enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ES

De enero de 2019 a abril de 2020

Malware

Panorama de Amenazas de la ENISA

Sinopsis

El *malware* es un tipo común de ciberataque en forma de programa informático malintencionado. Las familias de *malware* incluyen: virus, gusanos, programas espía, programas de *cryptomining* y de *ransomware*. Sus objetivos comunes son el robo de información o de identidades, espionaje y la interrupción de servicios.[1]

Durante el año 2019 los programas de *cryptomining* fueron una de las familias de *malware* predominantes en el panorama de amenazas,[2] y produjeron elevados costes en tecnología informática, aumento del consumo eléctrico y reducción de la productividad de los empleados.[3] Los programas de *ransomware* aumentaron ligeramente en 2019 con respecto a 2018, aunque seguían al final de la lista de los tipos de *malware*.[2]

Los protocolos *web* y de correo electrónico fueron los vectores de ataque iniciales más comunes utilizados para propagar el *malware*. Aun así, con el uso de técnicas de fuerza bruta o con la explotación de las vulnerabilidades del sistema, determinadas familias pudieron propagarse aún más dentro de una red. Aunque las detecciones globales de ataques han permanecido al mismo nivel del año anterior, se observó un cambio notable de ataques al consumidor a los dirigidos a objetivos comerciales.[4]

Conclusiones

400 000_ detecciones de programas de *spyware* y *adware* preinstalados en dispositivos móviles.[4]

13 %_ de aumento de las detecciones de *malware* en Windows en empresas de todo el mundo.[4]

71 %_ de las organizaciones sufrió actividad de *malware* que se propagó de un empleado a otro.[47]

46,5 %_ de todo el *malware* en mensajes de correo electrónico estaba en documentos de tipo «.docx».[24]

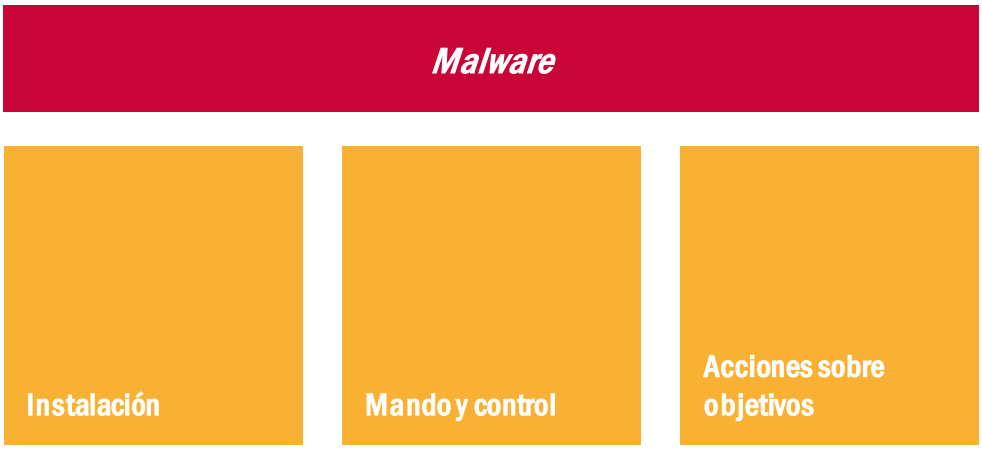
50 %_ de aumento en *malware* diseñado para robar datos personales o para espiar a personas (*stalkerware*)[15]

67 %_ de los programas de *malware* se distribuyeron mediante conexiones HTTPS encriptadas.[48]

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

Los tipos de *malware* más frecuentes

Emotet fue la variedad de *malware* más frecuente en 2019 y está evolucionando en 2020. Emotet fue descubierto inicialmente en 2014 como troyano bancario. Desde entonces, el programa se ha actualizado con la funcionalidad de mando y control (C2), mecanismos de evasión adicionales, como la capacidad para saber si se está ejecutando en un entorno aislado y la capacidad para distribuir descargas peligrosas como Trickbot y Ryuk.[7] La figura anterior representa la clasificación de los programas de *malware* bancarios detectados en 2019.

