ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Ataques que afectan a aplicaciones *web*

Panorama de Amenazas de la ENISA

Sinopsis

Las aplicaciones y tecnologías *web* se han convertido en una parte fundamental de Internet al adoptar usos y funcionalidades diversas. El aumento de la complejidad de las aplicaciones *web* y sus amplios servicios crea retos a la hora de protegerlos contra amenazas que tienen diversos motivos, desde económicos o daños a la reputación, hasta el robo de datos vitales o personales.[1] Los servicios y aplicaciones *web* dependen sobre todo de bases de datos que almacenan o proporcionan la información necesaria. Los ataques de tipo inyección SQL (SQLi) son un ejemplo bien conocido y la amenaza más frecuente contra estos servicios. Otro ejemplo son los ataques tipo *cross-site scripting* (XSS). En este tipo de ataque, el agente malintencionado utiliza puntos débiles de los formularios u otras funcionalidades de entrada de las aplicaciones *web* para llevar a otras funciones malintencionadas, como el desvío a un sitio *web* peligroso.[2]

Aunque las organizaciones acumulan conocimiento y están desarrollando procesos de automatización más uniformes en el ciclo de vida de sus aplicaciones *web*, la seguridad es para ellas la parte más importante de su oferta y escala de prioridades. Esta introducción de entornos complejos lleva a la adopción de nuevos servicios, como las interfaces de programación de aplicaciones (API). Las API, que crean nuevos retos para la seguridad de las aplicaciones, fuerzan a las organizaciones a considerar más medidas de prevención y detección. Por ejemplo, aproximadamente un 80 % de las organizaciones adoptan controles desplegados por API en su tráfico de entrada.[3] En este apartado se revisa el panorama de amenazas que afectaron a las aplicaciones *web* durante 2019.

_Tendencias

*20 %*_ de las empresas y organizaciones notificaron ataques DDoS en sus servicios de aplicaciones a diario.[5]

La técnica más usada fue la del desbordamiento del búfer (24 %). Otras técnicas de uso frecuente fueron la saturación de HTTP (23 %), reducción de recursos (23 %), saturación de HTTPS (21 %) y Low Slow (21 %).

*63 %*_ de los participantes en una encuesta de CyberEdge utilizan un cortafuegos de aplicaciones *web* (WAF).

Un 27,5 % tiene planes de utilizar esta tecnología y un 9,5 % no los tiene.[15]

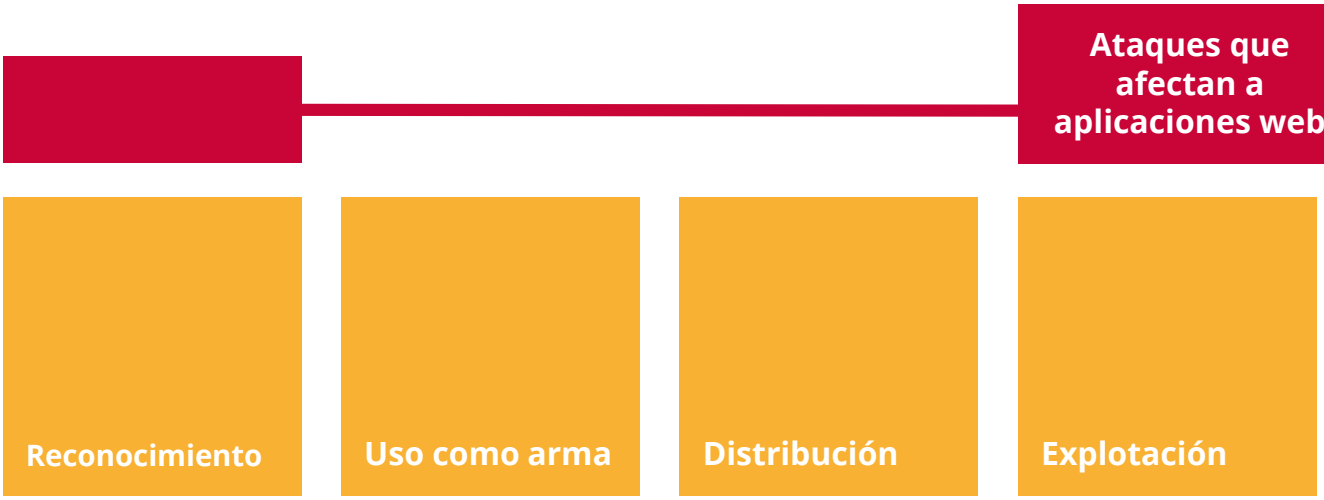
*52 %*_ es el aumento en el número de ataques a aplicaciones *web* en 2019 con respecto a 2018.

