DESIGNED FOR Microsoft 365 ENVIRONMENTS

2024

CYBER SECURITY REPORT

UN ANÁLISIS EN PROFUNDIDAD
DEL PANORAMA DE AMENAZAS DE MICROSOFT 365

HORNETSECURITY

CYBER SECURITY REPORT 2024

Acerca de Hornetsecurity

Hornetsecurity permite a las empresas y organizaciones, independientemente de su tamaño, centrarse en su actividad principal protegiendo las comunicaciones por correo electrónico, asegurando los datos y garantizando la continuidad y el cumplimiento de la empresa con soluciones de última generación basadas en la nube.

Nuestro producto estrella, 365 Total Protection, es la solución de seguridad en la nube para Microsoft 365 más completa del mercado, e incluye seguridad del correo electrónico, cumplimiento normativo y backup.

¿Qué es el Cyber security Report?

El informe sobre ciberseguridad (antes conocido como Informe de ciberamenazas) es un análisis anual del panorama actual de las ciberamenazas basado en datos del mundo real recopilados y estudiados por el equipo especializado del Security Lab, nuestro laboratorio de seguridad. Hornetsecurity procesa más de 3.500 millones de correos electrónicos al mes. Mediante el análisis de las amenazas identificadas en estas comunicaciones, combinado con un conocimiento detallado del panorama más amplio de amenazas, Security Lab revela las principales tendencias. Además, puede hacer proyecciones informadas sobre el futuro de las amenazas a la seguridad de Microsoft 365, lo que permite a las empresas actuar en consecuencia. Las conclusiones y los datos se detallan en el presente informe.

¿Qué es Security Lab?

Security Lab es una división de Hornetsecurity que realiza análisis forenses de las amenazas a la seguridad más actuales y críticas, especializándose en la seguridad del correo electrónico. El equipo multinacional de especialistas en seguridad cuenta con una amplia experiencia en investigación de seguridad, ingeniería de software y ciencia de datos.

Para desarrollar contramedidas eficaces, es fundamental conocer en profundidad el panorama de las amenazas mediante el examen práctico de virus, ataques de phishing y malware reales, entre otros. Los conocimientos detallados descubiertos por Security Lab sirven de base para las soluciones de ciberseguridad de última generación de Hornetsecurity.

Cómo utilizar este informe

Este informe se divide en cinco secciones:

El capítulo 1 contiene el resumen ejecutivo. Si solo te interesan los aspectos más destacados, recomendamos consultar esta sección.

El capítulo 2 se centra en el panorama actual de amenazas en torno a la plataforma Microsoft 365.

El capítulo 3 aborda las preocupaciones actuales y los debates sobre las amenazas y tendencias más significativas a partir de 2023.

El capítulo 4 contiene las predicciones de Security Lab sobre las amenazas a la ciberseguridad en 2024, junto con consejos y directrices para ayudar a proteger tu empresa.

El capítulo 5 enumera todas las referencias, enlaces de apoyo y conjuntos de datos utilizados en este informe.

Tabla de Contenidos

Capítulo 1 - Resumen ejecutivo

Aprovechando su enorme conjunto de datos de usuarios, Hornetsecurity se encuentra en una posición única para llevar a cabo un examen detallado de las amenazas basadas en el correo electrónico y destilarlo en ideas importantes para los profesionales de la seguridad informática. El email sigue siendo un canal de comunicación esencial. En nuestro análisis de más de 45.000 millones de correos electrónicos, el 36,4 % se clasifican como «no deseados». El 96,4 % de los emails no deseados son spam o se rechazan directamente debido a indicadores externos, y algo más del 3,6 % se marcaron como maliciosos.

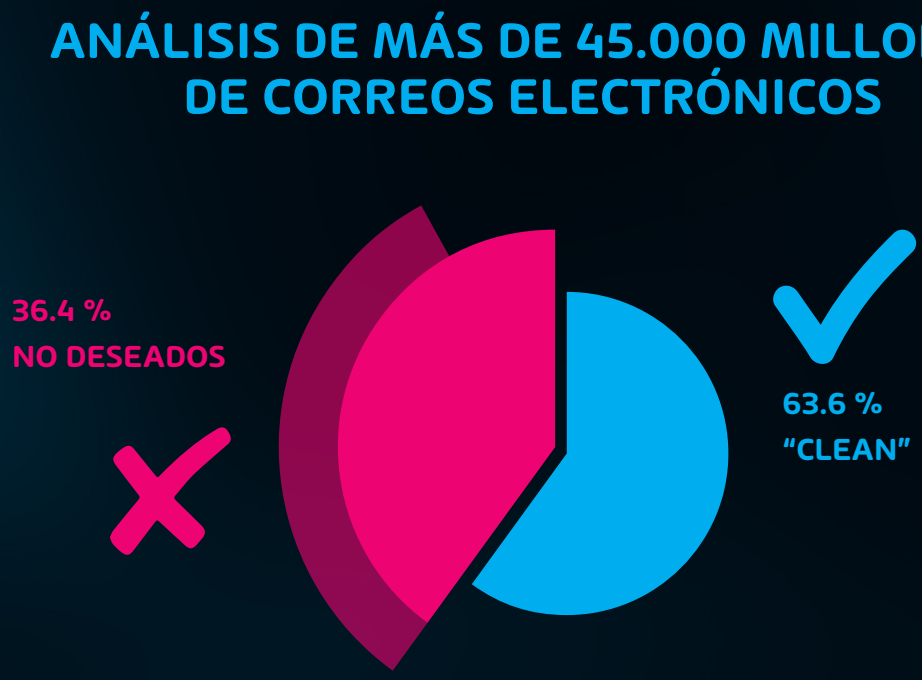


Fig. 1: Clasificación de correos electrónicos escaneados por Hornetsecurity

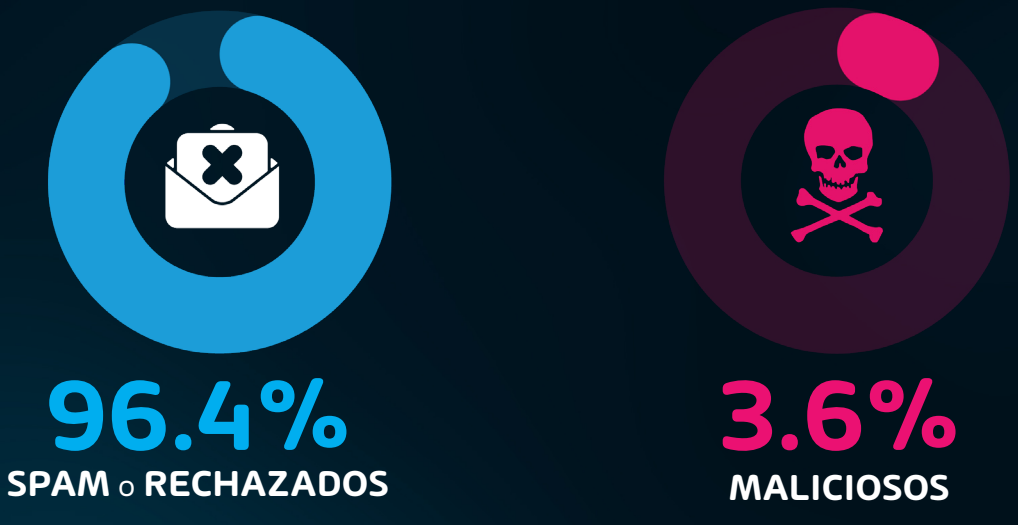


Fig. 2: Clasificación de correos electrónicos no deseados

Otra estadística de alto nivel que observamos cuando se trata de ataques basados en el correo electrónico es el estilo del ataque: nuestros resultados para este periodo de datos muestran que el phishing mantiene el primer puesto, representando el 43,3 % de los ataques basados en el email. Esto supone un aumento de casi el 4 % con respecto al año anterior. El segundo tipo de ataque más común durante 2023 fue el uso de URLs maliciosas en el correo electrónico, con un 30,5 %, lo que supuso un aumento significativo del 18 % con respecto al informe del año pasado.

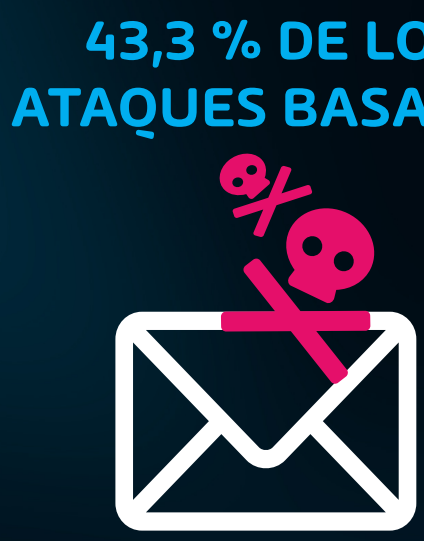


Fig. 3: Ataques basados en correo electrónico

Además de los tipos de ataques, también controlamos los tipos de archivos adjuntos que utilizan actualmente los agentes de amenazas para enviar cargas maliciosas. Los archivos HTML (37,1 %) y PDF (23,3 %) fueron los que se observaron con mayor frecuencia, junto con los Archive (20,8 %) en tercer lugar. El uso de archivos HTML experimentó un aumento del 16,1 % por parte de los agentes de amenazas a lo largo del periodo observado, así como un aumento del 11 % en el uso de archivos PDF. Esto fue impulsado en gran medida por amenazas como Qakbot y botnets similares que utilizan estos tipos de archivos para facilitar la propagación de su software. También cabe destacar un notable descenso del uso de archivos DOCX en un 9,5 % y de archivos XLSX en un 6,7 %. Estos tipos de archivo eran muy populares entre los creadores de amenazas y, desde que Microsoft desactivó las macros por defecto en Office, su uso se ha reducido drásticamente.

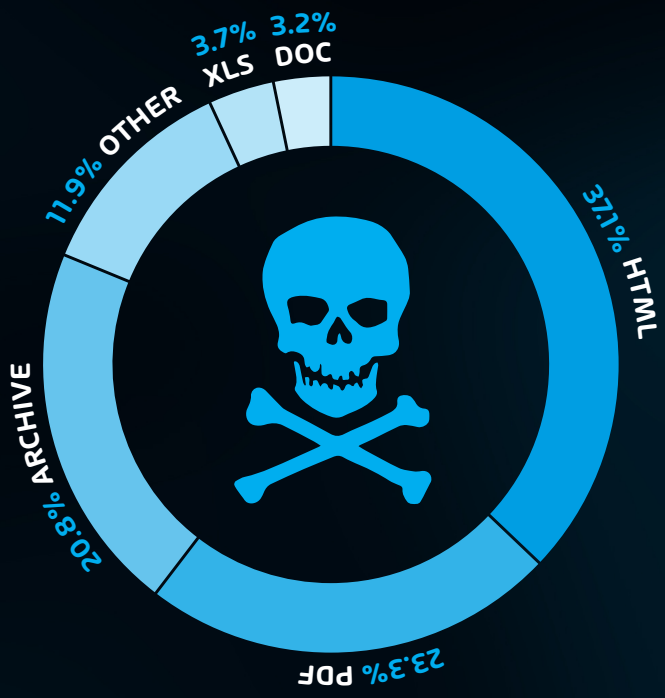


Fig. 4: Tipos de archivo más utilizados en emails maliciosos

El índice de amenazas por sector fue prácticamente el mismo en la mayoría de ellos durante el periodo de referencia. El índice de amenazas por correo electrónico es una medida con la que comparamos entre el número de emails clasificados como amenazas y el número de emails limpios entregados en función del sector. Esto proporciona una buena idea de los tipos de empresas que son actualmente objetivo de los agentes de amenazas. Al igual que el año pasado, nuestros datos muestran que casi todos los tipos de empresas están actualmente amenazados. En resumen, si tu organización tiene la capacidad de pagar un rescate, eres un objetivo. Sin embargo, las organizaciones de investigación, el sector del entretenimiento y la industria manufacturera se encuentran en la cúspide del espectro, con un número ligeramente superior de ataques contra estos tipos de organizaciones frente al resto.

