



De enero de 2019 a abril de 2020

# Ataques basados en la web

Panorama de Amenazas de la ENISA



# Sinopsis

Los ataques basados en la *web* son un método atractivo que permiten a los atacantes utilizar como vector el engaño a las víctimas que usan sistemas y servicios *web*. Esto cubre una gran superficie de ataque, por ejemplo hacer que una URL o *scripts* malintencionados dirijan a la víctima o usuario al sitio *web* deseado o descarguen contenido malintencionado (ataques de abrevadero<sup>1</sup> o *watering hole* y *drive-by*<sup>2</sup>) e inyecten código malintencionado en un sitio *web* legítimo, pero comprometido, con el fin de robar información (por secuestro de formularios *formjacking*<sup>3</sup>) para obtener ganancias financieras, robar información o incluso para chantajear utilizando *ransomware*.<sup>4</sup> Además de estos ejemplos, también son vectores importantes, observados por los equipos de investigación y utilizados por los ciberdelincuentes, los programas intrusos (*exploits*) de los programas navegadores y de los sistemas de gestión de contenido comprometidos.

Los ataques por fuerza bruta, por ejemplo, atacan desbordando una aplicación *web* con intentos de inicio de sesión con nombres de usuario y contraseñas. Los ataques basados en la *web* pueden afectar a la disponibilidad de los sitios *web*, aplicaciones e interfaces de programación de aplicaciones (API), infringiendo la confidencialidad y la integridad de los datos.

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

*en PAE 2020*

# Kill chain


## Ataques basados en la web

Reconocimiento

Uso como arma

Distribución

Explotación

 Paso del proceso de ataque

 Amplitud de la intención





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

## Generales

- **MALWARE DE SECUESTRO DE FORMULARIOS PARA ROBAR DATOS DE USUARIOS.** La inyección de código malintencionado en sitios *web* es una de las técnicas bien conocidas usadas por los ciberdelincuentes. El *formjacking* o secuestro de formularios ya se había notificado, sobre todo en actividades de minería de criptomoneda. No obstante, según un investigador especializado en temas de seguridad<sup>4</sup>, los atacantes están empezando a usar esta técnica con datos de usuario y datos bancarios. Los sitios *web* atacados permanecieron infectados durante un promedio de 45 días. Durante el mes de mayo de 2019, un investigador notificó el bloqueo de casi 63 millones de solicitudes *web* malintencionadas relacionadas con el *formjacking*.
- **«MAGECART» VA MÁS ALLÁ AL ATACAR A LA CADENA DE SUMINISTRO.** Según un investigador especializado en temas de seguridad, una de las empresas de medios digitales francesas fue atacada por el agente malintencionado Group12, que infectó el inventario de publicidad del sitio, plantó el código de copia de datos de tarjetas (*skimmer*) e infectó miles de sitios *web* que alojaban su publicidad en este sitio.<sup>5</sup> Se observó que la operación del grupo más eficaz al establecer la infraestructura de clonación justo unos meses antes de iniciar la campaña. En resumen, el usuario final se podía infectar con tan solo visitar el sitio *web* que alojaba este anuncio.<sup>6</sup>
- **PLATAFORMAS DE COLABORACIÓN Y MENSAJERÍA WEB.** Se están convirtiendo en la pasarela entre los ciberdelincuentes y las víctimas a través de lo que se denomina puerta trasera SLUB. Durante el mes de marzo de 2019, un investigador especializado en temas de seguridad detectó una campaña que utilizaba ataques «abrevadero» para infectar a las víctimas al explotar la vulnerabilidad CVE-2018-81747. El ataque implicaba procesos de infección multietapa. Un ejemplo de cómo funcionan estos procesos es la descarga de un archivo DLL, utilizando un PowerShell para ejecutarlo, la descarga del *malware* y la ejecución de la puerta trasera principal. Curiosamente, el *malware* se conectaba con un servicio de mensajería del espacio de trabajo Slack para enviar los resultados del comando, que a su vez se distribuían por un fragmento de código de GitHub Gist en el que potencialmente el atacante añadía comandos.<sup>7,8</sup>