Según un investigador especializado en temas de seguridad, el número de ataques a aplicaciones *web* fue casi el mismo en comparación con 2018 y subió más tarde ese año.[4]

*84 %*_ de las vulnerabilidades observadas en aplicaciones *web* se debieron a errores de configuración de la seguridad.

A esto le siguen los ataques de *cross-site scripting* (53 %) y la autenticación descifrada (45 %).[9]

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

Mejora de la colaboración entre la seguridad de las aplicaciones y su desarrollo

Según una encuesta realizada por un investigador especializado en temas de seguridad[5], uno de los factores que contribuyen a que la seguridad sea tan poco eficaz podría deberse a la toma de decisiones sobre la propiedad de las herramientas de seguridad. La encuesta presentaba las opiniones de los representantes más influyentes en este campo, nombrando a los responsables de TI y propietarios de empresas, y no al responsable principal de la seguridad de la información (CISO).

Aumento de la importancia de las API

Las API no son algo nuevo en la arquitectura de las aplicaciones *web* y su uso, ampliamente aceptado, reintroduce riesgos existentes y sus posibilidades de explotación como resultado de la ampliación del panorama de amenazas. En este sentido, el proyecto OWASP (Open Web Application Security Project) para la seguridad de las aplicaciones *web* publicó una lista con las 10 medidas de seguridad principales para las API, y 6 de ellas proporcionaban una forma priorizada de asegurar esta capacidad en la arquitectura de las aplicaciones *web*. Un ejemplo de este tipo de amenaza son los ataques a las API de PHP: según otro investigador especializado en temas de seguridad, el 87 % de la vigilancia del tráfico de API se hacía buscando las API de PHP disponibles.[7]

Fallos de autorización y autenticación

Suelen ser la causa principal del acceso a información vital por parte de los atacantes (como el ataque sufrido por Fast Retailing[8]). Según un investigador especializado en temas de seguridad, las filtraciones de datos vitales son la segunda amenaza más apremiante para la seguridad de las aplicaciones *web*.[9]

Tendencia en aumento de la inyección SQL (SQLi)

En un estudio reciente en materia de seguridad se informaba de que dos terceras partes de los ataques a aplicaciones *web* incluían ataques SQLi. Mientras que otros vectores de ataque permanecen estables o van en aumento, los ataques SQLi siguieron aumentando considerablemente, y aumentaron especialmente durante el período vacacional de 2019.[11] Los resultados de este estudio también indicaban que el sector financiero se enfrenta a más ataques de inclusión de archivo local (LFi) que el resto de los sectores.[12]

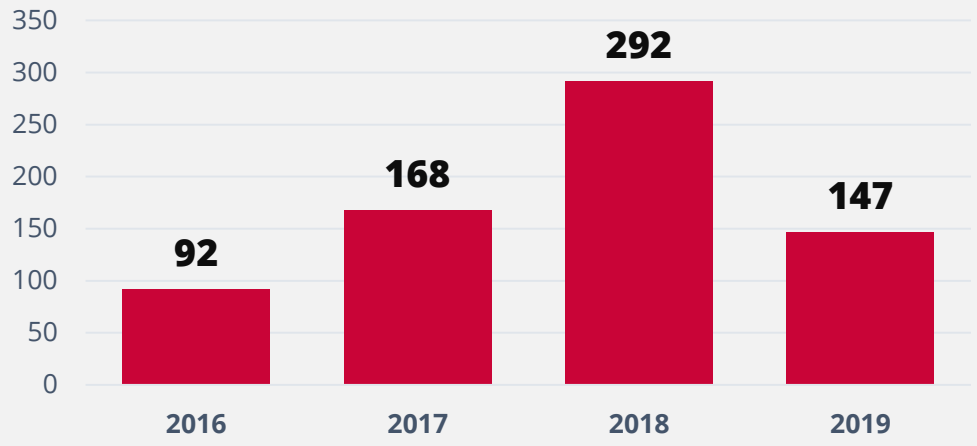


Figura 1: Reducción del número de archivos borrados por sitio comprometido. Fuente: Sucuri[10]

Vectores de ataque

Vectores de ataque de aplicaciones *web*

La percepción general es que los ataques a las aplicaciones *web* son bastante diversos. Sin embargo, los datos procedentes de estudios de seguridad sugieren que la mayoría de los ataques a estas aplicaciones son SQLi o LFi.[11,13,14] En otro informe se sugiere que SQLi, salto de directorio, XSS, infracción de autenticación y gestión de la sesión son los vectores principales utilizados en estos tipos de ataque.[4]

SONICWALL también notificó una tendencia similar de los ataques a aplicaciones *web* principales en 2019. En la lista SQLi, salto de directorio, XSS, infracción de autenticación y gestión de sesión iban en cabeza.[4]

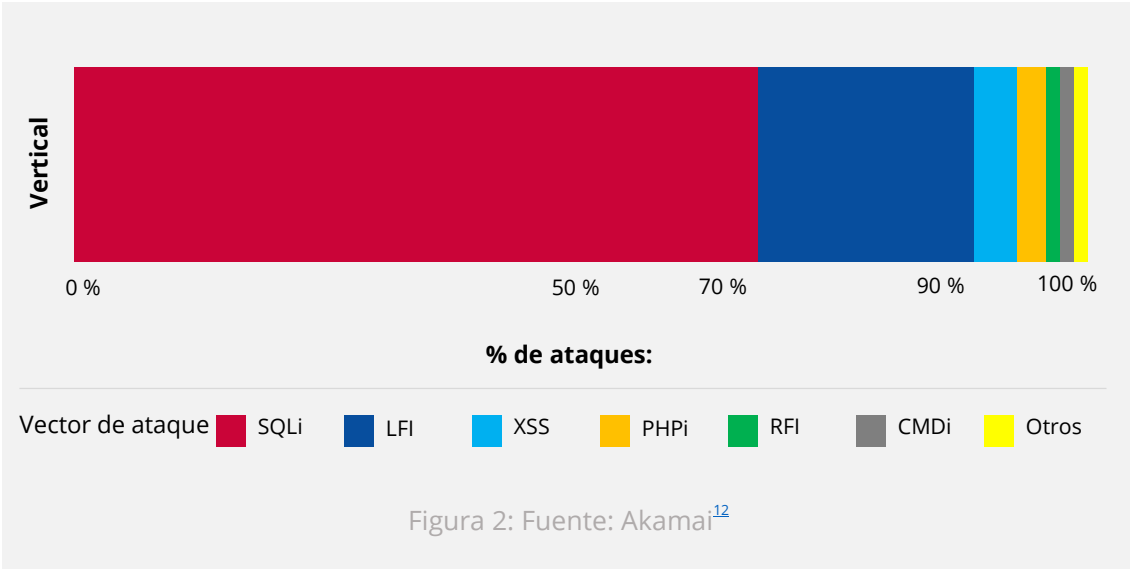


Figura 2: Fuente: Akamai[12]

