HORNETSECURITY

CYBERTHREAT REPORT
1ª EDICIÓN 2020

En tiempos en los que los sistemas de tecnología de la información ya no se utilizan de forma aislada, sino que están conectados en red a nivel mundial a través de Internet y de las comunicaciones móviles, la amenaza de los ataques cibernéticos también está aumentando. Las actividades ilegales en Internet van desde los intentos de fraude, el phishing y los ataques DDos hasta la venta de productos en el mercado negro, como drogas y armas. Según la Oficina de la Policía Criminal Federal Alemana, apenas hay otro ámbito delictivo en el que se haya producido un aumento tan continuo de la actividad criminal.[1]

El ciberespacio está cambiando rápidamente – y también los métodos utilizados por los hackers y los estafadores. El Cyberthreat Report de Hornetsecurity, edición tercera, analiza: ¿por qué el crimen cibernético es una de las amenazas globales?, ¿qué papel desempeñará la inteligencia artificial en los futuros ciberataques, y ¿por qué los hackers se dirigen cada vez más a Microsoft Office 365?

Ciberdelincuencia: un riesgo global

El Global Risk Report 2019 muestra que por tercer año consecutivo, los ciberataques junto a los fenómenos meteorológicos extremos, el fracaso de la protección del clima y los desastres naturales, se encuentran entre las amenazas mundiales más graves. Los ciberataques a gran escala y el consiguiente **colapso de las infraestructuras críticas debido a un ciberataque se ordenaron como la segunda amenaza más común.** Existe una creciente preocupación por la ciberdelincuencia en las empresas de servicios públicos (infraestructuras críticas), ya que la consecuencia - de una interrupción prolongada - es enorme y casi equivalente a los efectos de condiciones climáticas extremas.[2]

La ciberseguridad es cada vez más importante respecto a las cuestiones más importantes de protección de las empresas. Por ejemplo, el 92 por ciento de los encuestados en un estudio sobre ciberseguridad realizado por TÜV considera que los ataques cibernéticos son una amenaza grave.[3]

Global Threat Report: Puestos 1º a 3º de la lista de riesgos globales en 2019

1. Extremos climáticos y fracaso en la protección del clima
2. **Ataques cibernéticos a gran escala y posterior colapso de las infraestructuras críticas**
3. Desempleo masivo y otras consecuencias negativas del progreso técnico

La integración de la tecnología en casi todos los componentes de la vida humana no solo abre nuevas posibilidades, sino que también ofrece innumerables puertas de entrada, aún no claramente definidas, para las actividades delictivas. Se introducen nuevas tecnologías – más rápido de lo que se puede comprobar y garantizar la seguridad de las mismas.

Spam: adjuntos maliciosos y espionaje

Existen diferentes tipos de spam, incluido el tradicional, en el que, por ejemplo, se anima al destinatario a realizar un pago previo por un servicio o producto. Otra forma es el spam de malware. Los ciberdelincuentes intentan infectar los sistemas del destinatario con malware adjunto o mediante un enlace en el correo electrónico. La tercera forma es el phishing – aquí el usuario debe introducir los datos de acceso, por ejemplo, para la banca online o las cuentas de redes sociales.[4]

Los expertos del Security Lab de Hornetsecurity han analizado los correos electrónicos de spam desde octubre de 2018 hasta octubre de 2019 y han sido capaces de determinar que, **en un 91,7 por ciento, se trataba de spam** clásico. El **8,3 por ciento restante eran correos electrónicos maliciosos (archivos adjuntos, URLs o phishing).**

Fig. 1: Top 5 adjuntos maliciosos

1 **Word** (.doc, .docx)

2 **Excel** (.xls, .xlsx)

3 **Archivos zip** (con archivos ejecutables)

4 **Archivos de imagen de disco** (.img)