Una última área de seguridad del correo electrónico que rastreamos es el uso de suplantaciones de marca. Esto nos ayuda a informar a nuestros equipos de producto, a nuestros clientes y a la comunidad sobre qué tipos de phishing orientado a marcas se están utilizando actualmente en el ecosistema. Nuestros datos para este informe muestran que las marcas de distribución siguen siendo una opción popular. Por ejemplo, DHL (26,1 %), Amazon (7,7 %) y FedEx (2,3 %) figuran entre los 10 primeros. Otros nombres destacados de la lista son Microsoft (2,4 %), LinkedIn (2,4 %) y Netflix (2,2 %). En la mayoría de estos casos, las amenazas buscaban credenciales de usuario final para venderlas o utilizarlas en otros ataques.

26.1%	DHL
7.7%	AMAZON
2.4	LINKEDIN
2.4	MICROSOFT
2.2	NETFLIX
2.3	FEDEX

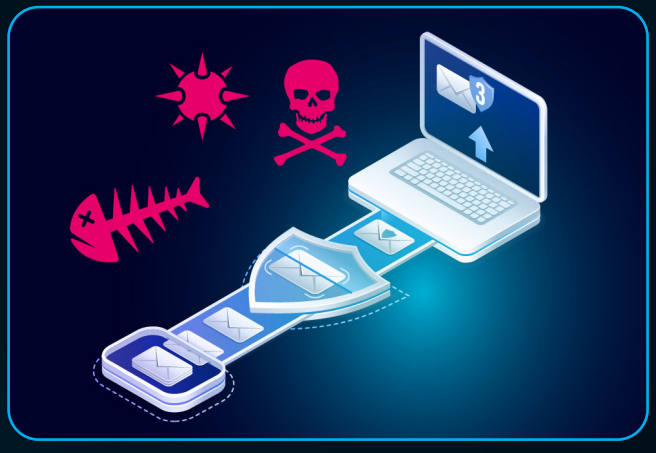
Fig. 5: Marcas/organizaciones explotadas para

La cuestión de la seguridad de los datos en el ecosistema cloud de Microsoft sigue ocupando un lugar importante en el debate actual sobre la nube. Varias brechas de seguridad recientes, incluida una protagonizada por una amenaza de estado-nación china, han hecho que muchos (incluido el Gobierno de EE. UU.) reevalúen su actitud de seguridad en la era de la nube. Esto también ha planteado la cuestión de la dependencia excesiva de los proveedores y el grado de confianza que las organizaciones deben depositar en un único proveedor.

Microsoft también ha cambiado su posición sobre la necesidad de realizar copias de seguridad de los datos de M365. Durante un período considerable fue un simple «no se necesitan copias de seguridad», ya que confiaba únicamente en las capacidades de retención integradas en M365. Sin embargo, Microsoft parece haber puesto fin a ese enfoque con una nueva aplicación de backup M365 y una API asociada que se anunciaron apresuradamente en verano. Dicho esto, en el momento de redactar este artículo no hay más novedades sobre este producto de backup.

Los permisos de objetos y recursos compartidos en M365 son temas que también tratamos en este informe. Teniendo en cuenta la facilidad para compartir y colaborar que ofrece M365, es muy fácil que los datos confidenciales se filtren fuera de los tenants de M365. Esto puede ocurrir por error o de forma malintencionada. SharePoint Online y OneDrive for Business han sido los «servidores de archivos» por excelencia de la era cloud durante algún tiempo, por lo que muchas organizaciones se enfrentan a la cruda realidad de tratar de gestionar el uso compartido y los permisos en M365 DESPUÉS de que hayan aumentado de forma descontrolada. Esta seguirá siendo un área que las empresas deberán tener en cuenta en 2024 y ante la que prepararse teniendo en cuenta el previsible incremento de fugas de datos a futuro.

El correo electrónico sigue siendo uno de los principales métodos que utilizan los agentes de amenazas para lanzar ataques, por lo que una sólida estrategia de seguridad del email es esencial para navegar por el complejo panorama de amenazas y desarrollar la resiliencia de la seguridad en 2023.



Capítulo 2 - Panorama actual de las amenazas en Microsoft 365

Cada año, el laboratorio de seguridad especializado de Hornetsecurity revisa el amplio conjunto de datos de la empresa y analiza el estado de las amenazas globales por correo electrónico y las estadísticas de comunicación. Además, el equipo realiza periódicamente ejercicios de prospectiva y aporta información sobre posibles amenazas futuras. Este capítulo se centra en la revisión de los datos desde el 1 de noviembre de 2022 hasta el 1 de noviembre de 2023, que constituyen la base de las proyecciones sobre la evolución del panorama de amenazas expuestas en el Capítulo 4.

Tendencias en seguridad del correo electrónico

A pesar del creciente uso de aplicaciones de colaboración y mensajería instantánea, como Microsoft Teams, el correo electrónico sigue siendo una de las principales áreas de preocupación en términos de ciberataques. Aunque hemos observado un ligero descenso en el número de correos electrónicos clasificados como amenazas (el 3,6 % este año, frente al 5,48 % del año pasado), el riesgo para las empresas de todo el mundo sigue siendo elevado. Los ataques se están volviendo más sofisticados que nunca y, con el aumento de los ataques basados en inteligencia artificial, las empresas deben mantenerse alerta y no caer en la complacencia en su actitud hacia la seguridad. A continuación se ofrecen datos más detallados.

Mediante la revisión de más de 45.000 millones de correos electrónicos recopilados durante el periodo de notificación actual (del 1 de noviembre de 2022 al 1 de noviembre de 2023), Security Lab ha llegado a las siguientes conclusiones:

Métricas de Spam, Malware y Amenazas Avanzadas

El correo electrónico sigue siendo uno de los principales métodos que utilizan los agentes de amenazas para lanzar ataques. Esto se ejemplifica en nuestros datos, que clasificaron el 36,4 % de todos los correos electrónicos como «no deseados», lo que significa que no son comunicaciones auténticas deseadas por el destinatario. El siguiente gráfico muestra nuestro desglose de correos electrónicos no deseados frente a los correos electrónicos limpios.

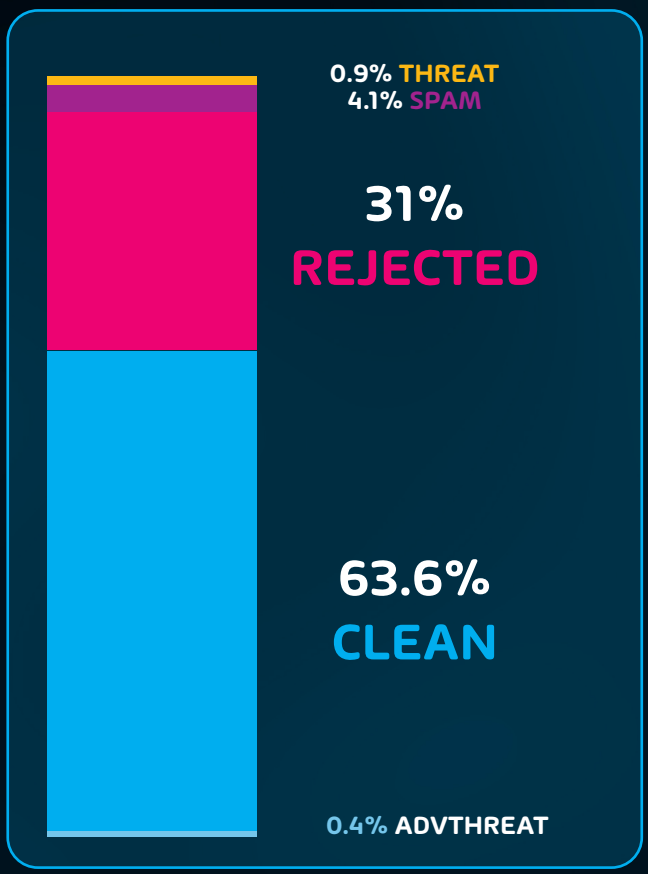


Fig. 6: Correos electrónicos no deseados junto con correos electrónicos limpios

Esta cifra contrasta con la del año pasado, en la que el 40,5 % de todos los correos electrónicos se clasificaron como «no deseados», lo que muestra un descenso (aunque ligero) de los emails no deseados de un año a otro en términos de porcentaje.

Teniendo en cuenta que en el informe del año pasado procesamos solo 25.000 millones de correos electrónicos, frente a los 45 000 millones de este año, el peligro actual que suponen las amenazas basadas en el correo electrónico sigue siendo ALTO.

Durante el periodo de datos analizado este año, encontramos el siguiente desglose de emails **no deseados**:

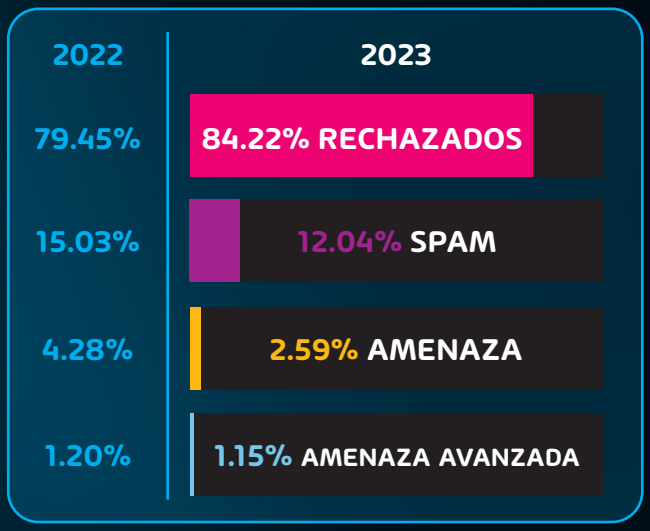


Fig. 7: 2023 Emails no deseados por categoría

CATEGORÍA	DESCRIPCIÓN
Spam	Estos emails no son deseados y suelen ser promocionales o fraudulentos. Este tipo de correos electrónicos se envían simultáneamente a un gran número de destinatarios.
Amenaza	Estos emails incluyen contenidos dañinos, como archivos adjuntos o enlaces maliciosos, o se envían para cometer delitos como el phishing.
Amenaza Avanzada	La protección contra amenazas avanzadas (ATP) ha detectado una amenaza en estos correos electrónicos. Los correos electrónicos se utilizan con fines ilegales e implican medios técnicos sofisticados que solo pueden repelerse mediante procedimientos dinámicos avanzados.
Rechazado	Nuestro servidor de correo electrónico rechaza estos correos directamente durante el diálogo SMTP debido a características externas, como la identidad del remitente, por lo que los correos no se siguen analizando.

NOTA: Para detallar un poco más, la categoría «rechazado» se refiere a los correos electrónicos que los servicios de Hornetsecurity rechazaron durante el diálogo SMTP debido a características externas, como la identidad del remitente o la dirección IP. Si un remitente ya está identificado como comprometido, el sistema no realiza más análisis. El servidor SMTP deniega la transferencia de correo electrónico justo en el punto inicial de la conexión basándose en la reputación negativa de la IP y la identidad del remitente.

Técnicas utilizadas en los ataques por correo electrónico

En nuestro análisis de emails observamos el siguiente desglose de los tipos de ataque utilizados en los ataques por correo electrónico:

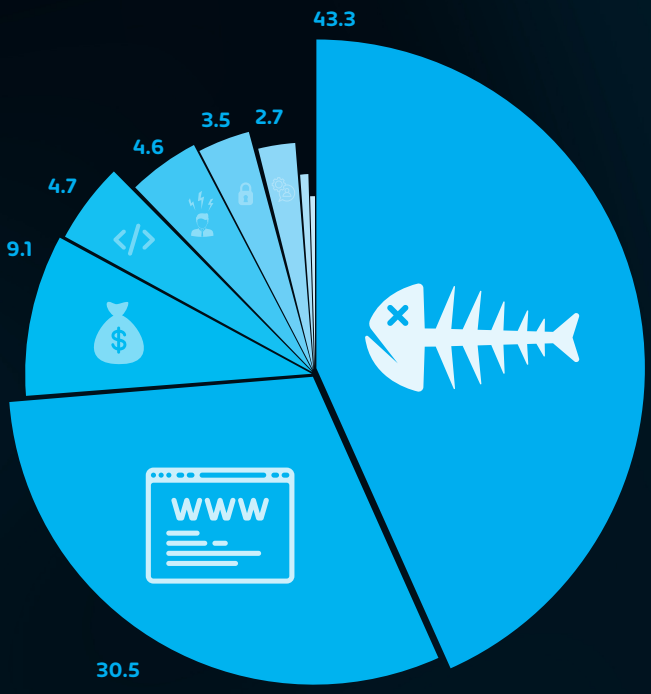


Fig. 8: Tipos de ataque en 2022 y 2023

Unsurprisingly, phishing and the use of malicious URLs remain near the top of the list and continue to be popular (and highly successful) attack types for threat actors. When looking at the data from last year (shown below), several comparisons can be made:

2022 %	2023 %	TÉCNICA DE ATAQUE
39.6	43.3	Phishing
12.5	30.5	URL
8.2	9.1	Estafa 419
1.8	4.7	HTML
3.7	4.6	Extorsión
3.5	3.5	Exe. en un archivo/imagen de disco
1.1	2.7	Suplantación de identidad
2.8	1.0	Maldoc (documento malicioso)
0.4	0.6	PDF

Fig. 9: Técnicas de ataque utilizadas en los ataques por correo electrónico en 2022 y 2023

Como era de esperar, el phishing y el uso de URLs maliciosas siguen ocupando los primeros puestos de la lista y continúan siendo tipos de ataque populares (y con gran éxito) para los agentes de amenazas. Si se observan los datos del año pasado (mostrados a continuación), pueden hacerse varias comparaciones:

La ingeniería social y las amenazas basadas en el correo electrónico siguen siendo dos de los principales métodos que utilizan los actores de amenazas para hacerse un hueco inicial en una organización objetivo. También hemos visto un aumento de los casos en los que los usuarios objetivo son manipulados socialmente para interactuar con un enlace malicioso, por lo que el uso de URLs maliciosas va de la mano del aumento general del phishing.

Uso y tipos de documentos adjuntos en los ataques

Los adjuntos en los emails siguen siendo uno de los métodos más utilizados para entregar una carga útil de ataque en 2023. Los agentes de amenazas siguen utilizando los archivos adjuntos para ocultar programas maliciosos y dar un aire de autenticidad a sus comunicaciones maliciosas. Además, algunos filtros rudimentarios de spam/malware pueden ser incapaces de escanear archivos adjuntos comprimidos, lo que aumenta el riesgo para ciertas organizaciones.

A continuación, se muestra el desglose de los tipos de archivos utilizados para la entrega de cargas maliciosas durante el periodo analizado:

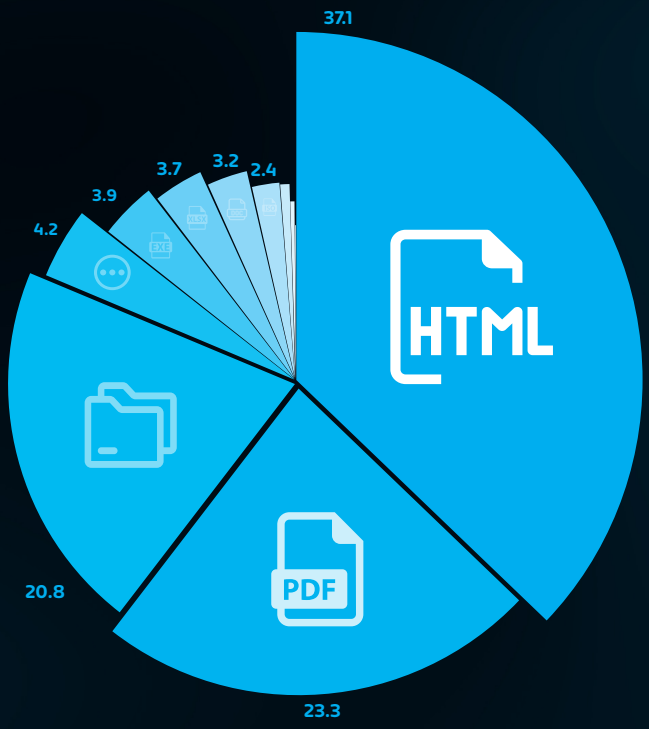


Fig. 10: Tipos de archivos con cargas maliciosas en 2023

A pesar de la disminución de los archivos HTML utilizados en los ataques por correo electrónico de la que hablábamos antes, HTML es el tipo de archivo adjunto número uno utilizado por los atacantes, con PDF en segundo lugar, seguido de Archive en tercer lugar. HTML, en primer lugar, no es ninguna sorpresa debido al hecho de que es un tipo de archivo que se puede leer y con el que se puede interactuar en casi cualquier plataforma. Independientemente del sistema operativo del usuario objetivo, el archivo HTML podrá abrirse, lo que aumenta las posibilidades de éxito para el agente de la amenaza.

Si comparamos los datos anteriores con los del año pasado (mostrados a continuación), hay una serie de diferencias que saltan a la vista.

	2022	2023	
HTML	21.0	37.1	HTML
PDF	12.4	23.3	PDF
ARCHIVE	28.0	20.8	ARCHIVE
OTROS	4.8	4.2	OTROS
EXE	4.3	3.9	EJECUTABLE
XLSX	10.4	3.7	EXCEL
DOC	12.7	3.2	WORD
ISO	5.4	2.4	ARCHIVO IMAGEN DISCO
SCRIPT	0.7	0.8	SCRIPT
ONENOTE	0.0	0.4	ONENOTE
EMAIL	0.1	0.1	EMAIL
LNK	0.1	0.0	LNK
PPTX	<0.1	0.0	POWERPOINT

Fig. 11: Tipos de archivos con cargas maliciosas en 2022 y 2023

En el último año ha habido cierta actividad entre los grupos de ciberdelincuentes y en el sector que puede explicar estos cambios. En cuanto al aumento de archivos HTML y PDF, podemos atribuirlo en cierta medida a Qakbot. A pesar de la detención de Qakbot por parte de las autoridades mundiales durante el verano de 2023, Qakbot aún tuvo bastante actividad este año. Además, se sabía que Qakbot utilizaba documentos HTML y PDF para ayudar en la infección de las máquinas objetivo. Dicho esto, este seguirá siendo un mecanismo de despliegue popular también para futuros operadores de malware/botnet.

El gran descenso en el uso de archivos DOCX y XLSX en comparación con el año pasado puede atribuirse a la nueva práctica de Microsoft de bloquear por defecto las macros en Office. Esto hace que estos tipos de archivos sean menos atractivos para los agentes de amenazas.

Índice de amenazas por correo electrónico por sectores

Una de las áreas clave que revisamos anualmente (y mensualmente) es el número de amenazas que se ciernen sobre diferentes sectores. Esto nos permite determinar si existen campañas determinadas o ataques dirigidos a determinadas empresas. Además, también proporciona algunas ideas que las empresas pueden utilizar para ayudar a determinar si están expuestas a un mayor riesgo de ataque o no.

Un cambio clave que observamos en los datos del año pasado fue el hecho de que el índice de amenaza era prácticamente el mismo en todos los sectores.

Dichos datos respaldan la conclusión de que no importa el sector empresarial al que pertenezca la empresa: si la organización tiene la capacidad de pagar un rescate, esta ES un objetivo. Los datos de este año (disponibles a continuación) muestran que la tendencia continúa. El índice de amenazas es prácticamente el mismo entre los diez principales sectores.

Sin embargo, algunos se han visto más afectados que otros.

- **Investigación:** Estas organizaciones acaban siendo objetivos simplemente por la propiedad intelectual que suelen manejar.
- **Entretenimiento:** Organizaciones que suelen dedicarse al juego, la venta de entradas, etc. se convierten en un objetivo debido a la gran cantidad de dinero que manejan. Un ejemplo de ello es el ataque de 2023 a MGM y Caesars Entertainment.
- **Industria manufacturera:** Tiene un largo historial como objetivo frecuente de las amenazas. Por lo general, se trata de amenazas contra la propiedad intelectual. Muchos ven este sector como un objetivo fácil para el ransomware y la interrupción de la producción debido a la naturaleza de la seguridad de su red y al hecho de que a menudo utilizan un gran número de dispositivos IoT inseguros.

La siguiente tabla muestra la clasificación del índice de amenaza por sector.

3.0	INVESTIGACIÓN
3.0	ENTRETENIMIENTO
3.0	INDUSTRIA MANUFACTURERA
2.9	MEDIOS
2.9	SALUD
2.7	TRANSPORTE
2.6	TURISMO
2.6	INDUSTRIA AUTOMOVILÍSTICA
2.5	UTILITIES
2.5	TECNOLOGÍA
2.5	EDUCACIÓN
2.4	OTROS
2.4	CONSTRUCCIÓN
2.4	MINERÍA Y METALÚRGICA
2.4	FINANZAS
2.4	AGRICULTURA
2.3	SERVICIOS PROFESIONALES
2.3	RETAIL
2.2	INMOBILIARIO
1.8	LOGÍSTICA
2.4	MEDIANA GLOBAL
99.3	MÁXIMO GLOBAL

Fig. 12: Índice anual de amenazas en la industria

NOTA: El valor del índice de amenazas se determina mediante el siguiente cálculo:

Porcentaje del índice de amenazas = número de correos maliciosos (amenazas + amenazas avanzadas) / (número de correos maliciosos (amenazas + amenazas avanzadas) + número de correos limpios) multiplicado por 100 - Se excluye el spam y el correo informativo.

Nota sobre la metodología

Las organizaciones, independientemente de su tamaño, reciben un número absoluto diferente de correos electrónicos. Por lo tanto, para comparar las organizaciones, calculamos el porcentaje de correos electrónicos de amenaza entre los correos electrónicos de amenaza y limpios de cada organización. A continuación, calculamos la mediana de estos valores porcentuales para todas las organizaciones dentro de la misma industria para formar la puntuación de amenaza final de la industria.

Suplantación de marca

La suplantación de marca sigue siendo una de las principales técnicas de ataque por correo electrónico dirigidas a los usuarios finales en 2023.

Las suplantaciones de marca durante el periodo de datos analizado siguen las tendencias habituales. DHL, Amazon y FedEx se mantuvieron entre los diez primeros afectados. Esta tendencia se repite desde hace tiempo. La pandemia del COVID impulsó un gran aumento de las compras online, y esa práctica se ha mantenido entre los consumidores desde entonces. Los agentes de amenazas lo saben y, si consiguen introducir un mensaje de phishing convincente relacionado con envíos en el buzón de correo del objetivo en el momento justo, tienen muchas posibilidades de éxito.

También destaca la inclusión de Microsoft, LinkedIn y Netflix entre los 10 primeros. La presencia de Microsoft aquí se debe principalmente a los intentos de obtener acceso a las credenciales de los servicios cloud de Microsoft mediante los populares ataques actuales de tipo adversario en el medio que utilizan kits de herramientas de proxy inverso como el kit de phishing W3ll. Estos tipos de ataque son expertos en eludir las protecciones MFA, y puede ser bastante difícil protegerse contra ellos.

La suplantación de las marcas LinkedIn y Netflix está un poco más matizada para los agentes de amenazas. Las cuentas de LinkedIn comprometidas dan a los atacantes acceso a grandes cantidades de información sobre la cuenta que han comprometido, junto con las conexiones de la cuenta comprometida. También hemos visto casos en los que los agentes de amenazas utilizan una cuenta de LinkedIn comprometida para atacar en última instancia a otro usuario de LinkedIn haciéndose pasar por una conexión comercial de confianza. La suplantación de la marca Netflix se considera principalmente un medio para apoderarse de cuentas y venderlas o intentar utilizar esas mismas credenciales en ataques de relleno de credenciales.

A continuación se muestran los datos relativos a este punto durante el periodo de referencia:

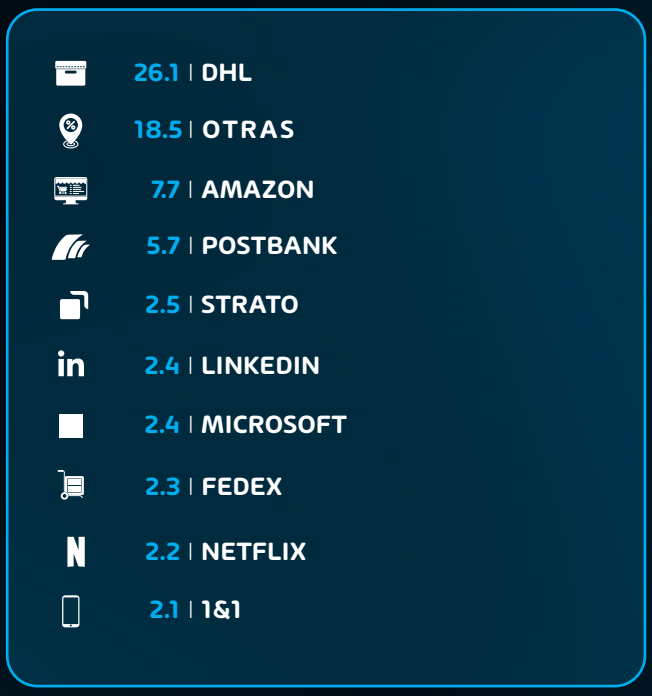


Fig. 13: Las 10 marcas más suplantadas anualmente

NOTA: Los datos sobre suplantación de marcas se ven muy afectados por las variaciones regionales. Algunas marcas alemanas figuran en esta lista debido a nuestra amplia cartera de clientes en este país.

Seguridad de los datos en la nube

Al hablar del estado de la seguridad en el entorno de Microsoft 365, debemos analizar mucho más que el correo electrónico. M365 ha cambiado la forma en que las organizaciones llevan a cabo sus negocios. Cada vez con más frecuencia, las empresas utilizan las funciones adicionales de M365, por lo que el debate sobre el estado de la seguridad de M365 debe traspasar las fronteras del correo electrónico.

En las secciones restantes de este informe se analizan muchas consideraciones de seguridad dentro de los servicios cloud de Microsoft, pero merece la pena discutir el estado general y la cultura de la seguridad actual de Microsoft que, dicho sea de paso, no son los mejores. Microsoft ha tenido varios problemas de seguridad en los últimos años. Por ejemplo, múltiples brechas de seguridad, como la situación Storm-0558, múltiples vulnerabilidades de Exchange Server locales, y la fuga de 32 TB de datos de una cuenta de almacenamiento en la nube.

Nota

Para un debate más exhaustivo sobre los recientes problemas de seguridad de Microsoft Cloud, consulte el episodio del podcast en el que los expertos Andy Syrewicze y Paul Schnackenburg hablan largo y tendido sobre este tema.

Todo esto pone en tela de juicio la idea del papel de Microsoft en la seguridad de las organizaciones. Actualmente, la cultura de seguridad de Microsoft está siendo cuestionada por muchas personas del sector, y sitúa en primer plano la idea de la excesiva dependencia de los proveedores.

¿Qué es la dependencia excesiva de los proveedores?

La dependencia excesiva de los proveedores es la práctica de poner muchos o casi todos los procesos y procedimientos fundamentales de la organización en manos de un único proveedor. El problema es que, si este proveedor tiene dificultades de algún tipo, la organización sufre de forma desproporcionada.
Aquí vemos algunos ejemplos:

1. Las copias de seguridad externas son desde hace tiempo un estándar de buenas prácticas en IT. Esto se aplica también a los datos almacenados en M365. Confiar en las capacidades de retención de M365 o aprovechar el producto de backup M365 de Microsoft (cuando finalmente se lance) es como almacenar las copias de seguridad en el mismo almacenamiento/plataforma que el sistema de producción. Si la nube de Microsoft no está disponible, posiblemente tampoco lo estén los métodos de recuperación de datos.
2. El tamaño y el alcance de la nube de Microsoft la convierten en un objetivo para los agentes de amenazas. Los atacantes saben que si vencen a Exchange Online Protection en un cliente, es probable que lo hagan en TODOS los clientes de M365. Este es un caso en el que una solución de seguridad de terceros puede proporcionar mejores capacidades que el proveedor nativo, especialmente contra ataques de alta intensidad.
3. Es raro, pero ha habido casos en los que la nube de Microsoft ha dejado de estar disponible durante un tiempo. En el último año se han producido varias interrupciones en Azure Active Directory (ahora llamado Azure Entra) que han imposibilitado a los clientes acceder a sus datos en M365.

Microsoft posee actualmente una cuota de mercado muy alta con Microsoft 365. Muchas personas en el sector cuestionan la práctica de utilizar el mismo proveedor tanto para el software de productividad/colaboración como para la seguridad. Existe un posible conflicto de intereses en el sentido de que, si hay un fallo o problema con uno de los productos de seguridad de dicho proveedor, es posible que NO revele o solucione adecuadamente dicho problema debido al riesgo de perder negocio.

Una vez más, cada organización debe tomar su propia decisión al respecto. Aun así, teniendo en cuenta los recientes problemas de seguridad y, en última instancia, hasta dónde llega la responsabilidad de Microsoft con respecto a los datos, la elección es fundamental.

¿De qué es responsable Microsoft?

Muchas personas se hacen la siguiente pregunta: «Si Microsoft no se ocupa de mis datos y mi seguridad, ¿de qué son realmente responsables?». La postura actual de Microsoft sobre esta cuestión sigue siendo la misma. Para entenderlo bien, debes estar familiarizado con el modelo de responsabilidad compartida de Microsoft.

La parte crítica es que el modelo de responsabilidad compartida afirma que «la responsabilidad de los siguientes elementos siempre la tiene el cliente»:

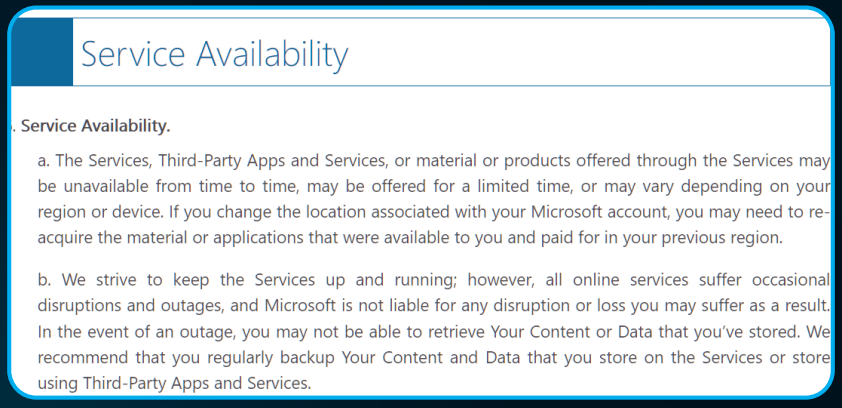
- Información y datos
- Dispositivos (móviles y PC)
- Cuentas e identidades

Básicamente, el cliente es responsable de asegurar y proteger su información y sus datos. Microsoft no se hace responsable de ello. A medida que las organizaciones se trasladan a la nube, deben tener esto en cuenta a la hora de implantar estrategias de protección.

Dicho esto, Microsoft ha cambiado en 2023 la posición que mantenía desde hace tiempo sobre el uso de aplicaciones de backup con M365. En un congreso a principios de este año, Microsoft anunció Microsoft 365 Backup, un servicio para proporcionar capacidades básicas de copia de seguridad para M365. A pesar de ello, se ha publicado muy poca o ninguna información adicional desde este escueto anuncio. Lo importante de este anuncio no es el servicio en sí, sino el cambio de la posición histórica de Microsoft de «no es necesario hacer copias de seguridad de los datos en M365». Muchas personas en el sector consideran que esto se ha visto impulsado por una de estas dos razones:

1. Microsoft finalmente ha capitulado y ahora está de acuerdo en que centrarse únicamente en la retención de datos NO es suficiente en M365.
2. Microsoft simplemente quiere un trozo del mercado de copias de seguridad M365 ahora que ha visto que existe un gran mercado para un servicio de este tipo.

Ambas opciones parecen probables, y la segunda se ve reforzada por el hecho de que también han lanzado una API de copia de seguridad que los proveedores pueden utilizar, previo pago. En cualquier caso, el mensaje es más claro que nunca. Las empresas **SON** responsables de la protección de los datos que almacenan en los servicios cloud de Microsoft.



Service Availability

. Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

Las dificultades de una correcta gestión de los permisos en M365

Otro reto especialmente preocupante para los informáticos son los permisos compartidos en los sitios de SharePoint y OneDrive para empresas. El entorno empresarial actual está formado por equipos virtuales de colaboración, a menudo en empresas distintas, que comparten documentos de diversas formas. No es factible bloquearlo (esto solo lleva a los usuarios a utilizar formas no autorizadas de compartir documentos en la nube, lo que afecta a la visibilidad de IT), pero tampoco se puede dejar la puerta abierta de par en par con enlaces a datos confidenciales que se comparten indiscriminadamente. Las herramientas integradas para gestionar esto en Microsoft 365 están fragmentadas en varios portales y son difíciles de manejar a escala, por lo que la gestión de permisos en la nube de Microsoft también es un área de gran preocupación en relación con el estado de la seguridad en M365. Dicho esto, el exclusivo 365 Permission Manager de Hornetsecurity facilita la gestión de las políticas de uso compartido en miles de cuentas, incluida la posibilidad de auditar quién tiene acceso a qué y alinear el acceso a diferentes sitios con la gestión de riesgos de la empresa.

Capítulo 3 - Análisis de los principales incidentes de seguridad y noticias sobre ciberseguridad de 2023

En 2023 se han producido varios ataques y problemas de seguridad notables que guardan relación directa con los datos recogidos para este informe. Esta sección se centra en los siguientes ataques:

Storm-0558

En los últimos 12 meses varios incidentes de seguridad de gran repercusión afectaron al servicio cloud de Microsoft 365, pero el más impactante fue sin duda el ataque Storm-0558. En resumen, el grupo de hackers chinos patrocinado por el estado que Microsoft designa como Storm-0558 comprometió la cuenta de un ingeniero en 2021. Aunque el entorno de producción estaba aislado de la red corporativa, en abril de 2021 un sistema de firma de consumidores (parte de Azure AD, ahora Entra ID) se bloqueó y generó un volcado de errores. Esto se trasladó a la red de producción para la depuración, y el sistema automatizado diseñado para detectar credenciales en los volcados falló.

Así, cuando los atacantes accedieron a esta cuenta, obtuvieron acceso al volcado y a la clave.

Esto les permitió acuñar sus propias claves, a pesar de que la clave en el volcado había caducado, y debido a un fallo en la separación de las claves de consumo (Hotmail, Xbox, etc.) de las claves corporativas (M365, Azure), el sistema para validar esto no se aplicó, solo documentó que las claves eran válidas. Esto ofreció a los atacantes esencialmente «la llave de una puerta trasera» para cualquier tenant de M365 (y cualquier tenant de Azure, aunque no hay pruebas de que se utilizase). En el momento de escribir este informe, «solo» se había producido la violación de algunas decenas de cuentas de correo electrónico del Departamento de Estado de Estados Unidos y el robo de 60.000 mensajes de correo electrónico.

Por lo tanto, se trata posiblemente de la brecha en la nube más grave de la historia, que compromete la plataforma de identidad de una forma que socava claramente la confianza en la nube y en las plataformas de Microsoft. Para ser claros, la detección de esta actividad maliciosa por parte de las empresas que utilizan M365 fue muy difícil, y solo en junio de 2023, un analista de seguridad de una agencia federal estadounidense detectó eventos MailItemsAccessed sospechosos e informó de ello a Microsoft y a la agencia CISA. Esta agencia solo disponía de estos registros porque pagó por la licencia M365 más alta de Microsoft, la E5.

Esta infracción ha tenido los siguientes resultados: Microsoft ha cambiado por fin su enfoque de la disponibilidad de registros para los distintos niveles de licencia, y todas las SKUs corporativas tienen ahora acceso ampliado a los registros. Esto se pidió por primera vez en 2020 tras el ataque a Solarwinds. Además, el próximo informe de la Junta de Revisión de la Ciberseguridad (CSRB) de Estados Unidos se centrará en esta brecha. Sin embargo, queda por ver si esta brecha obligará a Microsoft a ajustar cuentas y a mejorar su seguridad general, y en qué medida.

nOAuth

Otro fallo de seguridad, denominado nOAuth, explotaba el uso habitual de cuentas de correo electrónico como identificadores y aplicaciones registradas en Entra ID (antes Azure AD) que permitían iniciar sesión con cuentas de consumidores. Microsoft advierte explícitamente contra el uso del correo electrónico como identificador en estas reclamaciones, pero esto no disminuye la complejidad y los riesgos asociados con el registro de aplicaciones multi-tenant en Azure.

Ciberataques a MGM / Caesars Entertainment

Dos de las violaciones más notables de los dos últimos meses son las de los casinos MGM y Caesars. Aunque no presentan los mismos síntomas, ambos nos dan lecciones importantes para proteger a las empresas. En el caso de MGM, un atacante del grupo Scattered Spider utilizó ingeniería social en una llamada telefónica para engañar a un representante del servicio de asistencia para que restableciera todos los métodos de MFA de su cuenta de superadministrador de Okta,

que luego utilizó para configurar la federación y suplantar a los usuarios. Una vez comprometida, se filtraron 6 TB de datos, y los datos corporativos se cifraron en un ataque de ransomware.

MGM optó por no pagar y ha informado de que esperan que el coste total para ellos sea de 100 millones de dólares. Afortunadamente, su seguro de seguridad cibernética ofrecía una cobertura de hasta 200 millones de dólares. MGM sufrió interrupciones generalizadas de los sistemas mientras trabajaba en la recuperación. Sin embargo, el daño reputacional probablemente se extiende mucho más allá de lo monetario, especialmente porque los atacantes obtuvieron datos confidenciales de las interacciones con los clientes anteriores a marzo de 2019.

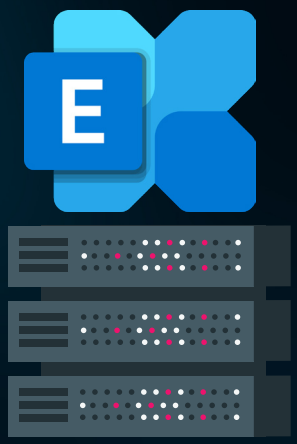
Caesars se vio comprometida a través de una brecha en un proveedor de servicios de IT de terceros, y optó por pagar el rescate (originalmente los atacantes querían 30 millones de dólares, pero se negoció hasta reducirlo a 15 millones de dólares).

De estas violaciones se pueden extraer varias lecciones para mejorar la ciberresiliencia de la organización:

- ¿El personal del servicio de asistencia técnica está lo suficientemente alerta como para detectar estos ataques? Es fundamental formar a los usuarios para que sean conscientes de todos los vectores de ataque, no solo de los emails de phishing. El vishing («phishing de voz») es más eficaz que un simple correo electrónico, sobre todo porque a menudo los datos personales necesarios para suplantar la identidad de alguien están a disposición del público general en LinkedIn, Facebook y sitios web de empresas. El qishing (suplantación de identidad mediante códigos QR) es otro método cada vez más popular.
- No permitir que el servicio de asistencia técnica restablezca la MFA y las contraseñas de las cuentas con privilegios especiales. Es fundamental tener en cuenta que la autenticación sea tan fuerte como sus métodos de restablecimiento, y si alguien puede engañar a un usuario del servicio de asistencia para añadir o resetear métodos de MFA, a menudo se llega al «game over».
- Supervisar y alertar sobre la adición de organizaciones federadas en su IdP (proveedor de identidades), ya sea Okta, Ping, Entra ID en Microsoft 365 o Google. Este vector fue utilizado por los atacantes en la brecha de Solarwinds en 2020, y sigue siendo popular.
- Exigir pruebas de ciberresiliencia a los proveedores externos. Las empresas modernas están entrelazadas, de modo que, incluso aunque su personal lo haga todo bien, es posible que sufra una infracción debido a la falta de seguridad de un proveedor de confianza.

Vulnerabilidades de Microsoft Exchange

Algunas organizaciones todavía ejecutan Exchange Server de forma local, a menudo en una configuración híbrida con Microsoft 365. Estos servidores siguen siendo un objetivo principal para los atacantes: en 2021 tuvimos ProxyShell, seguido de ProxyNotShell en 2022, y luego en agosto de 2023 se publicaron parches para tres vulnerabilidades de ejecución remota de código. En total, hubo 31 vulnerabilidades de Exchange Server en 2021, 18 en 2022 y 23 (hasta ahora) en 2023. Nuestra recomendación es retirar los servidores Exchange locales y completar la migración a Exchange Online lo antes posible.



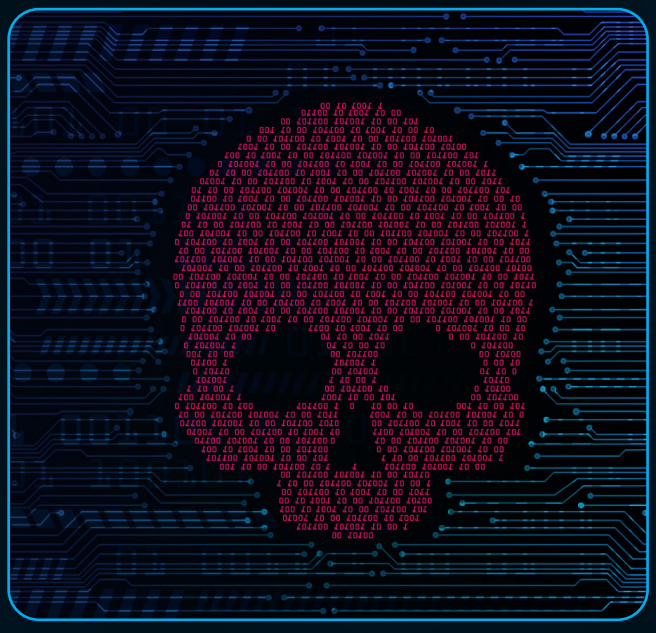
AÑO	VULNERABILIDADES DEL SERVIDOR EXCHANGE
2023	23 hasta ahora
2022	18
2021	31

Fig. 14: Vulnerabilidades del servidor Exchange

La disrupción de Qakbot

Qakbot era una conocida botnet maliciosa utilizada por los agentes de amenazas durante un período de tiempo significativo. Esta botnet fue responsable de innumerables ataques en toda la web, y los medios de ciberseguridad y los investigadores de seguridad (¡incluidos nosotros!) se ocuparon ampliamente de ella.

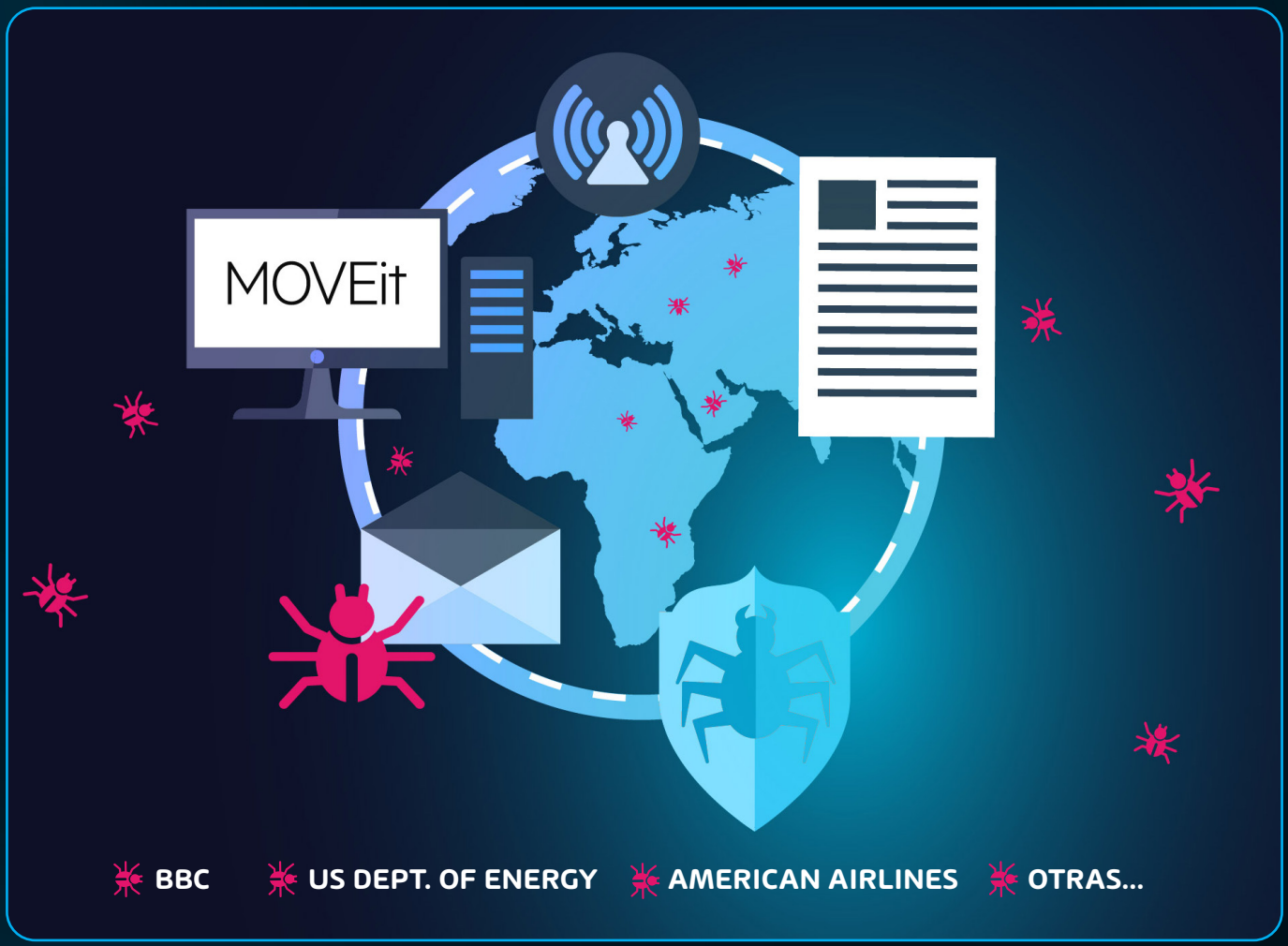
En agosto de este año, el FBI y otras fuerzas de seguridad de todo el mundo lograron controlar y cerrar la botnet Qakbot. Aunque esto es sin duda positivo, deja un cierto vacío. Los agentes de amenazas asociados con Qakbot no van a renunciar a los ataques, sino que trabajarán para traer de vuelta a Qakbot o se trasladarán a otras herramientas. Como ya comentamos en un episodio del podcast de Security Swarm, el malware DarkGate parece ser un posible candidato a llenar el vacío dejado por Qakbot. Los equipos de seguridad tendrán que estar atentos a este malware y a otros en 2024.



El ataque a la cadena de suministro MOVEit

No sería un año completo en noticias de ciberseguridad sin grandes ataques al estilo de la cadena de suministro. En 2023 se produjeron varios ataques de este tipo, pero el de la cadena de suministro MOVEit fue, con diferencia, el peor. MOVEit es una aplicación informática que ofrece servicios de transferencia de archivos para un gran número de empresas de todo el mundo. El ataque consistió en la explotación de varias vulnerabilidades (principalmente de inyección SQL) en el código base de MOVEit y se utilizó para robar la información personal de innumerables víctimas. Entre las víctimas se encontraban organizaciones como la BBC, el Departamento de Energía de Estados Unidos y American Airlines, entre otras.

Este tipo de ataque sigue poniendo de relieve la necesidad de contar con procesos de aplicación de parches eficaces y ágiles en los departamentos de IT de las empresas. A pesar de la publicación de mitigaciones y parches, muchas organizaciones han seguido siendo vulnerables a estos ataques durante demasiado tiempo. Por lo tanto, la industria de la seguridad y los proveedores de software deben seguir trabajando en soluciones para mitigar el impacto de futuros ataques a la cadena de suministro.



¿Acertamos con las predicciones del año pasado?

En el informe de ciberseguridad del año pasado hicimos algunas predicciones sobre el tipo de ataques que veríamos en 2023, y en gran medida acertamos.

Algunos grupos delictivos aprovecharon la «pasividad» percibida de los objetivos gubernamentales del hemisferio sur, con Costa Rica, Ecuador y Chile en 2022, seguidos de Brasil, Bermudas y Colombia en 2023, por no mencionar numerosos objetivos en la región de Asia Oriental. Nosotros pensábamos que el Business Email Compromise superaría al ransomware como el vector de ataque más popular, pero resulta que el «negocio» del ransomware sigue gozando de buena salud, y se dirige a su segundo año de mayores ingresos en general en 2023, con alrededor de 900 millones de dólares (tras los 939 millones de dólares en 2021).

Las técnicas para eludir la MFA están aumentando su sofisticación y facilidad de uso, tal como predijimos, dado el crecimiento de las empresas que protegen la identidad con MFA. También estamos encontrando atacantes a empresas utilizando los mensajes externos de Teams como señuelos de phishing, y muchos usuarios no son conscientes de este vector, pero el hecho de que el nuevo cliente de Teams no esté construido en Electron al menos hará que el cliente esté más seguro.

El robo de tokens de una máquina comprometida y su posterior reutilización en nuevos ataques ha aumentado, como también lo ha hecho el robo de cookies en general para ayudar al robo de identidad, personificado en el desmantelamiento del mercado Genesis por parte del FBI en abril de 2023 en la operación Cookie Monster.

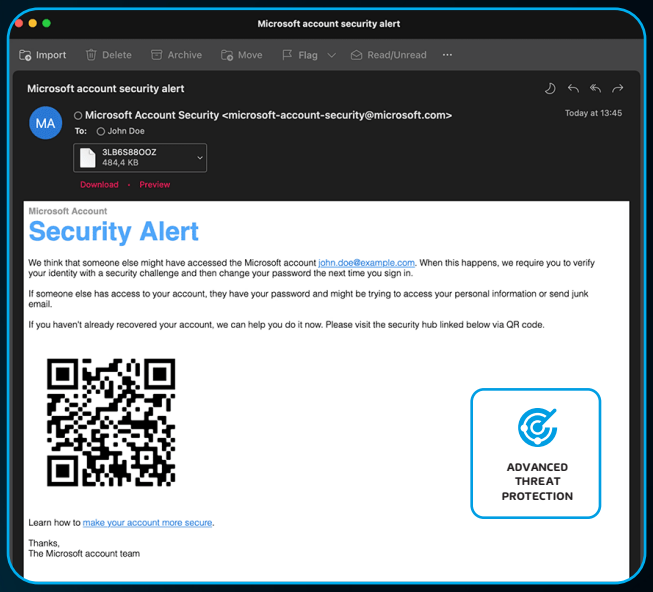
También analizamos los programas espía para móviles y su importancia, ya que varios países utilizan Predator y Pegasus no solo para espiar a delincuentes, sino también a disidentes, enemigos políticos y periodistas (Grecia es un ejemplo).

Microsoft 365 como plataforma no se ha vuelto menos compleja de configurar de forma segura. Como predijimos, el tiempo que transcurre entre que se hace pública una vulnerabilidad y se pone a disposición el código de explotación es cada vez más corto, lo que supone un reto para los equipos de SOC.

Las operaciones de información (OI) y la desinformación son un riesgo cada vez mayor para las empresas y la sociedad en general, especialmente con la falta de moderación de contenidos de X (antes Twitter) bajo la nueva dirección como ejemplo destacado, y con ChatGPT y otras IA generativas de Large Language Model facilitando más que nunca la producción de desinformación a escala.

Una «predicción» que no figuraba en el Informe sobre ciberseguridad del año pasado, pero que ha resultado especialmente destacada recientemente, es la inclusión del phishing de correo electrónico mediante códigos QR en la plataforma de Advanced Threat Protection de Hornetsecurity. En los últimos meses se ha observado un enorme aumento de este vector de ataque, ya que otras soluciones de higiene del correo electrónico tienen dificultades para proteger a los usuarios finales contra los enlaces maliciosos incrustados en códigos QR.

Por último, acertamos al predecir el auge de las soluciones sin contraseña, aunque no vimos que las passkeys se popularizaran tanto como en el ámbito de consumo.



Los ataques a las APIs también están aumentando rápidamente, como decíamos en el informe del año pasado, y este es un ámbito en el que los equipos de seguridad tendrán que centrarse, ya que a menudo se trata de infraestructuras «ocultas en segundo plano» que apenas se supervisan. La brecha en Optus en Australia (10 millones de clientes) a finales de 2022 es un ejemplo, pero hay muchos otros.

Predicciones de Security Lab para 2024

Cada año, como parte de este informe, el equipo de Security Lab de Hornetsecurity examina el estado del sector, nuestros datos, las tendencias de ataque y más información para hacer una serie de predicciones para el próximo año. Esto sirve para informar a las empresas de las posibles amenazas a las que pueden enfrentarse el año que viene, también de cómo puede cambiar el sector. Estas son las predicciones de Security Lab para 2024:

La Inteligencia Artificial seguirá impulsando el sector de la ciberseguridad

Con el lanzamiento de ChatGPT de OpenAI a finales de 2022, y su creciente popularidad a principios de 2023, la Inteligencia Artificial generativa comenzó rápidamente a alterar el sector de la ciberseguridad. Además, se ha hecho evidente de inmediato que la IA generativa podría ser utilizada por agentes de amenazas novatos no solo para lanzar ataques, sino incluso para aprender CÓMO lanzarlos. De hecho, en el Security Lab investigamos este tema y compartimos algunas de nuestras conclusiones en el primer episodio del podcast Security Swarm.

Estas nuevas capacidades impulsaron un aumento de los ciberataques a lo largo del año y siguieron elevando aún más el nivel de preocupación. Sin embargo, hay esperanzas sobre el uso de la IA generativa por parte de los agentes de amenazas: el hecho es que los atacantes experimentados ya tenían estas habilidades, por lo que los agentes de amenazas novatos que buscan aprovechar herramientas como ChatGPT para lanzar ataques todavía tienen que dedicar una cantidad considerable de tiempo a comprender toda la cadena de ataque para un ataque determinado, debido al hecho de que la IA generativa no es capaz de hacer eso por ellos.

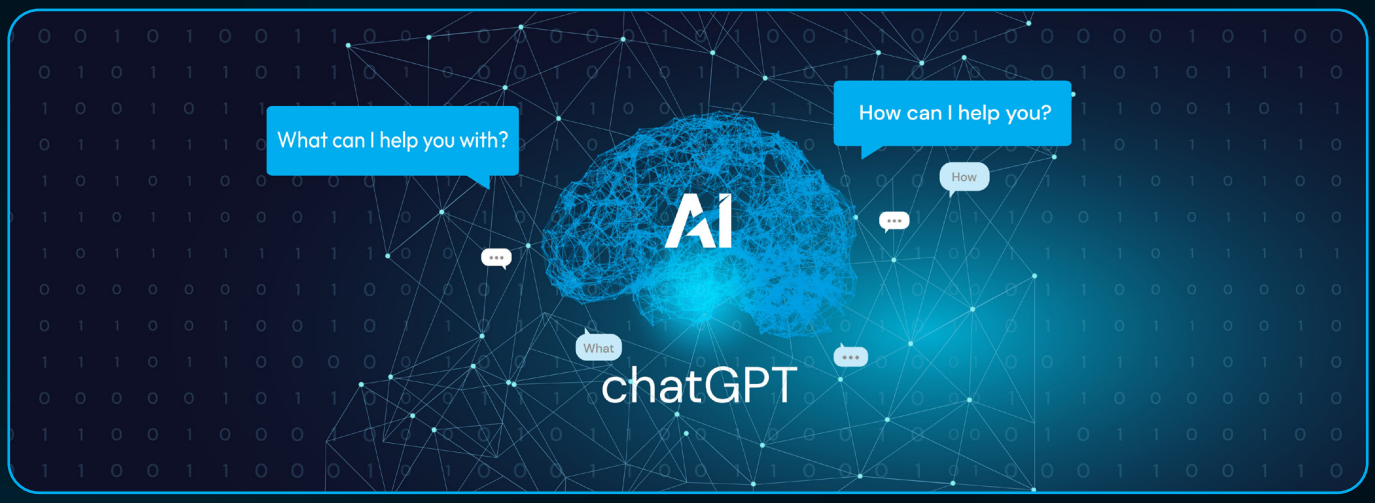
Dicho esto, una de nuestras predicciones para el próximo año es que los agentes de amenazas seguirán desarrollando sus variantes de dark web de ChatGPT (como DarkBERT y

WormGPT) para comprender mejor y poder automatizar partes adicionales de la cadena de ataque. Esto dará lugar a más capacidades para los agentes de amenazas novatos y acelerará el ritmo de los ciberataques en el sector. La capacidad de los modelos de lenguaje de gran tamaño (LLM) para traducir textos a otros idiomas de forma creíble también abre «nuevos mercados» para los delincuentes, sobre todo, porque muchos de esos países no están tan acostumbrados culturalmente a los ataques de phishing, por ejemplo.

Además, un ataque potencialmente interesante que aún no hemos visto a gran escala es un ataque de un agente de amenazas CONTRA un servicio de IA generativa. Lo más probable es que esto se hiciera de forma encubierta, y que el objetivo final fuera envenenar las respuestas de la IA con el único fin de difundir información errónea. Cualquier ataque de este tipo será muy sofisticado y muy probablemente estará dirigido por un estado-nación cuando se produzca, si es que se produce.

Aunque las noticias sobre ciberseguridad se han centrado casi por completo en las repercusiones negativas de la IA generativa en nuestro sector, también hay buenas noticias. A medida que prosigue la carrera armamentística de la ciberseguridad, los expertos en seguridad y los proveedores están poniendo en práctica la IA generativa también en los conjuntos de herramientas defensivas. Incluso ha habido algunas iniciativas de organizaciones de IA, como OpenAI, que han creado programas de subvenciones diseñados específicamente para ayudar a las organizaciones de ciberseguridad a «habilitar sus ofertas para la IA». Predecimos que esto se manifestará de varias maneras, desde el uso de la IA para la detección de valores atípicos, análisis de registros, ataques simulados (ver a continuación), modelado de amenazas y más.

Las empresas tendrán que mantenerse al tanto de estas evoluciones y ajustar su actitud de seguridad en consecuencia en el próximo año.



Los LLM como compañeros de combate para Blue Teams

En realidad, esta predicción entra dentro del debate anterior sobre la IA generativa, pero es lo bastante interesante como para merecer su propia sección.

Una cosa que históricamente ha sido difícil para los Blue Teams son las simulaciones adecuadas de agentes de amenazas. Usted puede contratar a una organización externa, o poner en nómina a su propio penetration tester, pero su visión del entorno de destino es probable que sea sesgada por el conocimiento previo del entorno. El coste también podría ser un problema.

Se trata de un ámbito en el que los modelos de lenguaje de gran tamaño (LLM) podrían desempeñar un papel importante en las operaciones de seguridad. Un atacante simulado por IA podría ejecutar múltiples simulaciones de ataque contra su organización. Esto no solo desempeña un papel importante para encontrar vulnerabilidades desconocidas en su infraestructura, sino que también sirve para formar a los miembros del equipo sobre cómo responder con seguridad durante un ataque.

Nuestra predicción es que los LLM empezarán a utilizarse en nuevas soluciones de software en un esfuerzo por cubrir esta necesidad.

Tecnologías como Co-Pilot impulsarán la necesidad de aumentar la seguridad del código y la exploración de su calidad

Otra predicción importante relacionada con la IA es que tecnologías como Co-Pilot facilitan más que nunca la codificación. Sin embargo, plantean un problema evidente: si un enorme número de programadores utiliza código generado con Co-Pilot, ¿no existe la posibilidad de que se genere código similar en múltiples respuestas? ¿Qué pasaría si un servicio como Co-Pilot fuera víctima de un ataque de envenenamiento de los LLM como el que hemos mencionado antes? Además, ¿podrían los actores de amenazas utilizar Co-Pilot como modelo para ver cómo los objetivos pueden estar creando aplicaciones?
Teniendo claro este problema, las organizaciones deberían hacer lo siguiente:

1. Verificar que el código generado por Co-Pilot es único y no dará lugar a litigios.
2. Verificar que el código sea lo suficientemente único (y seguro) como para que no sea un objetivo fácil para los agentes de amenazas.
3. ¿Cómo saben las empresas que el código generado por las herramientas de IA está libre de código malicioso?
4. ¿Cómo construyen las empresas los procesos necesarios en torno a este tipo de herramientas para hacer una revisión adecuada del código que aborde los puntos anteriores?

Nuestra predicción es que todas estas preocupaciones impulsarán la necesidad de mejorar la seguridad de los códigos y los procesos de escaneado de calidad en el próximo año.

Se prevé un aumento de los ataques para eludir la MFA

Los ataques para eludir la MFA aumentarán en volumen y sofisticación. A medida que las empresas en general adoptan formas de autenticación más sólidas que el nombre de usuario y la contraseña, el «mejor amigo» del delincuente, los atacantes se adaptan. Actualmente han aparecido varios «kits para eludir la MFA» que simplifican el proceso de configuración de un proxy para que actúe como atacante en el medio, presentando una página de inicio de sesión convincente para el usuario, y cuando este introduce sus credenciales (incluida una solicitud de MFA), estas se pasan a la página de inicio de sesión real, con lo que el usuario inicia sesión en el servicio legítimo, mientras que el kit obtiene una copia de las cookies de sesión, lo que permite al atacante hacerse pasar por el usuario. Algunos ejemplos son Evilginx (código abierto), el panel W3LL y las herramientas asociadas para facilitar el Business Email Compromise. Las distintas tecnologías de MFA tienen puntos fuertes diferentes, por tanto, asegúrate de que tu empresa utiliza las más potentes para acceder a datos y aplicaciones sensibles.

Aumento de la adopción de XDR y MDR

La tendencia y la necesidad de aumentar la seguridad en la industria no hacen sino acelerarse. En consecuencia, prevemos un aumento de la adopción de soluciones XDR (detección y respuesta ampliadas) y MDR (detección y respuesta gestionadas) en todos los sectores. Dada la naturaleza omnipresente de las ciberamenazas, ninguna solución por sí sola constituye una protección adecuada. Las empresas deben adoptar un enfoque multicapa, que incluya el registro y la difusión adecuados de los eventos de seguridad en todo el patrimonio digital de la organización. Sin la visibilidad adecuada, muchos ataques pasan completamente desapercibidos, por lo que los CISOs y los líderes tecnológicos están empezando a dar prioridad a su nivel de visibilidad de la seguridad.

Aumento de los ataques a la cadena de suministro

Los ataques a la cadena de suministro no son algo realmente nuevo para nosotros en el sector. Recientemente ha habido una serie de ataques a cadenas de suministro, como un ataque a la cadena de suministro en marzo de 2023 que involucró a 3CX, así como el conocido ataque a MOVEit a principios del verano de 2023. El problema de este tipo de ataques es el impacto potencial. Los dos casos mencionados ponen en peligro a innumerables organizaciones y los datos privados de millones de personas.

A medida que los servicios digitales se arraigan en nuestra sociedad, adquieren mayor alcance y, en última instancia, se convierten en un objetivo más fácil de alcanzar. Los agentes de amenazas saben que, si consiguen vulnerar a un proveedor que ofrezca un servicio de este tipo, es más probable que consigan un gran botín.

No solo pueden pedir un rescate por los datos, sino que muchos también venden estos datos en la dark web en una campaña de doble extorsión. Sin embargo, este no es el único riesgo. En el caso del ataque a la cadena de suministro de MOVEit, el exploit permitió a los atacantes acceder fácilmente a todas las organizaciones afectadas. Así, en lugar de poder atacar a una sola organización, TODAS las empresas que utilizan el software afectado corren el riesgo de sufrir una fuga de datos, además de extorsiones.

Por lo tanto, podemos predecir fácilmente que este tipo de ataques continuará e incluso aumentará el año que viene.

La complejidad de la nube seguirá provocando incidentes de seguridad

Una de las predicciones que hicimos el año pasado se centraba en cómo la creciente complejidad de la nube provocaría más incidentes de seguridad. Esta predicción continúa para el año que viene.

A medida que las empresas siguen adoptando tecnologías en la nube a gran velocidad, y con el aumento de las innovaciones relacionadas con la nube en el sector, la seguridad parece a veces algo secundario. Ha habido innumerables ejemplos de cubos de Amazon S3 que se han dejado sin protección, e incluso una filtración de 38 TB de datos de Microsoft debido a una cuenta de almacenamiento de Azure mal configurada. Estos son solo algunos ejemplos relacionados con el almacenamiento en la nube. Eso sin contar la adopción masiva de APIs en la nube, las configuraciones de red cada vez más complejas, la creciente mano de obra que trabaja desde cualquier lugar, etc. Con estas complejidades, aumenta la probabilidad de cometer errores, lo que dará lugar a nuevas brechas el año que viene.

El aumento de la adopción del 5G y la dependencia de las VNI de fragmentación de redes por parte de las operadoras impulsarán los ataques a redes móviles

Los dispositivos móviles se han convertido en omnipresentes en la vida cotidiana. En un intento por seguir el ritmo de la insaciable necesidad de más ancho de banda de la sociedad, la mayoría de las operadoras de telefonía móvil han desplegado la infraestructura 5G en sus redes.
Para facilitarlo, muchos operadores han empezado a recurrir a una estrategia conocida como «fragmentación de la red». Aquí, el operador dividirá su red en varias redes lógicas a distintos niveles y utilizará redes definidas por software (SDN) para gestionar el enrutamiento, la conmutación y el tráfico.

El problema de las redes definidas por software es la parte del «software» en la ecuación. El software es (generalmente) más difícil de mantener seguro, y puede ser aprovechado por los agentes de amenazas para lanzar ataques. De hecho, la NSA y la CISA han publicado un informe sobre los peligros de la fragmentación de redes y han proporcionado algunas orientaciones sobre esta práctica.

Dicho todo esto, con el aumento de la huella del 5G, la creciente dependencia de las redes móviles y la mayor dependencia de las SDN, esperamos ver más ataques en el próximo año centrados en las redes móviles.

Agentes de amenazas más hábiles y tiempos de permanencia más cortos

A medida que los grupos de ransomware se vuelven más hábiles y complejos, observamos un esfuerzo renovado por ejecutar los ataques en un tiempo récord. En consecuencia, el tiempo de permanencia se ha reducido significativamente en el último año, y esperamos que esta tendencia continúe. El tiempo de permanencia es la cantidad de tiempo que los agentes de amenazas permanecen en las redes antes de emprender acciones agresivas que puedan alertar a los sistemas de seguridad o dar a conocer su presencia. Con el aumento de los días cero y un sector de la ciberseguridad que corre frenéticamente para seguirles el ritmo, los atacantes saben que deben ejecutar sus ataques en un tiempo récord antes de que se pongan en marcha las medidas de defensa.

Una vez más, esto apunta al hecho de que seguimos viendo pruebas de que los grupos de agentes de amenazas son cada vez más sofisticados (CONTI, por ejemplo). Estos grupos están probando activamente nuevas vulnerabilidades, estudiando las aplicaciones antivirus e ideando soluciones y exploits. Todo esto apunta a una mayor probabilidad de que aumenten los ataques de ransomware, así como a un esfuerzo deliberado por eliminar las copias de seguridad de los datos en el próximo año.

Novedades sobre computación cuántica y cifrado

En el informe del año pasado incluimos un riesgo futuro: que la computación cuántica pueda romper fácilmente los estándares de cifrado actuales. A diferencia de otros riesgos de este informe, este no es inminente (los servicios de computación cuántica disponibles en el mercado siguen siendo muy propensos a errores), pero dado que los datos cifrados y el tráfico de red registrado hoy podrían descifrarse fácilmente en el futuro, es importante empezar a planificarlo.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Agencia de Seguridad Nacional (NSA) y el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos están de acuerdo y acaban de publicar esta breve hoja informativa. Tres de las cuatro normas que mencionamos el año pasado son ahora proyectos de normas y se espera que estén finalizadas en 2024.

¿Qué riesgo correrá mi organización en 2024?

La respuesta corta y simple aquí es, de nuevo, que si tu organización es capaz de pagar un rescate, tu organización ES un objetivo. Así lo demuestran nuestros datos relativos al índice de amenazas por correo electrónico en todos los sectores. Dicho esto, si tu organización maneja datos confidenciales, participa en el espacio de defensa o en infraestructuras críticas, o posee propiedad intelectual de gran valor, se convierte en un objetivo de mayor prioridad.

¿Qué deben hacer las organizaciones para defenderse?

Empezar por lo básico

Las organizaciones tienden a reaccionar ante amenazas específicas y a adquirir soluciones de seguridad puntuales para cada área, centrándose así en soluciones tecnológicas, en lugar de cubrir primero los aspectos básicos de la higiene de la seguridad. La gran mayoría de las empresas que sufren ataques no son víctimas de un oscuro exploit ni de una técnica de hacking avanzada. Sus defensas fallan porque no implantaron una autenticación fuerte (MFA, preferiblemente hardware resistente al phishing), permitieron contraseñas simples, configuraron a los usuarios como administradores locales en sus dispositivos o no formaron a los usuarios para que tuvieran cuidado al hacer clic en enlaces de correos electrónicos. No validar las copias de seguridad probando los procedimientos de restauración puede causar un gran problema en un ataque de ransomware, al igual que tener una política de parches laxa.

En otras palabras, es fundamental ocuparse primero de la higiene básica de la seguridad, que incluye la tecnología, los procesos y las personas. Empezar con una mentalidad de confianza cero:

- **Verifica cada conexión:** que un dispositivo esté gestionado no lo convierte automáticamente en seguro, y que un usuario se conecte desde una red conocida no significa que no se trate de un atacante que utiliza credenciales robadas.
- **Utiliza el mínimo privilegio:** concede a los usuarios y a las identidades de carga de trabajo los permisos que necesitan para desempeñar su función y realiza revisiones periódicas para asegurarte de que los permisos concedidos no se acumulan.
- **Asume que se producirá una violación:** construir las defensas tan fuertes como permita el presupuesto, pero también analizar los posibles escenarios cuando fallen. Si un atacante compromete a un usuario, ¿cómo se detectará? ¿Cómo se puede limitar la capacidad de un atacante para moverse lateralmente en el entorno?

Una lista más completa está disponible en los mandamientos ZT de Open Groups.

La cultura devora a la estrategia

El proceso de transformar la organización en una empresa ciberresiliente llevará tiempo, esfuerzo y persistencia. No se puede convertir una empresa en una ciberfortaleza bien defendida sin implicar a todos los miembros y ayudarles a ver cómo les afecta, y por qué deben formar parte de la solución.

A la hora de implantar una MFA, asegúrate que la alta dirección predica con el ejemplo y que ellos (y la junta directiva) entienden la razón de añadir la fricción adicional para la autenticación. Parte de este cambio cultural consiste en comprender que la ciberresiliencia no es solo tarea de los departamentos de IT o de seguridad. IT no puede proteger cargas de trabajo que desconoce, y si el departamento de marketing está desplegando un sitio web y una solución SaaS de seguimiento de clientes potenciales sin

involucrar al área de IT y seguridad, el riesgo que esto implica pertenece al departamento de marketing. Toda elección tecnológica o decisión de proceso que defina cómo funcionará una empresa conlleva un riesgo, y la forma en que se gestionará ese riesgo debe ser transparente para la empresa, de modo que pueda tomar decisiones acertadas.

Una lección importante para los departamentos de IT y seguridad es hablar el idioma correcto: la gestión de riesgos. Si se empieza a hablar de detalles técnicos y de cómo funcionan, cualquier persona de la empresa se perderá, pero si se traducen los cambios tecnológicos y de procesos al lenguaje de los riesgos empresariales (o de las oportunidades de negocio), todo el mundo se involucrará.

Esta ciberresiliencia empresarial no es estática, como otros riesgos para las empresas (geopolíticos, económicos, competencia), sino que está en constante cambio. Por lo tanto, la empresa debe aprender y adaptarse continuamente. Algunos ejemplos recientes son la forma en que los atacantes están eludiendo o derrotando formas «más débiles» de MFA, con kits de herramientas de atacantes en el medio o ataques de fatiga de la MFA. La ingeniería social es un riesgo siempre presente, así que hay que preguntarse: ¿habría actuado mejor el servicio de asistencia técnica en la defensa del negocio que el de Caesars o MGM?

Una estrategia de seguridad equilibrada

Está claro que el ecosistema de seguridad actual es más diverso y peligroso que nunca. Como resultado, las empresas deben pensar en implementar un enfoque equilibrado de seguridad. Esto significa ser conscientes y tomar medidas para mitigar las amenazas avanzadas que puedan estar dirigidas a un sector empresarial determinado, al tiempo que se aseguran de que también se gestionan los aspectos básicos.

Ninguna organización debería confiar en una única aplicación o dispositivo de seguridad, sino adoptar un enfoque de varios niveles que cubra los vectores de ataque más comunes, así como los específicos de su sector de actividad. Esto incluye:

- Detección de spam y malware de última generación con ATP para el análisis de comportamientos con el fin de proteger contra el continuo aluvión de amenazas basadas en el correo electrónico que vemos en este sector.
- Formación de concienciación en seguridad para usuarios finales, con el fin de formarles en la detección de ataques de ingeniería social y spear-phishing.
- Capacidades de copia de seguridad y recuperación TANTO para los datos locales como para los que se encuentran en servicios en la nube, como M365, con el fin de recuperarlos en caso de que se produzca un ataque de ransomware.
- Funciones de cumplimiento y gobernanza que ayudan a proteger contra la fuga accidental de datos y garantizan que se cumplan los controles de cumplimiento.

Al estratificar las estrategias de seguridad con estas capacidades, las empresas pueden confiar en su posición de seguridad.

HORNETSECURITY

365 TOTAL PROTECTION

Protección de última generación para microsoft 365- Seguridad email backup, cumplimiento y concienciación en seguridad

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT

PHISHING & ATTACK SIMULATION	COMMUNICATION PATTERN ANALYSIS	
SECURITY AWARENESS	AI RECIPIENT VALIDATION	
ESI® REPORTING	SENSITIVE DATA CHECK	

START FREE TRIAL

Acerca de los autores

Basado en datos directamente de nuestro Hornetsecurity Lab

ESCRITO POR

Andy Syrewicze

Andy tiene más de 20 años de experiencia en soluciones tecnológicas en diferentes sectores. Está especializado en Infraestructura, Cloud y la suite Microsoft 365.

Andy posee el premio MVP de Microsoft en Cloud y Datacenter Management y es uno de los pocos que también es experto en VMware.

Paul Schnackenburg

Paul Schnackenburg comenzó en IT cuando los procesadores DOS y 286 eran la vanguardia. Dirige Expert IT Solutions, una consultora de IT para pequeñas empresas en Sunshine Coast, Australia. También trabaja como profesor de IT en una Academia de Microsoft.

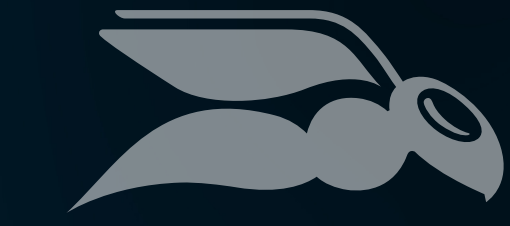
Paul es un autor de tecnología muy respetado y activo en la comunidad, escribiendo artículos técnicos en profundidad, centrados en Hyper-V, System Center, nube privada e híbrida y Office 365 y tecnologías de nube pública Azure.

Posee certificaciones MCSE, MCSA, MCT.

Capítulo 5 - Recursos

- https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
- https://www.bleepingcomputer.com/news/security/w3ll-phishing-kit-hijacks-thousands-of-microsoft-365-accounts-bypasses-mfa/
- https://www.hornetsecurity.com/us/podcast-us/can-you-trust-microsoft-security/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/us/services/365-permission-manager/
- https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
- https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
- https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility/
- https://www.descope.com/blog/post/noauth
- https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
- https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
- https://www.hornetsecurity.com/us/podcast-us/monthly-threat-report-discussion-october-2023/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/
- https://www.hornetsecurity.com/us/podcast-us/we-used-chatgpt-to-create-ransomware/
- https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/
- https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/
- https://www.hornetsecurity.com/us/podcast-us/generative-ai-in-defensive-tools/

- https://openai.com/blog/openai-cybersecurity-grant-program
- https://github.com/features/copilot
- https://github.com/kgretzky/evilginx2
- https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
- https://www.bleepingcomputer.com/news/security/the-moveit-hack-and-what-it-taught-us-about-application-security/
- https://www.theregister.com/2023/05/17/another_security_calamity_for_capita/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-leaks-38tb-of-private-data-via-unsecured-azure-storage/
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3459888/esf-members-nsa-and-cisa-publish-second-industry-paper-on-5g-network-slicing/
- https://therecord.media/ransomware-deployment-dwell-time-decreasing
- https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
- https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
- https://pubs.opengroup.org/security/zero-trust-commandments/
- https://salt.security/api-security-trends



HORNETSECURITY