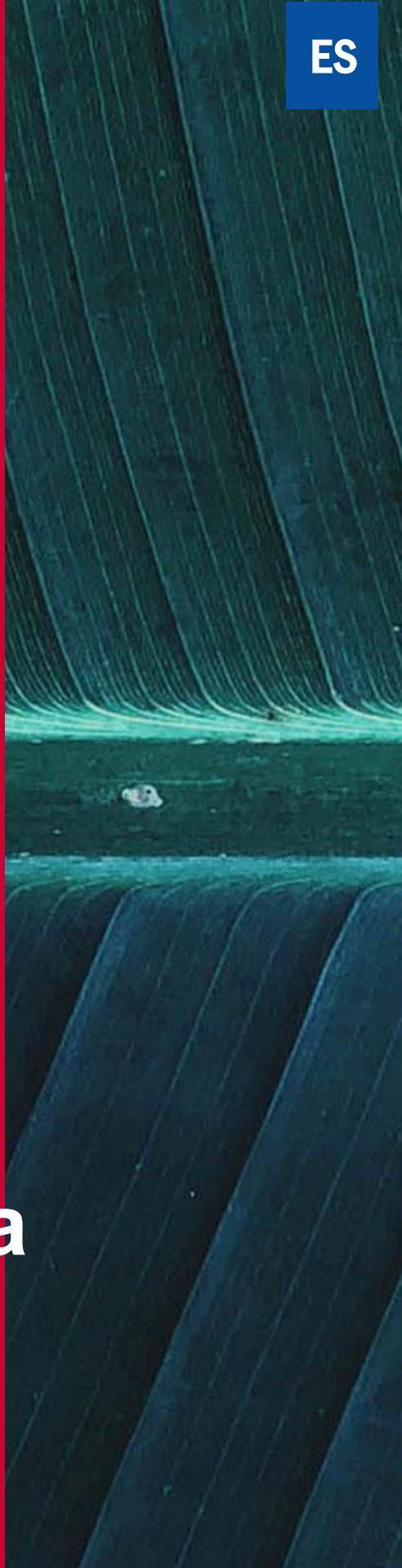
ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



De enero de 2019 a abril de 2020

Correo basura (*spam*)

Panorama de Amenazas de la ENISA

Sinopsis

El primer mensaje de correo basura lo envió en 1978 un gerente de *marketing* a 393 personas a través de ARPANET. Se trataba de la campaña publicitaria de un nuevo producto de la empresa para la que trabajaba, la Digital Equipment Corporation. Para las 393 personas que recibieron este mensaje el hecho de recibirlo fue tan molesto como lo es hoy en día, independientemente de lo novedosa que fuera la idea.[1] Recibir correo basura es fastidioso, pero para un agente malintencionado también puede ser la oportunidad de robar información personal o de instalar un programa de *malware*.[2] El correo basura consiste en enviar mensajes no deseados en masa. Se considera una amenaza para la seguridad informática cuando se usa como vector de ataque para distribuir o facilitar otras amenazas.

Otro aspecto destacable es que el correo basura a veces se confunde o se clasifica erróneamente como campaña de *phishing*. La diferencia principal entre los dos es el hecho de que el *phishing* es una acción dirigida que utiliza tácticas de ingeniería social y cuyo objetivo es robar los datos del usuario. Por el contrario, el correo basura es una táctica para enviar mensajes no deseados a una lista de destinatarios. Las campañas de *phishing* pueden usar tácticas de correo basura para distribuir mensajes, pero los mensajes de correo basura pueden llevar al usuario a sitios *web* peligrosos con el fin de instalar *malware* y robar datos personales.