5 **Documentos RTF**

Fig. 2: Porcentaje de emails de spam recibidos %

91,7 %
Spam clásico

8,3 %
Correos electrónicos spam maliciosos

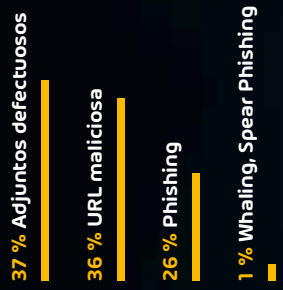


Fig. 3
Distribución de los tipos de amenaza en email con spam maliciosos

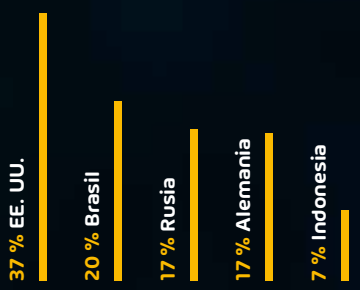


Fig. 4:
Origen de los correos electrónicos de spam

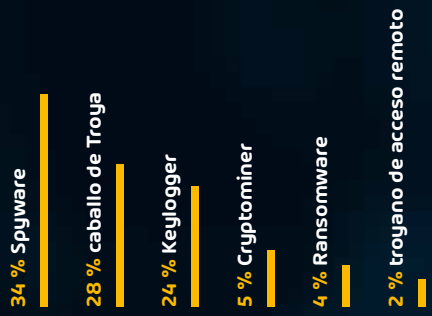


Fig. 5
Porcentaje de malware en correos electrónicos maliciosos

Más de la mitad del spam malicioso contiene spyware, troyanos y keylogger. Los hackers los están utilizando cada vez más para llevar a cabo espionaje y recoger información para otro ciberataque.[5] Aunque el número total de correos electrónicos de spam ha disminuido, el peligro que representa el spam no debe subestimarse. El creciente esfuerzo que invierten los ciberdelincuentes y el mayor uso de los datos personales procedentes de las fugas de datos aumentan significativamente el riesgo de infección.[6]

Ingeniería social: la debilidad humana como base de los ciberataques

La ingeniería social ha sido durante mucho tiempo la base de prácticas fraudulentas de todo tipo, pero especialmente en la era de la digitalización, esta pérfida forma de manipulación abre las puertas a los ciberdelincuentes. Las empresas son presa de los **ciberataques de ingeniería social casi tres veces más a menudo** que por vulnerabilidades reales de su arquitectura de seguridad informática.[7]

Los ciberdelincuentes no solo utilizan direcciones de correo electrónico de remitentes falsos, anuncios y sitios web falsos. También colocan claves sensibles en sus mensajes. En 2019, por ejemplo, la incertidumbre en torno a la normativa básica de protección de datos se utilizó como contexto para varios correos electrónicos falsos.

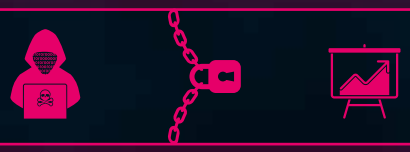
Ransomware: pérdidas millonarias

Ryuk, GandCrab y Locky están de vuelta – y son más peligrosos que nunca. Incluso el FBI advirtió en octubre de 2019 de los ataques ransomware que amenazan a empresas y organizaciones de los EE. UU. La última vez que hubo un mensaje de este tipo fue en 2016, unos meses antes de la ola de ataques con WannaCry y NotPetya.[8] El Ransomware es claramente una de las mayores amenazas del mundo cibernético, ya que los ataques conllevan **fallas completas de redes informáticas y plantas de producción.**[9] Según un estudio de KPMG, **el 60 por ciento de los encuestados en los últimos dos años fueron objeto de un ataque de ransomware.** En una de cada cinco empresas, hasta el 75 por ciento del entorno informático se vio afectado tras un exitoso ataque de ransomware.[10]

En el tercer trimestre de 2019, la aseguradora Beazley pudo comprobar un **aumento del 37 % en los ataques de ransomware** en comparación con los tres meses anteriores.[11]

Los ciberdelincuentes todavía huelen el negocio lucrativo del ransomware. Ryuk también ilustra esto: Según BSI, la observación dirigida de las direcciones de Bitcoin utilizadas permite sacar conclusiones sobre un rescate de **600.000 dólares americanos.** Para los hackers de hoy en día, el ransomware es un modelo de negocio establecido que está en constante evolución: GandCrab, por ejemplo, tiene un número de versión y también se ofrece como ransomware-as-a-service, es decir, como un servicio en Internet.[12]

60 % de las empresas encuestadas en Alemania fueron el objeto de un ataque de ransomware



+37 % Aumento de ataques de ransomware en el tercer trimestre de 2019

Emotet: ¿el malware más peligroso del mundo?

