EN

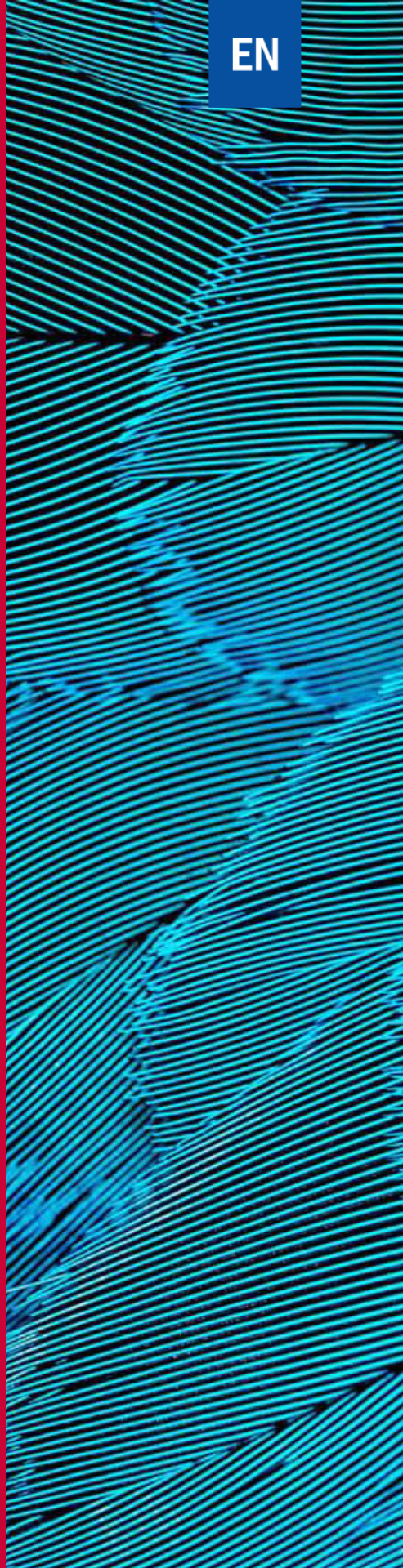
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Ataques distribuidos de denegación de servicio

Panorama de Amenazas de la ENISA



Sinopsis

Los ataques distribuidos de denegación de servicio (DDoS) se producen cuando los usuarios de un sistema o servicio no pueden acceder a la información, servicios o recursos relevantes. Se puede llegar a este estado bien extenuando el servicio o sobrecargando el componente de la infraestructura de red.[1] Los atacantes aumentaron el número de ataques al atacar a más sectores por diversos motivos. Mientras que los mecanismos y estrategias de defensa cada vez se hacen más robustos, los atacantes mejoran sus capacidades técnicas. Hay informes[3,4,5] que sugieren que ha aumentado el uso de las técnicas de ataque reflejadas y amplificadas que facilitan nuevos vectores, distintos a los ya más conocidos (amplificación de UDP, etc.).[6] Los atacantes también han ido mejorando sus tácticas comerciales y han empezado a anunciar sus servicios en la *web*. Históricamente los servicios DDoS se anunciaban en foros de la *dark web*, pero ahora los delincuentes usan los canales habituales de las redes sociales como YouTube y Redit para promover sus servicios.[2]

En 2019 observamos nuevas entradas en la lista de los 10 países principales donde se generaba el tráfico DDoS (Hong Kong, Sudáfrica, etc.).[7] Ese año también se observó un aumento en la actividad DDoS de las *botnets*. Los dispositivos IdC son un vivero para las *botnets* de DDoS, y se consideró que China (24 %), Brasil (9 %) e Irán (6 %) eran los países más infectados con agentes de *botnets*.[3] Un investigador especializado en temas de seguridad predijo que la implantación y la distribución de las redes 5G haría aumentar exponencialmente el número de dispositivos conectados, de ahí la expansión de las redes de *botnets*.[3]

Aunque los ataques DDoS no son nuevos en el mundo de la ciberseguridad y de los defensores de las redes, su nivel de sofisticación va en aumento, y se ha observado que los atacantes están llevando a cabo más actividades de reconocimiento que antes.[3,8]