Durante el período de este informe, Emotet ha evolucionado y ha pasado a convertirse en una *botnet*[8], ha aumentado su actividad[8] y ha iniciado nuevas campañas de correo basura localizadas con funcionalidad de *spear-phishing* para instalar *ransomware* o robar información.[5] Durante 2019, las detecciones de Emotet aumentaron un 73 % con respecto al año anterior, principalmente con ataques a objetivos comerciales en Estados Unidos y el Reino Unido, como se indica en la figura siguiente.[4]

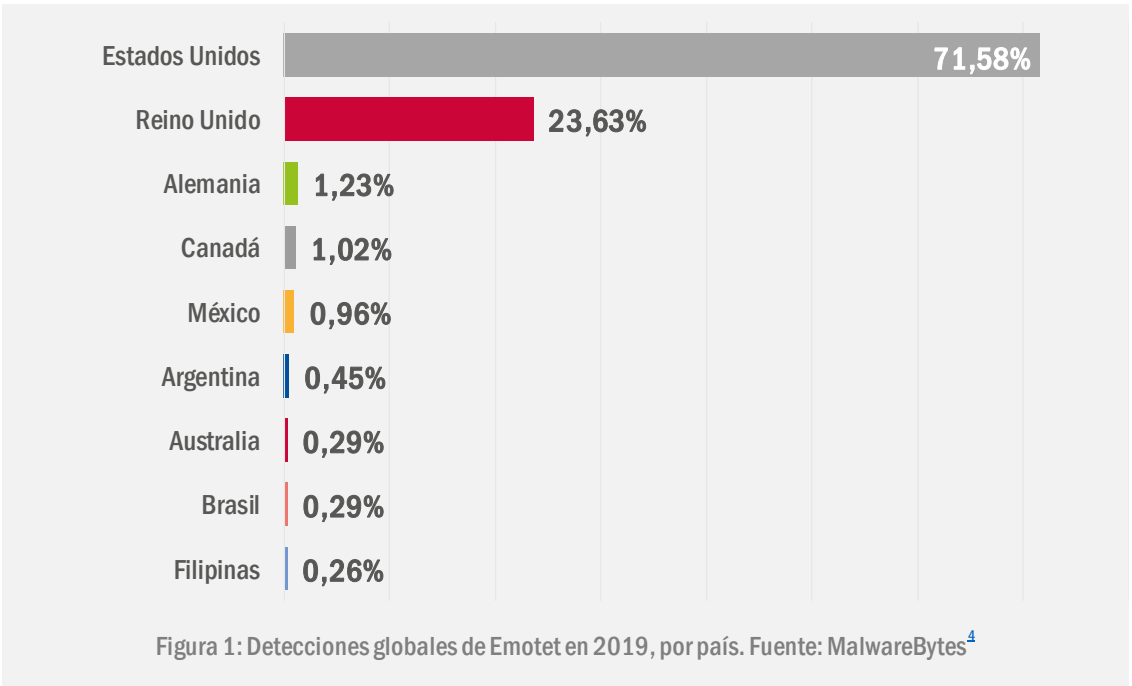


Figura 1: Detecciones globales de Emotet en 2019, por país. Fuente: MalwareBytes[4]

_Cambio a objetivos comerciales

Aunque las detecciones de *malware* en todo el mundo permanecieron similares a las de 2018[4,9], sí se observó un aumento del 13 % de *malware* dirigido contra empresas, y los sectores más afectados fueron el de servicios, educación y comercios.[4] Se estima que más de una tercera parte de los ataques de *malware* bancario en 2019 tuvieron como objetivo a usuarios corporativos, con la intención de comprometer los recursos financieros de la empresa.[10] Los cinco tipos de *malware*[4] principales utilizados para atacar a las empresas fueron: Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner y Virus.Renamer. En 2019 aumentaron los ataques de *ransomware* dirigidos al sector público por su capacidad para pagar rescates más altos.[11] Al mismo tiempo que los ciberdelincuentes apuntan hacia objetivos de alto valor, se diseñan nuevos tipos de *malware* para propagarse lateralmente dentro de una red corporativa en vez de por Internet.[12]