Si se menciona el nombre Ransomware, a menudo también se nombra a Emotet en el mismo contexto. Emotet causó un daño considerable el año pasado, no solo a la economía alemana, sino también a las autoridades y organizaciones públicas. En septiembre de 2019, el BSI informó **de varios miles de cuentas de correo electrónico comprometidas** a los proveedores responsables.[13]

¿Pero qué hace a Emotet tan peligroso? Desde su primera aparición en 2014, el malware ha demostrado ser extremadamente mutable. La primera versión de Emotet se distribuyó a través de enlaces o archivos adjuntos en campañas de spam con mensajes falsificados de los bancos. Más tarde, Emotet también estuvo disponible a través de PDFs disfrazados de facturas, así como falsas confirmaciones de envío de Amazon.[14, 15] En particular, el llamado **«Outlook Harvesting», el análisis del contenido de la comunicación por correo electrónico** en un dispositivo infectado, juega un papel crucial en la detección de Emotet. El malware no solo lee las relaciones con los contactos del historial, sino también el contenido de los correos electrónicos. Los ciberdelincuentes pueden así perfeccionar sus técnicas de ingeniería social y enviar correos electrónicos aún más precisos y dirigidos.[16]

Mientras tanto, Emotet se comporta como un Dropper y carga más malware después de una infección exitosa: en la actualidad, por ejemplo, el troyano bancario Trickbot, que entre otras cosas es capaz de extenderse en redes de forma autónoma leyendo los datos de acceso. A menudo aparece a continuación el ransomware Ryuk, que puede encriptar sistemas completos.[17]

Fig. 6: Extensiones y peligros de Emotet

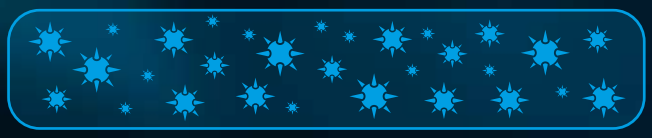
- Outlook-Harvesting
- Robo de datos de los navegadores web
- Recarga de malware, ransomware
- Explotación de vulnerabilidades no parcheadas
- Difusión en redes locales

Ya en 2018 el BSI **calificó a Emotet como el malware más peligroso del mundo. Esta reputación permanece claramente inalterada en 2019.**

Malware destructivo: la furia destructiva de los hackers

Los ataques de malware con elementos destructivos son cada vez más populares entre los ciberdelincuentes. De acuerdo con un estudio de IBM, **el número de ataques de este tipo en todo el mundo se duplicó en la segunda mitad de 2019.**[18] Desde agosto de 2019, por ejemplo, el **Ransomware GermanWiper** encripta no solo los datos de los ordenadores afectados, sino que además los sobreescribe con ceros. Aunque los desarrolladores de GermanWiper exigen un rescate a las víctimas de sus ataques, no hay forma de recuperar los datos encriptados. También el **Ransomware RobinHood** contiene elementos destructivos y ya ha causado grandes daños en Baltimore (EE. UU.), no solo cifrando los archivos de los ordenadores de los usuarios, sino también impidiendo las funciones de copia de seguridad y de servicio.[19]

2019: Ataques en la primera mitad del año



2019: Ataques en la segunda mitad del año **(+116 %)**

Los ataques destructivos cuestan a las empresas multinacionales un promedio de alrededor de **239 millones de dólares;** en comparación, las filtraciones de datos cuestan un promedio de 3,92 millones de dólares. Según IBM, las empresas necesitan alrededor de **512 horas** para recuperarse de un ataque con malware destructivo, y un solo ataque puede, en promedio, dañar **12 000 dispositivos por empresa**.[20]

Fig. 7: Daño medio que puede causar el malware con elementos destructivos

512 horas	239 millones de $	12 000 equipos
... es lo que necesitan las compañías para recuperarse de los daños causados por el malware.	... es lo que cuesta un ataque con malware destructivo.	... son perjudicados en un ataque por cada empresa.

El creciente número de ciberataques con malware destructivo es preocupante. Los daños que los ciberdelincuentes causan con esta forma de ataque son inmensos y si no se paga el rescate por la información encriptada, esto puede llevar a interrupciones a largo plazo en los procesos operativos y resultar en grandes pérdidas monetarias.

Phishing: sigue siendo una amenaza

Los expertos de Security Lab de Hornetsecurity pudieron identificar en torno a **un 12,3 por ciento de todos los correos electrónicos entrantes como ataques de** phishing. A pesar del descenso en verano, el número de correos electrónicos de phishing vuelve a aumentar hacia finales de año, ya que los hackers esperan mayores tasas de éxito, especialmente durante la temporada de Navidad y el consiguiente aumento del uso de tiendas online como Amazon.[21]

En 2018, el 51 por ciento de las organ zaciones británicas adoptaron medidas para aumentar la seguridad cibernética, en comparación con el 57 por ciento en 2019.[22] A pesar del aumento en concienciación respecto a los peligros que plantean los correos electrónicos de phishing, todavía existe un alto riesgo para los usuarios.