- **EXTENSIÓN DEL NAVEGADOR, FRAUDE Y PUBLICIDAD MALINTENCIONADA (MALVERTISING).** Un investigador especializado en temas de seguridad descubrió una campaña de publicidad malintencionada que utilizaba las extensiones de Google Chrome y que afectó a aproximadamente 1,7 millones de usuarios. Estas extensiones de Chrome trastornaban la función de publicidad subyacente dirigida a los usuarios finales con el objetivo de mantener el navegador infectado conectado a la infraestructura de los C2. El investigador concluyó que la campaña aumentó su actividad entre los meses de marzo y junio de 2019, aunque se sospecha que llevaba activa desde hacía mucho más tiempo.<sup>9</sup> Otro investigador observó que la actividad de *adware* NewTab, que facilita las extensiones del navegador, aumentó a finales de 2019.<sup>11</sup>
- **LOS SITIOS DE GOOGLE SE UTILIZAN PARA ALBERGAR CARGA DE DRIVE-BY.** El *malware* 'LoadPCBanker' (Win32.LoadPCBanker.Gen) se encontró en la plantilla Archivador de Google Sites (Classic Google Sites). Según un investigador especializado en temas de seguridad, el responsable utilizó primero Classic Google Sites para crear una página *web* y luego preparó la plantilla Archivo para albergar las cargas. A continuación, utilizó el servicio SQL como canal de salida para enviar y almacenar los datos de las víctimas.<sup>12,13</sup>
- **RANSOMWARE MEDIADO POR EL CONVERTIDOR DE VÍDEO EN LÍNEA COMO MECANISMO DE DESCARGA DRIVE-BY.** Según un investigador especializado en temas de seguridad, ShadowGate o WordJScampaign lleva activo desde 2015, infectando programas informáticos de publicidad y sitios *web*. Durante 2016 se desarrolló el *kit* de programas intrusos Greenflash Sundown para mejorar la actividad de la campaña al inyectar el *kit* en servicios de publicidad comprometidos y propagando *ransomware*. Durante 2018 se detectó que durante un corto tiempo ShadowGate plantaba programas de criptominería en los servidores del este de Asia. En la Figura 1 de este informe se presenta la distribución de ShadowGate por país. Otro investigador especializado en temas de seguridad notificó que había detectado esta actividad, a la que se siguió la pista hasta llegar a onlinevideoconverter[.com], como uno de los sitios *web* principales para distribuir el *kit* de programas intrusos por *drive-by*.<sup>14,15,16,17,18</sup>

## Generales

- **LOS SISTEMAS DE GESTIÓN DE CONTENIDO SIGUEN SIENDO UN OBJETIVO IDEAL.** Dada la popularidad de los sistemas de gestión de contenido (Content Management Systems, CMS) entre los usuarios de Internet, estos sistemas son un objetivo atractivo para los ciberdelincuentes. Un investigador especializado en temas de seguridad observó un aumento en la explotación de una vulnerabilidad identificada durante 2018 (Drupalgeddon2) dirigida a la plataforma Drupal. De forma similar, otro investigador observó una tendencia en las vulnerabilidades de seguridad de WordPress dirigidas a vulnerabilidades y programas de complementos de terceros.<sup>19,20</sup>
- **LAS VULNERABILIDADES DE SEGURIDAD DEL NAVEGADOR DE INTERNET UTILIZADAS EN ATAQUES DE «ABREVADERO».** Se detectó a un ciberdelincuente realizando un ataque de «abrevadero» en un portal de noticias en coreano. En este ataque el *script* (JavaScript) malintencionado se inyectaba automáticamente en la página de inicio de un sitio *web* (aprovechando otro código) al comprobar el programa navegador de la víctima y, a continuación, explotando la vulnerabilidad CVE-2019-13720 de Google Chrome. Es más, en julio de 2019, se encontró una nueva versión del *malware* de puerta trasera SLUB que infectaba al navegador de la víctima (vulnerabilidad CVE-2019-0752 de Internet Explorer) utilizando un sitio web «abrevadero» específico. En otro estudio, el equipo de seguridad de un desarrollador de programas informáticos identificó una serie de sitios *web* comprometidos que se estaban utilizando en ataques de «abrevadero» que explotaban las vulnerabilidades del iPhone.<sup>21,22</sup>