Las campañas de correo basura de los últimos 41 años han aprovechado muchos de los eventos deportivos y sociales populares y globales, como la final de la Liga Europa de la UEFA o el Abierto de Estados Unidos, entre otros. Pero nada en comparación con la actividad de correo basura que se ha visto este año con la pandemia de COVID-19.[8]

Conclusiones

85 %_ de todos los mensajes enviados en abril de 2019 fueron correo basura, el valor más alto en 15 meses.[1]

14_ millones de mensajes de correo basura de sextorsión detectados en 2019.[23]

58,3 %_ de las cuentas de correo electrónico en la industria minera recibieron correo basura.[17]

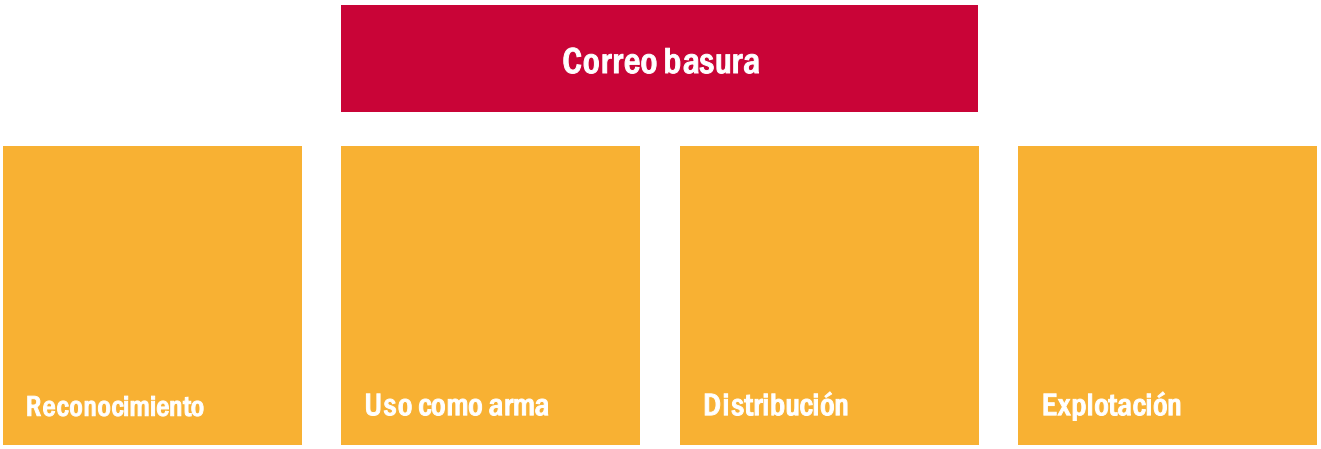
10 %_ de todas las detecciones de correo basura tenían como objetivo cuentas de correo electrónico alemanas.[2,3]

13 %_ de las filtraciones de datos fueron causadas por correo basura malintencionado.[16]

83 %_ de las empresas estaban desprotegidas contra los mensajes de correo electrónico con simulación de marcas.[20]

42 %_ de los responsables de la seguridad de la información han tenido que afrontar al menos un incidente de seguridad provocado por el correo basura.[1]

Kill chain



Paso del proceso de ataque

Amplitud de la intención

Lockheed Martin desarrolló el marco cibernético de Kill Chain® que adaptó a partir de un concepto militar relacionado con la estructura de un ataque. Para estudiar un vector de ataque determinado, utilice este diagrama de *kill-chain* para trazar cada paso del proceso y anotar las herramientas, técnicas y procedimientos utilizados por el atacante.

MÁS INFORMACIÓN

Descripción

_Mente vieja en cuerpo joven

Tras 41 años de existencia, el correo basura sigue siendo una amenaza de seguridad importante, aun cuando otras amenazas son mucho más eficaces. No obstante, de nuevo, durante el período de este informe, en las campañas de correo basura han aparecido nuevos grupos objetivo, nuevos medios y nuevas pérdidas. Por ejemplo, en agosto de 2019 se enviaron mensajes de correo basura a varias cuentas y en ellos se animaba a los destinatarios a compartir, no solo una copia escaneada de su identidad, también una foto para que pudieran «ganar» un teléfono inteligente. En otra campaña de correo basura, se pedía a los usuarios que enviaran una foto personal. El grupo objetivo de los ciberdelincuentes se fue expandiendo para incluir la dirección de correo electrónico utilizada por el usuario para activar servicios de televisión por pago o de retransmisión en directo. Estas cuentas recibieron correo basura con mensajes que incluían la expiración o renovación falsas de una licencia y se pedía a los destinatarios que contestaran e incluyeran sus datos bancarios e información personal para renovar la suscripción.[2]

_El correo basura al servicio del *malware*, el *ransomware* y los troyanos de acceso remoto