Fig. 8: Desarrollo de la cuota de phishing de todos los correos electrónicos entrantes en 2019[24]

Los hackers utilizan cada vez más temas de actualidad para hacer que sus correos electrónicos de phishing parezcan lo más reales posible. Como ya se mencionó en el capítulo sobre ingeniería social, la incertidumbre de muchos usuarios en relación con la normativa básica de protección de datos se utilizó indeb damente como base para auténticos correos electrónicos de phishing, además de otros temas delicados, como los actuales desastres naturales.

Industrias amenazadas: el sector energético y logístico son más vulnerables

El Security Lab de Hornetsecurity ha analizado los 1000 dominios con el mayor volumen de correo electrónico y los ha clasificado por sectores. Nuestros expertos pudieron determinar un resultado claro: **las empresas de servicios públicos encabezan la lista de los 10 sectores más atacados con un 16 por ciento.** Les siguen el sector logístico con un 14 por ciento y el sector automoción con un 13 por ciento. Sin embargo, las empresas de software, la industria farmacéutica y el sector financiero también se convirtieron en objetivos cada vez más importantes para los hackers en 2019.

Figura 9: los 10 principales sectores bajo ataque en 2019

El suministro de energía es una de las infraestructuras críticas, al igual que las áreas individuales del sector logístico, como el transporte de alimentos. En ambos sectores, los procedimientos operativos tienen influencia en el bienestar general de la sociedad. Un ciberataque con ransomware ejerce una gran presión sobre los operadores. La probabilidad de que el dinero para la desencriptación se pague en estos casos puede ser mayor que en otras empresas.

También es concebible que los ataques a estas zonas tengan a menudo una motivación política. Los hackers del Estado podrían, por ejemplo, utilizar la instalación de una puerta trasera en un sistema de infraestructura crítica como medio de presión en caso de crisis.

Figura 10: tipos de ataque al **sector energético**

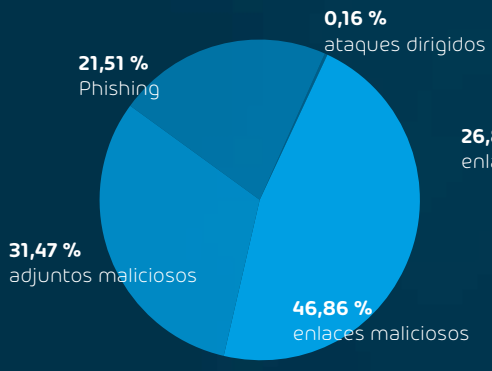


Figura 11: tipos de ataque al sector **logístico**

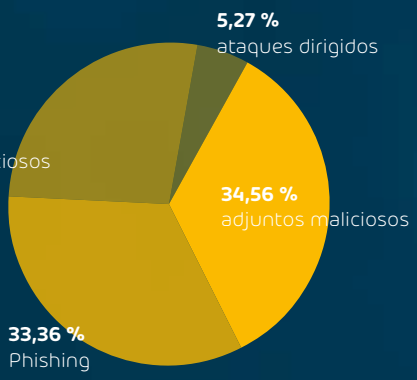
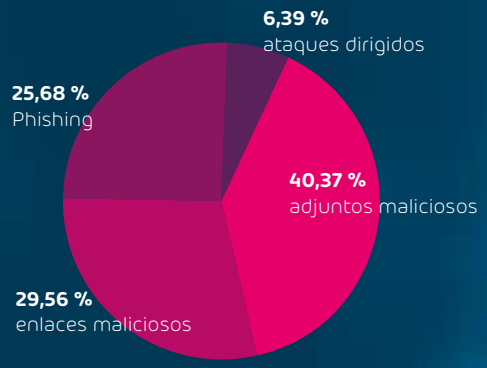


Figura 12: tipos de ataque al **sector automoción**



Casi la mitad de los ataques a las empresas energéticas se realizaron a través de correos electrónicos con enlaces maliciosos. Esta tendencia se debe al hecho de que muchas soluciones antispam ya pueden detectar los virus en los archivos adjuntos. Sin embargo, los correos electrónicos con archivos adjuntos maliciosos siguen siendo una vía común de infección. Casi el 20 por ciento de los ataques se identificaron como correos electrónicos de phishing; solo el 0,16 por ciento como ataques dirigidos.

En los sectores de logística y automoción, el Security Lab de Hornetsecurity pudo detectar principalmente los adjuntos maliciosos como un método popular de ataque de los ciberdelincuentes. Pero las campañas de phishing también son especialmente adecuadas para que las grandes empresas recopilen información interna. La información puede ser utilizada para el espionaje industrial, pero también puede emplearse para otros ciberataques, como el spear-phishing.