Conclusiones

241 %_ **es el porcentaje de aumento del número total de ataques durante el tercer trimestre de 2019 con respecto al mismo período de 2018.[3]**

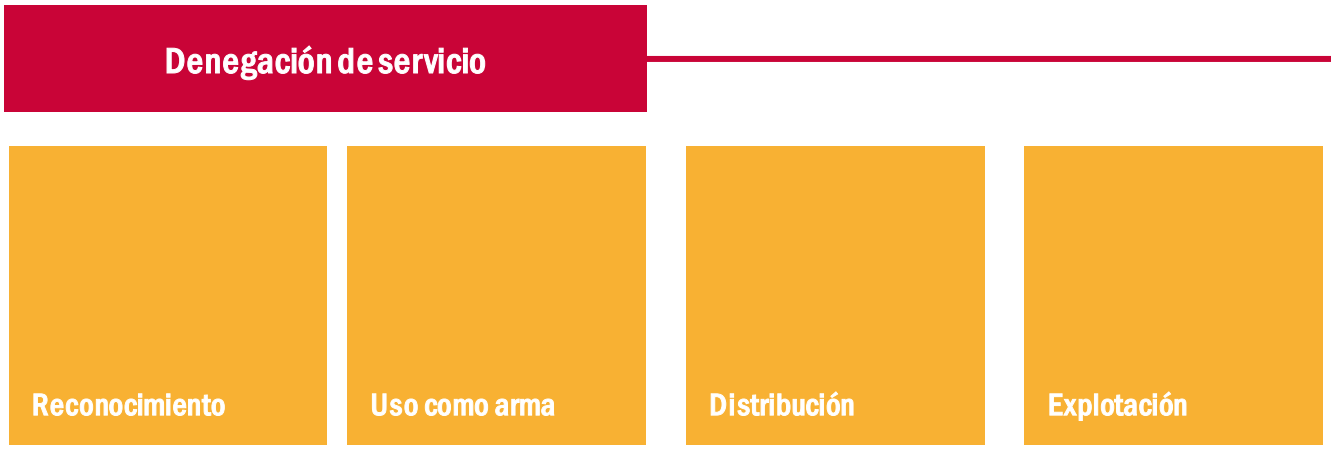
79,7 %_ **de los ataques de DDoS fueron SYN-Floods.[7]**

86 %_ **de los ataques mitigados durante el tercer trimestre de 2019 usaron más de dos vectores.[9]**

84%_ **de los ataques DDoS duraron menos de 10 minutos.[10,11]**

509_ **horas fue la duración del ataque DDoS más largo en el segundo trimestre de 2019.[3]**

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 cinco ataques DDoS más importantes

ATAQUES DE TIPO SYN FLOODS QUE GENERAN 500-580 MILLONES DE PAQUETES POR SEGUNDO. Entre las técnicas utilizadas por los atacantes, la de SYN Flood se sigue considerando difícil de mitigar debido a sus características, a la infraestructura a la que va dirigida y también al hecho de que requiere más *hardware* para controlar el alto volumen de paquetes. En enero de 2019, un investigador especializado en temas de seguridad observó una actividad récord de SYN Flood, con una distribución de 500 millones de paquetes por segundo (mpps) dirigidos a uno de sus clientes; más tarde, en abril del mismo año, el volumen aumentó a 580 mpps.[12]

WS-DISCOVERY. El descubrimiento dinámico de servicios Web[13] (WS-Discovery) es un protocolo de descubrimiento multidifusión. Se ha observado que lo usan mayoritariamente los dispositivos IdC para descubrir automáticamente todos los nodos en las redes de área local (LAN) pero, como ocurre con otros protocolos, puede que no se utilice para su uso previsto, especialmente en el dominio de la IdC[5]. Los atacantes se han dado cuenta de que puede ser un buen terreno para amplificar los ataques. Un investigador especializado en temas de seguridad[3] notificó un factor de amplificación de 95 veces, y otro investigador notificó un aumento del 15 000 % frente al tamaño original del byte.[14]

