ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Crypto-jacking

Panorama de Amenazas de la ENISA

Sinopsis

El *cryptojacking* o criptosecuestro (también conocido como *cryptomining* o criptominería) es el uso no autorizado de los recursos de un dispositivo para generar criptomonedas. Los objetivos incluyen cualquier dispositivo conectado, como un ordenador o un teléfono móvil, pero los ciberdelincuentes han aumentado los ataques a las infraestructuras en la nube.[1] Este tipo de ataque no ha atraído mucho la atención de las fuerzas y cuerpos de seguridad y su abuso se notifica muy raramente[2], principalmente porque tiene relativamente pocas consecuencias negativas. No obstante, las organizaciones sí pueden notar unos costes informáticos más altos, degradación de los componentes de *hardware*, un consumo más alto de electricidad y una productividad reducida por parte de los empleados causada por la ralentización de las estaciones de trabajo.[3]

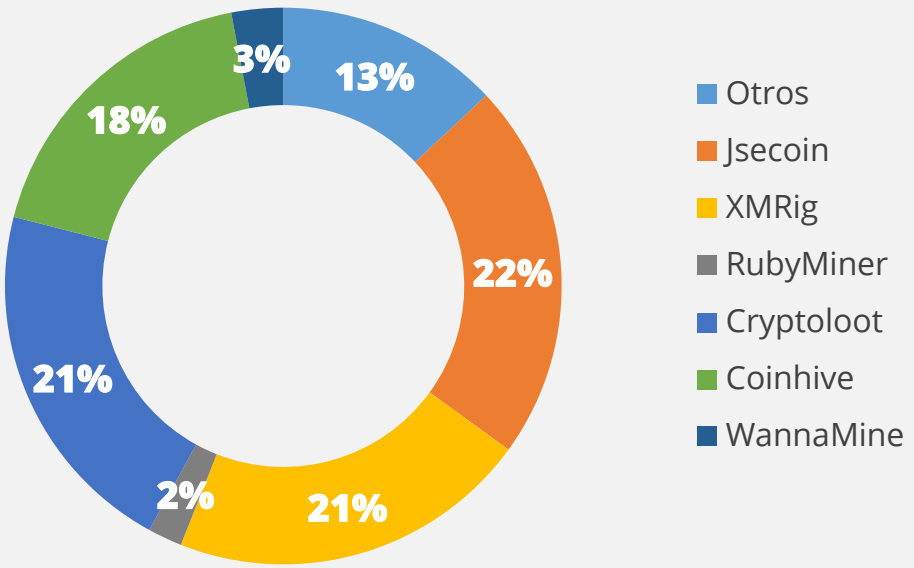


Figura 1: Principales programas de *malware* dedicados a la criptominería. Fuente: Check Point[9]

Conclusiones

64,1_millones de ataques de criptosecuestro hacia finales de 2019.

78 %_es el porcentaje de descenso en las actividades de criptosecuestro en el segundo semestre de 2019 con respecto al primero.

Las actividades aumentaron un 9 % en la primera mitad de 2019 en comparación con los 6 meses anteriores de 2018.[4,5]

65 %_de las 120 transacciones más populares en el tercer trimestre de 2019 usaban procesos débiles o porosos de «conoce a tu cliente» (know your customer, KYC).

El 32 % de las transacciones se hicieron con monedas de privacidad.[6]

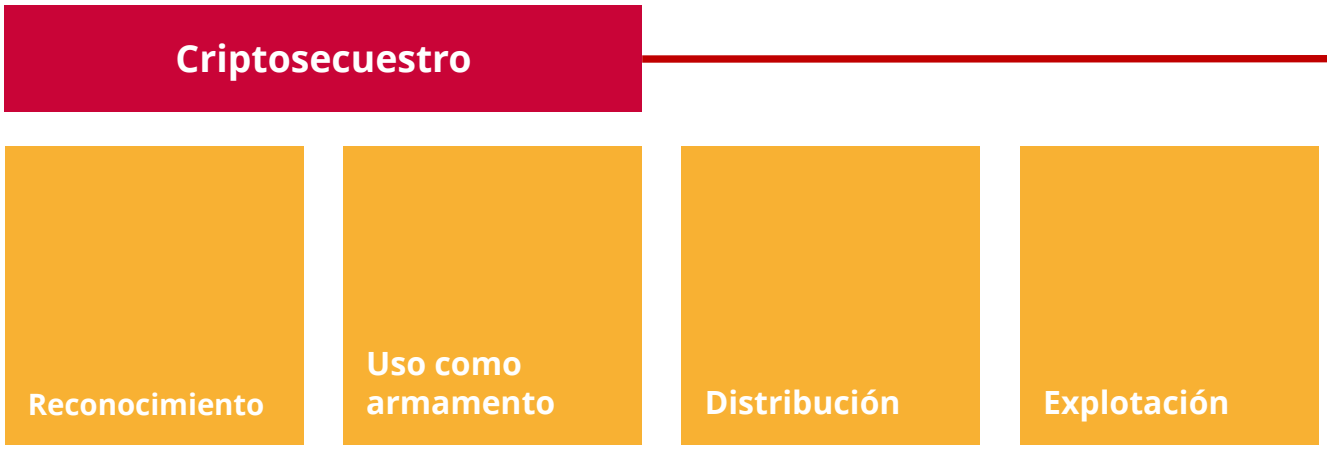
39,3 %_de las infecciones de criptominería de 2019 iban dirigidas a Japón.