Los ataques dirigidos, como el fraude del CEO, también son utilizados por los hackers para atacar a empleados individuales a través de ingeniería social para exigir la transferencia de grandes sumas de dinero o para realizar espionaje industrial. **Los métodos de ataque utilizados por los hackers individuales varían de un sector a otro, pero son sus motivos los que juegan un papel decisivo.**

Especialmente en el área de las infraestructuras críticas, se puede asumir que el motor de las actividades cibercriminales no se reduce a grandes sumas de dinero. Los servicios públicos se consideran dignos de protección, como lo demuestran los estrictos requisitos del gobierno en materia de seguridad de los sistemas. En el siguiente capítulo, se examinará el tema de las infraestructuras críticas con mayor detenimiento.

Cuando la corriente deja de fluir: ataques a infraestructuras críticas

Según el BSI, en el segundo semestre de 2018 se produjeron alrededor de 157 incidentes de seguridad informática – En 2017 solo fueron 145 en todo el año.[25] En 2019, la situación de amenaza se mantuvo en un nivel alto y constante, tal como lo demuestra el análisis del Security Lab en el capítulo anterior. Mientras que los ciberdelincuentes solo necesitan identificar una vulnerabilidad, los operadores de infraestructuras críticas se enfrentan al reto de proteger sus sistemas completamente y de forma integral.[26]

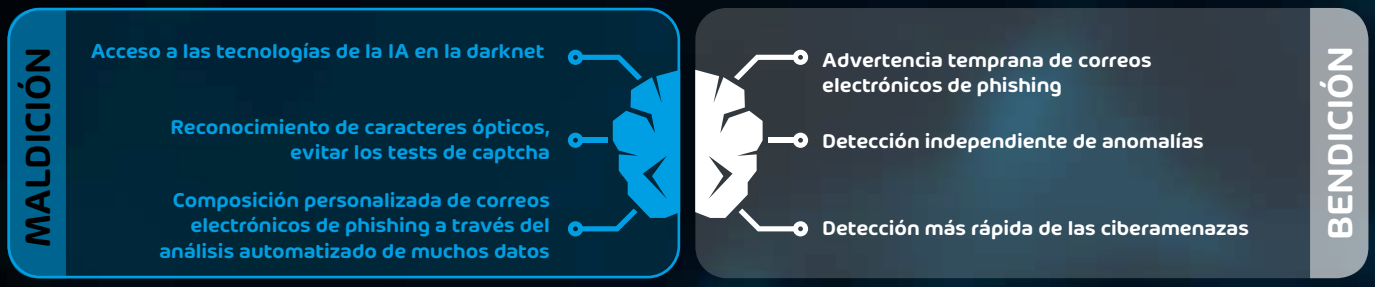
También en un estudio del Ministerio Federal de Educación e Investigación sobre el tema **de la seguridad informática de infraestructuras críticas,** más de la mitad de los encuestados declararon que habían sido víctimas de ataques cibernéticos en el último año. El espectro de ataques es diverso: en relación con las infraestructuras críticas, se menciona sobre todo el uso del phishing y ransomware. **El 60 por ciento de los encuestados dijo haber sido objeto de ciberataques de este tipo.**[27]

Como se puede leer en el capítulo anterior, los expertos del Security Lab de Hornetsecurity llegaron a conclusiones similares: el sector energético ha sido el más atacado desde principios de 2019. Una gran parte de los ataques se realizaron a través de correos electrónicos que contenían enlaces o archivos adjuntos maliciosos; alrededor del 20 por ciento de los ataques fueron ataques de phishing. Incluso un solo ataque exitoso a un servicio público puede tener graves consecuencias para la vida cotidiana. Por lo tanto, la ciberseguridad de las infraestructuras críticas merece una atención especial.

Inteligencia artificial: ¿maldición o bendición?

Las tecnologías de IA están evolucionando, así como la complejidad de los ciberataques que utilizan la inteligencia artificial como herramienta, a medida que crece el alcance de la IA en la darknet. Con el fácil acceso a las tecnologías, el riesgo de que los hackers se aprovechen de ellas también aumenta.

Las técnicas de seguridad convencionales, como las pruebas de captcha, ya pueden ser eludidas con un software de IA capaz de reconocer y evaluar los caracteres ópticos.[28] Los ciberdelincuentes también pueden utilizar la inteligencia artificial para analizar los datos de los usuarios, por ejemplo, **para hacer que los correos electrónicos de phishing sean aún más creíbles.** El aumento de la automatización a través de la IA también aumentará el número de ataques, lo que supondrá otro gran reto para los responsables informáticos.[29]



Pero las empresas pueden combatir a los ciberdelincuentes con sus propias armas. **El 72 por ciento de los responsables de la toma de decisiones empresariales cree que la IA puede apoyar la ciberseguridad en las tareas rutinarias.** Por ejemplo, la inteligencia artificial puede advertir contra los correos electrónicos de phishing en una etapa temprana y detectar independientemente las anomalías mediante el análisis automático de los metadatos. La IA también puede reducir el número de notificaciones de falsos positivos porque puede evaluar grandes cantidades de datos de forma precisa y rápida.[30, 31]

Además, el tiempo que los virus, malware y ransomware permanecen sin ser detectados ha disminuido en un 11 por ciento con el uso de la IA.[32] La inteligencia artificial desempeñará un papel importante en el futuro en el ámbito de la ciberseguridad, ya sea en los ataques cibercriminales o para la defensa.

Microsoft Office 365: el hijo predilecto del hacker

La externalización de infraestructuras informáticas es cada vez más popular, especialmente entre las empresas y organizaciones. En 2017, dos tercios ya utilizaban la nube, y una de cada cinco organizaciones planeaba implementarla. **En el futuro, se espera que una gran parte del tráfico de datos fluya por la nube.** La nube de Office 365 de Microsoft es uno de los servicios más populares de este tipo; entre 2015 y 2017 el número de suscriptores aumentó **en un 320 por ciento**.[33]

Alrededor de 100 millones de clientes empresariales utilizan Microsoft Office 365 Suite – allí se intercambian y almacenan datos sensibles, secretos comerciales e información personal. Pero el alto número de usuarios también atrae a los ciberdelincuentes. Ya en 2018 se pudo determinar un considerable aumento de los ataques. De acuerdo con Recorded Future, Microsoft ocupó el octavo lugar en la lista de los diez primeros con vulnerabilidades más explotadas – **seis de estas debilidades en aplicaciones de Office**.[34] El propio Microsoft informó de **un aumento de los ataques en un 250 por ciento.**[35]

El Top 6 de las vulnerabilidades se encuentran en las aplicaciones de Office

¿Cómo de vulnerable es MS Office Cloud?

En la nube **ya no se requieren mecanismos de protección controlados por las empresas, como firewall.** Para acceder a una gran cantidad de datos, los ciberdelincuentes solo necesitan encontrar una única debilidad en el sistema. Utilizando varios métodos de ocultación, los ciberdelincuentes se infiltran en los buzones de los usuarios y, en caso de emergencia, acceden a los datos de acceso de una cuenta de Office.

Incluso una sola cuenta comprometida en la nube de datos proporciona a los ciberdelincuentes una plataforma para muchos más ataques.[36]Desde aquí, los hackers pueden animar a otros usuarios a transferir grandes sumas de dinero o espiarlos usando por ejemplo, Business Email Compromise (BEC).

Business Email Compromise: pérdidas globales

El daño financiero causado por Business Email Compromise (BEC) es inmenso. El FBI averiguó que, entre junio de 2016 y julio de 2019, se produjeron 166.349 incidentes en EE. UU. que dieron lugar a más de 26 millones de dólares en pérdidas. Si comparamos la media de ganancias que los delincuentes obtienen de un atraco a un banco con las devoluciones generadas por el Business Email Compromise, resulta innecesario preguntarse la razón del aumento de la tasa de ciberdelincuencia.

Robo de banco: **$ 3.000**
Business Email Compromise: **$ 130.000**

Según el FBI, los ciberdelincuentes tienen como objetivo a cualquiera que tenga dinero, pero especialmente las grandes empresas y organizaciones que trabajan con sumas de dinero más elevadas son víctimas de los hackers.[37]

Debido al elevado número de usuarios, Microsoft Office 365 Cloud se ha convertido en un atractivo objetivo para los ciberdelincuentes. Se aconseja a las empresas que utilicen soluciones de terceros para protegerse de forma integral. Mecanismos adicionales de autenticación impiden los inicios de sesión no autorizados, el cifrado de datos en la nube proporciona seguridad contra el acceso no autorizado por parte de terceros.

Resumen

La amenaza del cibercrimen está creciendo y no se espera una tendencia a la baja en el futuro próximo. Según los últimos descubrimientos de la BSI, Emotet sigue siendo el malware más peligroso del mundo y se considera que el ransomware es, en general, la mayor amenaza para las empresas y organizaciones. A pesar de la creciente concienciación sobre la seguridad cibernética, los mensajes de correo electrónico de phishing también siguen siendo una gran amenaza, ya que los ciberdelincuentes siguen perfeccionando sus técnicas de fraude para burlar incluso a los usuarios formados.

Las infraestructuras críticas también están cada vez más en riesgo. Los ciberataques a los servicios públicos representan **una amenaza a la seguridad** nacional. Esto se debe a que un ataque a la red de energía o al suministro de agua puede causar cuellos de botella masivos en el suministro.

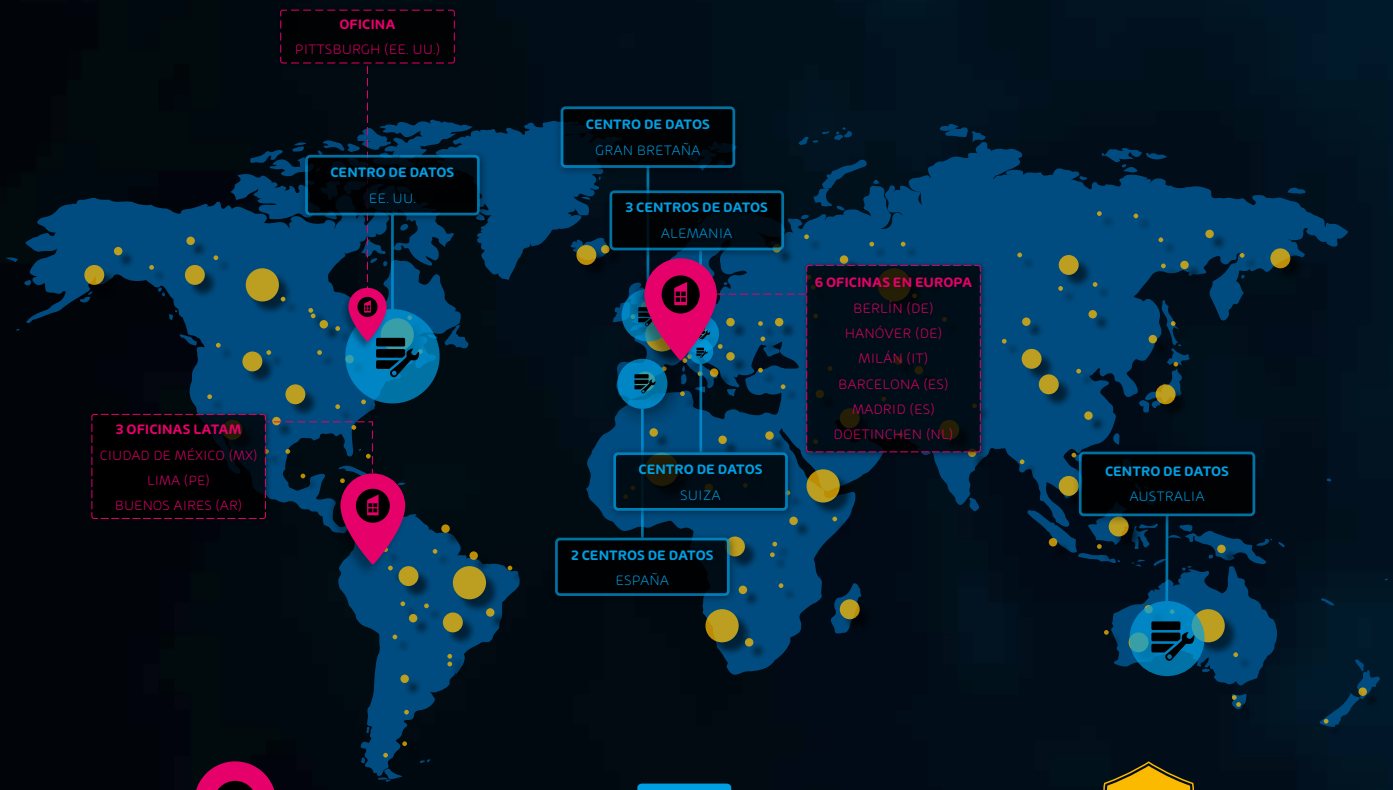
En conclusión, se puede decir que los ciberdelincuentes también se desarrollan junto con el progreso tecnológico. Los patrones de ataque se vuelven más complejos; los ataques multivectoriales ya no son una rareza. Cada vez es más difícil para las empresas protegerse de tales ataques. **El correo electrónico sigue siendo el principal vector de incidencia para una gran parte de los ataques cibernéticos.** Los usuarios de Office 365 Suite son especialmente vulnerables a los ataques cibernéticos a través de la puerta de entrada del correo electrónico. En su caso, es esencial asegurar la comunicación por correo electrónico a todos los niveles con soluciones de seguridad de terceros.