En agosto de 2019, se utilizaron mensajes de correo basura que contenían archivos de imagen de disco ISO malintencionados para propagar el *malware* LokiBot y para plantar el troyano de acceso remoto (RAT) FlawedAmmyy. El correo basura también se utilizó para propagar el troyano TrickBot, el troyano espía Negasteal (también conocido como Agent Tesla), el RAT Ave Maria (también conocido como Warzone) y el notorio, desde 2018, *malware* de macros Pawload. El correo basura también ayudó a propagar varias familias de *ransomware*, como Dharma, Crysis y Ryuk, cuya actividad fue muy elevada durante el año de este informe.[15][21]

_SMS basura

Este año se llevó a cabo una operación de SMS basura[1] que expuso los datos de más de 80 millones de usuarios. Un gran número de usuarios de móvil recibió mensajes que contenían frases como «dinero gratis» o «esto es cierto» y enlaces a sitios fraudulentos. A partir de ese punto, se efectuaba una llamada a todos los que seguían el enlace para que dieran datos sensibles. Se probó que la base de datos utilizada por los ciberdelincuentes era propiedad de ApexSMScompany, cuya legitimidad aún está por aclarar. Aunque algunos investigadores especializados en temas de seguridad pudieron acceder a la base de datos e intentaron recuperar toda la información posible porque se temían que la operación pudiera detenerse de forma inesperada, aún no se sabe ni quién ni por qué querría acceder a esta base de datos y usar sus datos, ya que sigue estando disponible.[4]

_Los formularios como puerta de entrada

Los organizadores de este ataque manipularon los formularios de comentarios que utilizan las grandes empresas para que los usuarios pregunten, indiquen sus deseos o se suscriban a boletines. No obstante, durante el año de este informe, en vez de enviar correo basura a los buzones de correo asociados a la empresa, los atacantes han explotado los bajos niveles de seguridad del sitio *web*, evitado los controles de reCAPTCHA y registrado numerosas cuentas con información de direcciones electrónicas válidas. El resultado ha sido que las víctimas han recibido una respuesta legítima de la empresa, en la que se incluía el mensaje del atacante.[2] Este método se ha utilizado para manipular incluso los formularios de Google para recabar datos de usuarios y enviar correo basura comercial. Un ejemplo de caso más agresivo fue el ataque de correo basura dirigido contra cuentas de empresa y en el que el atacante pedía una transferencia de dinero. Para convencer a la víctima, los atacantes amenazaban con enviar mensajes abusivos desde la dirección de correo de la víctima a más de 9 millones de direcciones, lo que haría que la dirección de la empresa entrara en las listas negras.[3]

Descripción

_ Correo basura camaleón

En 2019 varias campañas utilizaron el mismo sistema de *botnet* para distribuir mensajes de correo basura, aunque utilizaban encabezados y plantillas aleatorias para formatear el contenido. Por esa razón, los investigadores especializados en seguridad empezaron a estudiar estas campañas como pertenecientes a un mismo grupo bajo el alias de «correo basura camaleón».[5]

Los mensajes de correo basura camaleón se originaban en varios países e incluían enlaces falsos a ofertas o anuncios de trabajo falsos, sitios de reserva de billetes de avión, ofertas especiales para la compra de productos o simplemente servicios bien conocidos. Estos mensajes de correo basura utilizaban plantillas similares a las utilizadas por las empresas reales, como Google, Qatar Airways, FedEx, LinkedIn o Microsoft, para que el usuario no notara la diferencia.[2]

_ La fortaleza de las viejas *bots*

En octubre de 2019 se distribuyeron numerosos mensajes de correo electrónico con plantillas en inglés, alemán, italiano y polaco, con la línea de asunto común: «Aviso de pago». Estos mensajes incluían un documento adjunto que llevaba una macro, y se pedía a los destinatarios que la activaran al abrir el documento. Una vez activada, la macro podía empezar el proceso de infección intentando descargar el troyano Emotet.[13]

La *botnet* de correo basura Necurs[7] estuvo muy activa durante este período tras haber estado muy poco activa durante mucho tiempo. La *botnet* Gamut fue la tercera con más actividad en 2019. Los mensajes de Gamut suelen estar relacionados con sugerencias para citas o para conocer a personas, ofertas de productos farmacéuticos y oportunidades de trabajo.[1]