India fue el objetivo del 20,8 % de las infecciones de criptominería y Taiwán del 14,2 %. La Figura 2 representa los cinco países con la mayoría de los intentos de infecciones por *malware* de criptominería detectados en 2018 y en 2019.[7]

13 %_ de los incidentes de criptosecuestro se atribuyen a trojan.Win32.Miner.bbb

Durante el período de noviembre de 2018 a octubre de 2019, los programas de minería más activos después del anterior fueron Trojan.Win32.Miner.ays (11,35 %) y Trojan.JS.Miner.m (11,12 %).[6]

Kill chain



Paso del proceso de ataque

Amplitud de la intención

Criptosecuestro

Instalación	Mando y control	Acciones sobre objetivos

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

Tendencias

El popular servicio de criptominería Coinhive ha cerrado

Coinhive empezó a funcionar en septiembre de 2017 y se anunciaba como una fuente de ingresos alternativa para los desarrolladores de *web* en lugar de los anuncios en páginas *web*.[24] Utilizaba bibliotecas de JavaScript, que se podían instalar en sitios *web*, y la capacidad de procesamiento del visitante para generar criptomoneda de forma legítima. Hasta su cierre en marzo de 2019, había sido objeto de numerosos abusos por parte de ciberdelincuentes que inyectaban código en sitios *web* comprometidos a fin de generar la criptomoneda Monero y desviar fondos a sus propios bolsillos. Tras el cierre, el volumen de ataques de criptosecuestro basados en la *web* descendió un 78 % durante la segunda mitad de 2019.[4] Como resultado de este descenso, los ciberdelincuentes empezaron a centrarse en objetivos de más alto valor, como servidores potentes[9] e infraestructuras en la nube.[1] Coinhive, que figuraba en el primer lugar en la lista, ha sido adelantado por[9] Jsecoin (22 %), XMRig (21 %) y Cryptoloot (21 %). La distribución de los programas de *malware* de criptominería más importantes globalmente se presenta en la Figura 1.

Más ataques en infraestructuras en la nube

En la primera mitad de 2019 se hizo visible la tendencia en ascenso de los incidentes de criptominería en la nube.[15,25] Los entornos de nube suelen emplear mecanismos que ajustan los recursos a medida de la demanda y, por lo tanto, son objetivos lucrativos para ejecutar el *software* de minería. Sin embargo, esto se consigue a expensas de los propietarios del sitio *web*, que quienes pagan facturas más altas por exceder las cuotas.[15] En la primera mitad de 2019 las vulnerabilidades del *software* de almacenamiento en la nube aumentaron un 46 % con respecto al mismo período en 2018.[26] Los atacantes han tenido éxito explotando las interfaces de programación de aplicaciones (API) y las plataformas de gestión de almacenamiento para instalar imágenes malintencionadas (p. ej., Docker y Kubernetes) y proceder a la criptominería.[25]

_Incidentes

*Abril de 2019*_ La campaña de criptosecuestro, apodada Beapy, explotó la vulnerabilidad EternalBlue y afectó a empresas de China[3]

*Mayo de 2019*_ El *malware* PCASTLE de minado de Monero atacó mayoritariamente a sistemas ubicados en China empleando técnicas de llegada sin archivos.[19]

Se encontraron más de 50 000 servidores que pertenecían a empresas de los sectores de la salud, telecomunicaciones, medios y TI infectados con el *malware* TurtleCoin (TRTL) de criptominería.[20] Una nueva familia de *malware*, denominada BlackSquid, utilizó ocho programas intrusos (*exploits)* conocidos, entre ellos EternalBlue y DoublePulsar, y seguidamente se propagó a servidores *web* de Tailandia y Estados Unidos para suministrar código de minería de Monero.[17,21]

*Agosto de 2019*_ Se encontró *malware* de criptosecuestro en 11 repositorios de idiomas de RubyGem que expuso a cientos de usuarios al código de criptominería[22]