ATAQUES REFLEJADOS Y AMPLIFICADOS. Se sabe que estos tipos de ataque utilizan una pequeña solicitud para descargar una carga grande. Brevemente: el atacante falsifica la dirección de IP del remitente (la víctima) y, a continuación, el anfitrión del destinatario envía a la víctima todas las respuestas relacionadas.[9] Esta metodología es efectiva principalmente con el protocolo basado en UDP dada su naturaleza sin conexiones y su factor de amplificación (es decir, CLDAP tiene un factor de amplificación de 50 a 70 veces). No obstante, el protocolo TCP no suele ser propenso a este tipo de ataque.[15]

Un buen ejemplo de este tipo de intentos son los ataques de inundación SYN-ACK reflejados y amplificados, que no necesitan necesariamente tener un gran ancho de banda para tener impacto. Por el contrario, tener una buena tasa de paquetes por segundo puede hacer que el ataque pase inadvertido y, así, aumentar su eficacia.[3]

ATAQUES DDoS BIT-AND-PIECE/CARPET BOMBING. Este tipo de ataque de denegación de servicio distribuido y reflejado (DRDoS) suele atacar principalmente a los sectores de las telecomunicaciones y de los proveedores de servicios.[17] Un ejemplo[18] de este método es el ataque a una selección aleatoria de direcciones IP de un proveedor de servicios de Internet para reflejar el tráfico en los enrutadores periféricos del proveedor. Por lo tanto, la víctima no puede identificar el ataque hasta que el servicio se ve desbordado por su propia selección de direcciones IP.[19]

ATAQUES MULTIVECTOR. Los atacantes a veces llevan a cabo ataques DoS con varios vectores para añadir complejidad y variedad al ataque. Esto quiere decir que simplemente automatizando tipos de ataque en capas de aplicación (HTTP Flood, DNS Flood, etc.) y capas de red (UDP/TCP reflejo/amplificación, etc.) distintas intentarán maximizar el impacto saturando el ancho de banda y los recursos o servicios del entorno atacado.[16]

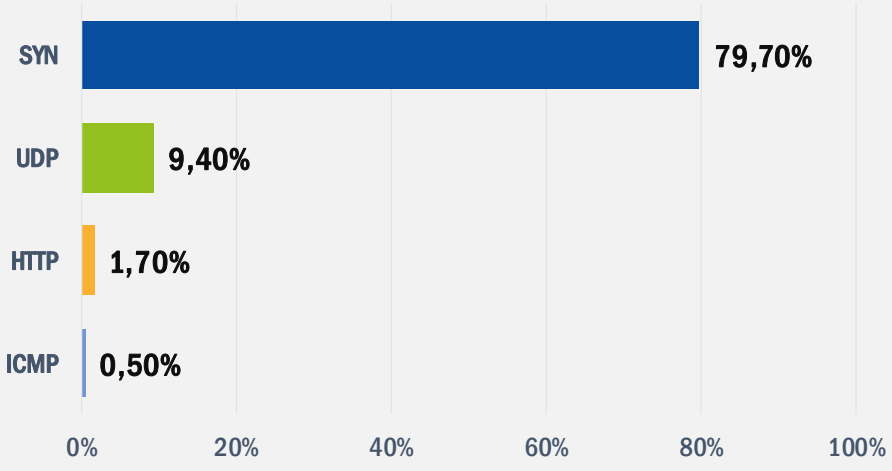


Figura 1: Distribución de los ataques DDoS por tipo. Fuente: Kapersky[16]

Vectores de ataque

Cómo

Como en los años previos, 2019 no fue una excepción en términos de inundaciones UDP. Según un investigador especializado en temas de seguridad, las inundaciones UDP fueron el vector de ataque más popular y su equipo cree que podría estar relacionado con la adopción dominante de este protocolo en sectores de alto riesgo, como el de los juegos de ordenador. Los ataques de tipo inundación SYN, respuesta DNS y los basados en TCP fueron los siguientes (después de las inundaciones UDP) en la lista de los principales vectores de ataque.