_Número de *botnets* C2 asociadas a las familias de *malware*

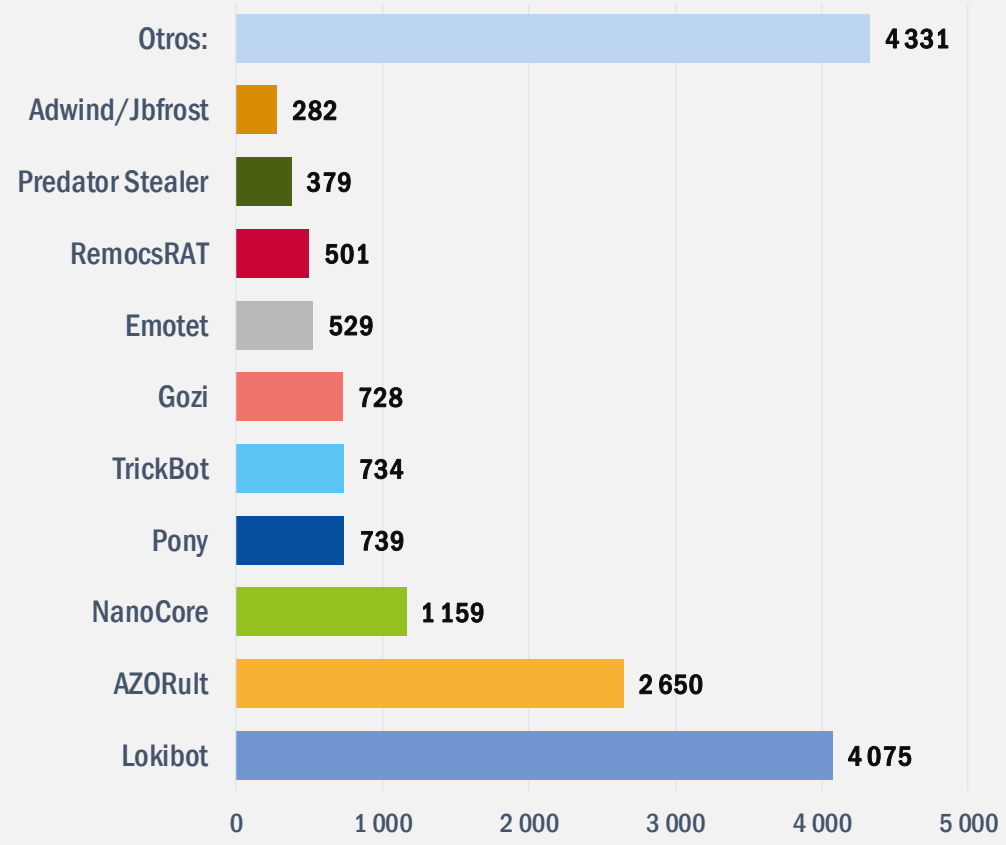


Figura 1 - Fuente: Spamhaus[14]

Descripción

_ La COVID-19 abrió nuevas puertas

Al poco tiempo de que se iniciara la pandemia de COVID-19, aparecieron sitios *web* de *phishing* y la distribución de archivos malintencionados por correo electrónico con los términos coronavirus o COVID-19. Se notificó que una campaña de correo basura de COVID-19 estaba distribuyendo Eeskiri-COVID.chm19, un archivo que se encarga de registrar las pulsaciones que se realizan en el teclado para guardarlas en un archivo (keyloggerfile). El nombre del archivo podría sugerir que la campaña se originó en Estonia (eeskiri significa «regla» en estonio).[11] A mediados de febrero de 2020 solo se registraron unos cientos de ataques de COVID-19 al día, pero en marzo de 2020 se produjeron más de 2 500 ataques diarios, lo que indicaba que el año iba a ser duro en este aspecto.[12]