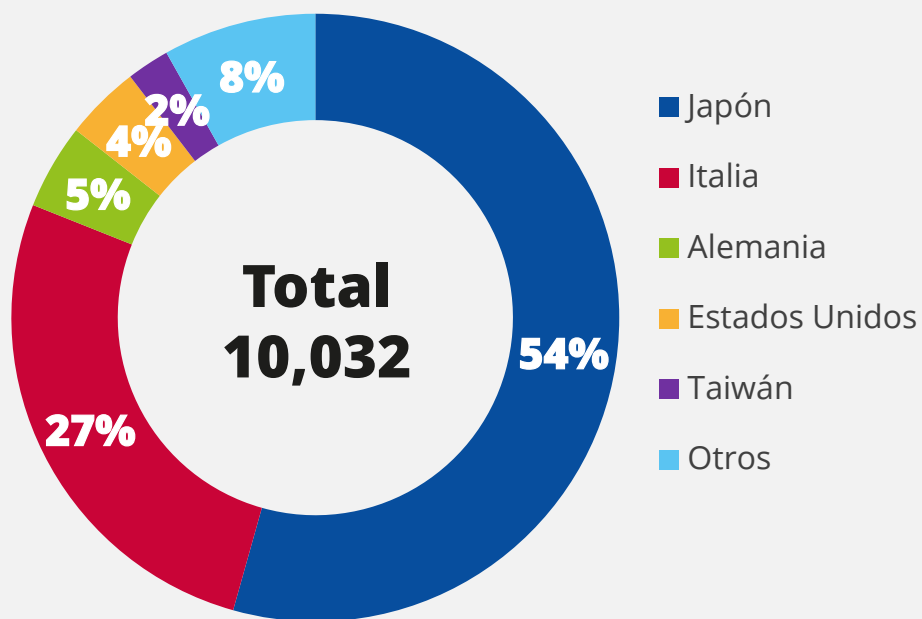


Figura 1: Porcentaje de distribución de ShadowGate por país

# Vectores de ataque

## — Cómo

- **DESCARGAS DRIVE-BY.** Este vector de ataque descarga contenido malintencionado en el dispositivo de la víctima. En este tipo de ataque el usuario final necesita visitar un sitio *web* legítimo que ha sido comprometido. Esto se consigue bien utilizando *scripts* malintencionados que se inyectan en el sitio *web* legítimo; bien ejecutando programas basados en un navegador *web* que atacan sus vulnerabilidades; o bien dirigiendo al usuario al sitio comprometido desde un segundo plano.<sup>25,26</sup>
- **ATAQUES DE «ABREVADERO».** Esta técnica se utiliza en ataques dirigidos que utilizan los *kits* de explotación de vulnerabilidades con funciones ocultas. En otras palabras, es el tipo de ataque que se utiliza cuando un ciberdelincuente quiere comprometer a un grupo de usuarios específico utilizando un programa de explotación de vulnerabilidades u otro contenido malintencionado (como *scripts* o anuncios) que se inyecta en el sitio *web*.<sup>27</sup>
- **FORMJACKING.** Los ciberdelincuentes utilizan esta técnica para inyectar código malintencionado en los formularios de pago de sitios *web* legítimos. Este ataque recoge principalmente datos de identificación personales y bancarios. En este tipo de escenario, el usuario introduce sus datos bancarios o de tarjeta de crédito en el portal de pago de comercio electrónico. Cuando se ha recogido y enviado la información, el *script* malintencionado envía los datos simultáneamente al portal y al ciberdelincuente. A continuación, la información se utiliza para perpetrar varios delitos: ganancias financieras, chantaje y venta de datos en mercados ilegales.<sup>3,4</sup>
- **URL MALINTENCIONADA.** Se define como un enlace creado con la intención de distribuir *malware* o facilitar un engaño. El proceso implica obtener información de la víctima por ingeniería social para persuadirla para que visite la URL malintencionada, que planta el *malware* o contenido malintencionado e infecta el equipo de la víctima.<sup>28</sup>



## Operación WizardOpium

Se ha encontrado una vulnerabilidad de ataque del día cero de Google Chrome en ataques basados en la *web*. La vulnerabilidad, registrada como CVE-2019-13720, afecta a versiones anteriores a 78.0.3904.87 en sistemas Microsoft Windows, Mac y Linux. El defecto se encuentra en el componente de sonido del programa navegador y su explotación podría dar como resultado la ejecución arbitraria de código.