Ataques que afectan a aplicaciones *web*

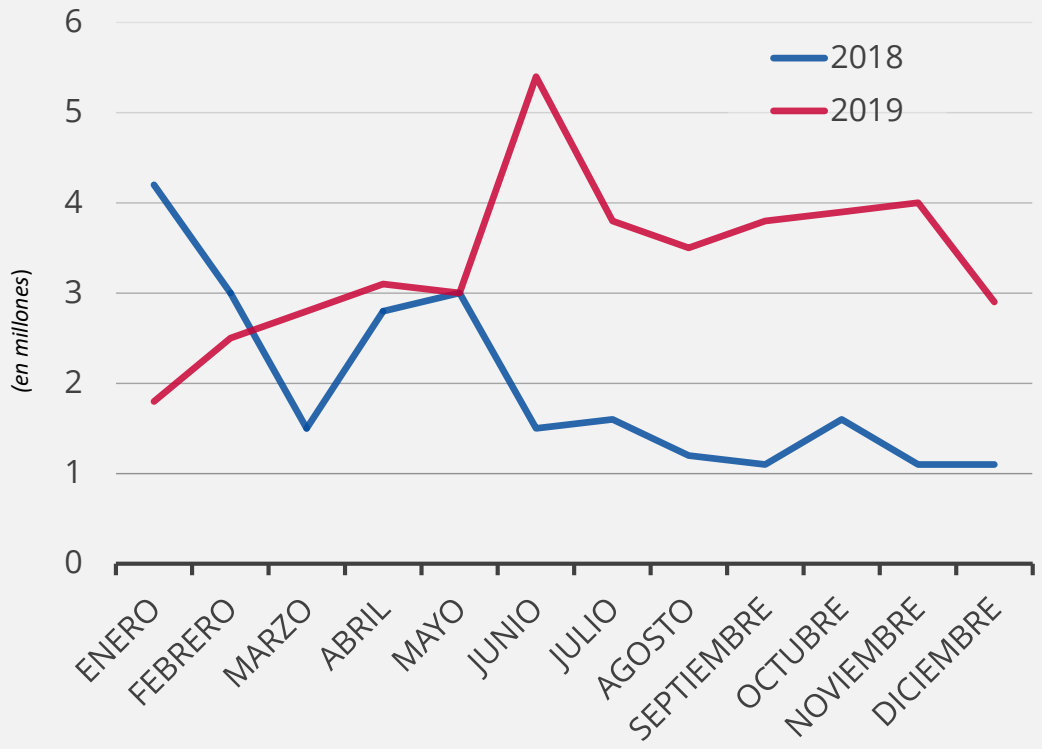


Figura 3 - Fuente: Sonicwall[4]

Mitigación:

Acciones propuestas

- Utilizar técnicas de validación de entrada y aislamiento para los ataques de tipo inyección (como las declaraciones parametrizadas, escapar la entrada de usuario, validación de entrada, etc.)[16].
- Implementar un cortafuegos para aplicaciones como medida preventiva de defensa[17] (también llamados parches virtuales).[18]
- Para las API de aplicaciones web[19]:
    - implementar y mantener un inventario de las API y validarlas en barridos del perímetro y de descubrimiento interno a través de equipos de desarrollo y operativos;
    - encriptar la comunicación y conexión de las API;
    - proporcionar los mecanismos y niveles de autorización correctos para la autenticación.
- Incorporar procesos de seguridad de aplicaciones en el desarrollo de las aplicaciones y en el ciclo de vida del mantenimiento.[20]
- Restringir el acceso al tráfico de entrada solo para servicios requeridos.[20]
- Desplegar capacidades de gestión del tráfico y del ancho de banda.
- Imponer el endurecimiento del servidor de aplicaciones *web* y mantener una buena gestión de parches y de procesos de prueba.[21]
- Realizar evaluaciones de vulnerabilidades y riesgos antes y durante el desarrollo de la aplicación *web*.
- Realizar pruebas periódicas de penetración durante la implementación y después del despliegue.