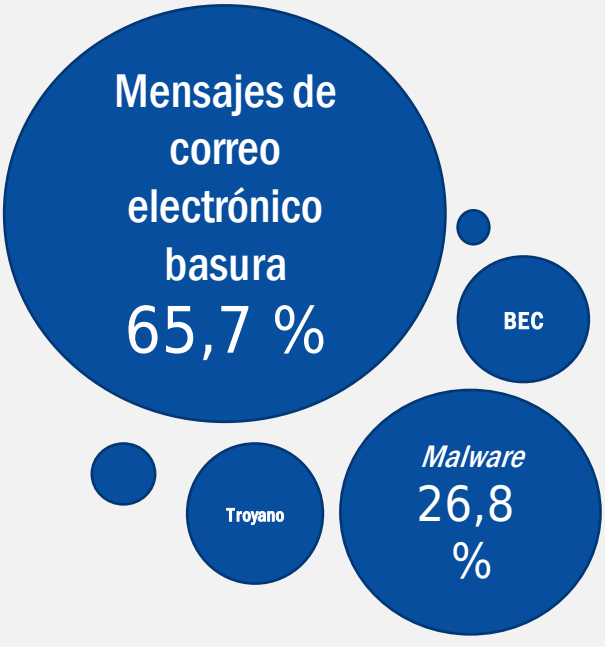


Figura 2: Amenazas que aprovecharon la COVID-19. Fuente: Trend Micro[11]

_ Ejemplos

01_La operación de correo basura ApexSMS

ApexSMS, una empresa de *marketing* por SMS, sufrió una filtración de datos que expuso la información de contacto de más de 80 millones de personas.

02_La operación de correo basura camaleón

Un sistema de *botnet* enviaba un volumen de correo basura elevado y persistente con mensajes que contenían encabezados aleatorios y que con frecuencia cambiaban de formato.

03_Campaña de distribución de correo basura con Emotet

Una campaña de correo basura que facilitaba la distribución del *malware* Emotet.