Al igual que cualquier crimen, los ataques cibernéticos deben tomarse muy en serio. Además del robo de datos sensibles de particulares, también el daño financiero y de reputación de una organización a través de los ciberataques es inmenso. No en vano, los gobiernos de todo el mundo han formado alianzas o creado oficinas para informar y proteger a la población sobre el cibercrimen y sus efectos.

Acerca de Hornetsecurity

Hornetsecurity es el proveedor alemán líder en seguridad en la nube para el correo electrónico en Europa y protege la infraestructura informática, la comunicación digital y los datos de empresas y organizaciones de todos los tamaños. El especialista en seguridad informática de Hannover presta sus servicios a través de nueve centros de datos. La cartera de productos incluye soluciones en las áreas de seguridad de correo electrónico, web y archivos. Todos los servicios de la empresa pueden implementarse en un breve periodo de tiempo y están disponibles las 24 horas del día. Hornetsecurity está representada globalmente en diez ubicaciones con alrededor de 200 empleados. Los clientes incluyen a Swisscom, Telefónica, KONICA MINOLTA, seguros LVM, DEKRA y Claas.

Hornetsecurity International



10 OFICINAS
EN TODO EL MUNDO, 6 EN EUROPA

9 CENTROS DE DATOS
EN TODO EL MUNDO, 3 EN ALEMANIA

40 000 EMPRESAS
PROTEGIDAS POR NOSOTROS

Fuentes

(1) https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html

(2) http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

(3) https://www.vdtuev.de/dok_view?oid=769635

(4) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

(5) Spam-Statistik Security Lab, Jan 2019 bis September 2019

(6) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=6

(7) https://www.securitymagazine.com/articles/88907-verizon-2018-data-breach-investigations-report-ransomware-still-a-top-cybersecurity-threat

(8) https://www.it-daily.net/shortnews/22517-neue-ransomware-warnung-des-fbi-was-sie-wissen-muessen

(9) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

(10) https://klardenker.kpmg.de/der-erpresser-aus-dem-internet/

(11) https://www.beazley.com/news/2019/beazley_breach_insights_october_2019.html

(12) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

(13) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Emotet-Warnung_230919.html

(14) https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

(15) https://www.stern.de/digital/online/emotet--darum-ist-der-trojaner-so-gefaehrlich---und-so-schuetzen-sie-sich-8548334.html

(16) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html

(17) https://www.heise.de/security/meldung/Trojaner-Alarm-BSI-warnt-vor-zunehmenden-Emotet-Angriffen-4537594.html

(18) https://siliconangle.com/2019/08/05/ibm-report-finds-destructive-malware-attacks-doubled-since-january/

(19) https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/

(20) https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/

(21) https://www.welivesecurity.com/deutsch/2016/12/13/12-sicherheitstipps-zur-weihnachtszeit/

(22) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

(24) https://www.heise.de/newsticker/meldung/Mehr-Hacker-Angriffe-auf-kritische-Infrastruktur-beim-BSI-gemeldet-4311172.html

(25) Phishing-Statistik aus dem Hornetsecurity Security Lab

Fuentes

(26) https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4

(27) https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf

(28) https://www.it-daily.net/it-sicherheit/cyber-defence/20434-cyberangriffe-kuenstliche-intelligenz-als-fluch-oder-segen

(29) https://www.wissenschaftsjahr.de/2019/neues-aus-der-wissenschaft/das-sagt-die-wissenschaft/kuenstliche-intelligenz-schutzschild-und-einfallstor-fuer-cyberattacken/

(30) https://www.eco.de/presse/internet-security-days-2019-mit-ki-cyberangriffe-abwehren/

(31) https://www.eco.de/presse/das-sind-die-it-security-trends-2019/

(32) https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/07/Report_AI_in_Cybersecurity_Capgemini_Research_Institute.pdf

(33) https://www.computerwoche.de/a/datenschutz-in-microsoft-office-365-ist-lueckenhaft,3546637

(34) https://www.recordedfuture.com/top-vulnerabilities-2018/

(35) https://businessinsights.bitdefender.com/microsoft-phishing-attacks-increased-250-from-january-to-december-2018

(36) https://www.beazley.com/news/2018/beazley_breach_insights_april_2018.html

(37) https://www.secureworldexpo.com/industry-news/new-business-email-compromise-statistics-bec