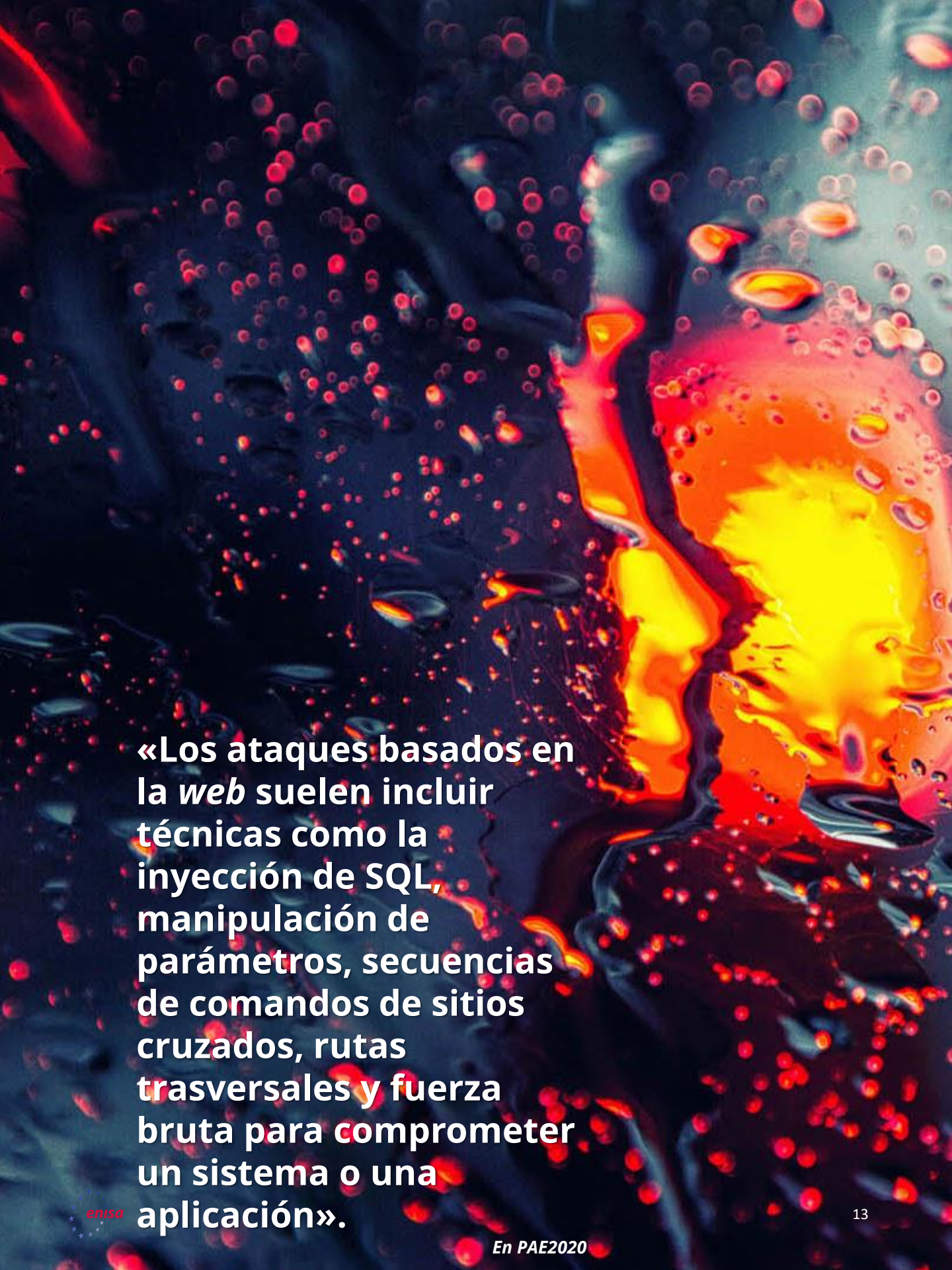
La vulnerabilidad del día cero la descubrió un investigador especializado en temas de seguridad y la registró como CVE-2019-13720, pero aunque no se atribuyó a ningún agente de amenaza específico sí se vio que formaba parte de una campaña denominada Operation WizardOpium. Entretanto, Google ha publicado una actualización para la versión de 78.0.3904.87 de Chrome. Según este investigador, el ataque aprovecha la oportunidad de una inyección al estilo «abrevadero» en un portal de noticias en coreano. Un código de JavaScript malintencionado insertado en la página de inicio permite cargar el código de perfilado desde un sitio remoto. <sup>23,24</sup>

La explotación de las vulnerabilidades del programa navegador son una forma de infección con código malintencionado que utiliza las vulnerabilidades de software (sistema operativo y navegador) o de los programas complementarios relacionados con el objetivo de conseguir entrar en el equipo de la víctima.