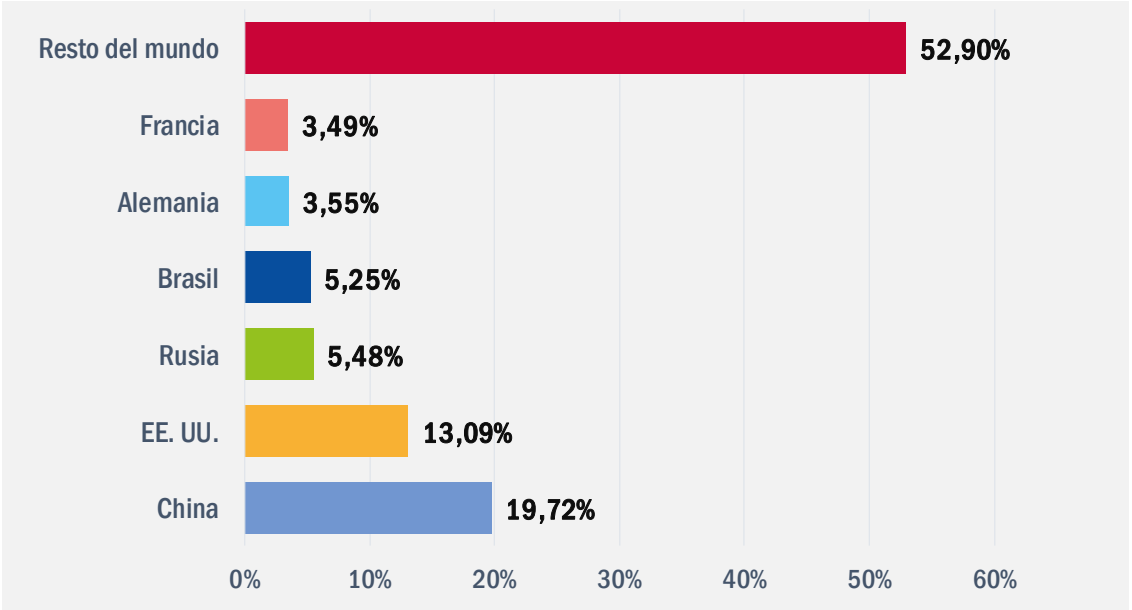
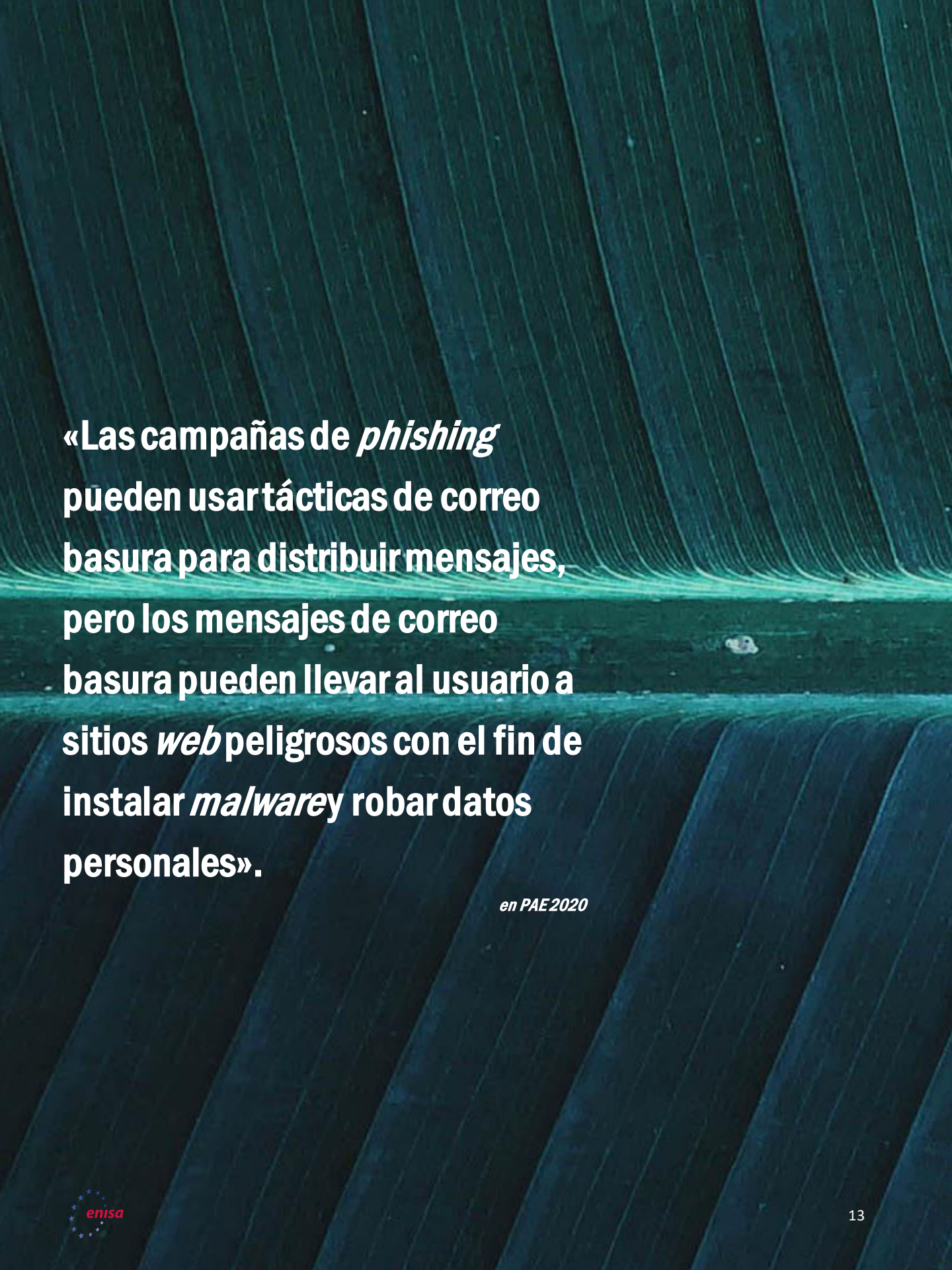


Figura 3: Fuentes de correo basura más comunes. Varias fuentes[17]

Mitigación:

Acciones propuestas

- Implementar programas de filtro de contenido para filtrar documentos adjuntos no deseados, mensajes de correo electrónico con contenido malintencionado, correo basura y tráfico de red no deseado.
- Actualizaciones periódicas del *hardware*, *firmware* (soporte lógico inalterable), sistema operativo, controladores o *software*.
- Utilizar autenticación multifactor para acceder a las cuentas de correo electrónico.
- Evitar las transferencias de dinero a cuentas bancarias sin verificar.
- Evitar pinchar en enlaces nuevos recibidos en mensajes de correo electrónico o SMS.
- Desarrollar procedimientos operativos estándar y políticas para el procesamiento de datos sensibles.
- Utilizar pasarelas de correo electrónico seguras con un mantenimiento periódico (posiblemente automatizado) de los filtros (filtros *antispam*, *antimalware* y basados en políticas).
- Desactivar la ejecución automática de código, la activación de macros y la precarga de gráficos y enlaces enviados por correo electrónico.
- Establecer técnicas de seguridad como la del marco de directivas de remitente (SPF), autenticación de mensajes basada en dominios, notificación y conformidad (DMARC) y el mecanismo de autenticación de mensajes (DKIM).
- Actualizar las listas blancas, filtros de reputación y las listas RBL o Real-Time Blackhole List (RBS) periódicamente.
- Utilizar la inteligencia artificial y el aprendizaje automático para realizar los controles de detección de anomalías.



«Las campañas de *phishing* pueden usar tácticas de correo basura para distribuir mensajes, pero los mensajes de correo basura pueden llevar al usuario a sitios *web* peligrosos con el fin de instalar *malware* y robar datos personales».

en PAE 2020

Bibliografía

1. "Email: Click with Caution - How to protect against phishing, fraud, and other scams". Junio de 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

2. "Spam and phishing in Q3 2019". 26 de noviembre de 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

3. "Spam and phishing in Q2 2019". 28 de agosto de 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. "SMS Spammers Doxxed". 9 de mayo de 2019. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. "Tracking the Chameleon Spam Campaign". 25 de septiembre de 2019. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6. "5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned". 7 de junio de 2019. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. "The world worst spammers". 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. "Naming the coronavirus disease (COVID-19) and the virus that causes it". 2020. OMS. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. "WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus". 6 de febrero de 2020. OMS. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. "COVID-19 situation update worldwide, as of 11 June 2020" 2020. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. "Developing Story: COVID-19 Used in Malicious Campaigns". 24 de abril de 2020. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. "2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape". 6 de abril de 2020. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. "Emotet is back: botnet springs back to life with new spam campaign". 16 de septiembre de 2019. Malwarebytes Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

14. "Spamhaus Botnet Threat Report 2019". 28 de enero de 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

15. "Evasive Threats, Pervasive Effects". 27 de agosto de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

16. "Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study". 28 de febrero de 2019. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. "Internet Security Threat Report" Volume 24, Febrero de 2019. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. "Spam and phishing in Q1 2019". 5 de mayo de 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. "Total Global Email & Spam Volume for May 2020". Mayo de 2019. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

20. "Q3 2019: Email Fraud and Identity Deception Trends". Junio de 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

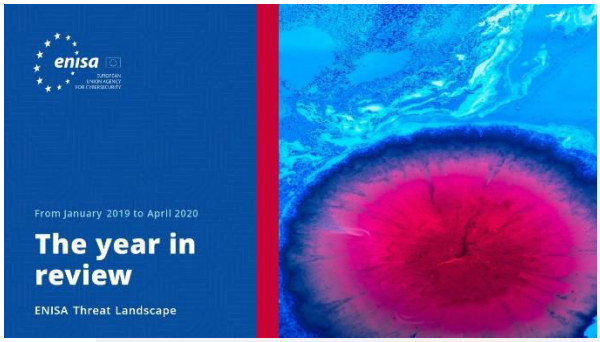
21. "The World's Most Abused TLDs" Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. "Trend Micro Cloud App Security Report 2019". 10 de marzo de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. "The Sprawling Reach of Complex Threats". 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. "SONIC WALL Security Center Metrics". SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

Lecturas relacion



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Revisión anual**

Un resumen de las tendencias en materia de ciberseguridad durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

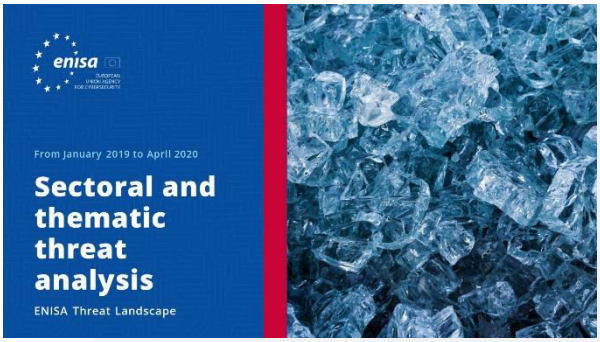
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

Lista de la ENISA con las 15 amenazas principales durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA
Temas de investigación

Recomendaciones sobre temas de investigación de varios cuadrantes de la ciberseguridad y de la inteligencia sobre las ciberamenazas.