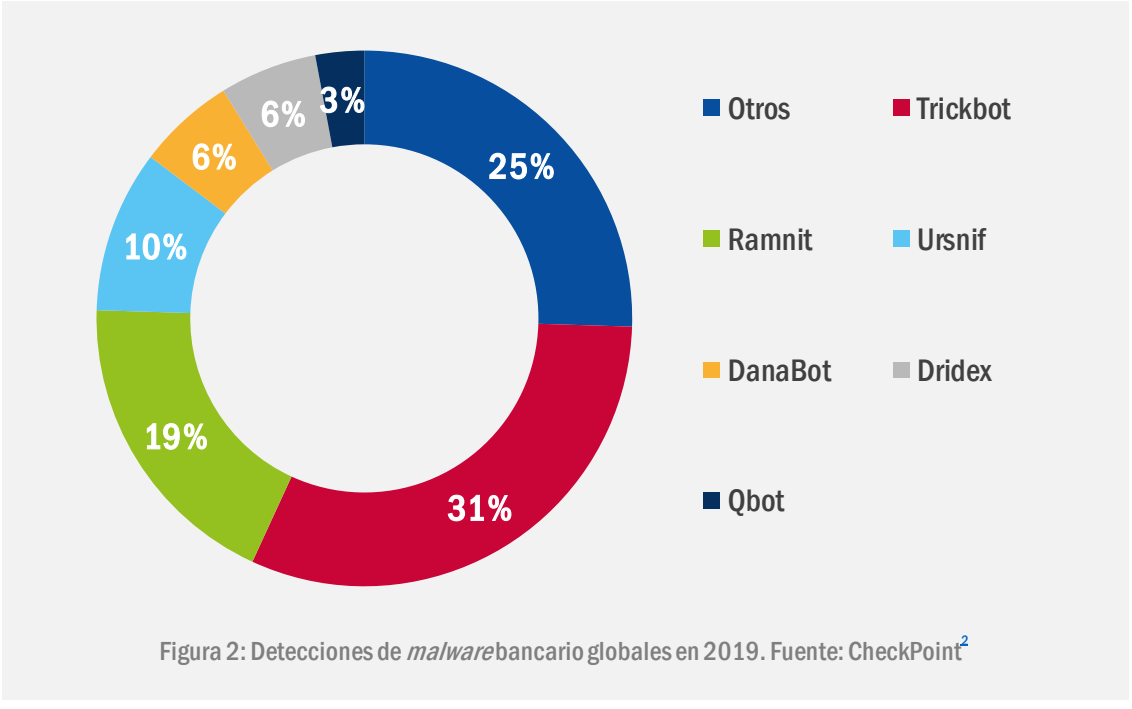


Figura 2: Detecciones de *malware* bancario globales en 2019. Fuente: CheckPoint[2]

Tendencias

_ Malware como servicio (MaaS)

El *malware* como servicio (MaaS, *malware-as-a-service*) se refiere a un tipo específico de *malware* a la venta en foros clandestinos que proporciona a los clientes (ciberdelincuentes) las herramientas e infraestructura necesaria para llevar a cabo ataques dirigidos. Un propietario de MaaS proporciona este servicio mediante la distribución de un *kit* que incluye cargador inicial, servidor de mando y control (C2) y puerta trasera para hacerse con el control del ordenador infectado.

Un investigador especializado en temas de seguridad[13] identificó recientemente cuatro tipos de ataque en los que se usaban varias herramientas de la cartera de productos de Golden Chickens (GC) Malware-as-a-Service (MaaS), lo que confirmaba la puesta en funcionamiento de variantes mejoradas con códigos actualizados en tres de estas herramientas.

- **TerraLoader**. Un cargador multifunción programado en PureBasic. TerraLoader es un producto insignia de la cartera de servicios de GC MaaS.
- **more_eggs**. Un programa de *malware* de puerta trasera capaz de señalizar a un servidor C2 fijo y ejecutar descargas adicionales desde un recurso *web* externo. La puerta trasera está programada en JavaScript.
- **VenomLNK**. Un archivo de atajo de Windows seguramente generado por una nueva versión del *kit* de VenomKit.

Aumento del *malware* dirigido a la banca móvil

Las aplicaciones para móviles diseñadas para robar datos de pago, credenciales y fondos de las cuentas bancarias de las víctimas aumentaron un 50 % durante el primer semestre de 2019.[14] Por lo habitual, los ciberdelincuentes han usado técnicas de *phishing* para obtener las credenciales bancarias, bien mostrando una página falsa que copia la página de apertura de sesión del banco, o introduciendo aplicaciones de móvil falsas que se parecen a las reales del banco. No obstante, en 2019 los ciberdelincuentes han hecho uso de su creatividad, como en el caso de Trojan-Banker.AndroidOS.Gustuff.a, que pudo hacerse con el control de una aplicación bancaria legítima al hacer un uso indebido de las funciones de accesibilidad del sistema operativo a través de las cuales pudo automatizar transacciones malintencionadas.[15] Se podían encontrar nuevas versiones de *malware* financiero para móviles a la venta en foros clandestinos[15] y se produjo un desarrollo continuo de nuevas técnicas de evasión. Una nueva adición importante descubierta en 2019 fue la capacidad del *malware* para usar sensores de movimiento y de activarse solo cuando un teléfono inteligente estaba en movimiento, este era por ejemplo el modo de operar del troyano bancario Anubis para detectar los entornos de aislamiento o pruebas.[16] El *malware* bancario más popular durante 2019[11] fue Asacub (44,4 %), seguido de Svpeng (22,4 %), Agent (19,1 %), Faketoken (12 %) y Hqwar (3,8 %).