# Mitigación:

## Acciones propuestas

- Seguir un buen proceso y plan de gestión de parches.
- Actualizar el programa navegador y los programas complementarios relacionados para mantenerlos actualizados y parcheados para proteger las vulnerabilidades conocidas.
- Mantener las páginas basadas en el sistema de gestión de contenido y el portal actualizados con los últimos parches para evitar programas complementarios y otros complementos sin verificar.
- Asegurarse de que los puntos finales y los programas instalados se mantienen actualizados, parcheados y protegidos.
- Aislar aplicaciones (listas blancas de aplicaciones) y crear un espacio de aislamiento para reducir el riesgo de ataques por *drive-by-compromise*. Por ejemplo, la técnica de aislamiento del navegador puede proteger puntos finales contra la explotación del programa navegador y contra los ataques *drive-by-compromise*.<sup>29,30,31</sup>
- Para los propietarios de sitios *web*: endurecer los servidores y los servicios es un enfoque proactivo para mitigar los ataques basados en la *web*. Esto incluye el control de los comandos de contenido así como el escaneo de archivos locales y comandos para el servidor o servicio *web*.<sup>32</sup>
- Restringir el contenido *web* es otra técnica para protegerse contra los ataques basados en la *web*. Facilitar herramientas como los bloqueadores de anuncios o los bloqueadores de JavaScript también limita la posibilidad de que se ejecute código malintencionado cuando se visitan sitios *web*.<sup>29,30</sup>
- Monitorizar el correo electrónico de *web* y filtrar el contenido para detectar y evitar la distribución de URL y archivos/cargas malintencionadas.



«Los ataques basados en la *web* suelen incluir técnicas como la inyección de SQL, manipulación de parámetros, secuencias de comandos de sitios cruzados, rutas transversales y fuerza bruta para comprometer un sistema o una aplicación».

# Bibliografía

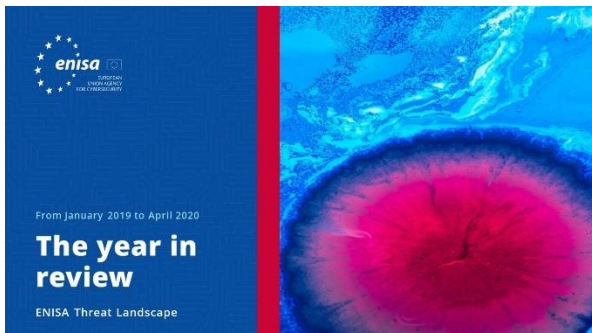
1. "Watering Hole" Proofpoint. <https://www.proofpoint.com/uk/threat-reference/watering-hole>
2. "What Is a Drive-By Download?" Kaspersky. <https://www.kaspersky.com/resource-center/definitions/drive-by-download>
3. "Formjacking: Major Increase in Attacks on Online Retailers", Broadcom. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers>
4. "What is Formjacking and How Does it Work?", Norton. <https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html>
5. "Magecart's 7 Groups: Hackers Dropping Counter-Intelligence Code in JavaScript Skimmers". 14 de noviembre de 2018. CBR. <https://www.cbronline.com/in-depth/magecart-analysis-riskiq>
6. "How Magecart's Web-Based Supply Chain Attacks are Taking Over the Web ". 10 de marzo de 2019. CBR. <https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks>
7. "CVE-2018-8174 Detail". 5 de septiembre de 2019. NIST. <https://nvd.nist.gov/vuln/detail/CVE-2018-8174>
8. "Join a Slack workspace". Slack. <https://slack.com/intl/en-gb/help/articles/212675257-Join-a-Slack-workspace>
9. "New SLUB Backdoor Uses GitHub, Communicates via Slack". 7 de marzo de 2019. Trend Micros. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/>
10. "Security Researchers Partner With Chrome To Take Down Browser Extension Fraud Network Affecting Millions of Users". 13 de febrero de 2020. Cisco Duo Security. <https://duo.com/labs/research/crxcavator-malvertising-2020>
11. "Mac threat detections on the rise in 2019". 16 de diciembre de 2019. Malware Bytes. <https://blog.malwarebytes.com/mac/2019/12/mac-threat-detections-on-the-rise-in-2019/>
12. "File Cabinet", Google. <https://sites.google.com/site/tiesitestutorial/create-a-page/file-cabinet>
13. Google Sites. <https://sites.google.com/site/>
14. "Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted". 1 de septiembre de 2016. <https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html>
15. "New Bizarro Sundown Exploit Kit Spreads Locky" Trend Micro. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/>
16. "Incoming! Multiple Popular Websites Attacked for Cryptocurrency Mining via GreenFlash Sundown Exploit Kit" 360 Blog. <https://blog.360totalsecurity.com/en/incoming-multiple-popular-websites-attacked-cryptocurrency-mining-via-greenflash-sundown-exploit-kit/>
17. "ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit". 27 de junio de 2019. Trend Micro. <https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/>





18. "GreenFlash Sundown exploit kit expands via large malvertising campaign". 26 de junio de 2019. Malware Bytes. <https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/>
19. "FAQ about SA-CORE-2018-002". 28 de marzo de 2018. Drupal. <https://groups.drupal.org/security/faq-2018-002>
20. "Drupalgeddon2 still used in attack campaigns". 7 de octubre de 2019. Akamai. <https://blogs.akamai.com/sitr/2019/10/drupalgeddon2-still-used-in-attack-campaigns.html>
21. "Trustwave Global Security Report 2019", 2019. Trustwave.
22. "Stable Channel Update for Desktop". 31 de octubre de 2019. [https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop\\_31.html](https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html)
23. "Chrome 0-day exploit CVE-2019-13720 used in Operation WizardOpium". 1 de noviembre de 2019. Kaspersky. <https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/>
24. "CVE-2019-13720 flaw in Chrome exploited in Operation WizardOpium attacks". 1 de noviembre de 2019. Security Affairs. <https://securityaffairs.co/wordpress/93278/hacking/cve-2019-13720-lazarus-attacks.html>
25. "Web Browser-Based Attacks". Morphisec. <https://www.morphisec.com/hubfs/1111/briefs/BrowserAttacksBrief-190327.pdf>
26. "The 5 most common cyber attacks in 2019". 9 de mayo de 2019. IT Governance. <https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks>
27. "Exploit Kits: Their Evolution, Trends and Impact". 7 de noviembre de 2019. Cynet. <https://www.cynet.com/blog/exploit-kits-their-evolution-trends-and-impact/>
28. "Web-Based Threats: First Half 2019". 1 de noviembre de 2019. Palo Alto. <https://unit42.paloaltonetworks.com/web-based-threats-first-half-2019/>
29. "Mitigating Drive-by Downloads", abril de 2020. ACSC. <https://www.cyber.gov.au/publications/mitigating-drive-by-downloads>
30. "MITRE ATT&CK: Drive-by compromise". 5 de diciembre de 2019. MITRE. <https://resources.infosecinstitute.com/mitre-attck-drive-by-compromise/#gref>
31. "Protecting users from web-based attacks with browser isolation". 26 de septiembre de 2019. Shi Blog – Security Solutions. <https://blog.shi.com/solutions/protecting-users-from-web-based-attacks-with-browser-isolation/>
32. "https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es\_p=9346257". 11 de abril de 2019. Broadcom. [https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es\\_p=9346257](https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257)

# 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.



SOBRE EL REPORTAJE



## 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

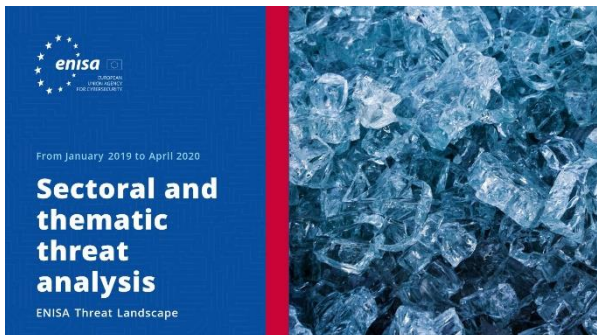


## Informe Panorama de Amenazas de la ENISA **Temas de investigación**

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.



## — 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](http://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](mailto: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](mailto: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.

## 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](mailto:info@enisa.europa.eu)  
[www.enisa.europa.eu](http://www.enisa.europa.eu)



Reservados todos los derechos. Copyright

ENISA 2020.

<https://www.enisa.europa.eu>