Durante este período también se observaron ataques multivector. Sin embargo, un investigador especializado en temas de seguridad cree que algunos ataques multivector no son intencionados y son un producto secundario de los intentos DoS.[11]

En un informe de ciberseguridad[17] se indicaba que habían observado los ataques de amplificación DNS como el vector de ataque DDoS principal, seguido por los de inundación HTTP y TCP SYN. Las observaciones de vectores de ataque en el tercer trimestre de 2019 fueron similares al número de inundaciones SYN, como vector principal, seguido de los ataques UDP, TCP y HTTP.

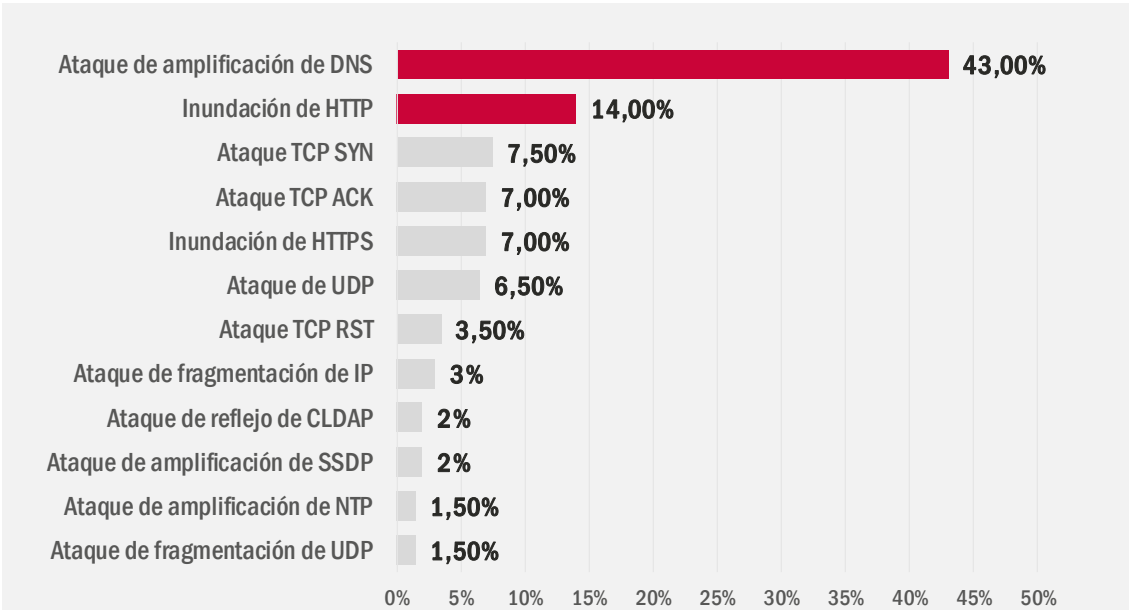


Figura 2: Distribución de los ataques de vectores DDoS. Fuente: NexusGuard[17]

Duración del ataque

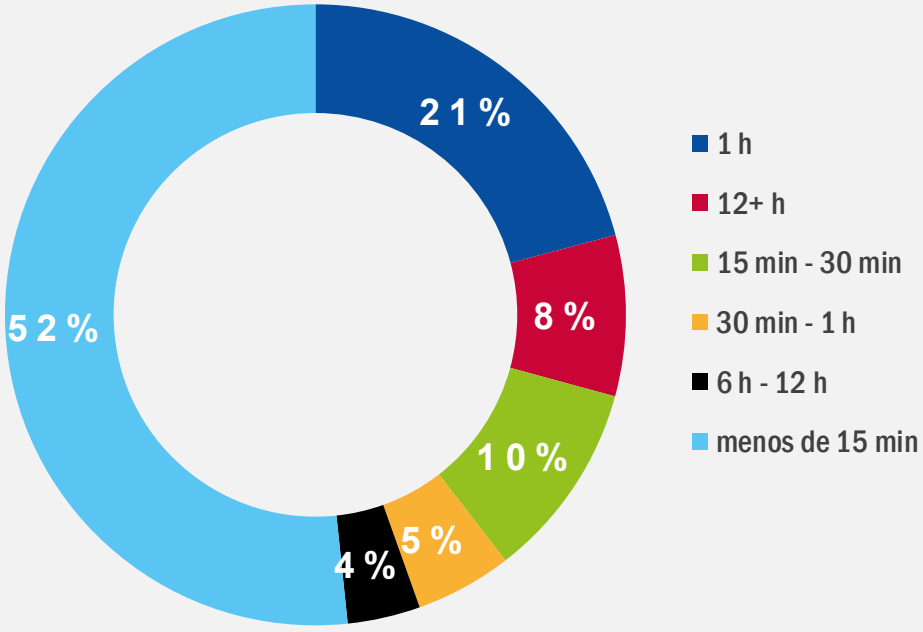


Figura 3 - Fuente: Imperva[11]

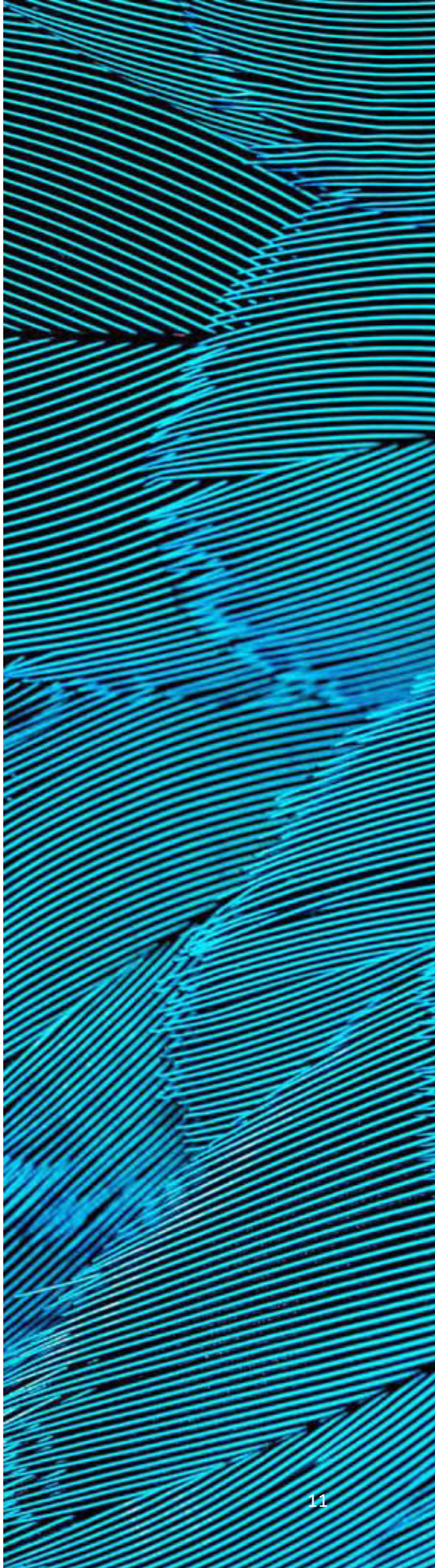
Mitigación:

Acciones propuestas

- Entender los servicios y los recursos vitales y priorizar la defensa en los puntos en los que estos pueden desbordarse. Asegurarse de contar con un plan de respuesta para estos escenarios.[20]
- Según los requisitos, considerar un servicio de protección DDoS o un proveedor de servicios gestionados de DDoS. Usar métodos como la monitorización para identificar infecciones de forma rápida.[1]
- Al igual que en el punto anterior, los servicios de publicación mediante redes de suministro de contenidos pueden ser una forma eficaz de absorber los intentos volumétricos (requieren otras técnicas para realizar ataques más sofisticados).[21]
- Los proveedores de servicios de Internet y en la nube desempeñan una función decisiva en la defensa contra los ataques DDoS. Contar con un plan de comunicación claro y un canal para ellos es la clave para conseguir una respuesta de éxito contra un ataque de denegación de servicio.
- Buenos ejemplos de medidas proactivas son: desarrollar una postura defensiva robusta antes de que se produzca un fallo crítico, en la que participe el equipo y los proveedores adecuados para configurar y afinar los controles basados en requisitos específicos de las empresas.[22] Facilitar servidores de *caché* o dejar preguntas o solicitudes inapropiadas en la capa de la aplicación en el origen y, para los proveedores de servicios, implementar BCP[23].
- Asegurarse de que las técnicas de defensa, tecnologías y proveedores se prueban y vuelven a evaluar.
- Producir un registro del riesgo analizando el entorno de forma exhaustiva. Se empieza por los activos vitales internos y se sigue hasta llegar a la huella y presencia en Internet.[24]

«Aunque los ataques DDoS no son nuevos en el mundo de la ciberseguridad y de los defensores de las redes, su nivel de sofisticación va en aumento, y se ha observado que los atacantes están llevando a cabo más actividades de reconocimiento que antes».

en PAE 2020



Bibliografía

1. "Understanding Denial-of-Service Attacks". 20 de noviembre de 2019. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q1 2019". 21 de mayo de 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

3. "Q4 2019 - The State of DDoS Weapons Report." 2019. A10 Networks. https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

4. Chad Seaman. "Anatomy of a SYN-ACK Attack." 2 de julio de 2019. Akamai. https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html

5. Brandon Vigliarolo. "A new type of DDoS attack can amplify attack strength by more than 15,300%." 18 de septiembre de 2019. TechRepublic. https://www.techrepublic.com/article/a-new-type-of-ddos-attack-can-amplify-attack-strength-by-more-than-15300/

6. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q4 2018". 7 de febrero de 2019. Kaspersky. https://securelist.com/ddos-attacks-in-q4-2018/89565/

7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q3 2019". 11 de noviembre de 2019. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

8. "2019 Website Threat Research Report." 2019. sucuri

9. "DDoS attacks up 241% in Q3 2019 compared to same period last year." 19 de noviembre de 2019. Neustar. https://www.home.neustar/about-us/news-room/press-releases/2019/ddos-attacks-up-241--in-q3-2019-compared-to-same-period-last-year#

10. "2019 Half-Year DDoS Trends Report." 2019. Corero Security. https://www.corero.com/blog/infographic-2019-mid-year-ddos-trends-report/

11. Nadav Avital, Avishay Zawoznik, Johnathan Azaria, Kim Lambert. "2019 Global DDoS Threat Landscape Report." 2019. Imperva. https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

12. Tomer Shani. "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important." 30 de abril de 2019. Imperva. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

13. "Web Services Dynamic Discovery (WS-Discovery) Version 1.1". 1 de julio de 2009. OASIS. http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html

14. Jonathan Respeto. "New DDoS Vector Observed in the Wild: WSD attacks hitting 35/Gbps." 18 de septiembre de 2019. Akamai. https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

15. "Threat Alert: TCP Amplification Attacks." 9 de noviembre de 2019. Radware. https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/

16. "Kaspersky report finds over half of Q3 DDoS attacks occurred in September." 11 de noviembre de 2019. Kaspersky. https://usa.kaspersky.com/about/press-releases/2019_kaspersky-report-finds-over-half-of-q3-ddos-attacks-occurred-in-september

17. "DDoS Threat Report 2019 Q1." 2019. NexusGuard. https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

18. "International traffic – DDoS." 22 de septiembre de 2019. Cool Ideas. https://coolzone.cisp.co.za/announcements.php?announcement=2038-international-traffic-ddos-cool-ideas

19. Catalin Cimpanu. "Carpet-bombing' DDoS attack takes down South African ISP for an entire day." 24 de septiembre de 2019. ZDNet. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

20. "Guidance following recent DoS attacks in the run up to the 2019 General Election." 13 de noviembre de 2019. NCSC. https://www.ncsc.gov.uk/guidance/guidance-following-recent-dos-attacks-2019-general-election

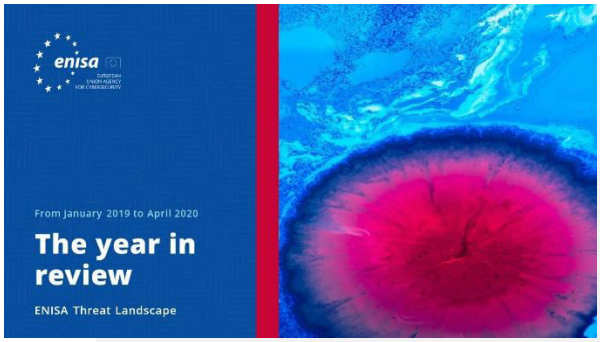
21. V. Revuelto, S. Meintanis, K. Socha. "DDoS Overview and Response Guide." 10 de marzo de 2017. CERT-EU. https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

22. "State of the Internet/Security DDoS and Application Attacks, Volume 5, Issue 1." 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

23. P. Fergusson, D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing." Mayo de 2000 IETF Tools. https://tools.ietf.org/html/bcp38

24. Pierluigi Paganini. "Cyber Defense Magazine Sept Edition 2019." 4 de septiembre de 2019. SecurityAffairs. https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html

Lecturas relacion



LEER EL INFORME

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

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

LEER EL INFORME

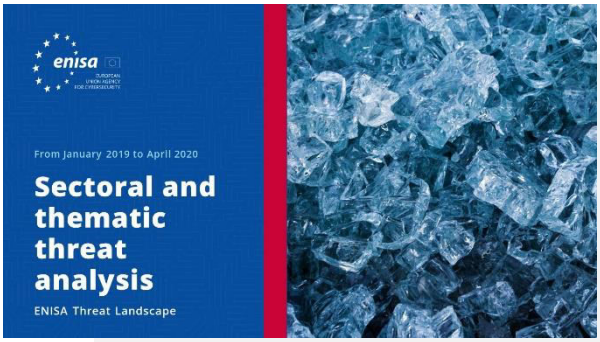
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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

LEER EL INFORME

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

Recomendaciones sobre temas de investigación de varios cuadrantes de la ciberseguridad y de la inteligencia contra 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 som

_ 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.

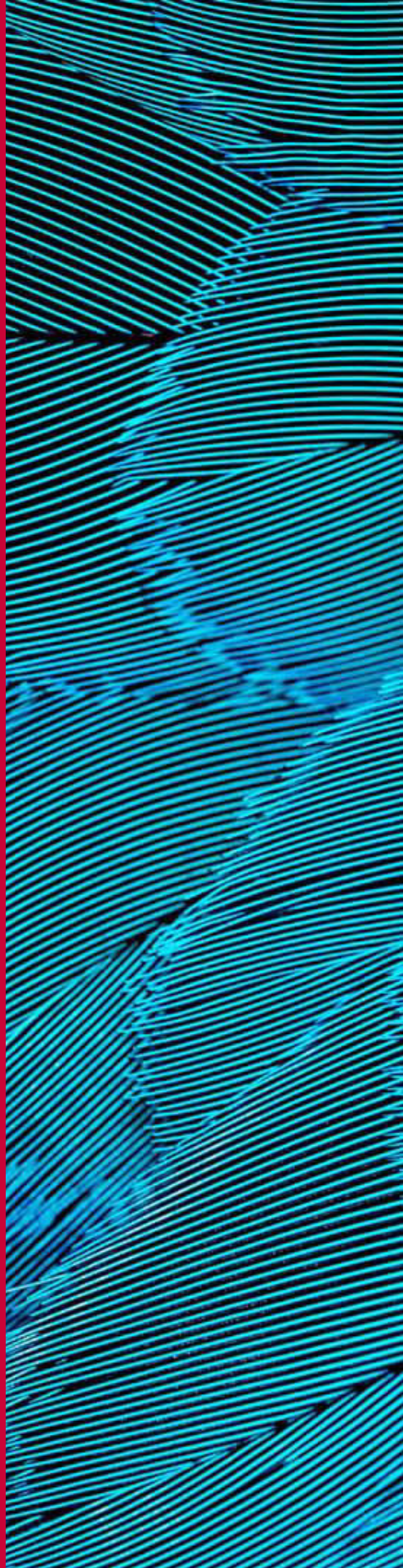
Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

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



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu