencia que rebotan en los objetos, proporcionándoles un mapa detallado de su entorno. Esto les ayuda a evitar obstáculos, incluso en la oscuridad total.

04.1

REPRESENTACIÓN GRÁFICA DEL PANORAMA

El panorama de amenazas en la segunda mitad de 2024 experimentó un notable cambio caracterizado por un uso creciente de servicios en la nube, tanto para consumidores como para empresas, como método para evitar la detección. Esta tendencia ha llevado a la proliferación de contenido malicioso en plataformas cloud populares y al creciente uso de enlaces como vector de distribución de malware.

En la segunda mitad de 2024, se observó un viraje de los atacantes hacia los sectores de Artes, Ocio y Entretenimiento, Servicios legales y Software y SaaS. Este cambio contrasta con la primera mitad del año, cuando los sectores de la Banca, Viajes y Hostelería, y Artes y Entretenimiento fueron los principales objetivos. Aunque todos los sectores sufrieron un número importante de ataques masivos de correo electrónico provenientes de fuentes de baja reputación, los atacantes dirigieron más ataques con archivos maliciosos al sector de Artes y Entretenimiento, mientras que los Servicios Legales registraron más ataques de suplantación de identidad.

Siga leyendo para descubrir cómo el análisis de datos de Mimecast ilustra el panorama de amenazas.

W 41°24'12.2 "
E 23°44'54.4"
PE-3 Nvgt B

GRÁFICO — ABUSO DE SERVICIOS EN LA NUBE

01

Los atacantes están recurriendo cada vez más a servicios de confianza (LOTS, Living Off Trusted Services) en su afán por eludir las defensas que solo identifican los ataques mediante la detección de código, recursos y servicios en línea no fiables. Si bien algunas opciones para alojar la infraestructura de los atacantes son evidentes, como Google Docs, Evernote, y Dropbox DocSend, otros servicios en línea son menos conocidos, como el sitio de publicaciones interactivas Publuu, la plataforma seminarios web en línea Wave Compliance y el sitio de presentaciones de diapositivas Gamma.

Los atacantes también emplearon plataformas específicas para enviar correos electrónicos de phishing y distintos sitios para alojar la carga útil, que a menudo es simplemente un formulario web o un archivo con un enlace. El sitio de marketing integral GetResponse, por ejemplo, fue identificado como una fuente significativa de correos electrónicos de phishing; sin embargo, es importante destacar que muchos de estos correos pueden no ser maliciosos, sino simplemente no deseados. Aunque los sitios de Adobe no son los principales hosts de cargas útiles, los atacantes utilizan al menos dos de sus sitios para alojar las páginas de destino iniciales.

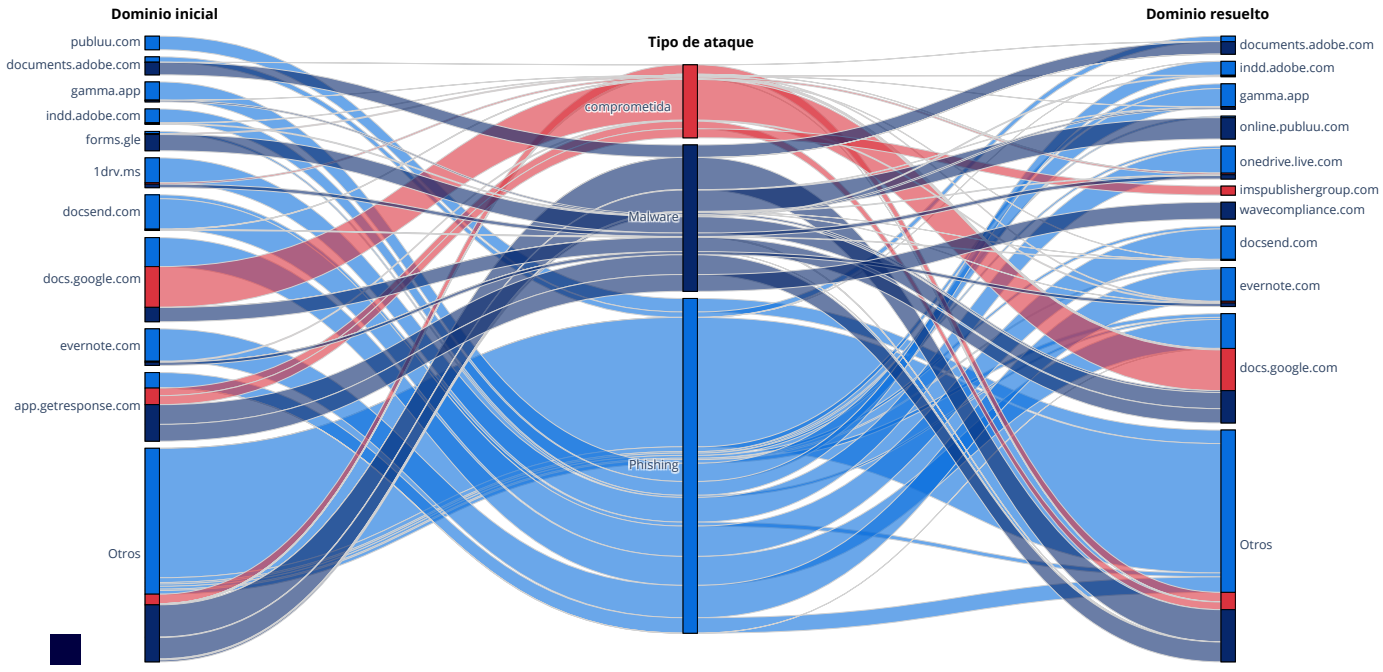


Gráfico 1: La mayoría de los dominios iniciales corresponden a dominios finales similares; por ejemplo, la mayoría de los ataques que utilizan Evernote inicialmente, también alojan ahí una carga útil. Sin embargo, hay varios casos destacados, donde una plataforma aloja la página de redireccionamiento inicial —como un gran volumen de spam procedente del servicio de marketing GetResponse.com— y una segunda plataforma aloja la página de destino, como el servicio de formación y seminarios web WaveCompliance.

GRÁFICO - TPU POR TIPO DE ATAQUE

#02

Aunque el spam sigue representando la gran mayoría de los mensajes bloqueados por Mimecast en el segundo semestre de 2024, en verano se produjo un aumento en los mensajes de correo electrónico no deseados. Aunque ese aumento disminuyó al final del año, los ataques de phishing, que suelen incluir una URL a un sitio o servicio controlado por un atacante, experimentaron un crecimiento lento durante el semestre.

Mimecast clasifica la actividad maliciosa y no deseada por la etapa en la que se detecta.

SPAM detecta correos masivos de dominios no fiables y aquellos que contienen contenido ampliamente difundido.

MENSAJES SOSPECHOSOS son aquellos que pueden ser mensajes, archivos o URL potencialmente maliciosos; es decir, no se ha detectado contenido malicioso, pero hay indicadores que demuestran que el mensaje debe tratarse con precaución, si proceden de un servicio habitualmente utilizado para fraudes o de una fuente poco fiable.

NO DESEADO incluye mensajes bloqueados por el usuario.

AMENAZAS DE PHISHING diseñadas para engañar a las víctimas para que revelen información sensible, como credenciales o información de pago. Esto incluye enlaces de phishing, estafas BEC, suplantación de identidad o archivos adjuntos HTML diseñados para hacerse pasar por páginas de inicio de sesión.

MENSAJES DE MALWARE incluyen archivos adjuntos detectados como maliciosos o enlaces que conducen a malware.

El aumento significativo del spam entre la primera y la segunda mitad de 2024 se debe a la evolución del sistema de detección y recopilación de datos de Mimecast, y no a una tendencia en el volumen de spam. El aumento en las detecciones de spam se debe a que Mimecast incorporó a los datos de detección el spam que estaba retenido por la puerta de enlace, que pueden configurarse a nivel administrativo, y no solo rechazos de alta confianza.

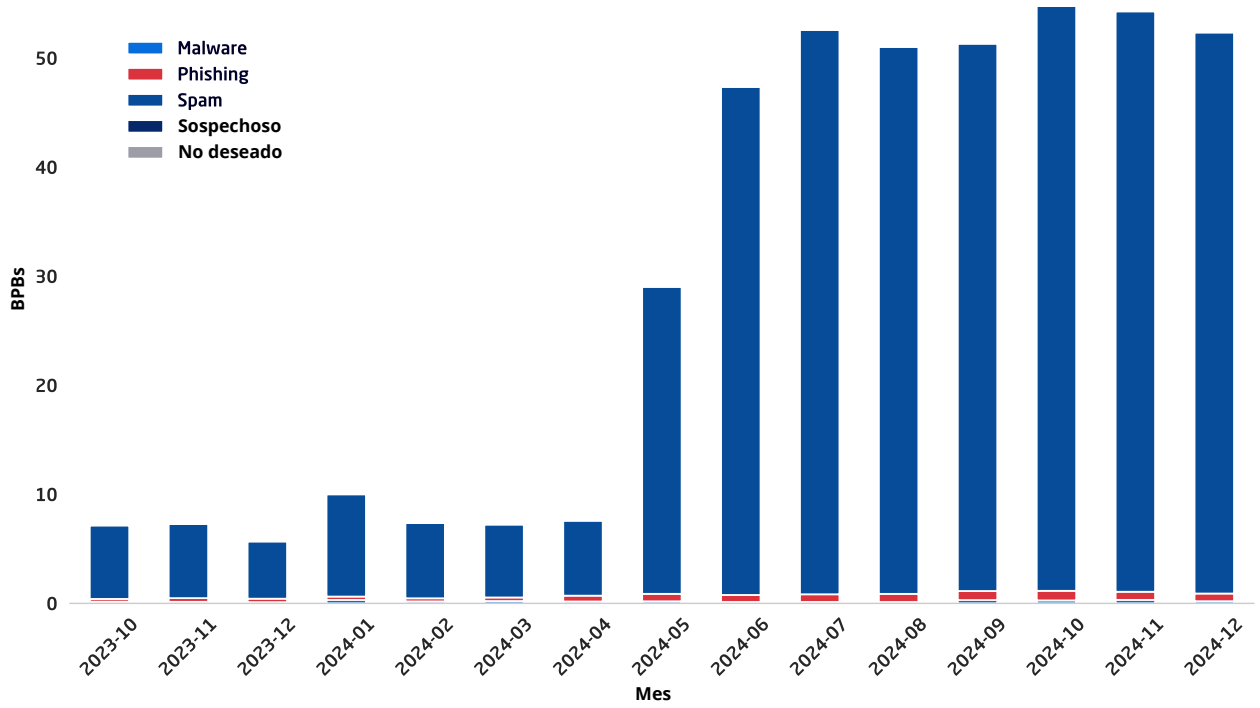


Gráfico 2a: El aumento significativo en las detecciones de spam se debe a la integración del spam retenido en la puerta de enlace, en lugar de limitarse únicamente a los rechazos de spam. Además, este cambio permite a los administradores configurar la gestión de los correos retenidos,

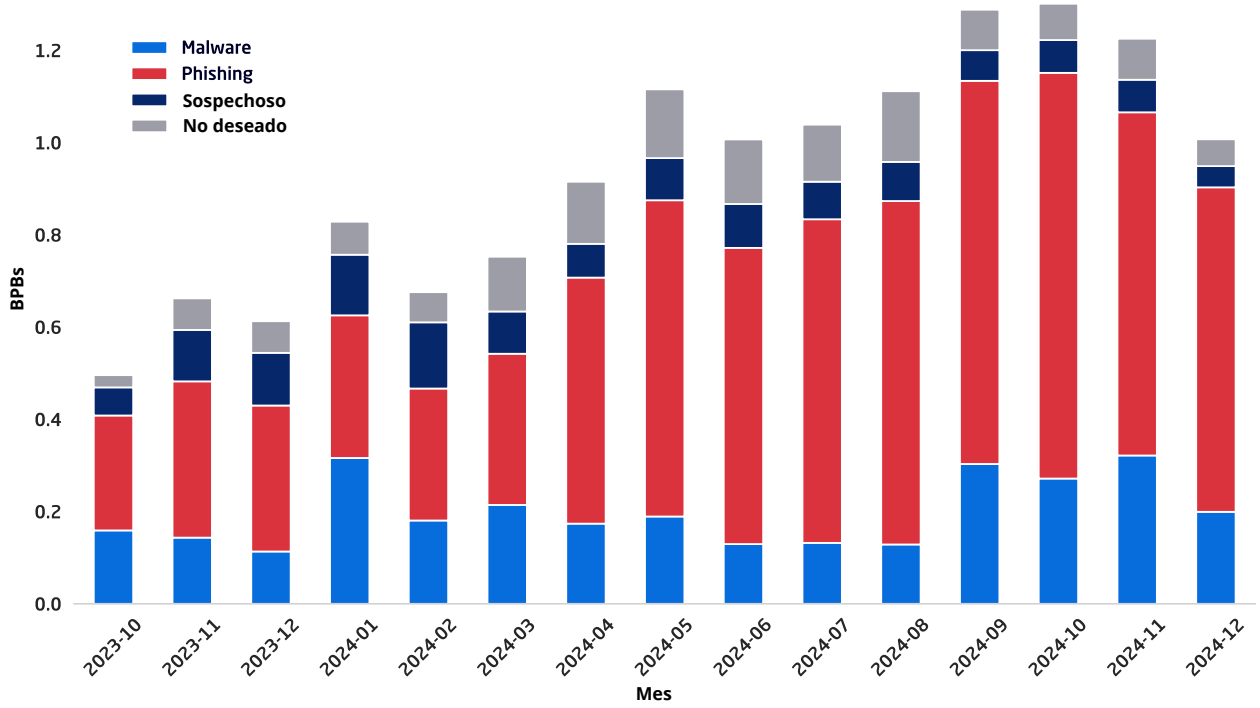


Gráfico 2b: Al eliminar la abrumadora influencia del conjunto de datos de spam, se observa que el phishing está en aumento y un repunte en los ataques de malware a finales de la segunda mitad de 2024. En diciembre de 2024, la detección de malware en el África subsahariana aumentó un 42,14 %, un incremento importante respecto al año anterior, impulsado por la inestabilidad política y el aumento de los ciberataques. Además, la región está presenciando un aumento de los ataques de ransomware, que se están volviendo más oportunistas, a menudo aprovechando vulnerabilidades y propagándose como infecciones secundarias, lo que indica una tendencia preocupante en el panorama de amenazas.

GRÁFICO — PRINCIPALES SECTORES OBJETIVO POR TPU

#03

Los ciberdelincuentes varían sus métodos según el sector, lo que genera un perfil de amenaza específico. Tras excluir el elevado volumen de spam, el sector de Artes, Ocio y Entretenimiento lideró en número de amenazas por usuario (TPU), con ataques mayormente basados en correos electrónicos y mensajes con cargas útiles maliciosas.

Los sectores de Servicios profesionales: Legal y Medio de comunicación y Publicaciones estuvieron entre los más afectados, con casi 9 TPU cada uno. El sector Legal fue blanco de numerosos ataques de suplantación de la identidad, mientras que en Medios de comunicación y Publicaciones predominaron las URL maliciosas.

Cada industria se enfrenta a un volumen significativo de spam, así como a amenazas cuya detección se debe al uso por parte de los atacantes de infraestructura de infraestructura de baja reputación. Como parte del análisis, Mimecast eliminó los mensajes de correo electrónico masivos —detectados como spam o de baja reputación— que representaban 17 TPU y 5 TPU, respectivamente.

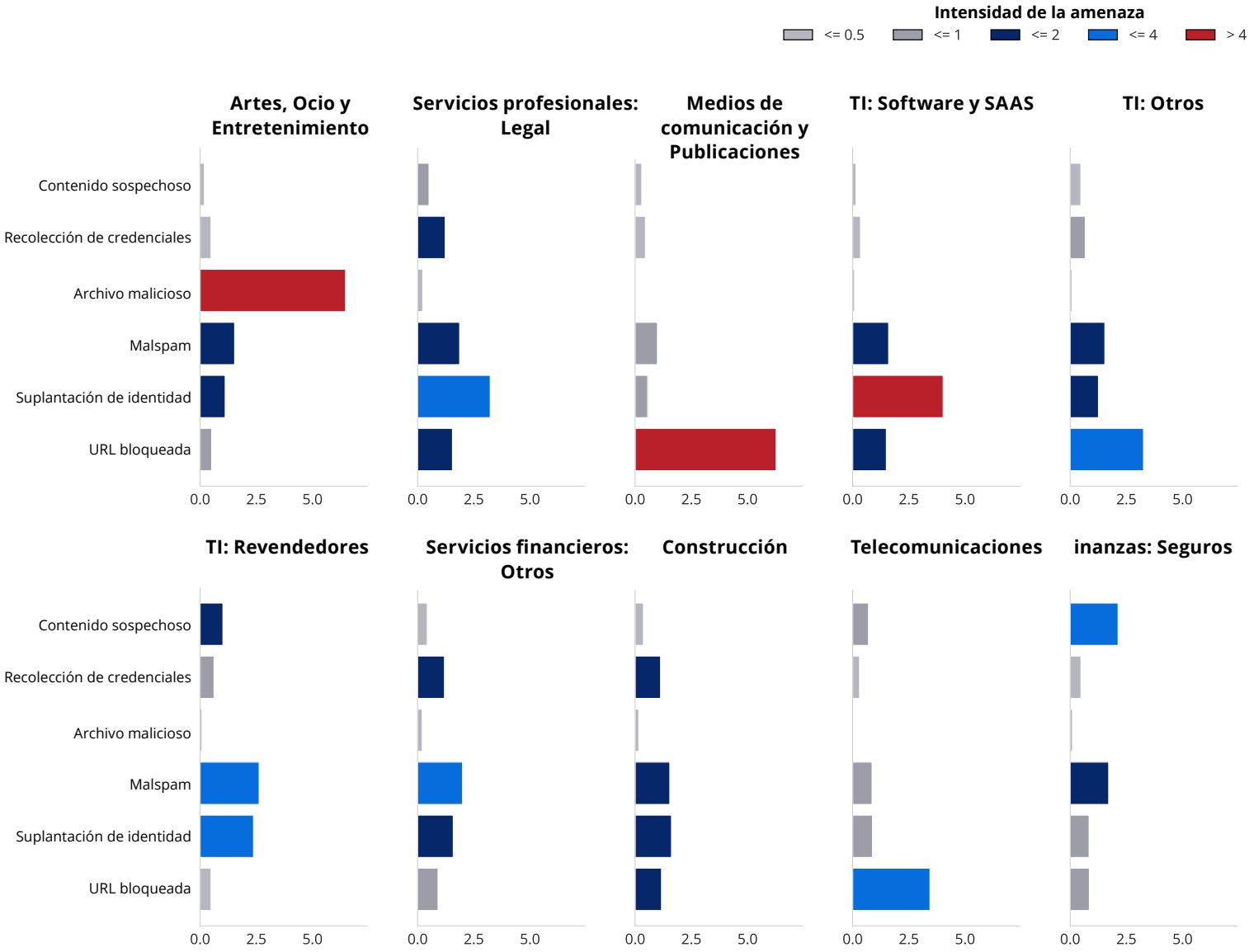


Gráfico 3: Perfil de amenazas de los 10 principales sectores, excluyendo las categorías de spam y baja reputación, ya que tienden a distorsionar los datos. El eje X muestra los valores de TPU en formato logarítmico.

GRÁFICO — GRUPOS DE AMENAZAS

#04

Atribuir un ciberataque es cada vez más complicado debido a las tácticas híbridas de los atacantes y la proliferación de modelos de ciberdelincuencia como servicio, como Ransomware-as-a-Service (RaaS), Phishing-as-a-Service (PhaaS) y los agentes de acceso inicial (IAB; Initial Access Brokers). Estos servicios permiten que múltiples actores de amenazas reutilicen las mismas herramientas e infraestructura, lo que da lugar a campañas similares lanzadas por grupos completamente diferentes. Los actores de amenazas a menudo emplean una combinación de técnicas de diferentes vectores de ataque y cambian con frecuencia sus métodos, lo que hace especialmente difícil atribuir cada ataque a un solo actor o determinar su propósito.

Los métodos de atribución tradicionales, basados en infraestructura o firmas de malware, son cada vez menos fiables. Por ello, Mimecast se centra en el análisis de Tácticas, Técnicas y Procedimientos (TTP) para clasificar y contextualizar las operaciones de amenazas de forma sistemática. Al rastrear cómo actúan los atacantes, podemos agrupar amenazas e identificar patrones entre campañas, incluso cuando los enfoques tradicionales fallan. Este enfoque permite una comprensión más clara y precisa de la evolución de sus capacidades. A continuación, destacamos las operaciones de amenazas más activas, con sus respectivas campañas y su posible impacto.

Operación de amenaza

MCTA1014

Primera observación: 2020

OBJETIVO

ROBO DE INFORMACIÓN Y ESPIONAJE

DIRIGIDO

NORTEAMÉRICA
EUROPA
ORIENTE MEDIO

Sector

AVIACIÓN
AEROESPACIAL
TRANSPORTE

OCT. 2021

Últimas campañas

Operación de amenaza

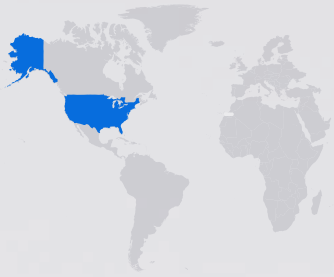
MCTA1003

Primera observación: 2018

OBJETIVO

ROBO DE DATOS

DIRIGIDO



PREDOMINANTEMENTE ESTADOUNIDENSE

Sector

TI
EDUCACIÓN

OCT. 2021

Últimas campañas

Operación de amenaza

MCTA3010

Primera observación: 2018

OBJETIVO

CREDENCIALES PARA SU DISTRIBUCIÓN

DIRIGIDO

SUDÁFRICA

Sector

TODOS

NOV. 2021

Últimas campañas

Operación de amenaza

MCTA5004

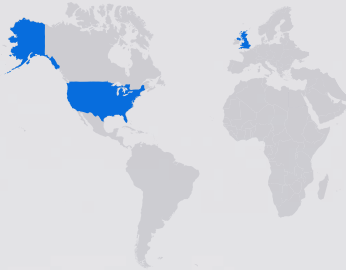
Primera observación: 2024

OBJETIVO

ECONÓMICO

Información de la campaña

DIRIGIDO



PRINCIPALMENTE
REINO UNIDO
EE. UU.

Sector

MANUFACTURA
BIENES RAÍCES
VENTA AL POR MENOR

DIC. 2021

Últimas campañas

Operación de amenaza

MCTA3028

Primera observación: 2018

OBJETIVO

RECOLECCIÓN DE CREDENCIALES

Información de la campaña

DIRIGIDO

GLOBAL

Sector

TODOS

DIC 2021

Últimas campañas

Operación de amenaza

MCTA3001

Primera observación: 2023

OBJETIVO

ROBO DE CREDENCIALES Y DATOS

DIRIGIDO

AUSTRALIA

Sector

PRINCIPALMENTE EDUCACIÓN

DIC 2021

Últimas campañas

Operación de amenaza

MCTA5005

Primera observación: 2020

OBJETIVO

ECONÓMICO

DIRIGIDO

GLOBAL

Sector

TODOS

DIC 2021

Últimas campañas

Operación de amenaza

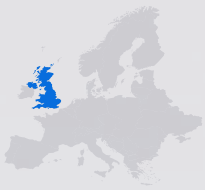
MCTA3022

Primera observación: 2021

OBJETIVO

RECOLECCIÓN DE CREDENCIALES

DIRIGIDO



PRINCIPALMENTE REINO UNIDO

Sector

TODOS

DIC 2021

Últimas campañas

GRÁFICO - PRINCIPALES VULNERABILIDADES A LO LARGO DEL TIEMPO

#05

Si bien la gran mayoría de los ataques que intentaron explotar problemas de software se centraron en dos vulnerabilidades populares (CVE-2017-0199 y CVE-2022-42889), los atacantes intentaron explotar 89 problemas diferentes en la segunda mitad de 2024. Al comparar las 10 principales vulnerabilidades detectadas por Mimecast como parte de un correo electrónico o entregadas como enlace, siete problemas tienen una puntuación del sistema de puntuación de predicción de exploits (EPSS, Exploit Prediction Scoring System) de al menos 0,88, lo que equivale a un 88 % de probabilidades de explotación en los próximos 30 días, mientras que dos vulnerabilidades, ambas descubiertas en 2024, aún no se han registrado como explotadas.

El análisis también muestra la divergencia entre la puntuación del EPSS y la sistema común de puntuación de vulnerabilidades (CVSS, Common Vulnerability Scoring System), que suele asociarse con la gravedad futura de la explotación.

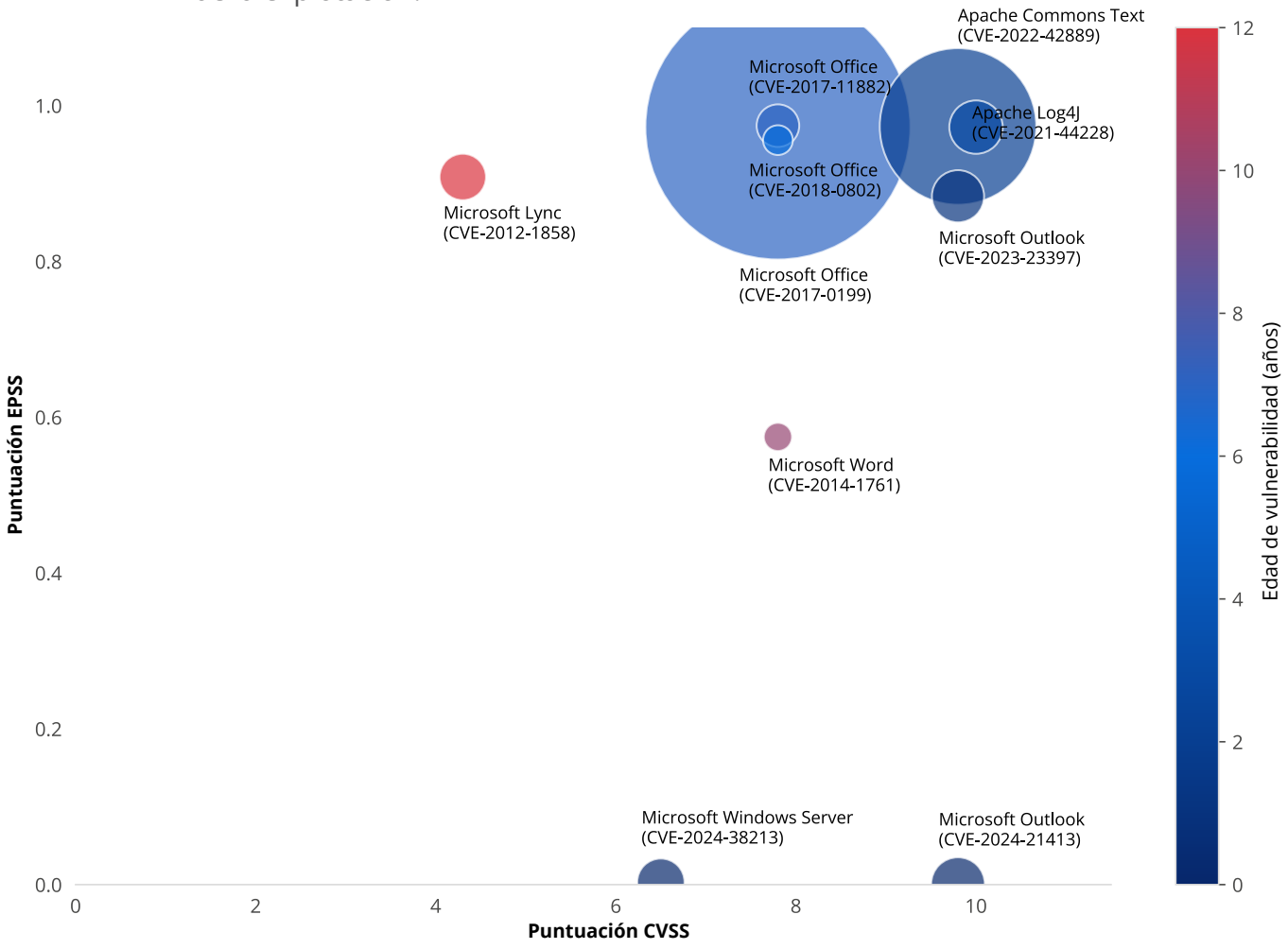


Gráfico 5: Las 10 principales vulnerabilidades detectadas en los mensajes, comparadas según las puntuaciones EPSS y CVSS. Dos vulnerabilidades populares tienen al menos 10 años. Datos de EPSS recopilados a fecha de 15 de enero de 2025.

PRINCIPALES AMENAZAS Y CAMPAÑAS

04.2

01
SPOOFING ABIERTO

02
NOTIFICACIÓN DE INFRACCIÓN DE DERECHOS DE AUTOR/SUSCRIPCIÓN

03
USUARIO ENGAÑADO PARA QUE COPIE/PEGUE ENLACES — ESTAFA DE CUENTAS A PAGAR

04
ESTAFA BEC DIRIGIDA DCON DEEPFAKE DE AUDIO

05
NOTIFICACIÓN DE ENTREGA NO REALIZADA

06
USURPACIÓN DE CUENTAS DE FACEBOOK — SUPLANTACIÓN DE MARCA

#01 SPOOFING ABIERTO

TÉCNICA Uso de enrutadores domésticos como proxy para enviar envían mensajes de correo electrónico de phishing suplantados a través de los servicios de correo electrónico del proveedor de servicios de Internet (ISP)

SERVICIOS UTILIZADOS Zimbra, MagicMail

OBJETIVOS A nivel global. - Todos los sectores

Enlace a la Notificación

Actor de amenazas

↓

Enrutadores domésticos de ISP explotados mediante vulnerabilidades o contraseñas débiles

↓

Enrutador configurado para su uso como proxy

↓

Correos electrónicos de phishing retransmitidos a través de los servidores de correo de ISP

↓

Enlaces maliciosos alojados en varios servicios de nube

↓

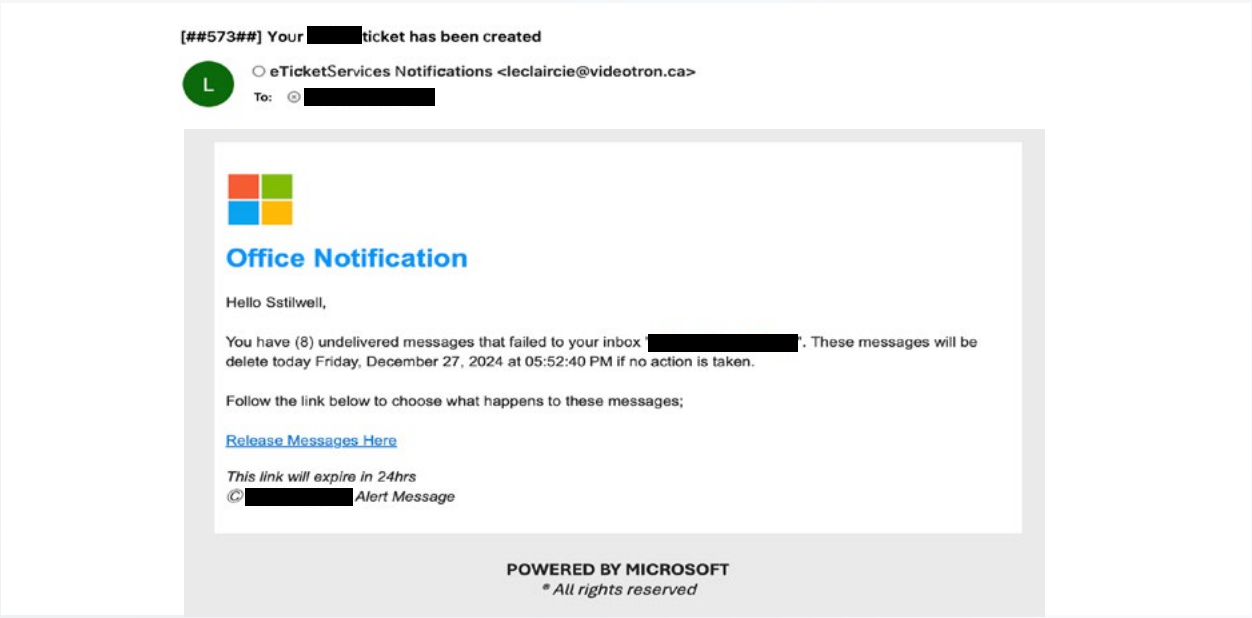
Se solicita el nombre de usuario y la contraseña de M365

↓

Se recopilan las credenciales y se redirige al usuario a la página de inicio de sesión genuina de M365

Los actores de amenazas están utilizando enrutadores domésticos comprometidos como proxies para enviar campañas de phishing de credenciales a gran escala a través de los servicios de correo electrónico de los ISP, ocultando su infraestructura y eludiendo la autenticación del correo electrónico. Al aprovechar los proveedores de servicios de Internet con autenticación de correo electrónico saliente débil o inexistente, los ciberdelincuentes logran una distribución masiva y la capacidad de suplantar la identidad de los remitentes sin restricciones.

Los ISP afectados identificados a partir de nuestra investigación utilizan soluciones de correo electrónico como Zimbra y MagicMail, y no parecen contar con medidas robustas antispam para el correo saliente. La combinación de una autenticación insuficiente y controles de seguridad poco estrictos permite a los atacantes enviar grandes volúmenes de mensajes y realizar campañas de spam masivas sin grandes obstáculos.


[##573##] Your [redacted] ticket has been created

L eTicketServices Notifications <leclaircie@videotron.ca>

To: [redacted]

Office Notification

Hello Sstilwell,

You have (8) undelivered messages that failed to your inbox [redacted]. These messages will be delete today Friday, December 27, 2024 at 05:52:40 PM if no action is taken.

Follow the link below to choose what happens to these messages;

Release Messages Here

This link will expire in 24hrs

© [redacted] *Alert Message*

POWERED BY MICROSOFT

** All rights reserved*

#02 NOTIFICACIÓN DE INFRACCIÓN DE DERECHOS DE AUTOR/SUSCRIPCIÓN

TÉCNICA Suplantación de identidad de bufetes de abogados con notificaciones de derechos de autor como señuelo para el robo de información

SERVICIOS UTILIZADOS Gmail, Mail Merge

OBJETIVOS A nivel global, pero con mayor concentración en el Reino Unido: sectores del Comercio minorista, Mayorista, Viajes y Hostelería

Enlace a la Notificación

Actor de amenazas

↓

Correo electrónico de phishing mediante el servicio de combinación de correo

↓

Enlaces a contenido alojado en Dropbox

↓

Descarga del archivo zip que contiene el archivo ejecutable

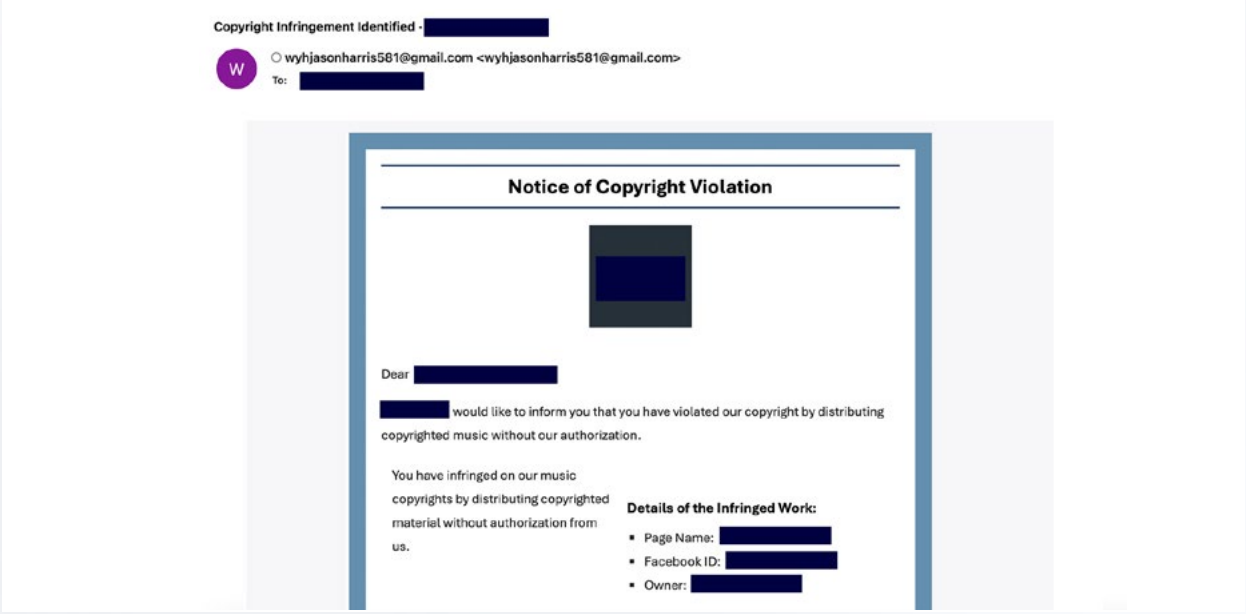
↓

El archivo ejecutable descarga un infostealer desde Github

↓

Filtra datos confidenciales

Correos electrónicos maliciosos enviados a través de Gmail mediante un servicio de combinación de correo se hacen pasar por bufetes de abogados de renombre y afirman que las empresas están infringiendo derechos de autor. El correo electrónico contiene un enlace directo a Dropbox o una redirección a Dropbox, lo que lleva a la descarga de un archivo zip que contiene un ejecutable. El objetivo de las campañas es utilizar varios ladrones de información para apoderarse de información (infostealer) confidencial de las máquinas infectadas, como credenciales y datos financieros.



#03 USUARIO ENGAÑADO PARA QUE COPIE/PEGUE ENLACES — ESTAFA DE CUENTAS A PAGAR

TÉCNICA Convencer a los usuarios a copiar y pegar un enlace para eludir las defensas

SERVICIOS UTILIZADOS Amazon Simple Email Service, programas de envío de correo en Python

OBJETIVOS Principalmente EE. UU. – Sectores de Fabricación, Minorista y Legal

Enlace a la Notificación

Actor de amenazas

↓

Correo electrónico de phishing a través de AWS usando el programa en Python

↓

Se le pide al usuario que pegue una URL manipulada en el navegador

↓

Redirige a un archivo compartido alojado en un recurso de SharePoint falso

↓

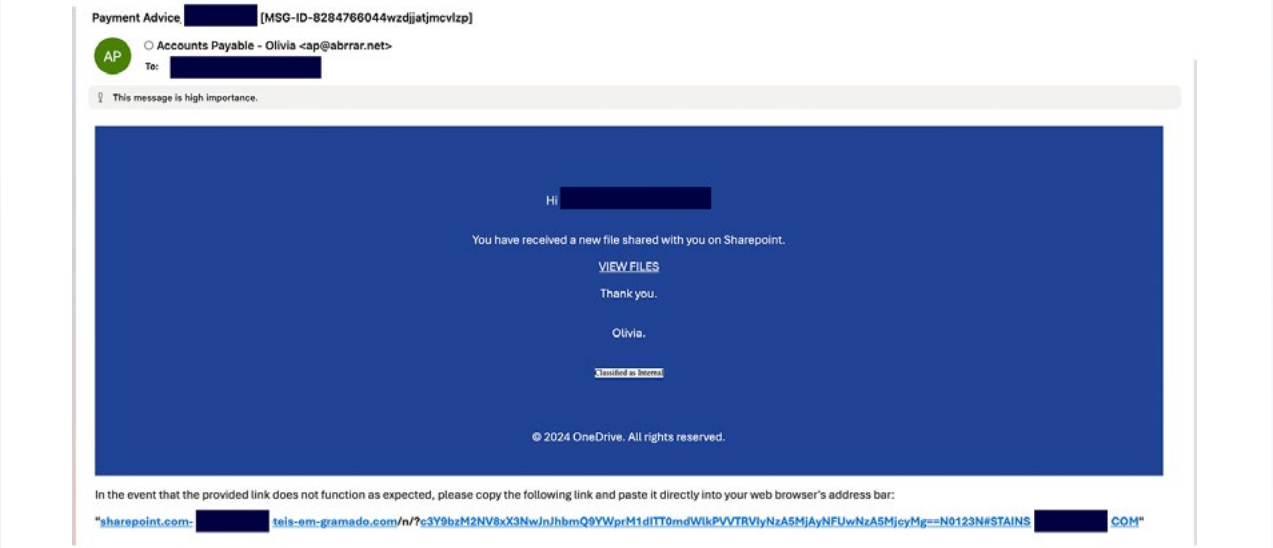
Se le solicita el nombre de usuario y la contraseña de M365

↓

Tarjeta de crédito utilizada o vendida en un mercado clandestino

Para evadir la detección por parte de software y servicios de seguridad, los ciberdelincuentes han recurrido a tácticas que inducen a los usuarios a copiar enlaces manipulados de un correo electrónico (por lo general, les falta el prefijo "http://") y peguen esos enlaces en sus navegadores. En los casos analizados por Mimecast, los correos suelen contener un botón con un enlace roto acompañado de un mensaje del tipo: "Si el enlace no funciona, copie y pegue la siguiente dirección".

Esta técnica se suma a otros métodos de ofuscación, como el uso de códigos QR para hacer que los enlaces sean ilegibles para los usuarios y el uso de tácticas intimidatorias junto con números de teléfono para incitar a las víctimas a llamar a un centro de llamadas operado por los atacantes. El objetivo de las campañas actuales que utilizan este método suele ser recopilar credenciales de la víctima.



#04 ESTAFA BEC DIRIGIDA DCON DEEPFAKE DE AUDIO

TÉCNICA Deepfake deaudio, suplantación de identidad de correo electrónico empresarial (BEC)
SERVICIOS UTILIZADOS Adobe Sign, DocuSign
OBJETIVOS A nivel global. Principalmente sectores financieros

Enlace a la Notificación

Actor de amenazas

↓

Correo electrónico BEC a través de Docusign o AdobeSign

↓

El usuario firma un NDA digital

↓

El usuario llama a un número falso para la verificación del NDA

↓

La interacción a través del correo electrónico da lugar a una factura para el pago

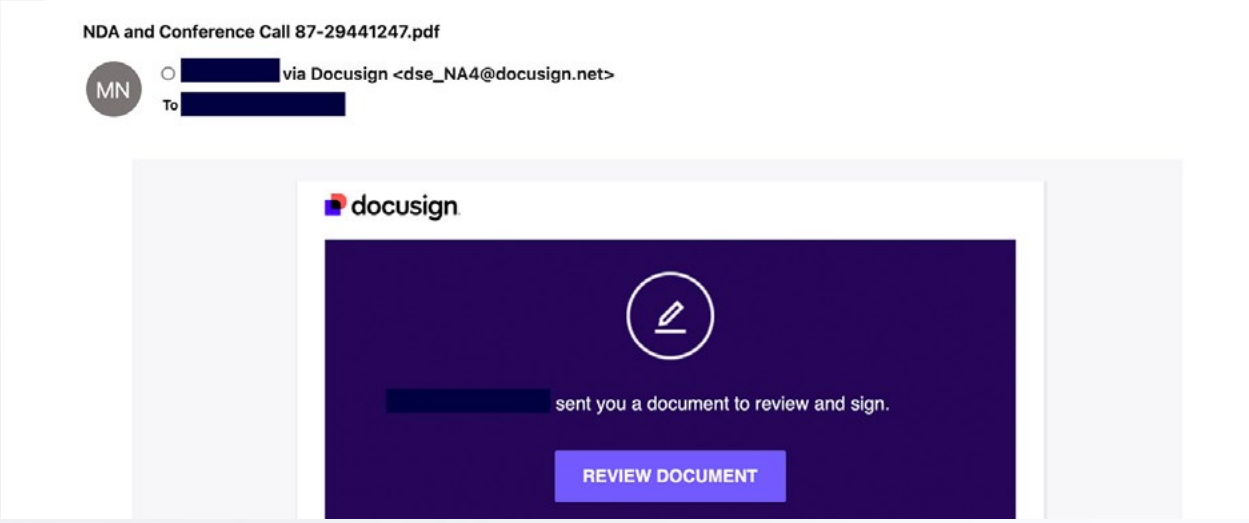
↓

Deepfake de audio de un ejecutivo que confirma el pago

↓

Pago realizado a la cuenta bancaria del ciberdelincuente

Los empleados de los sectores bancario, de seguros y otros sectores financieros son objetivo de correos electrónicos de spearphishing que afirman proceder de un bufete de abogados y se envían mediante un servicio de confianza como DocuSign y Adobe Sign. Los mensajes dirigidos solicitan al empleado que firme el acuerdo de confidencialidad (NDA) y luego llame a un número que se supone pertenece a un bufete de abogados, pero que en realidad está controlado por el atacante. El ciberdelincuente se hace pasar por el bufete de abogados utilizando técnicas de deepfake de audio para disfrazar su voz y envía un correo electrónico desde un dominio controlado por un atacante que parece similar al del bufete de abogados suplantado. Finalmente, enviará una factura supuestamente del bufete de abogados y realizará un seguimiento con una llamada falsa en la que se hace pasar por el CEO de la empresa u otro alto ejecutivo.



#05 NOTIFICACIÓN DE ENTREGA NO REALIZADA

TÉCNICA Aprovechamiento de servicios de confianza (LOTS)
SERVICIOS UTILIZADOS Buckets de S3 en AWS para alojar archivos HTML
OBJETIVOS Reino Unido, organizaciones sin ánimo de lucro y el sector de la Vivienda

Enlace a la Notificación

Actor de amenazas

Correo electrónico de phishing a través del ISP Biglobe

Redirigido a un archivo HTML alojado en AWS

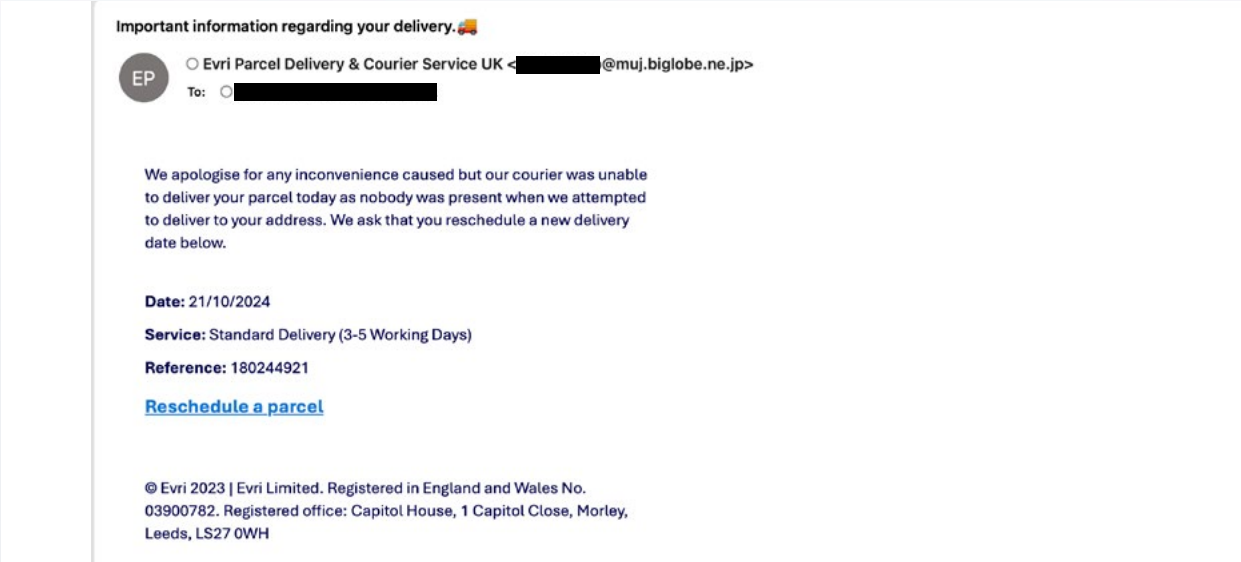
Un archivo HTML suplanta la página de envío no realizado de EVRI

Información de identificación personal (PII) y de tarjeta de crédito proporcionada para la actualización del envío

Tarjeta de crédito utilizada o vendida en un mercado clandestino

Los mensajes enviados a través de BIGLOBE, un servicio japonés explotado con frecuencia por actores de amenazas, están dirigidos a organizaciones sin ánimo de lucro y de vivienda en el Reino Unido, con notificaciones que afirman que no se ha podido realizar una entrega.

Los atacantes aprovechan este tipo de servicios y otros proveedores de servicios de Internet al adquirir cuentas autenticadas en mercados clandestinos, lo que les concede acceso legítimo a su infraestructura y les permite enviar correos electrónicos maliciosos que eluden la mayoría de los protocolos de autenticación de correo electrónico.



Important information regarding your delivery.🚚

EP ○ Evri Parcel Delivery & Courier Service UK <[redacted]@muj.biglobe.ne.jp>
To: ○ [redacted]

We apologise for any inconvenience caused but our courier was unable to deliver your parcel today as nobody was present when we attempted to deliver to your address. We ask that you reschedule a new delivery date below.

Date: 21/10/2024
Service: Standard Delivery (3-5 Working Days)
Reference: 180244921

Reschedule a parcel

© Evri 2023 | Evri Limited. Registered in England and Wales No. 03900782. Registered office: Capitol House, 1 Capitol Close, Morley, Leeds, LS27 0WH

#06 USURPACIÓN DE CUENTAS DE FACEBOOK — SUPLANTACIÓN DE MARCA

TECHNIK Señuelo de ofertas de trabajo en redes sociales suplantando marcas como Victoria's Secret, Red Bull y Coca-Cola

SERVICIO UTILIZADO Recruitee

OBJETIVOS Reino Unido y EE. UU. principalmente, énfasis en los sectores de Medios de comunicación y Publicaciones, y Comercio minorista

Enlace a la Notificación

Actor de amenazas

↓

Correo electrónico de phishing enviado a través del CMS Recruitee

↓

Página de inicio de sesión en un dominio similar de una marca suplantada

↓

Inicio de sesión a través de una página falsa de Facebook para enviar la solicitud

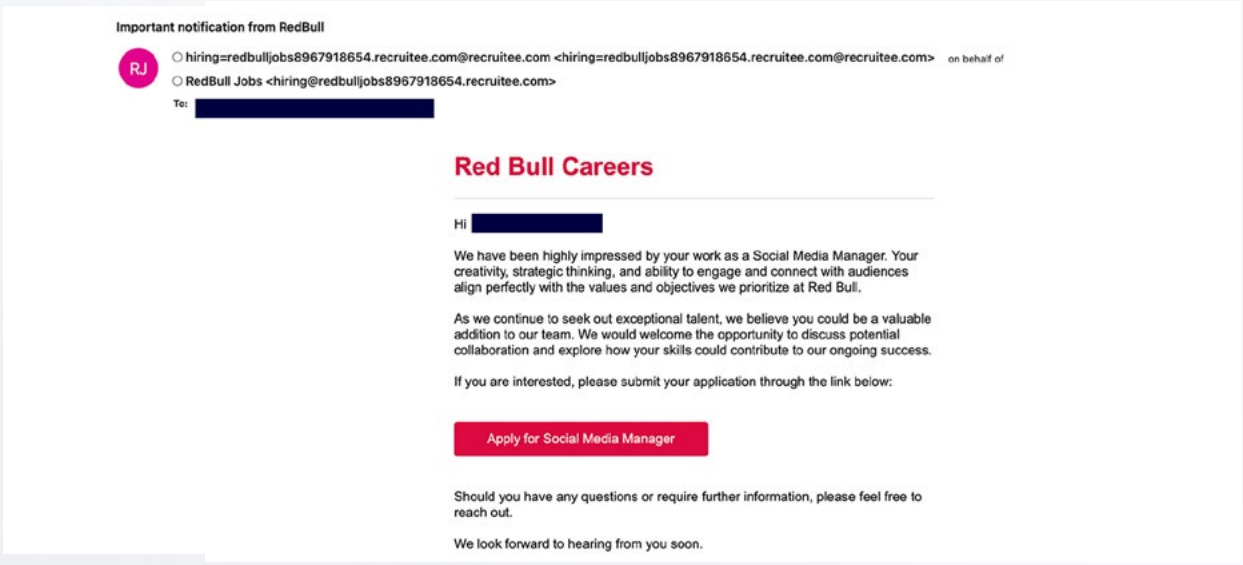
↓

Se requieren códigos MFA para completar la solicitud

↓

Credenciales de Facebook obtenidas y compartidas a través de un registrador de Telegram

Una reciente campaña de phishing aprovechó Recruitee, un sistema de gestión de contenidos (CMS) de reclutamiento de terceros legítimo, para enviar mensajes fraudulentos con ofertas de trabajo. Los actores de amenazas registran dominios que imitan a marcas conocidas para añadir credibilidad a la estafa. Las páginas de phishing emplean códigos CAPTCHA y filtrado de IP para evitar la detección automatizada y su principal objetivo es robar credenciales de Facebook.



Important notification from RedBull

RJ ○ hiring=redbulljobs8967918654.recruitee.com@recruitee.com <hiring=redbulljobs8967918654.recruitee.com@recruitee.com> on behalf of
○ RedBull Jobs <hiring@redbulljobs8967918654.recruitee.com>
To: [redacted]

Red Bull Careers

Hi [redacted]

We have been highly impressed by your work as a Social Media Manager. Your creativity, strategic thinking, and ability to engage and connect with audiences align perfectly with the values and objectives we prioritize at Red Bull.

As we continue to seek out exceptional talent, we believe you could be a valuable addition to our team. We would welcome the opportunity to discuss potential collaboration and explore how your skills could contribute to our ongoing success.

If you are interested, please submit your application through the link below:

Apply for Social Media Manager

Should you have any questions or require further information, please feel free to reach out.

We look forward to hearing from you soon.

04
.3

MIMECAST RISKRADAR

LOS ATACANTES SE APROVECHAN CADA VEZ MÁS DE SERVICIOS DE CONFIANZA (LOTS)

Desde proveedores de correo electrónico legítimos hasta sitios de intercambio de archivos y servicios de alojamiento de seminarios web, los atacantes han ampliado el uso de servicios de confianza para eludir las defensas basadas en la reputación y la confianza. Los ataques suelen utilizar proveedores de correo electrónico populares, como Gmail de Google y Outlook de Microsoft (antes Hotmail), mientras que los enlaces en los mensajes de correo electrónico suelen terminar en un servicio de alojamiento legítimo, como Google Docs, Evernote o los servicios OneDrive y SharePoint de Microsoft.

A medida que los servicios legítimos refuerzan sus medidas para el abuso, los atacantes buscan alternativas y recurren a proveedores más pequeños. Algunas de las principales campañas monitorizadas por Mimecast, por ejemplo, utilizaron proveedores, como Airtable, Publuu y WaveCompliance.

EL PANORAMA GEOPOLÍTICO SE RECRUDECE

El aumento delas tensiones geopolíticas a nivel mundial están provocando un cambio en el panorama de amenazas. Los ciberdelincuentes se han vuelto más activos, y utilizan el ciberespaciopara recopilar inteligencia, comprometer los activos de las naciones rivales y generar ingresos. La aparente falta de consecuencias concretas de los ciberataquesha alentado tanto a los países a ampliar sus operaciones como a los ciberdelincuentes a ejecutar ataques más audaces.

Pese a todo, las fuerzas de seguridad han conseguido avanzar en el desmantelamiento de la infraestructura de los ciberdelincuentes, mientras que los esfuerzos de los responsables de la defensa han conseguido reducir enormemente el número de objetivos fáciles de hackear. Tras la invasión de Rusia a Ucrania, ambos países agotaron su arsenal de exploits de día cero (zero-day) y día n (n-day o one-day), lo que provocó repunte (véase el Gráfico 1) que desde entonces se ha estabilizado. En 2024, el número total de vulnerabilidades explotadas registradas en el catálogo de vulnerabilidades conocidas explotadas (KEV, Known Exploited Vulnerability) se mantuvo en un nivel constante, pero relativamente bajo.

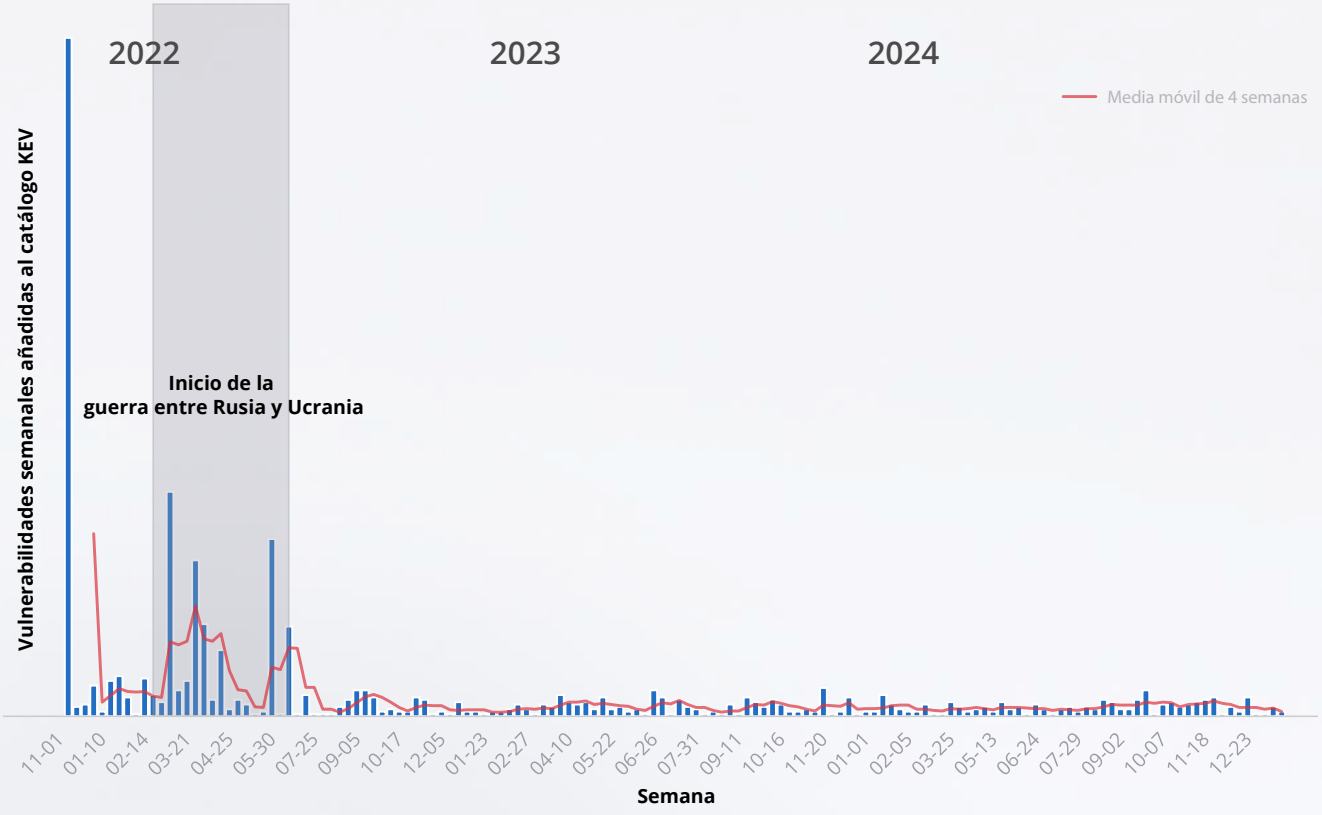


Gráfico 1: Desde mediados de 2022 hasta finales de 2024, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA)ha añadido unas 4 vulnerabilidades por semana al catálogo de KEV, según los datos recopilados por la propia agencia. Los datos muestran un fuerte repunte cuando se publicó por primera vez la lista, seguido de una notable actividad durante los primeros meses de la invasión de Rusia a Ucrania.

El contexto geopolítico ha intensificado el nivel de ciberamenaza, y al mismo tiempo, los eventos globales facilitan a los atacantes nuevas estrategias para manipular el elemento humano.

Los principales señuelos geopolíticos identificados por los investigadores de amenazas de Mimecast:

01
CHINA-TAIWÁN

02
CHINA-MAR DE CHINA MERIDIONAL

03
CHINA-CORTE DE CABLE

04
GUERRA RUSIA-UCRANIA

05
CONFLICTO ISRAEL-GAZA

06
LEGISLACIÓN DE LA UNIÓN EUROPEA

07
RUSIA-ELECCIONES DE EE. UU.

08
IRÁN-ELECCIONES DE EE. UU.

09
FENÓMENOS METEOROLÓGICOS EN EE. UU.

SECTORES MÁS ATACADOS

Los sectores con mayor exposición a amenazas son el de las artes y el de ocio y entretenimiento, que registraron más de 10 amenazas por usuario (TPU, Threats Per User), y los servicios profesionales: Legal y Medios de comunicación y Publicaciones, que registraron casi 9 TPU.

La mayoría de los sectores exhibieron un perfil de amenazas diferenciado. El sector de las Artes, Ocio y Entretenimiento experimentó una proporción mucho mayor de ataques utilizando archivos maliciosos, mientras que los empleados de bufetes de abogados sufrieron un número significativo de ataques de suplantación de identidad. Los atacantes dirigieron sus ataques principalmente a los trabajadores del sector de Medios de comunicación y Publicaciones con enlaces maliciosos, mientras que el sector de Software y SaaS tuvo que enfrentarse a numerosos ataques de suplantación de identidad.

Como parte del análisis, Mimecast eliminó los mensajes de correo electrónico masivos —detectados como spam o de baja reputación— que representaban 17 TPU y 5 TPU, respectivamente.

01
ARTES, OCIO Y ENTRETENIMIENTO 10.322010 TPU

02
SERVICIOS LEGALES 8.613564 TPU

03
MEDIOS DE COMUNICACIÓN Y PUBLICACIONES 8.622578 TPU

CRONOLOGÍA DE EVENTOS PRINCIPALES – SEGUNDO SEMESTRE DE 2024

04.4

JUL.
INTERRUPCIÓN DE SERVICIO DE CROWDSTRIKE

SEP.
ALGUNAS PLATAFORMAS DE INTERCAMBIO DE CRIPTOMONEDAS ASIÁTICAS AFECTADAS POR UNA SERIE DE ROBOS
FILTRACIÓN DE DATOS DEL INTERNET ARCHIVE

OCT.
SALZ-TAIFUN SORGT FÜR WACHSENDE BESORGNIS

NOV.
IRANISCHE „FAKE-ARBEITER“ NEHMEN SENSIBLE BRANCHEN INS VISIER

DIC.
EL DEPARTAMENTO DEL DE EE. UU. SUFRE UN CIBERATAQUE A TRAVÉS DE UN PROVEEDOR EXTERNO
DESARROLLADORES VÍCTIMAS DE PHISHING FACILITAN LA VULNERACIÓN DE UNA EXTENSIÓN DEL NAVEGADOR

JUL.

SE FILTRARON 000 MILLONES DE CONTRASEÑAS

VULNERABILIDAD contraseñas filtradas
IMPACTO Ataques de relleno de credenciales y de fuerza bruta

El descubrimiento del archivo RockYou2024, la mayor filtración de recopilación de contraseñas de la historia, reveló una cantidad asombrosa de 9 948 575 739 contraseñas únicas en texto plano. Este archivo masivo, publicado en un foro de piratería, genera gran preocupación, ya que incluye contraseñas acumuladas durante las últimas dos décadas, lo que podría exponer a muchos usuarios a ataques de relleno de credenciales y otras amenazas de seguridad.

SEP.

ALGUNAS PLATAFORMAS DE INTERCAMBIO DE CRIPTOMONEDAS ASIÁTICAS AFECTADAS POR UNA SERIE DE ROBOS

VULNERABILIDAD Brechas de seguridad de red

IMPACTO Más de 70 millones de USD en pérdidas

Los ataques a dos plataformas de intercambio de criptomonedas, BingX, con sede en Singapur, e Indodax, con sede en Indonesia, sufrieron pérdidas masivas tras sufrir ataques separados. Indodax, con sede en Yakarta, se comprometió a compensar a los usuarios tras unas pérdidas de 22 millones de dólares, mientras que BingX informó de unas pérdidas de 44 millones de dólares. En Estados Unidos, el Departamento de Justicia también anunció la detención de dos personas relacionadas con el robo de 230 millones de dólares en criptomonedas a un ciudadano estadounidense.

FILTRACIÓN DE DATOS DEL INTERNET ARCHIVE

VULNERABILIDAD Desconocida

IMPACTO Filtración de datos sobre 31 millones de cuentas

El Internet Archive sufrió múltiples violaciones de seguridad durante un periodo de 22 días. Alrededor del 28 de septiembre, un ciberdelincuente robó el archivo de la base de datos de la Wayback Machine del Internet Archive, apoderándose de nombres de usuario, direcciones de correo electrónico y contraseñas cifradas. Aunque el fundador del sitio dijo que habían limpiado los sistemas y mejorado la seguridad, en octubre se produjeron múltiples ataques de denegación de servicio y una segunda fuga de datos.

OCT.

AUMENTAN LAS PREOCUPACIONES POR SALT TYPHOON

VULNERABILIDAD Intrusión en la infraestructura de telecomunicaciones de EE. UU.

IMPACTO Ciberdelincuentes chinos consiguen el control generalizado de las comunicaciones

El grupo de amenazas patrocinado por el estado chino, Salt Typhoon, accedió a información altamente sensible sobre ciudadanos y funcionarios del gobierno de EE. UU. al comprometer a importantes proveedores de servicios de telecomunicaciones e Internet de EE. UU., incluidos Verizon y AT&T. Se informa de que hasta nueve proveedores diferentes se han visto afectados, incluido el acceso a la infraestructura de escuchas telefónicas autorizada por los tribunales en algunos proveedores, en lo que se ha denominado un "fallo de contrainteligencia del más alto nivel".

NOV.

AGENTES IRANÍES SE HACEN PASAR POR TRABAJADORES PARA INFILTRARSE EN INDUSTRIAS CRÍTICAS

VULNERABILIDAD Ingeniería social, abuso de LinkedIn

IMPACTO Los sectores aeroespacial, de aviación y de defensa de Israel y los Emiratos Árabes Unidos, Turquía, India y Albania también posibles objetivos

Se sospecha que hackers iraníes utilizaron sitios web de reclutamiento falsos para hacerse pasar por reclutadores en LinkedIn, contactando con empresas aeroespaciales, defensa y aviación de Israel, Emiratos Árabes Unidos, Turquía, India y Albania. Desde 2023, grupos de ciberdelincuentes se hicieron pasar por reclutadores en LinkedIn, ofreciendo trabajos falsos pero atractivos para distribuir malware. Su objetivo: espiar y robar datos sensibles. El malware y las tácticas son similares a las utilizadas por un grupo de hackers norcoreano que cuyo objetivo eran atacó fondos cotizados en criptomonedas.

DIC.

EL DEPARTAMENTO DEL DE EE. UU. SUFRE UN CIBERATAQUE A TRAVÉS DE UN PROVEEDOR EXTERNO

VULNERABILIDAD Proveedor externo, papel crítico del software de seguridad

IMPACTO Los atacantes consiguieron acceder a datos no clasificados en algunas estaciones de trabajo

El Departamento del Tesoro de EE. UU. informó que una brecha de seguridad en BeyondTrust, proveedor de seguridad de identidades, comprometió sus sistemas, permitiendo el acceso no autorizado a varias estaciones de trabajo y documentos no clasificados. La investigación en curso señala a un grupo de hackers patrocinado por el Estado chino como responsable del ataque. . Los atacantes supuestamente obtuvieron una clave API utilizada para soporte remoto. BeyondTrust aún no ha revelado cómo los atacantes accedieron a la clave crítica.

DESARROLLADORES VÍCTIMAS DE PHISHING FACILITAN LA VULNERACIÓN DE UNA EXTENSIÓN DEL NAVEGADOR

VULNERABILIDAD Ataque de spearphishing que otorga permisos elevados en las extensiones

IMPACTO Recopilación de información por extensiones maliciosas de las credenciales y la información de los usuarios finales

Grupos de amenazas han comprometido más de 30 extensiones de navegador en el último año mediante correos electrónicos de spearphishing que parecen ser de Google, dirigidos a los desarrolladores de las extensiones de Chrome objetivo. Al hacer clic en el correo electrónico, se les solicita que otorguen privilegios a una aplicación con un nombre inofensivo, pero en realidad están dando a los atacantes la capacidad de reemplazar su extensión con una aplicación maliciosa. La empresa de seguridad de datos Cyberhaven informó por primera vez sobre estas tácticas en diciembre, después de que uno de sus desarrolladores fuera víctima del ataque y otorgara permisos a la aplicación “Privacy Policy Extension”. Se estima que hasta 2,6 millones de usuarios podrían verse visto afectados por el ataque.

RECOMEN-
DACIONES

05

- CONTRAMEDIDAS ESPECÍFICAS FRENTE A AMENAZAS
- MEJORES PRÁCTICAS Y ADVERTENCIAS
- PASOS ESPECÍFICOS PARA LOS CLIENTES DE MIMECAST

CUERVO

ESPECIES

Conocidos por su capacidad para resolver problemas y enseñar. Siempre educando y tomando **medidas**. Su recurso de confianza para estrategias de mitigación de riesgos de ciberseguridad.

CONTRAMEDIDAS ESPECÍFICAS PARA AMENAZAS

05.1

Las organizaciones deberían implementar medidas concretas para fortalecer sus defensas y elevar el coste de los ataques para los ciberdelincuentes.

GESTIÓN DE RIESGOS HUMANOS

Las organizaciones deberían adoptar un marco de gestión de riesgos humanos que coordine los objetivos de seguridad con los objetivos empresariales. Al identificar los factores de riesgo humanos y los posibles resultados adversos, las empresas pueden desarrollar un sistema de respuesta multinivel que distinga entre errores no intencionados y acciones maliciosas. Las principales preocupaciones son la pérdida de propiedad intelectual u otra información estratégica, la filtración de datos sensibles y el uso indebido de los recursos de la empresa.

Las organizaciones deberían incorporar un enfoque escalonado que combine incentivos positivos o "empujoncitos" concomo medidas correctivas. Para ello, es fundamental establecer grupos de trabajo interfuncionales que garanticen el compromiso de los implicados y una gestión del cambio eficaz, además de mantener canales de comunicación claros con la dirección sobre las métricas de riesgo, posibles incidentes y estrategias de mitigación.

PROPORCIONE FORMACIÓN DE CONCIENCIACIÓN

En el complejo panorama actual, donde las tensiones geopolíticas a menudo se manifiestan como ciberamenazas, se vuelve esencial una formación integral de concienciación. Los empleados deben recibir formación no solo sobre los ciberriesgos generales, sino también sobre cómo los acontecimientos mundiales pueden influir en las campañas de phishing, las amenazas internas y los intentos de ingeniería social dirigidos a su organización. Al implementar programas robustos de formación en materia de concienciación y plataformas de gestión de riesgos asociados a las personas para proteger a los usuarios, las organizaciones pueden fortalecer su cortafuegos humano tanto contra ciberataques convencionales como contra aquellos motivados por razones geopolíticas. Este enfoque centrado en las personas de la seguridad ayuda a los empleados personal a identificar y responder eficazmente a las amenazas distribuidas a través del correo electrónico, las redes sociales, las herramientas de colaboración u otros vectores que se aprovechan de la psicología humana.

EXIJA MAYORES MEDIDAS DE SEGURIDAD A TERCEROS

Los ataques contra empresas en los sectores de la Fabricación, Transporte, Almacenamiento y Envíos, y Comercio minorista y mayorista representan un riesgo significativo de terceros para comprometer la cadena de suministro. Las empresas deberían revisar sus acuerdos de nivel de servicio para definir los estándares mínimos de seguridad de datos y ciberseguridad, así como reforzar la supervisión de sus proveedores. Para ellos, pueden recurrir a servicios de calificación externos y someter los procesos de adquisición a auditorías adicionales.

ANALICE EL ENTORNO EN BUSCA DE CONFIGURACIONES INCORRECTAS O PUERTOS ABIERTOS AL EXTERIOR

Las organizaciones deberían analizar regularmente su infraestructura en busca de rutas conocidas explotables, como puertos de red externos abiertos e inseguros o entornos de nube pública. Utilizando herramientas como las de administración de la postura de seguridad en la nube (CSPM, Cloud Security Posture Management), las empresas pueden identificar rápidamente las configuraciones incorrectas en su nube pública. Esto garantizará que todos los puertos de servidor de acceso público estén cerrados o adecuadamente asegurados y protegidos.

Como ejemplo, Mimecast ha observado un aumento continuo en los ataques contra los puertos del protocolo de escritorio remoto (RDP), que representan el 80 % de los casos efectivos de ransomware. Los atacantes continuarán buscando puertos RDP abiertos para atacar a las organizaciones.

BLOQUEE IMÁGENES EN MENSAJES DE CORREO ELECTRÓNICO

Los atacantes están aumentando el uso de tipos de archivos basados en imágenes para ocultar señuelos de phishing y código malicioso, con el fin de eludir los sistemas de detección. El análisis de Mimecast ha identificado que los actores de amenazas también utilizan cifrado y texto en idiomas extranjeros dentro de las imágenes para pasar desapercibidos. Las empresas deberían configurar los clientes de correo electrónico para evitar la carga de imágenes en los mensajes y aislar cualquier imagen que los usuarios marquen explícitamente. Nota: los usuarios de CyberGraph deben utilizar sitios de confianza para asegurarse de que los banners se cargan correctamente.

SEGMENTE LA RED Y REGISTRE EL TRÁFICO INTERNO

Los atacantes, especialmente durante un ataque de ransomware, pueden desplazarse lateralmente por una red de forma rápida. Segmente la red interna y coloque los activos críticos en sus propios enclaves para reducir el daño causado por el ransomware y otros ataques. La supervisión del tráfico interno, especialmente de las comunicaciones hacia segmentos específicos, permite la detección más temprana de posibles amenazas.

REFUERCE LAS CREDENCIALES DE USUARIO, IMPLEMENTE AUTENTICACIÓN MULTIFACTOR (MFA)

Muchas amenazas de malware explotan contraseñas comunes para infiltrarse en las redes. Los ataques recientes destacan cómo las contraseñas débiles contribuyen a las brechas de seguridad. Fortalezca todas las redes exigiendo contraseñas seguras, especialmente para los usuarios con privilegios. El departamento de seguridad de TI debe eliminar las contraseñas predeterminadas de administrador. Exigir la autenticación multifactor puede reducir drásticamente el compromiso de cuentas o credenciales robadas.

05.2

MEJORES PRÁCTICAS Y ADVERTENCIAS

AVISO APT40: TÉCNICAS DE MINISTERIO DE SEGURIDAD DEL ESTADO DE LA RPC EN ACCIÓN

8 de julio de 2024 LEER MÁS >

Organizaciones: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK, BND y otras

Las agencias gubernamentales responsables de la ciberseguridad y la aplicación de la ley en Australia, Canadá, Nueva Zelanda, Alemania, Corea del Sur, el Reino Unido y los Estados Unidos describieron las tácticas utilizadas por el actor de amenazas patrocinado por el estado chino APT40 (también conocido como Gingham Typhoon), que "ha atacado repetidamente las redes australianas, así como las redes gubernamentales y del sector privado en la región". El grupo puede rápidamente utilizar, adaptar y explotar el código de prueba de concepto para nuevas vulnerabilidades en ataques, e implementar esas herramientas en campañas.

DETECCIÓN Y MITIGACIÓN DE VULNERACIONES DE ACTIVE DIRECTORY

Septiembre de 2024 LEER MÁS >

Organizaciones: ASD, CISA, NSA, CCCS, NCSC-NZ, NCSC-UK

Las agencias de ciberseguridad de las naciones de los Cinco Ojos (Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda) describen 17 técnicas diferentes para atacar Microsoft Active Directory, que son las soluciones de identidad y acceso más comunes utilizadas en las empresas. Su papel crucial en la autenticación y autorización, junto con su vulnerabilidad debido a las configuraciones predeterminadas y la complejidad de la instalación, convierten a Active Directory en objetivo frecuente de los ciberdelincuentes.

CIBERACTORES MILITARES RUSOS ATACAN INFRAESTRUCTURAS CRÍTICAS DE EE. UU. Y DE OTROS LUGARES DEL MUNDO

5 de septiembre de 2024 LEER MÁS >

Organizaciones: CISA, FBI, NSA

Varios grupos de amenazas rusos vinculados con agencias militares atacaron a agencias gubernamentales ucranianas y otros objetivos de países aliados de la OTAN con el malware destructivo WhisperGate. Los atacantes suelen utilizar vulnerabilidades en dispositivos de red para obtener acceso inicial.

PRINCIPALES VULNERABILIDADES EXPLOTADAS DE FORMA HABITUAL EN 2023

12 de noviembre de 2024 LEER MÁS >
Organizaciones: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK

Quizás con retraso, las principales agencias de las naciones de los Cinco Ojos publicaron información sobre las 15 vulnerabilidades más explotadas habitualmente de 2023. Once de las 15 vulnerabilidades fueron explotadas en ataques de día cero, frente a las dos explotadas de esta forma entre las doce de la lista de 2022.

MEJORAR LA CIBERRESILIENCIA: DETALLES SOBRE LA EVALUACIÓN DEL EQUIPO ROJO DE CISA SOBRE UNA ORGANIZACIÓN DEL SECTOR DE INFRAESTRUCTURAS CRÍTICAS DE EE. UU.

21 de noviembre de 2024 LEER MÁS >
Organizaciones: CISA

La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) ha detectado debilidades significativas en la ciberseguridad en una organización de infraestructura crítica, durante una evaluación realizada por un equipo rojo. El equipo vulneró la organización utilizando un web shell que había quedado de una evaluación anterior. Esto afectó a su dominio y sus sistemas sensibles debido a las deficientes protecciones de red y a la lentitud en las respuestas.

CIBERACTORES VINCULADOS AL IRGC EXPLOTAN LOS (PLC) EN VARIOS SECTORES, INCLUYENDO LAS INSTALACIONES DE LOS SISTEMAS DE AGUA Y ALCANTARILLADO DE EE. UU.

18 de diciembre de 2024 LEER MÁS >
Organizaciones: FBI, CISA, NSA, US EPA, INCD, CCCS, NCSC

Las agencias de ciberseguridad de EE. UU., Israel, Canadá y el Reino Unido han emitido un comunicado actualizado. Describe ciberactividades maliciosas llevadas a cabo por actores vinculados al Cuerpo de la Guardia Revolucionaria Islámica de Irán (IRGC), incluidos ataques a controladores lógicos programables (PLC) e infraestructuras críticas en el Reino Unido e Israel.

PASOS PARA LOS CLIENTES DE MIMECAST

Los usuarios de Mimecast pueden adoptar medidas específicas y prácticas para proteger a sus usuarios de las amenazas mencionadas en el informe, con detalles técnicos de nivel intermedio.

PUERTA DE ENLACE EN LA NUBE DE SEGURIDAD DE CORREO ELECTRÓNICO

1. Se recomienda utilizar el inicio de sesión único de su proveedor de identidad o aprovechar la autenticación multifactor integrada de Mimecast para reducir la capacidad de un atacante de utilizar el correo electrónico como vector de ataque.
2. Asegúrese de que las políticas de autenticación de DNS respeten los registros DMARC. Una segunda política dirigida a un grupo de políticas con la acción de error de DMARC establecida en Ignorar/Gestionar y Remitentes permitidos proporcionará una exención efectiva para cualquier correo legítimo que sea rechazado o puesto en cuarentena por fallos de DMARC.
3. Optimice la protección contra la suplantación de identidad según las directrices de mejores prácticas de dos coincidencias configuradas para etiquetar Asunto/Cuerpo e incluya una política independiente para C-Level/VIP basada en la coincidencia de nombre con una retención para revisión por el administrador. Además, cree otra política para cualquier detección de tres coincidencias o más con la acción de retención por el administrador.
4. Implemente Protección BEC Avanzada con tres políticas: Aplicación Moderada para la detección de amenazas, Omitir Remitente para fuentes fiables y Omitir Destinatario para exclusiones internas.
5. Configurar una reescritura agresiva de URL garantizará que todas las URL se analicen al hacer clic. Tenga en cuenta que se reescribirá cualquier elemento que parezca una URL, por ejemplo, direcciones IP y enlaces internos.
6. Utilice integraciones preconstruidas con la mayoría de los proveedores de SIEM y XDR para ofrecer captura y análisis de registros para la aplicación de políticas de seguridad.
7. Aproveche su propia inteligencia sobre amenazas para beneficiarse de cualquier fuente de información sobre amenazas de terceros para el rechazo automático de indicadores coincidentes.
8. Los usuarios finales deben informar de los mensajes potencialmente maliciosos recibidos a través de las herramientas de usuario de Mimecast al SOC de Mimecast para su análisis ulterior.

INTEGRACIÓN EN LA NUBE

1. Habilite el aislamiento del navegador para minimizar el riesgo de que los usuarios accedan a sitios potencialmente sospechosos.
2. Personalice sus reglas de Permitir y Bloquear para especificar específicamente quién está permitido en su entorno.
3. Revise los informes semanales para obtener información sobre las amenazas detectadas en su entorno.
4. Los usuarios finales deben informar de los mensajes potencialmente maliciosos recibidos a través de las herramientas de usuario de Mimecast al SOC de Mimecast para su análisis ulterior.

Si no tiene claro el efecto de alguno de los ajustes propuestos, póngase en contacto con su gestor de cuentas de Mimecast, gestor de éxito de clientes o registre una llamada con el soporte de Mimecast.

CONCLUSIÓN

En la segunda mitad de 2024, el análisis de amenazas reveló una intensificación de las sofisticadas campañas de desinformación y las operaciones hacktivistas coordinadas, coincidiendo con la escalada de las tensiones geopolíticas que permitieron a los actores de amenazas convertir los acontecimientos mundiales en armas para perpetrar ataques dirigidos; estas tácticas evolucionadas ahora abarcan la filtración sistemática de datos, el despliegue de ransomware dirigido y los ataques DDoS orquestados, al tiempo que explotan las vulnerabilidades humanas a través de sofisticadas campañas de ingeniería social centradas en los principales desarrollos geopolíticos, que colectivamente plantean riesgos significativos para la continuidad del negocio y la disponibilidad de los sistemas.

La identificación de actividades maliciosas se ha vuelto técnicamente compleja debido a que los adversarios combinan acciones maliciosas con operaciones legítimas, incluida la explotación de servicios de confianza y archivos binarios de sistemas comunes. Los actores de amenazas aprovechan cada vez más las herramientas legítimas de los equipos rojos, lo que crea importantes retos para los controles de seguridad al diferenciar entre actividades autorizadas y no autorizadas. Esto requiere capacidades de supervisión mejoradas, incluyendo análisis avanzado del comportamiento y sistemas de detección de anomalías.

En otras áreas del panorama de amenazas, los ataques de ingeniería social mantienen altas tasas de éxito, evolucionando mediante la integración de tecnologías de inteligencia artificial automatizadas. Las amenazas persistentes avanzadas ahora aprovechan las sofisticadas tecnologías de deepfake y el contenido generado por IA para ataques dirigidos, lo que complica significativamente los mecanismos tradicionales de detección y prevención. La sofisticación técnica de estos ataques pone de relieve la compleja investigación de ingeniería social y el análisis de los patrones de comunicación en la cadena de suministro.

La seguridad perimetral sigue siendo una preocupación crítica, ya que los actores de amenazas explotan constantemente las vulnerabilidades en la infraestructura perimetral, incluidos los dispositivos VPN, los cortafuegos y los servicios orientados a Internet. La explotación de día cero combinada con el retraso en

la implementación de parches crea ventanas de vulnerabilidad prolongadas, especialmente en entornos de alta disponibilidad que requieren pruebas extensivas de parches. Este desafío se ve amplificado por las complejas arquitecturas de red y la expansión de la superficie de ataque impulsada por la migración a la infraestructura en la nube y la evolución de las tecnologías operativas. Las organizaciones requieren capacidades dedicadas de respuesta a incidentes, que incluyan herramientas forenses avanzadas, sistemas de análisis de red y mecanismos de detección automatizados.

Vulnerabilidades susceptibles de ser explotadas este año:

VPN

Como se ha observado en la reciente incorporación de CVE 2025 0282 Ivanti Connect Secure VPN al catálogo de vulnerabilidades explotables conocidas de CISA.

AUTENTICACIÓN

Observado recientemente en vulnerabilidades que explotan la omisión mediante una ruta o canal alternativo, y la ausencia de código de autenticación

DENEGACIÓN DE SERVICIO (DOS)

Una actividad maliciosa cada vez más popular diseñada para interrumpir las operaciones comerciales, p. ej. CVE 2024 3393 Denegación de servicio (DoS) del cortafuegos de PAN-OS

RECURSOS:

Seminario web
Traducir la inteligencia sobre amenazas en estrategias de seguridad prácticas (en inglés)

Informe de investigación
Estado de la seguridad del correo electrónico y la colaboración (en inglés)

TI HUB.

Mimecast TI Hub

Comunidad:

Mimecast central

mimecast