_Aplicaciones *web* por máxima gravedad de las vulnerabilidades encontradas

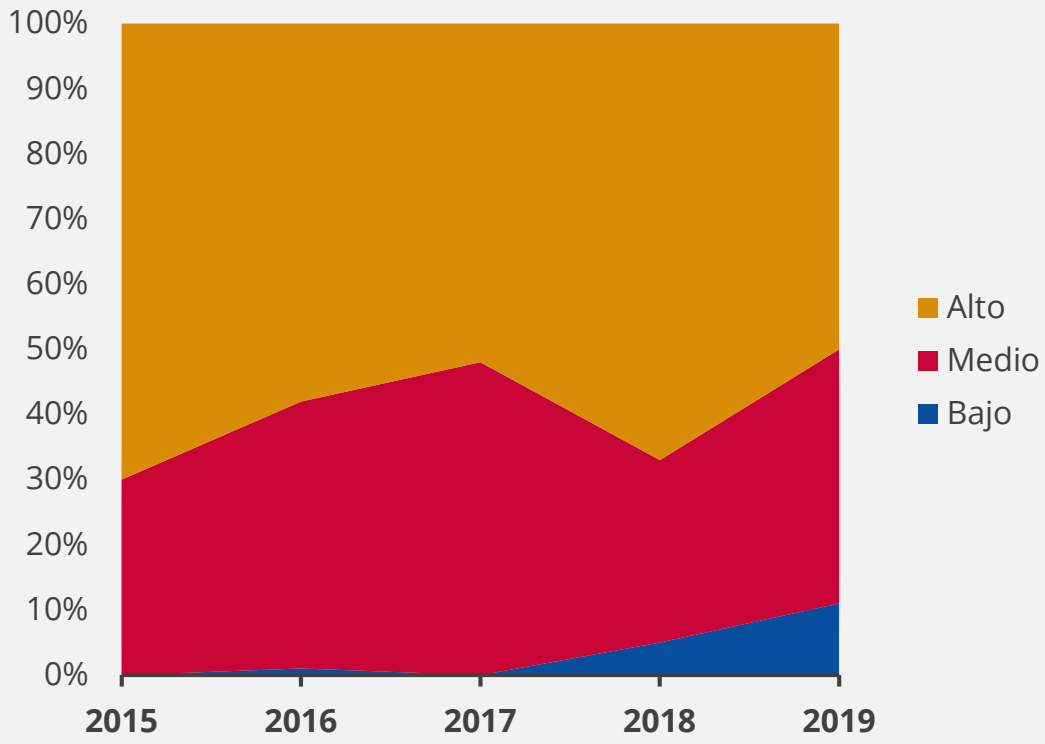


Figura 4 - Fuente: Positive Technologies[9]

Bibliografía

1. "The Future Is the Web! How to Keep It Secure?" Octubre de 2019. Acunetix. https://www.acunetix.com/whitepaper-the-future-is-the-web/

2.."What Is a Web Application Attack and how to Defend Against It". 2019. Acunetix. https://www.acunetix.com/websitesecurity/web-application-attack/

3. "2020 State of Application Services Report" F5 Networks, 2020. https://www.f5.com/state-of-application-services-report

4. "Sonicwall Cyber Threat Report". 2020. Sonicwall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. "The State of Web Application Security, Protecting Application in the Microservice Era." 2019. Radware. https://www.radware.com/resources/was-report-2019/

6. "API Security Top 10 2019." OWASP. https://owasp.org/www-project-api-security/

7. Raymond Pompon, Sander Vinberg. "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem." 13 de agosto de 2019. F5 Labs https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

8. "Unauthorized Logins on Fast Retailing Online Store Websites due to List Type Account Hacking and Request to Change Password." 13 de mayo de 2019. Fast Retailing. https://www.fastretailing.com/eng/group/news/1905132000.html

9. "Web Applications vulnerabilities and threats: statistics for 2019." 13 de febrero de 2020. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9

10. Esrtevao Avillez. "2019 Website Threat Research Report." 2019. Sucuri. https://sucuri.net/wp-content/uploads/2020/01/20-sucuri-2019-hacked-report-1.pdf

11. "State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3)." 2017-2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-executive-summary-2019.pdf

12. "State of the Internet Security | Financial Services – Hostile Takeover Attempts (Volume 6, Issue 1)." 2020. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

13. "Q4 2016 State of The Internet Security Report" 2016.Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf

14. "Q4 2017 State of the Internet Security Report" 2017. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

15. "2019 Cyberthreat Defense Report." 2019. CyberEdge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

16. "AppSec Advisor: Injection Attacks." Octubre de 2019 CIS Center for Internet Security. https://www.cisecurity.org/newsletter/injection-attacks/

17. "Cybersecurity threatscape: Q3 2019". 2 de diciembre de 2019. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/#id5

18. "Virtual Patching Best Practices." OWASP. https://owasp.org/www-community/Virtual_Patching_Best_Practices

19. Raymond Pompon, Sander Vinberg. "Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem." 13 de agosto de 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

20. "2020 Cyber Threats, Business Email Compromise." 22 de octubre de 2019. https://www.uscloud.com/blog/top-cyber-threats-in-2020/

21. Sara Boddy, Remi Cohen. "Regional Threat Perspectives, Fall 2019: Asia." 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives--fall-2019--asia

«El aumento de la complejidad de las aplicaciones *web* y sus amplios servicios crea retos a la hora de protegerlos contra las amenazas que tienen diversos motivos, desde económicos o daños a la reputación, hasta el robo de datos vitales o personales».

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

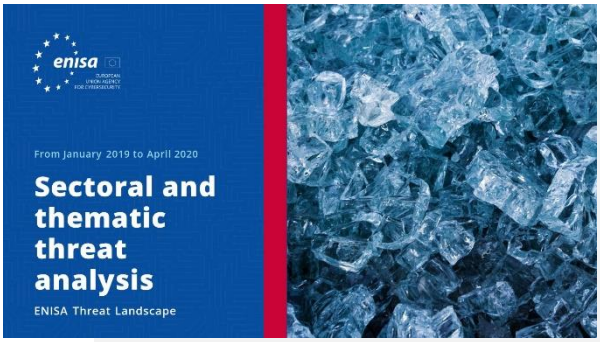
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

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

LEER EL INFORME

Informe ENISA: Panorama de amenazas
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.

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

https://www.enisa.europa.eu