Tendencias

Cambio hacia la criptominería basada en archivos

En 2019 se observó un descenso en las técnicas de criptosecuestro basadas en los programas navegadores y una subida en las basadas en archivos. Los ataques de criptominería basados en archivos[27] se propagan mediante *malware* y utilizan programas intrusos ya existentes en sistemas operativos no actualizados, como EternalBlue y otras vulnerabilidades de alto riesgo. Los factores que contribuyeron a este cambio fueron el cierre del popular proveedor de minería basada en la *web* Coinhive[1] y el descenso del valor de las criptomonedas.[10] Otro factor es que la criptominería basada en archivos siempre ha sido más eficiente que la basada en la *web* y es 25 veces más lucrativa.[3] Los atacantes adaptaron su *malware* con herramientas adicionales para extraer información sensible del ordenador de las víctimas.

El número de ataques de criptosecuestro desciende en todo el mundo

En 2019 se observó una tendencia de descenso[5] de los ataques de criptosecuestro, debida principalmente al cierre de Coinhive[6], los esfuerzos coordinados de las fuerzas y cuerpos de seguridad y la depreciación de la criptomoneda Monero. No obstante, como se sabe que los ataques de criptosecuestro siguen los valores de las criptomonedas, podría surgir un servicio similar al de Coinhive e impulsar un nuevo pico. Las estadísticas tempranas de 2020 indican un aumento interanual del 30 % en marzo.

_Monero siguió siendo la criptomoneda preferida

Al igual que en tendencias previas, Monero (XMR) fue la criptomoneda preferida para las actividades de criptosecuestro durante 2019. Esto se debe a dos razones: la primera es que Monero se centra en la privacidad y en el anonimato y, por tanto, las transacciones no se pueden trazar; la segunda es que el algoritmo Proof-of-Work se ha diseñado para hacer que las actividades de minería sean viables con una CPU estándar en vez de requerir *hardware* especializado. En el tercer trimestre de 2019, un 32 % de las transacciones fueron con criptomonedas privadas como Monero. No obstante, en anticipación a las nuevas normativas contra el blanqueo de dinero, muchas transacciones optaron por excluir las criptomonedas privadas.

_Los países más atacados

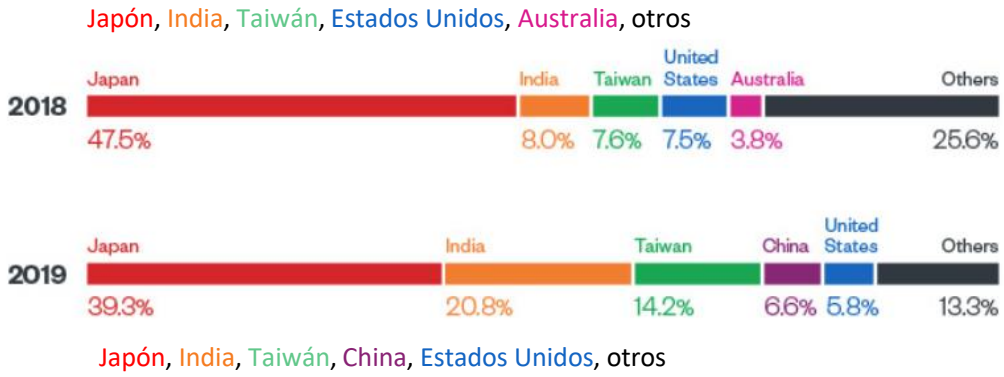


Figura 2: Los países con más ataques de criptosecuestro. Fuente: Trend Micro[7]

Vectores de ataque

Técnicas

Los ciberdelincuentes utilizaron las siguientes técnicas para ejecutar o instalar programas de criptominería:

- incorporación de capacidades de criptosecuestro en *malware* existente;[10]
- compromiso de la integridad de los sitios *web*;[11]
- ataques persistentes de descarga oculta (*drive-by*);[12]
- uso de redes sociales;[13]
- uso de aplicaciones móviles y tiendas de aplicaciones;[14]
- uso de *kits* de programas intrusos (*exploits*);[15]
- uso de redes de publicidad malintencionada (*malvertising*);[16]
- uso de dispositivos extraíbles;[17]
- y uso de gusanos criptomineros.[18]

Figura 3: ¿Cuánto puede ganar una *botnet* dedicada a la criptominería en 30 días?
Fuente: Broadcom[3]