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Análisis de las amenazas por sectores y temas**

Análisis contextualizado de las amenazas durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Tendencias emergentes**

Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Sinopsis de la inteligencia sobre las ciberamenazas**

Situación actual en materia de inteligencia sobre las ciberamenazas en la UE.

¿Quiénes somos?

_ La agencia

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. La agencia se estableció en 2004, se ha visto reforzada por el Reglamento sobre la Ciberseguridad y contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC con programas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. A través del intercambio de conocimientos, la capacitación y la sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Puede encontrarse más información sobre la ENISA y su labor en www.enisa.europa.eu.

Colaboradores

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) y *todos los miembros del grupo de partes interesadas de la CTI (inteligencia sobre las ciberamenazas) de la ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) y Thomas Hemker.

Editores

Marco Barros Lourenço (ENISA) y Louis Marinos (ENISA).

Datos de contacto

Las consultas acerca de este informe deben realizarse a través de enisa.threat.information@enisa.europa.eu.

Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

Nos gustaría conocer su opinión sobre este informe

Le pedimos que dedique unos minutos a rellenar el cuestionario. Para acceder al cuestionario haga clic aquí.

Aviso legal

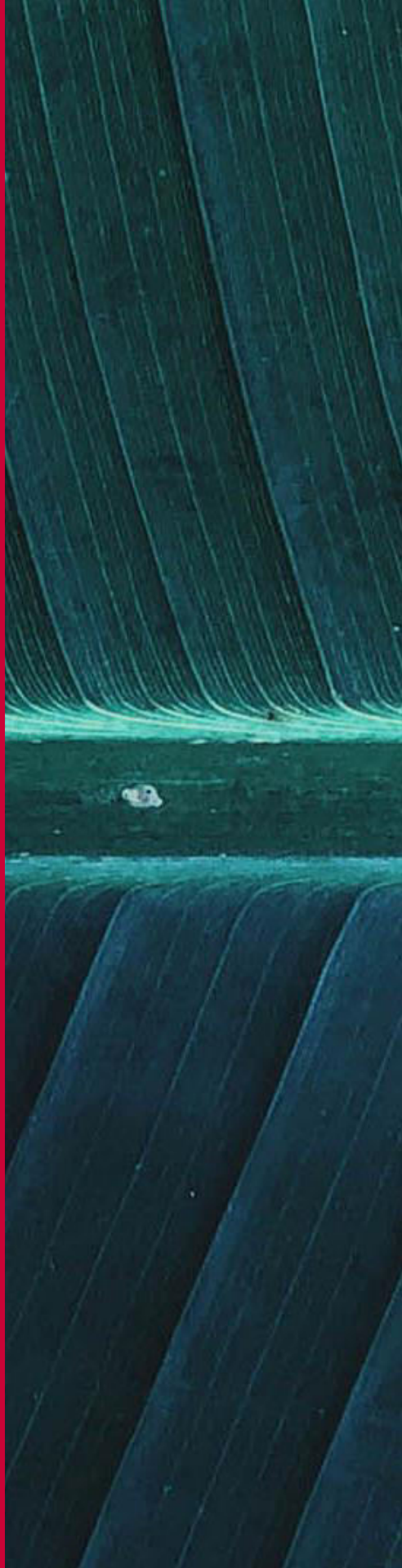
Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. La información tampoco refleja necesariamente el estado actual de la técnica y la ENISA se reserva el derecho a actualizarla en todo momento.

Las correspondientes fuentes de terceros se citan cuando proceda. La ENISA declina toda responsabilidad por el contenido de las fuentes externas, incluidos los sitios *web* externos a los que se hace referencia en esta publicación.

Esta publicación tiene un carácter meramente informativo. Además, debe poder accederse a la misma de forma gratuita. Ni la ENISA ni ninguna persona que actúe en su nombre aceptan responsabilidad alguna en relación con el uso que pueda hacerse de la información incluida en la presente publicación.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu