INFORME DE CIBERAMENAZAS
EDICIÓN 2021/22

¡El mundo de la ciberdelincuencia no se detiene! Por ello, en la nueva edición del **Informe de ciberamenazas** de 2021/22, los expertos en informática de Hornetsecurity vuelven a examinar la puerta de entrada de la comunicación por correo electrónico y analizan las últimas amenazas de los ciberdelincuentes. Para ello, examinan qué peligros han surgido en 2021, qué ha sido de Emotet y para qué tendrán que prepararse las empresas al abrir su bandeja de entrada en el futuro.

Con servicios de desarrollo interno, como Spam and Malware Protection, Advanced Threat Protection, así como la Security Suite integral para Microsoft 365, Hornetsecurity, proveedor de copias de seguridad y de seguridad en la nube para correos electrónicos, protege a día de hoy a más de 50.000 clientes. Al mismo tiempo, los analistas de seguridad pueden hacer afirmaciones fundadas sobre la situación actual de las amenazas de la ciberdelincuencia en base a datos de filtros evaluados y a sus conocimientos técnicos.

Capítulo 1: La ciberdelincuencia es una de las mayores amenazas a nivel mundial

Según el último informe "Hidden Costs of Cybercrime" del fabricante estadounidense de seguridad informática McAfee, las pérdidas económicas causadas por la ciberdelincuencia ascendieron en 2020 a **945.000 millones de dólares estadounidenses**[1] en todo el mundo. En 2018, las pérdidas monetarias ascendieron a unos 600.000 millones de dólares estadounidenses[1]. En sólo dos años el número se ha incrementado dramáticamente. Estos daños económicos incluyen, entre otros, **costes de oportunidad, pérdidas de sistemas y de productividad, así como daños a la marca.**

La seguridad y el perfecto funcionamiento de procesos informáticos se han convertido en algo tan importante en la vida social y económica, que el Foro Económico Mundial en su Informe de Riesgo Global de 2021 sitúa el fallo de las infraestructuras y medidas de ciberseguridad en empresas, gobiernos y hogares privados en la lista de amenazas actuales y a medio plazo más críticas para el mundo. Y es que el fallo de la seguridad informática podría provocar enormes limitaciones en la actividad económica, pérdidas financieras y tensiones geopolíticas y, por lo tanto, representa un riesgo importante para la estabilidad de la vida social.[2]

En general, cada vez más empresas reconocen la escala potencial de un ciberataque y el riesgo creciente de ser víctima de un ciberataque. Esto queda demostrado por las **inversiones cada vez mayores que la empresas realizan en su seguridad informática: en 2020, el gasto mundial en ciberseguridad ascendió a unos 133.800 millones de dólares estadounidenses.** Para el año 2021, se estima un gasto de unos 150.000 millones de dólares estadounidenses.[3]

El correo electrónico sigue siendo una de las puertas de entrada principales de ataques cibernéticos en empresas, organizaciones e instituciones gubernamentales. El Business Email Compromise, así como el ransomware, representan los tipos de ataques más peligrosos, en los que los hackers utilizan procedimientos más complicados año tras año para lograr sus objetivos. Sin embargo, el robo y el espionaje de datos, así como la instalación de backdoors, son también una amenaza cada vez más seria para autoridades y empresas.

Capítulo 2: Email Threat Review 2021 del Security Lab

Los investigadores de amenazas de Hornetsecurity Security Lab ofrecen a continuación un resumen de las cifras sobre el estado actual de las amenazas del correo electrónico a nivel mundial. Los expertos analizan y clasifican los correos electrónicos recibidos durante el año 2021.

Spam, amenazas y amenazas avanzadas: los peligros ocultos en el tráfico de correos electrónicos

Unos 300.000 millones de correos electrónicos se envían cada día. Según las previsiones, el número de correos electrónicos privados y comerciales, tanto enviados como recibidos, aumentará hasta los 361.600 millones en 2024.[4]

Así, el correo electrónico sigue siendo el principal método de comunicación de las empresas, por el que se transmite no solo información confidencial, sino también archivos internos de las empresas.

Los expertos de Hornetsecurity Security Lab han analizado el tráfico de correos electrónicos del primer semestre de 2021 y han podido determinar que, en total, el **60 % de los correos electrónicos recibidos por Hornetsecurity podían clasificarse como "limpios"**, es decir, deseados. Contribuyen a un intercambio productivo, así como a un funcionamiento normal. Sin embargo, un **40 % de los correos electrónico recibidos se clasifican como "no deseados".**

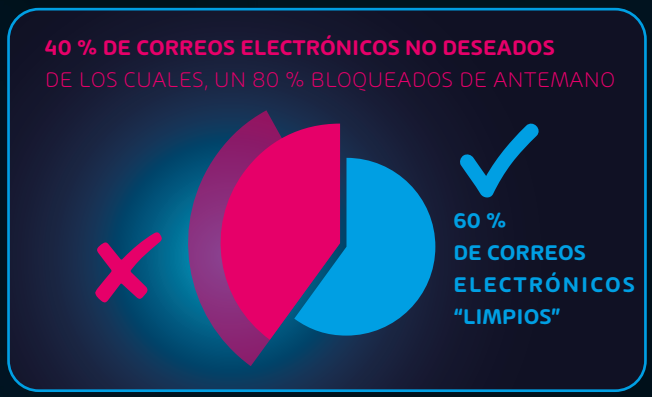


Fig. 1: Clasificación de los correos electrónicos escaneados por Hornetsecurity

De los correos electrónicos no deseados, **alrededor del 80 % ya se rechazados de antemano:** entre ellos, los correos electrónicos clasificados como spam con ayuda de una lista negra en tiempo real, mensajes que intentaron utilizar el servidor de correo de Hornetsecurity como open relay, así como fallos técnicos, listas grises o direcciones de correo electrónico no identificables.

El Security Lab clasificó el 15,54 % de todos los correos electrónicos no deseados como spam, el 4 % como amenazas y el 1 % fue identificado por el Advanced Threat Protection de Hornetsecurity y representan "amenazas avanzadas". Entre ellas, fraude del CEO, spear phishing o ataques con malware nuevo o parcialmente desconocido.

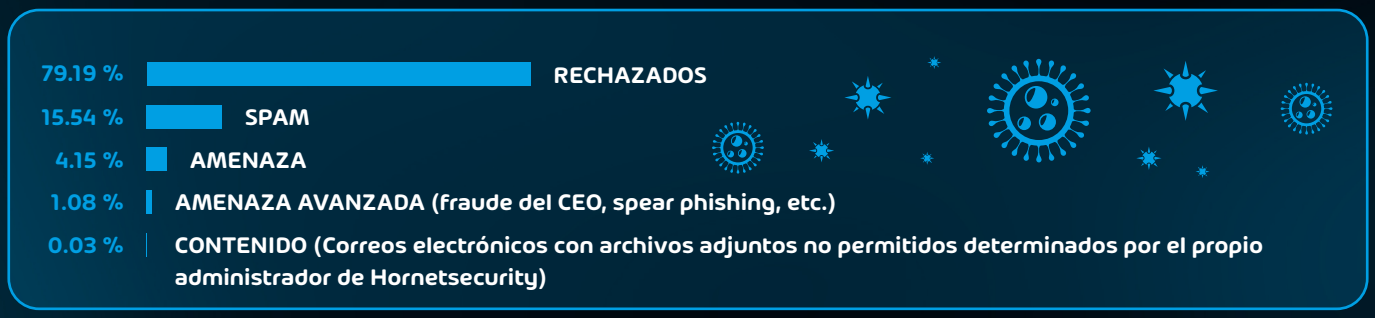


Fig. 2: Proporción de correos electrónicos no deseados según categoría

Adjuntos en correos electrónicos maliciosos

Para no ser descubiertos por los filtros de spam y virus de sus víctimas, los ciberdelincuentes ocultan el malware de diferentes modos en sus ataques por correo electrónico. En 2021, los archivos comprimidos, con un 33,6 %, fueron la forma más popular de propagación de malware. El malware ejecutable y los documentos infectados por malware se comprimen y se adjuntan directamente al correo electrónico del ataque. La esperanza es que el sistema de correo electrónico objetivo no pueda escanear los archivos adjuntos comprimidos. Los delincuentes con poca "experiencia" utilizan con frecuencia esta técnica, ya que no requiere conocimientos técnicos.

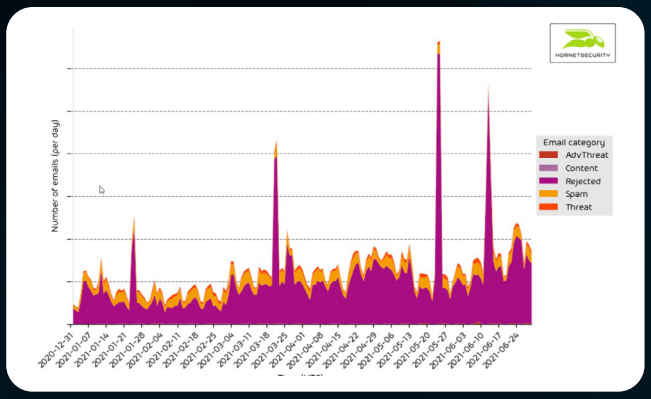


Fig. 3: Distribución de correos electrónicos no deseados según categoría en el primer semestre de 2021

En el 15,3 % de los casos, los ciberdelincuentes utilizaron archivos HTML en sus correos electrónicos de ataque. En un correo de phishing, la página web de phishing se adjunta directamente en el correo electrónico en forma de HTML, con lo que se pretende eludir los filtros de URL y redirigir a las víctimas a sitios web maliciosos para que descarguen malware. Por lo tanto, en el correo electrónico no se incluye una URL en la que hacer clic.