Tendencias

_Malware sin archivos

El *malware* sin archivos no contiene archivos ejecutables y puede evadir los filtros habituales de seguridad y técnicas de registro de listas blancas. Por esta razón, esta familia de *malware* puede tener hasta diez veces más posibilidades de tener éxito que los demás programas de este tipo.[18] En vez de tener un archivo ejecutable, este tipo de *malware* requiere que el atacante inyecte un código malintencionado en un programa informático ya instalado y de confianza, bien de forma remota (p. ej., como en el caso del Instrumental de administración de Windows o WMI y PowerShell) o bien descargando activamente archivos de documentos (de Office por ejemplo) con macros malintencionadas.[19] Después de efectuar un ataque con éxito, el *malware* puede ganar persistencia a través del registro, el programador de tareas incorporado o el WMI. Los ataques con *malware* sin archivos aumentaron un 265 % durante el primer semestre de 2019.[20] La mayoría de estos ataques estaban basados en *scripts* (38 %), otros ejecutaban un ataque accediendo a la memoria (24 %) y otros abusaron de las vulnerabilidades de las herramientas del sistema (20 %) ya incorporadas.[21]

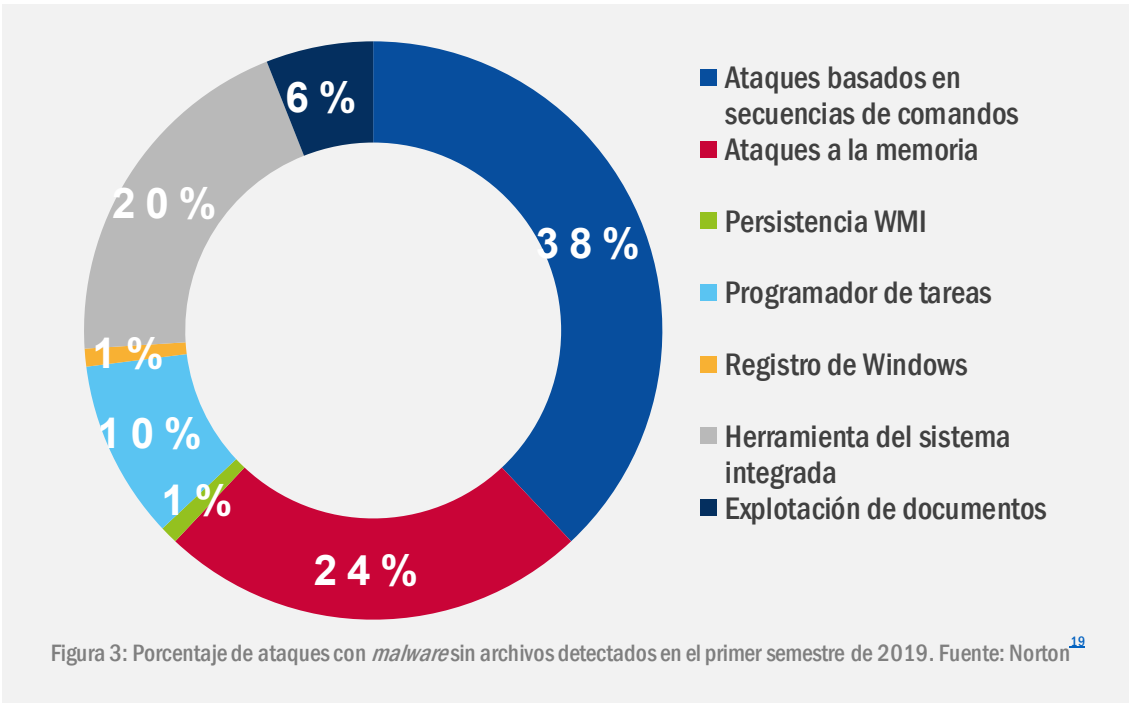


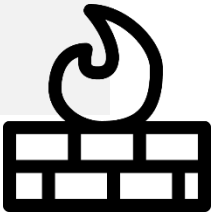
Figura 3: Porcentaje de ataques con *malware* sin archivos detectados en el primer semestre de 2019. Fuente: Norton[19]

¿Cómo prevenir y defenderse de un ataque sin archivos?

Para las organizaciones, la forma más eficaz de defenderse de un ataque sin archivos es mantener el *software* actualizado. Como la mayoría de las infecciones sin archivos ocurren en aplicaciones de Microsoft, especialmente en archivos «.docx», es de crucial importancia mantener estos programas actualizados a su última versión. Microsoft también ha actualizado el paquete de protección de aplicaciones Windows Defender para detectar actividad irregular en la aplicación PowerShell.

Según un investigador especializado en temas de seguridad[18], la clave para repeler con éxito una campaña de ataques sin archivos es abordando todas las fases del ciclo de vida de la amenaza con un enfoque defensivo multicapa e integrado. En este enfoque es importante investigar las distintas etapas del ataque y realizar las actividades siguientes:

- analizar y medir las acciones realizadas por el atacante;
- identificar las técnicas utilizadas;
- monitorizar las actividades en PowerShell u otros motores de *scripting*;
- acceder a datos de amenazas agregados;
- controlar el estado del sistema atacado;
- detener procesos arbitrarios;
- remediar los procesos que forman parte del ataque;
- aislar los dispositivos infectados.



Panorama de amenazas de *botnets* y mando y control

El tráfico de las *botnets* ha aumentado globalmente un 71,5 % desde 2018[2]. Las *botnets* observadas con más frecuencia fueron: Emotet (41 %), Trickbot (25 %) y DanaBot (5 %)[2]. Se observó un aumento notable del tráfico de *botnets* en Rusia (143 %), que se atribuyó principalmente a procedimientos de registro más relajados y a un menor interés por parte de las fuerzas y cuerpos de seguridad.[14] En 2019, Rusia fue el país anfitrión de la mayoría de los C2 de *botnets*, seguido por los Estados Unidos, los Países Bajos, China y Francia. Los ciberdelincuentes utilizaron algoritmos de generación de nombres de dominios (domain name generation algorithms, DGA) para respaldar la comunicación de muchos C2. El 50 % de estos registros se produjeron en dominios de nivel superior (top-level domains, TLD) «.com» y «.net».[15] Durante el período del informe, estos registros de nombres de dominios bajaron un 71 %, a favor de otros protocolos de comunicación como *peer-to-peer* (P2P).[13]

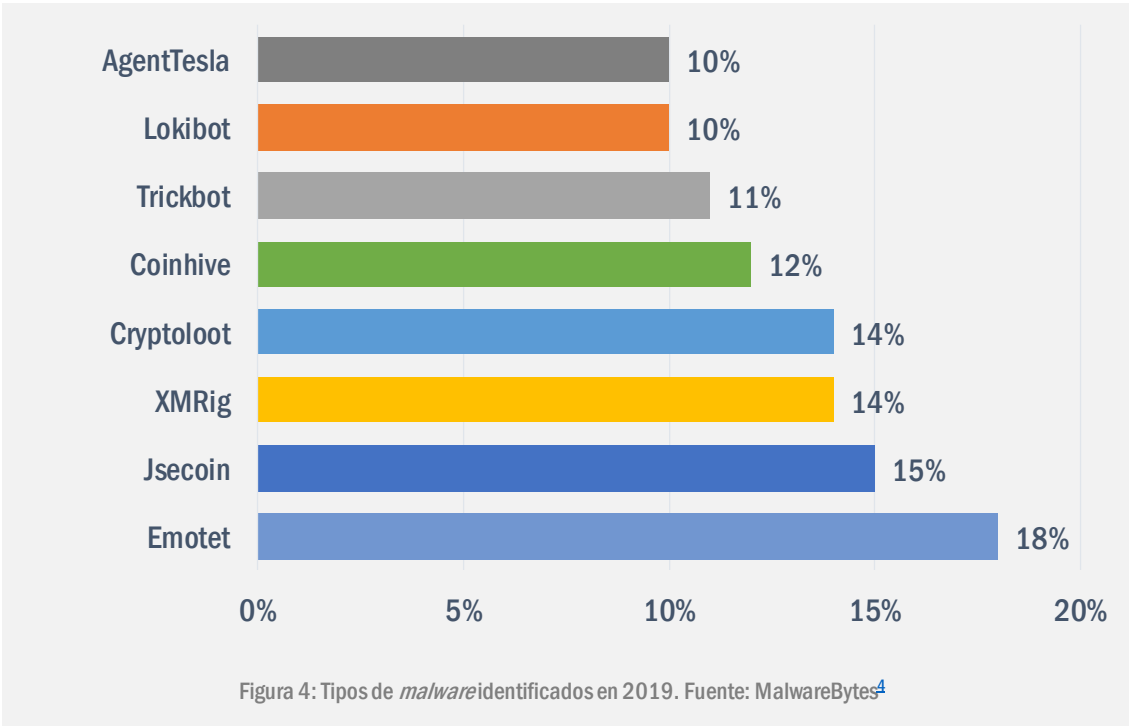


Figura 4: Tipos de *malware* identificados en 2019. Fuente: MalwareBytes[4]

_Cómo

Según un estudio de 2019, el 94 % de todos los tipos de *malware* se distribuyó por correo electrónico.[24] Aunque esto contaba como vector de punto de entrada, es interesante destacar que, tras un ataque con éxito, el *malware* podría descargar otro programa adicional que presenta un comportamiento similar al de un gusano para poder propagarse lateralmente por la red (Emotet y Trickbot). Además, después de la descarga inicial del *malware*, este se propagaba en la mayoría de los casos (71 %) a través de la actividad de los empleados. Otra vez, las nuevas vulnerabilidades del protocolo de estaciones de trabajo remotas (RDP) atrajeron la atención al permitir la ejecución de código de forma remota (RCE) y por lo tanto convirtiéndose en caldo de cultivo para los gusanos.[30] Aunque estas vulnerabilidades recién descubiertas no se han explotado a gran escala, se prevé que en un futuro cercano, un nuevo gusano ataque sistemas no actualizados.[31]

_Incidentes

- **Airbus** sufrió una filtración de los datos de sus empleados en Europa.[34,35]
- El *malware* de clonación de datos de tarjetas bancarias instalado en el sitio *web* de la **Agencia americana de cobro por servicios médicos** (AMCA) produjo el robo de los datos personales de 12 millones de pacientes.[36]
- Una de las empresas principales de pruebas diagnósticas de laboratorio **LifeLabs** fue víctima de un ataque de *ransomware* que permitió robar 15 millones de cuentas que contenían resultados de análisis médicos y números de tarjetas sanitarias.[37,38]
- Un ataque de *ransomware* en **Pensacola (Florida)** dio como resultado la publicación en línea de 2 GB de datos, posiblemente con información de identificación personal.[39]
- Los datos personales de 2 400 **miembros de las fuerzas armadas de Singapur** podrían haber sido filtrados en mensajes de *phishing* por un *malware*.[40]

Mitigación:

Acciones propuestas

- Implementar herramientas de detección de *malware* en todos los canales de entrada/salida, también para sistemas de correo electrónico, red, *web* y aplicaciones en todas las plataformas aplicables (servidores, infraestructura de red, ordenadores personales y dispositivos móviles).
- Inspeccionar el tráfico SSL/TLS y permitir al cortafuegos descifrar lo que se transmite hacia los sitios *web* y desde ellos, comunicaciones por correo electrónico y aplicaciones móviles.
- Establecer interfaces entre las funciones de detección de *malware* (búsqueda de amenazas dirigida por inteligencia) y gestión de incidentes de seguridad para establecer capacidades de respuesta eficaces.
- Usar las herramientas disponibles para el análisis del *malware* para compartir información y mitigar estas amenazas (como MISP).[32]
- Desarrollar políticas de seguridad que especifiquen los procesos a seguir en caso de infección.
- Entender las capacidades de varias herramientas de seguridad y desarrollar nuevas soluciones de seguridad. Identificar las brechas y aplicar el principio de «defensa en profundidad».
- Emplear filtros en el correo electrónico (o filtros de correo basura) para detectar mensajes malintencionados y eliminar los adjuntos ejecutables.
- Comprobar periódicamente los resultados de los barridos de los programas antivirus.[30,42]
- Registrar la monitorización usando una solución de gestión de la seguridad de la información y de eventos (SIEM). Fuentes de registro indicativas son las alertas antivirus, detección y respuesta en puntos finales (EDR), registros de servidores proxy, registros de Windows Event y Sysmon[43], registros de sistemas de detección de intrusión (IDS) [44], etc.
- Desactivar o reducir el acceso a las funciones de PowerShell.[45]

«La sofisticación de las capacidades de amenaza aumentó en 2019, y hubo muchos adversarios que usaron programas intrusos, robo de credenciales y ataques multietapa».

en PAE 2020

Bibliografía

1. "What is Malware". Veracode. https://www.veracode.com/security/malware
2. "Cyber Security Report". 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf
3. "Beapy: Cryptojacking Worm Hits Enterprises in China". 24 de abril de 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china
4. "2020 State of Malware Report". Febrero de 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
5. "Evasive Threats, Pervasive Effects" 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf
6. "SonicWall Cyber Threat Report". 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/
7. "Emotet is back: botnet springs back to life with new spam campaign". 16 de septiembre de 2019. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/
8. "Increased Emotet Malware Activity". 22 de enero de 2020. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity
9. "SonicWall Security Metrics" SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics
10. "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". 16 de abril de 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection
11. "Internet organised crime threat assessment" 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
12. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019". 6 de junio de 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019
13. "GOLDEN CHICKENS: Evolution of the MaaS". 20 de julio de 2020. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
14. "From Supply Chain to Email, Mobile and the Cloud". 25 de julio de 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/
15. "Mobile malware evolution 2019". 25 de febrero de 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/
16. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". 17 de enero de 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/
17. "Spamhaus Botnet Threat Report 2019". 28 de enero de 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
18. "What Is Fileless Malware?". McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
19. "What is fileless malware and how does it work?" . Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html
20. "Trend Micro Report Reveals 265% Growth In Fileless Events". 28 de agosto de 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html
21. "Understanding Fileless Threats". 29 de julio de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. "SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter". 22 de octubre de 2019. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. "2020 Vulnerability and Threat Trends". 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". 16 de abril de 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. "Internet organised crime threat assessment" 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019". 6 de junio de 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. "From Supply Chain to Email, Mobile and the Cloud". 25 de julio de 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. "Mobile malware evolution 2019". 25 de febrero de 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. "Mobile banking malware surges in 2019". 25 de julio de 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". 17 de enero de 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. "BlueKeep attacks are happening, but it's not a worm". 3 de noviembre de 2019. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. MISP Projects. http://www.misp-project.org/

33. "PowerShell, fileless malware's great attack vector". 25 de febrero de 2019. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. "Airbus Statement on Cyber Incident". 30 de enero de 2019. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. "Airbus data breach impacts employees in Europe". 30 de enero de 2019. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. "Massive Quest Diagnostics data breach impacts 12 million patients". 4 de junio de 2019. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. "Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers". 17 de diciembre de 2019. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. "Why the LifeLabs Hack Likely Is Worse than Most". 18 de diciembre de 2019. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. "Personal Information in City of Pensacola Cyberattack". 17 de enero de 2020. City of Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. "Personal data of 2,400 Mindef, SAF staff may have been leaked" 22 de diciembre de 2019. The Straits Times - Singapore. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

Bibliografía

41. AVTEST – The Independent IT-Security Institute. https://www.av-test.org/en/

42. "Real world protection tests." AV Comparatives. https://www.av-comparatives.org/dynamic-tests/

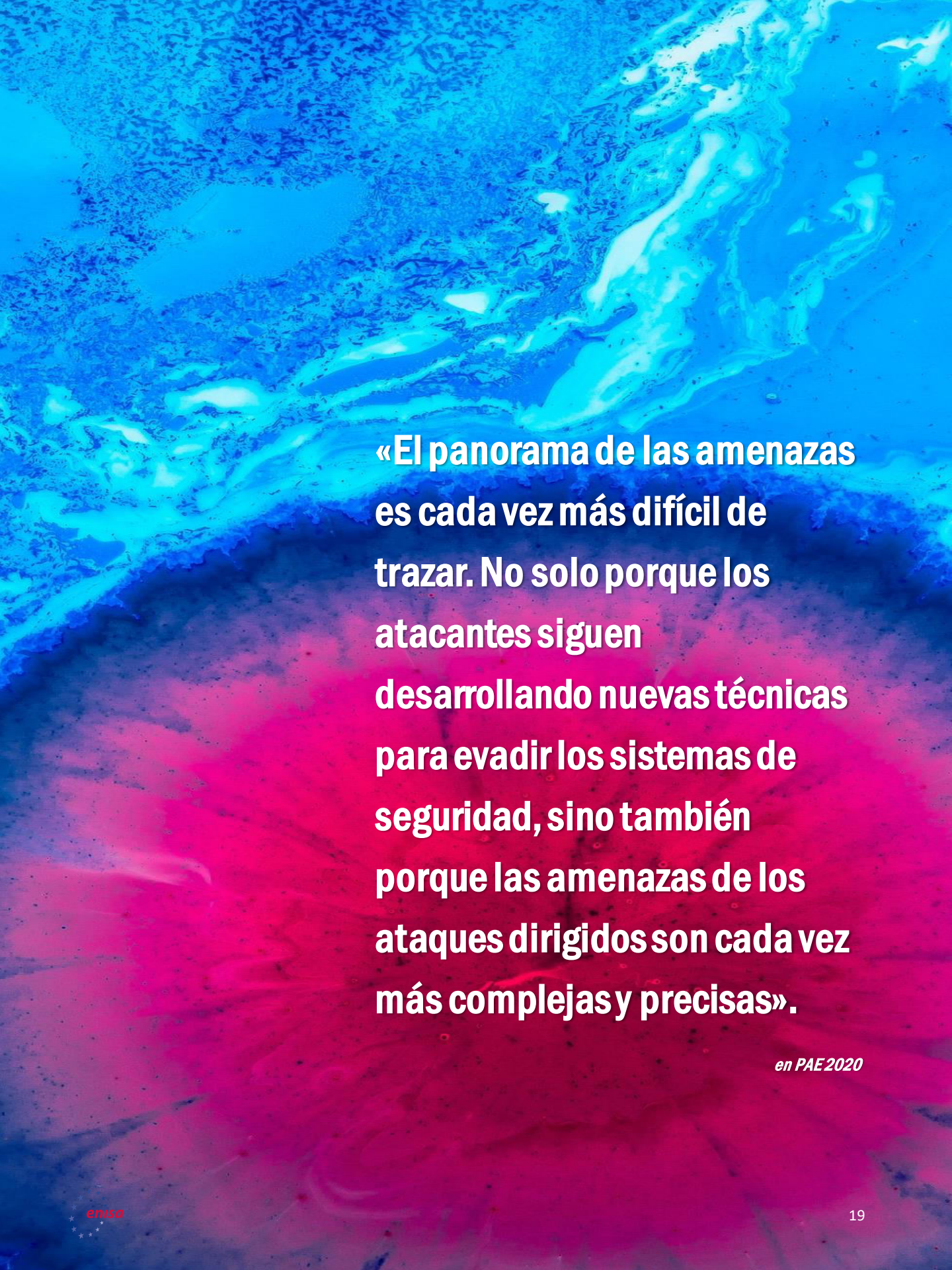
43. "The ThreatHunting Project." https://www.threathunting.net/data-index

44. Mark Russinovich, Thomas Garnier. "Sysmon v11.10." 24 de junio de 2020. Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

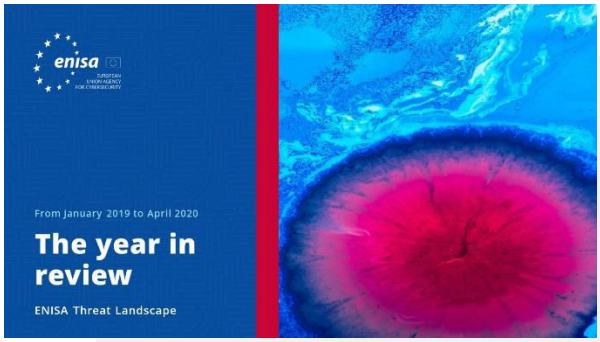
45. "Guide to Intrusion Detection and Prevention Systems (IDPS)." Febrero de 2007 CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

47. "Most malware in Q1 2020 was delivered via encrypted HTTPS connections". 25 de junio de 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

48. "Malware statistics and facts for 2020". 29 de julio de 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/


«El panorama de las amenazas es cada vez más difícil de trazar. No solo porque los atacantes siguen desarrollando nuevas técnicas para evadir los sistemas de seguridad, sino también porque las amenazas de los ataques dirigidos son cada vez más complejas y precisas».
en PAE 2020

Lecturas relacionadas



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

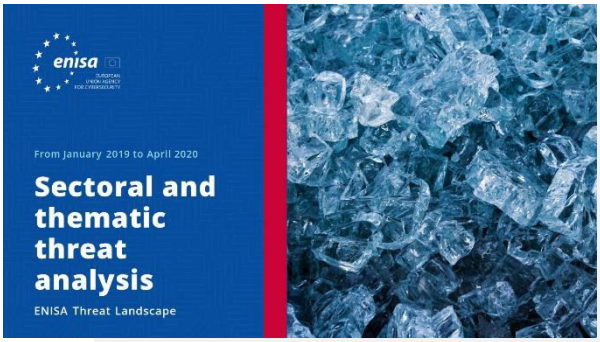
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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.



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.

LEER EL INFORME

¿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