Acciones propuestas

- Vigilar el nivel de carga de la batería de los dispositivos de los usuarios y, en caso de subidas sospechosas en el uso de la CPU, hacer un análisis del sistema para detectar la presencia de programas de minería basados en archivos.
- Instalar programas de filtrado de contenido para filtrar documentos adjuntos no deseados, mensajes de correo electrónico con contenido malintencionado y basura.
- Implementar el filtrado del protocolo de minería por estratos, hacer listas negras de direcciones de IP y de dominios de agrupaciones populares de minado.
- Instalar protección en los puntos terminales con programas antivirus o programas complementarios de navegadores para el bloqueo de agentes de criptominería.
- Realizar auditorías de seguridad periódicas para detectar anomalías en la red.
- Implementar una gestión robusta de vulnerabilidades e instalación de parches.
- Usar listas blancas para evitar que ejecutables desconocidos se ejecuten en los puntos terminales.
- Invertir en el aumento de la concienciación de los usuarios en materia de criptosecuestro, especialmente en lo que se refiere al uso seguro de navegadores.
- Instalar parches y correcciones contra programas intrusos bien conocidos como Eternal Blue, en objetivos menos evidentes, como los sistemas de gestión de colas, terminales POS e, incluso, máquinas expendedoras.
- Vigilar y añadir en listas negras los ejecutables más habituales de criptominería.

Bibliografía

1. Sergiu Gatlan. "Cryptominers Still Top Threat In March Despite Coinhive Demise." 9 de abril de 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. "Internet Organised Crime Threat Assessment (IOCTA)." 2019. EUROPOL. https://www.europol.europa.eu/iocta-report

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. Bill Conner. "SONICWALL Cyber Threat Report." 2020. SONICWALL https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. Yessi Bello Perez. "Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019." 24 de julio de 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6. Ben Noble. "A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule." 27 de noviembre de 2019. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. "Defending Systems Against Cryptocurrency Miner Malware." 28 de octubre de 2019. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. "Kaspersky Security Bulletin '19 Statistics." 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. "CYBER SECURITY REPORT." 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. "EternalBlue Exploit Serves Beapy Cryptojacking Campaign." 25 de abril de 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. "New mining worm PsMiner uses multiple high-risk vulnerabilities to spread." 12 de marzo de 2019. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. "New drive-by cryptocurrency mining scheme persists after you exit your browser window." 9 de noviembre de 2017. Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr. Michaeal McGuire. "Social Media Platforms and the Cybercrime Economy." 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. "Abusing cryptocurrencies on Android smartphones." 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. "2019 Midyear Security Roundup Evasive Treats Pervasive Effects." 2019. TrendMicro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. "YouTube shuts down hidden cryptojacking adverts." 29 de enero de 2018. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. "New cryptocurrency mining malware is spreading across Thailand and the US." 4 de junio de 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. "BlueKeep is back. For now, attackers are just using it for cryptomining." 4 de noviembre de 2019. CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. "Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques." 5 de junio de 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. "Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware." 29 de mayo de 2019. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. "BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner." 27 de agosto de 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. "Malicious cryptojacking code found in 11 Ruby libraries." 2 de agosto de 2019, Decrypt. https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. "Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play ." 6 de agosto de 2019. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. "Coinhive cryptojacking service to shut down in March 2019". 27 de febrero de 2019. ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

25. Tom Hegel. "Making it Rain - Cryptocurrency Mining Attacks in the Cloud". 14 de marzo de 2019. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. "How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model". Agosto de 2019. Carbon Black. https://www.carbonblack.com/resources/access-mining/

27. "Cryptojacking Attacks: Who's Mining on Your Coin?". 5 de abril de 2019. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. "Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz'. 12 de abril de 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

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

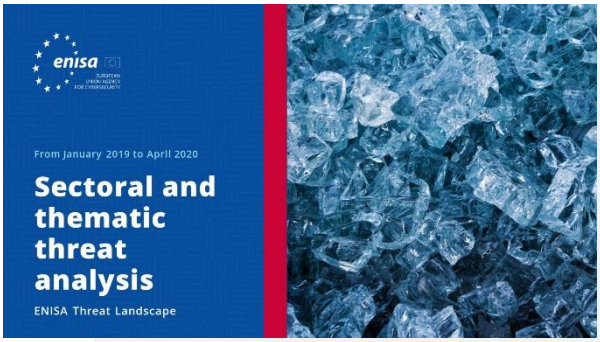
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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.



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 las 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) and 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. Esta publicación tampoco refleja necesariamente la información más actual 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.

Aviso de copyright

© Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2020
Reproducción autorizada siempre que se indique la fuente.

Copyright de la imagen de la portada: © Wedia. Para utilizar o reproducir fotografías o cualquier otro material de cuyos derechos de autor no sea titular la ENISA, debe obtenerse el permiso directamente de los titulares de los derechos de autor.

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

Reservados todos los derechos. Copyright
ENISA 2020.

https://www.enisa.europa.eu