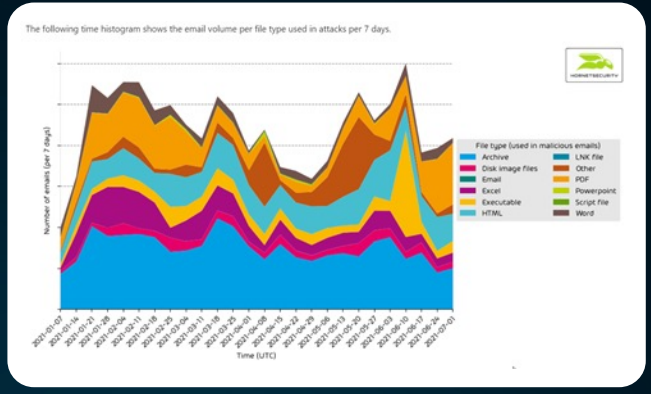


Fig. 4: Distribución de archivos adjuntos maliciosos por semana (en el 1.er semestre de 2021)

Los archivos de Excel (.xls, .xlsm, .xlsx, .xslb usw) con macros XLM se han vuelto cada vez más populares en los últimos años (10,2 % en el primer semestre de 2021). A diferencia del malware de macros VBA, el malware de macros XLM se detecta con menos frecuencia y, por tanto, es preferido por muchos delincuentes. De hecho, muchos ciberdelincuentes utilizaron el mismo generador de documentos, llamado "EtterSilent, para crear sus documentos con macros XML.

Otros tipos de archivos utilizados son PDF (14,5 %), Word (4,8 %) y PowerPoint (0,4 %). Los archivos PDF se utilizan principalmente para la distribución de enlaces maliciosos. Excel, PowerPoint y Word suelen contener macros.

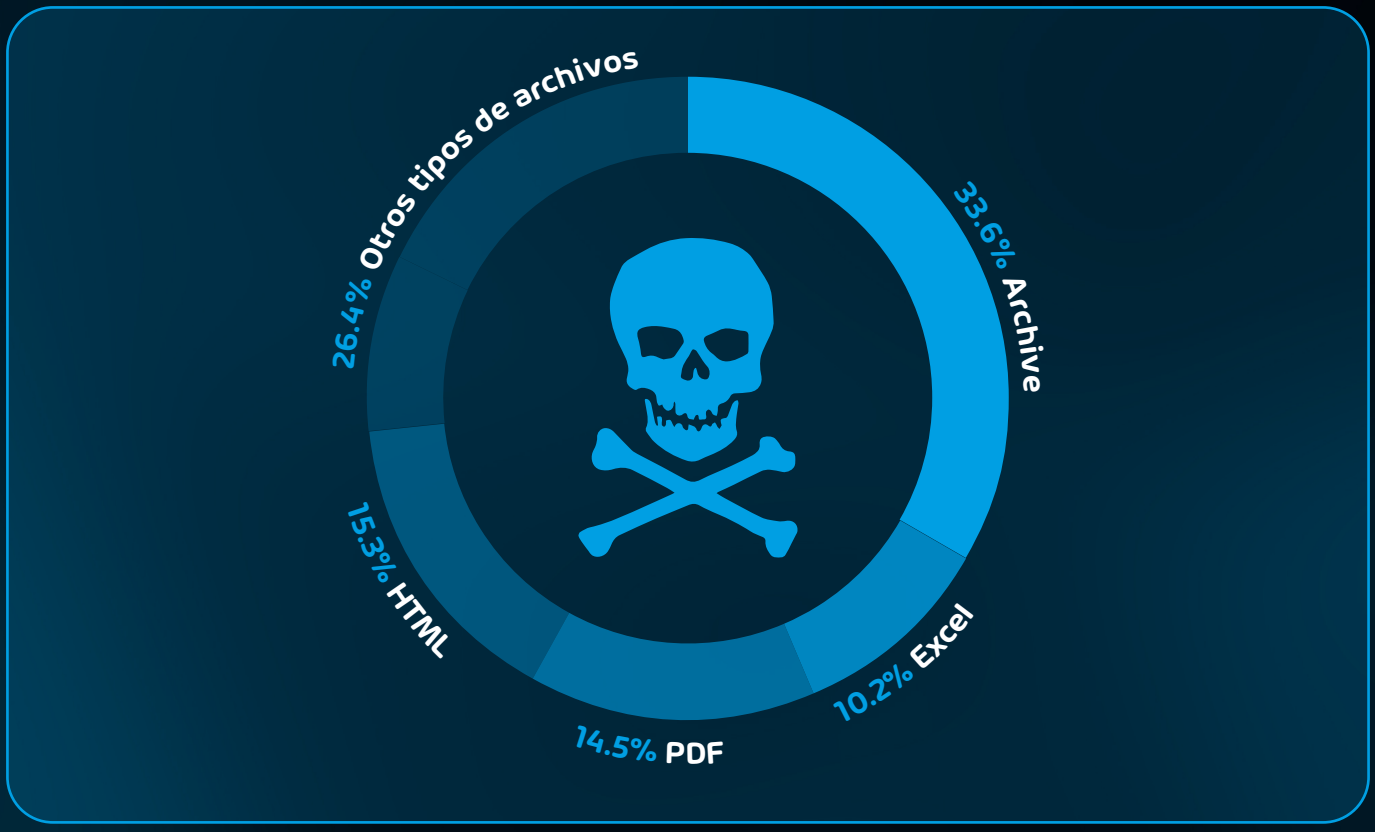


Fig. 5: Tipos de archivos más utilizados en correos electrónicos maliciosos

Industry Threat Index: Estos sectores son actualmente los más afectados

En la mayoría de los casos, un correo electrónico malicioso se envía a varias direcciones de correo electrónico. Sin embargo, algunas empresas y sectores son especialmente interesantes para los ciberdelincuentes, ya que, por ejemplo, suponen que las empresas correspondientes generan un volumen de negocio especialmente elevado o disponen de datos especialmente confidenciales y valiosos. Con el Threat Index, los expertos del Security Lab miden la tasa de ataques de los distintos sectores. En el primer semestre de 2021, el sector de fabricación, las instituciones de investigación y desarrollo, así como las empresas de transporte público, como autobuses, ferrocarril, aerolíneas y compañías de taxis, se vieron especialmente afectadas por los ciberataques.

- 4,9 | **SECTOR DE LA FABRICACIÓN**
- 4,8 | **INVESTIGACIÓN**
- 4,7 | **MEDIOS DE TRANSPORTE**
- 4,6 | **EDUCACIÓN**
- 4,6 | **MEDIOS**
- 4,5 | **AUTOMOCIÓN**
- 4,5 | **SECTOR DEL ENTRETENIMIENTO**
- 4,2 | **SECTOR HOTELERO**
- 4,1 | **SECTOR DE LA AGRICULTURA**
- 4,1 | **SECTOR SANITARIO**

Porcentaje de correos electrónicos de amenazas (en relación a los correos electrónicos válidos/limpios)*

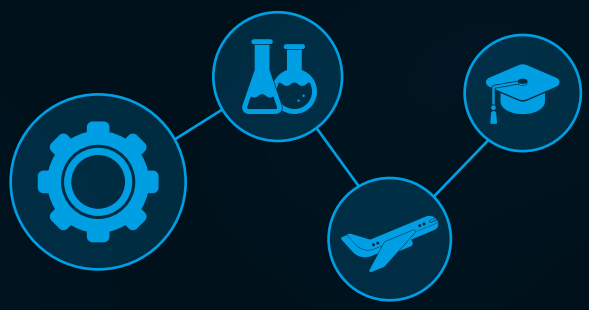
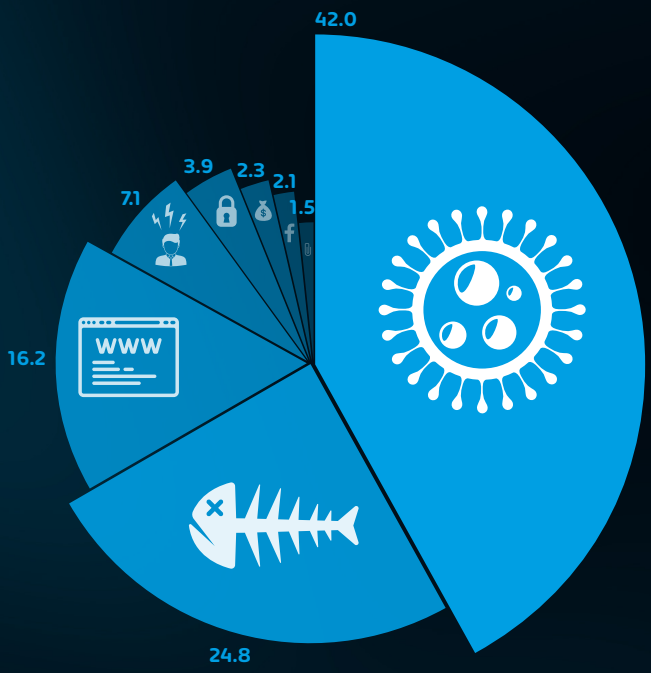


Fig. 6: Los sectores más amenazados según el Threat Index*

*Threat Index % = Número de emails maliciosos / (número de emails maliciosos + número de emails limpios) * 100 – excluyendo spam e infomails

Modus operandi de los hackers en 2021

Para burlar los filtros de virus y spam, los hackers varían el contenido y la presentación de sus correos electrónicos maliciosos. El phishing, la suplantación de marcas y el ransomware son solo algunas de las tácticas de ataque utilizadas para acceder a las bandejas de entrada de sus víctimas sin ser detectados y, finalmente, "tener éxito". **Los correos electrónicos de phishing son y siguen siendo una de las tácticas de ataque más populares:** Con este método, los hackers intentan acceder a diferentes tipos de datos confidenciales, desde datos de acceso hasta información de tarjetas de crédito. Con un 7,1 %, el "chantaje" es también muy popular entre los ciberdelincuentes. El llamado "Evergreen" son los correos electrónicos de "sextorsión": la víctima recibe un correo electrónico en el que se afirma que su ordenador se ha visto comprometido durante la visita a un sitio web de pornografía y se ha grabado un vídeo. Para evitar que el vídeo se haga público, deberá pagarse un rescate.



TÁCTICA DE ATAQUE	%
Otros	42.0
Phishing	24.8
URL	16.2
Chantaje	7.1
Ejecutable en archivo/imagen de disco	3.9
Advance-fee scam (fraude avanzado)	2.3
Suplantación de marcas	2.1
Maldoc (adjunto malicioso)	1.5

Fig. 8: Las tácticas de ataque más populares en el 1.er semestre de 2021

¿Amazon o Amaz0n? Cuidado con la "suplantación de marcas"

Los ciberatques en los que se imita una empresa específicamente también se conocen como **"suplantación de marca"**. En este caso, los ciberdelincuentes copian la imagen corporativa de una compañía y utilizan una dirección del remitente prácticamente idéntica a la dirección de correo electrónico original. Por lo general, el objetivo es acceder a datos de acceso a cuentas de usuario o a datos de tarjetas de crédito, aunque también hacer que el destinatario haga clic sobre un enlace malicioso para, por ejemplo, descargar malware sin que se dé cuenta.

Según los expertos de Hornetsecurity Security Lab, Amazon, con un 17,7 %, ocupa el primer puesto de las empresas más copiadas. DHL es también una de las preferidas por los ciberdelincuentes: especialmente en la era del coronavirus, el número de pedidos (en línea) de cualquier tipo de producto se disparó, por lo que se enviaron y recibieron un gran número de paquetes. Los correos electrónicos que anuncian la llegada de un paquete son especialmente fáciles de falsificar para los ciberdelincuentes. El mensaje del correo electrónico es breve, en la mayoría de los casos el destinatario no cuestiona su origen si, de hecho, está esperando un paquete y hace clic en el enlace de seguimiento del envío. Sin embargo, este enlace dirige a la descarga de un programa malicioso o a una página web de phishing, tal y como se ve en las siguientes imágenes:

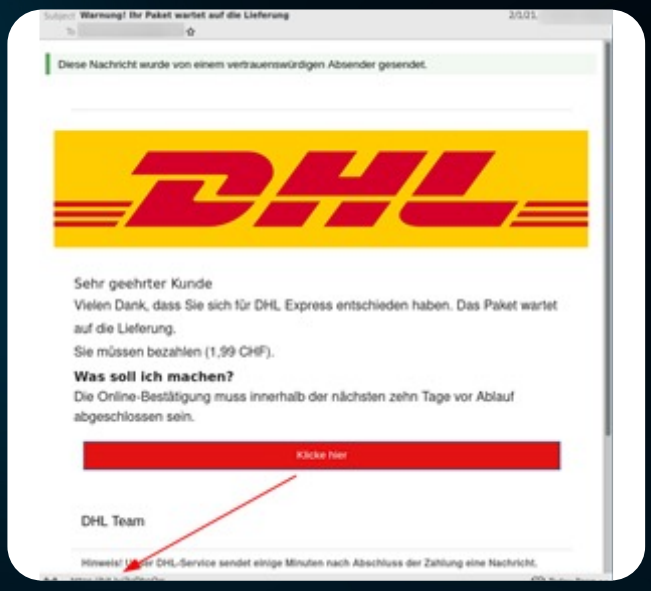


Fig. 9: Ejemplo de correo electrónico de suplantación de marca con URL malicioso

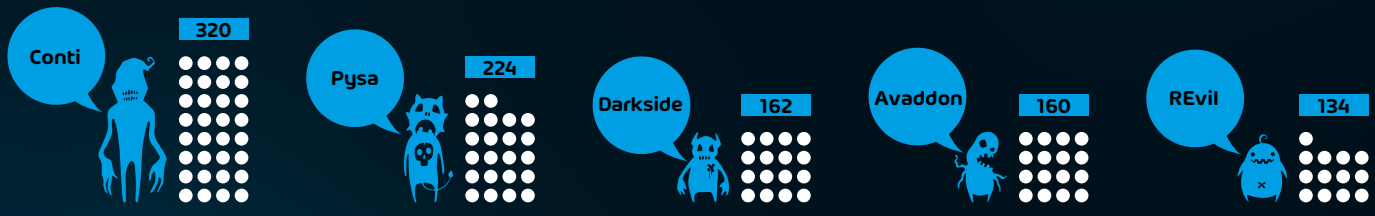
MARCA/ORGANIZACIÓN IMITADA

- 17.7 | AMAZON
- 17.1 | OTROS
- 16.5 | DEUTSCHE POST / DHL
- 12.7 | DOCUSIGN
- 5.7 | PAYPAL
- 3.5 | LINKEDIN
- 3.0 | MICROSOFT
- 2.5 | 1&1
- 2.3 | O2
- 2.2 | FACEBOOK
- 1.8 | HSBC
- 1.2 | FEDEX
- 1.1 | EBAY
- 1.1 | SANTANDER
- 1.0 | NETFLIX

Fig. 10: Marcas/Organizaciones utilizadas para infiltrar malware o solicitar datos

Ransomleaks & Double Extortion: la tendencia adquiere mayores proporciones

Ya el año pasado, los investigadores de amenazas de Hornetsecurity predijeron una tendencia al alza de ransomware que, además, extorsiona a sus víctimas mediante la publicación de datos. Esta evolución se intensificó en los meses siguientes. Antes de que los datos de la víctima se cifren en el ordenador comprometido, los atacantes copian los archivos en el servidor y, a continuación, amenazan con publicar esta información confidencial en las llamadas páginas de filtraciones. El grupo de hackers detrás del ransomware Conti es, con datos publicados de 320 víctimas, el "más activo". Los investigadores de amenazas de Hornetsecurity Security Lab observaron, además, filtraciones en las siguientes páginas de filtraciones de ransomware:



Y otros 23: Babuk (70), Cl0p (52), Doppelpaymer (43), Nephilim (40), Lorenz (27), Ragnarok (22), Promethous (22), Everest (19), Xing Team (18), Astro Team (17), MountLocker (16), Grief (16), RansomEXX (16), Vice Society (14), RagnarLocker (11), Cuba (9), Networm (5), Egregor (5), Synack (4), LV (3), Hive (3), Suncrypt (3), Lockbit (2)

Fig. 11: Las mayores páginas de filtraciones según el número de víctimas (número de personas cuyos datos ha sido publicados en la página correspondiente)

Clasificación de amenazas de Hornetsecurity Security Lab

Debido a la evolución observada del mercado "as a Service" en la darknet, los expertos en seguridad suponen que en el futuro, el aumento de la ciberdelincuencia procederá cada vez más de ciberdelincuentes altamente profesionales. El ransomware as a Service sigue siendo un problema importante en este sentido y la evolución de este procedimiento delictivo supone una amenaza cada vez mayor para empresase, instituciones públicas, por ejemplo, hospitales y gobiernos.

En general, la tendencia del ransomware aún no ha alcanzado su punto álgido. Según Bleeping-Computer, el grupo de ransomware REvil ha recaudado 1000 millones de dólares estadounidenses en Bitcoin en el plazo de un año.[5] Con esta elevada suma, los perpetradores detrás de grupos como REvil pueden, por ejemplo, contratar a profesionales de pruebas de penetración, que a su vez descubren a más víctimas, cuyos datos serán también objetivo del grupo de hackers.

Capítulo 3: Los "highlights de las amenazas" 2021

El 2021 fue testigo de algunos acontecimientos relacionados con la ciberdelincuencia que revisaremos en el siguiente capítulo.

La caída de Emotet: Los vaivenes del malware más peligroso del mundo

El "malware más peligroso del mundo" pudo detenerse al fin: a principios del 2021, las unidades policiales involucradas notificaron el desmantelamiento de la botnet Emotet.

Emotet se descubrió por primera vez en el año 2014: en ese momento, se trataba de un troyano bancario que robaba información bancaria y datos de acceso. Sin embargo, con el tiempo Emotet evolucionó hacia un malware como servicio (MaaS) que ofrecía la distribución de malware para otros ciberdelincuentes. Solo en Alemania, Emotet ha infectado un gran número de sistemas informáticos de empresas, además de decenas de miles de ordenadores privados. El hospital de Fürth y el Tribunal Superior de Justicia de Berlín fueron dos de las muchas víctimas de Emotet. Solo en Alemania, la Oficina Federal de Investigación (BKA, por sus siglas en alemán), calcula que los daños causados por Emotet ascienden a 14,5 millones de euros.

Después de infectar un sistema, Emotet podía leer las relaciones de los contactos y los contenidos de los correos electrónicos en las bandejas de entrada. Para distribuir el malware, Emotet respondía a estos correos electrónicos de manera muy auténtica en base a la información recopilada. Las falsificaciones eran muy difíciles de identificar. Este modus operandi se conoce también como secuestros de hilos de correo electrónico[6]. Hornetsecurity ya ha publicado numerosas entradas en el blog acerca de ataques de Emotet como este.

El 27 de enero de 2021, Euoropol informaba de que una operación internacional de autoridades policiales y judiciales de todo el mundo, incluidas las de Alemania, Países Bajos, Lituania, Ucrania, Francia, Inglaterra, así como las de Canadá y Estados Unidos, pudo hacerse con la infraestructura de Emotet y desmantelarla.

Los investigadores obtuvieron el control de la infraestructura al identificar varios servidores a través de los cuales se distribuía el malware. Paso a paso fueron descubriéndose otras partes de la infraestructura. De este modo, las autoridades encargadas de la investigación pudieron impedir el acceso de los autores, e incluso tomar el control de uno de los operadores sospechosos en Ucrania.

La comunicación C2 de Emotet se interrumpió y la información de las víctimas asociadas a la misma se redirigió a los CERT correspondientes del país, quienes informaron a las víctimas para que pudieran eliminar el malware.

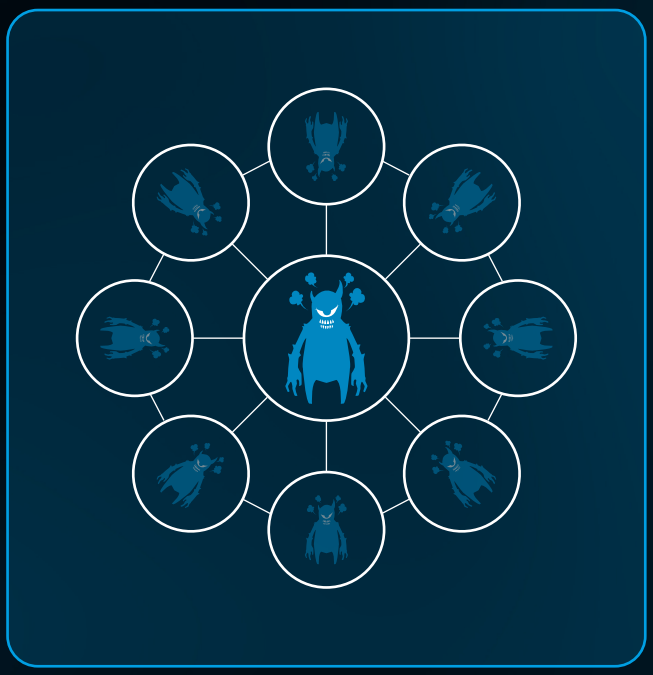
Hasta su desmantelamiento, Emotet representaba el 20 % de los correos electrónicos maliciosos analizados por Hornetsecurity. Sin embargo, el 15 de noviembre, los investigadores de amenazas de Hornetsecurity volvieron a registrar las primeras actividades del malware. En ellas, se distribuía el malware TrickBot a través de spam malicioso, se descargaba y, finalmente, se instalaba el malware de Emotet. A continuación, la botnet de Emotet volvía a crearse y comenzaba a enviar spam maliciosos desde su botnet.

Emotet – Las consecuencias

Con la caída de Emotet, son muchos los que buscan ocupar el puesto de la botnet: Quakbot dispone de la sofisticación necesaria. Sin embargo, su botnet no es aún tan grande como la de Emotet. Esto complica una distribución a gran escala del malware.

Otros como la botnet Cutwail, con su spam malicioso Dridex, o los actores detrás de las campañas de spam maliciosos Hancitor, pueden distribuir spam malicioso a gran escala, aunque aún no cuentan con la astucia de Emotet.

Es probable que haya más actores que planeen hacerse con el título de "malware más peligroso del mundo", ya que la base de clientes del malware como servicio (MaaS) de Emotet sigue existiendo y otro malware podría utilizar este método.[7]



Detenciones en torno a Clop, The Trick y Gozi

Además del desmantelamiento de la botnet Emotet, 2021 ha sido testigo de otras buenas noticias: una de ellas es que la policía nacional de Ucrania detuvo a varias personas sospechosas de infectar a empresas con el ransomware Clop. Sin embargo, la operación de ransomware Clop no se vio interrumpida, lo que da a los investigadores de amenazas de Security Lab razones para creer que los individuos detenidos no eran los cerebros detrás del ransomware.

Otra persona sospechosa y en busca desde 2013 por su posible relación con el malware Gozi fue también detenida. El sospechoso operaba un servidor antibalas que ayudaba a los ciberdelincuentes a distribuir el malware Gozi, el troyano Zeus y el troyano SpyEye. Además, el sospechoso está también acusado de iniciar ataques DDoS y transmisiones de spam.

También se detuvo en EE.UU. a un codiseñador del malware The Trick, acusado de 19 de los 47 cargos.[8]

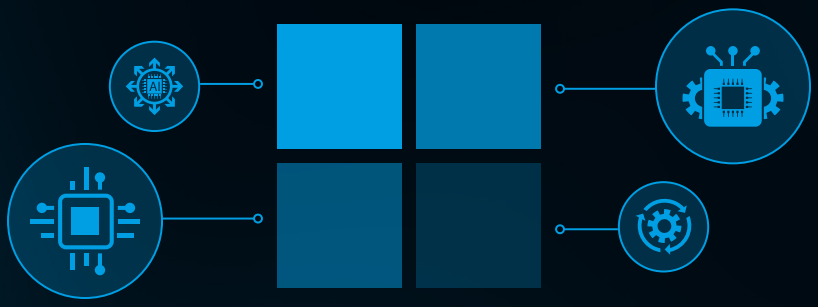
El ataque de Microsoft Exchange

En marzo, Microsoft acabó con cuatro vulnerabilidades en diferentes versiones de Microsoft Exchange Server con una actualización de seguridad no programada. Sin embargo, poco después de su publicación comenzaron las infecciones masivas de los servidores de Exchange no parcheados a través de Internet.

Se estima que los ataques afectaron a 250.000 servidores. Incluso la Casa Blanca ha pedido a los afectados que instalen parches de seguridad en sus respectivos sistemas Exchange, y la Oficina Federal Alemana de Seguridad de la Información (BSI, por sus siglas en alemán) ha declarado la alerta roja, ya que la agencia evaluó la situación de la amenaza como extremadamente crítica en ese momento.

Se sospecha que el grupo de hackers chino Hafnium, patrocinado por el estado y conocido por sus ataques altamente cualificados y sofisticados, es quien está detrás.[9]

En abril de 2021 se implicó incluso el FBI. Una orden judicial autorizó al FBI a penetrar en las redes corporativas para eliminar las webshells dejadas atrás por las infecciones que los ciberdelincuentes podrían utilizar para lanzar nuevos ataques.[10]



Capítulo 4: Previsiones y posible evolución de la ciberdelincuencia

La digitalización y la interconexión cada vez mayor entre dispositivos y cuentas no solo ofrece a los ciberdelincuentes más espacio para sus actividades, sino que la ciberdelincuencia atraviesa sin esfuerzos fronteras y continentes, lo cual dificulta su seguimiento. También según la Oficina de la Policía Criminal Federal Alemana, la delincuencia se desplaza cada vez más hacia el espacio digital. En comparación con el año anterior, los delitos a través de Internet han aumentado un 8,7 %, especialmente la ciberdelincuencia aumentó en 2020 un 7,9 % en comparación con el año 2019.[11]

En un estudio representativo de la asociación digital Bitkom quedaba claro que el 75 % de las empresas encuestadas en 2018/2019 se vieron afectadas por ataques. En los años 2020/2021, esta cifra aumentó hasta un 88 %. En el año 2018/2019, los daños económicos causados por robo, espionaje y sabotaje ascendieron a 103.000 millones de euros. A día de hoy, esa cifra se ha duplicado. Actualmente, los daños anuales ascienden a 223.000 millones de euros.

Figura 12: Daños causados por la ciberdelincuencia en empresas según Bitkom.

Según Bitkom, el principal causante de este enorme aumento es el ransomware. El malware de extorsión cifra los archivos de los ordenadores y otros sistemas y los inutiliza para, a continuación, chantajear a los operadores.

Los daños generados por ransomware se han más que cuadruplicado (+358 %) en comparación con los años previos 2018/2019. Actualmente, una de cada diez empresas (9 %) ve amenazada su existencia por culpa de los ciberataques.[12]

Una encuesta de Hornetsecurity entre más de 820 empresas demostró, además, que el **21 % de los encuestados ya había sido víctima de un ataque por ransomware**.

Por lo tanto, a pesar del desmantelamiento de Emotet, las empresas no pueden respirar aliviadas. La ciberdelincuencia sigue siendo un negocio lucrativo, especialmente gracias a una interconexión cada vez mayor.

El foco sobre Microsoft 365

En abril de 2020, Microsoft notificaba 258 millones de usuarios activos de Office 365. Si tan solo un 10 % de los ordenadores utilizados no cuentan con protección suficiente frente a ciberataques, esto hace que haya 25 millones de objetivos individuales potencialmente fáciles de infectar para los hackers.[13]

El ataque de Microsoft Exchange muestra también que incluso los grupos de hackers patrocinados por estados se centran cada vez más en Microsoft, ya que saben la presión que pueden generar sobre las empresas y sobre las autoridades afectadas en caso de ataque.

En el marco de una encuesta sobre la seguridad del correo electrónico entre más de 420 empresas que utilizaban Microsoft 365 para su comunicación por correo electrónico, Hornetsecurity pudo determinar que **1 de cada 4 empresas había sido víctima de un agujero de seguridad en el correo electrónico al menos una vez**.

Fig. 13: Encuesta de Hornetsecurity entre 420 empresas de la seguridad en Microsoft 365

En su mayor parte, se trataba de correos electrónicos de phishing que llegaban a las bandejas de entrada de los usuarios.

Dado que Microsoft 365 sigue extendiéndose como una de las aplicaciones en la nube más utilizadas en el entorno empresarial, es probable que los ataques a los usuarios sigan también aumentando.

Acerca de Hornetsecurity Group

Hornetsecurity es un proveedor líder de seguridad de correo electrónico en la nube y de copias de seguridad que protege a empresas y organizaciones de todos los tamaños y en todo el mundo. Su galardonada cartera de productos cubre todas las áreas importantes de la seguridad del correo electrónico, incluyendo los filtros de spam y virus, la protección contra el phishing y el ransomware, así como el archivado y el cifrado conformes a la ley. A esto hay que añadir copias de seguridad, replicaciones y recuperación de correos electrónicos, terminales y máquinas virtuales. El producto estrella es la solución de seguridad en la nube más completa del mercado para Microsoft 365. Con más de 350 empleados en 10 sedes, esta empresa con sede principal en Hannover cuenta con una red internacional de más de 5.000 socios de canal y MSP, así como 11 centros de datos redundantes y seguros. Más de 50.000 clientes utilizan los servicios premium, entre ellos, Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA y CLAAS.

Fuentes

(1) https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, pág. 6

(2) http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf, pág. 89 Global Risk Report 2021

(3) https://de.statista.com/statistik/daten/studie/1038510/umfrage/ausgaben-fuer-it-sicherheit-weltweit/

(4) https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/

(5) https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

(6) https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/

(7) https://www.hornetsecurity.com/de/threat-research/emotet-botnet-takedown/

(8) https://www.hornetsecurity.com/de/threat-research/email-threat-review-juni-2021/

(9) https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/ (Mayo, 2021)

(10) https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

(11) Bundeslagebild Cybercrime 2020, BKA, pág. 38

(12) https://www.all-about-security.de/management/angriffsziel-deutsche-wirtschaft-mehr-als-220-milliarden-euro-schaden-pro-jahr/

(13) https://securityboulevard.com/2021/06/microsoft-office-365-a-major-supply-chain-attack-vector/

HORNETSECURITY