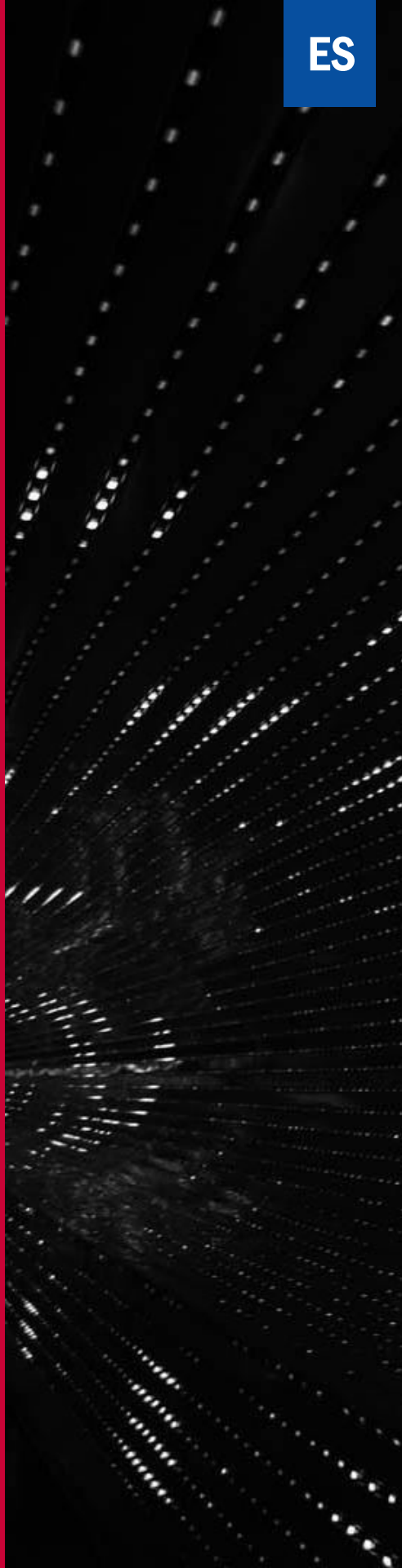
ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



De enero de 2019 a abril de 2020

Botnet

Panorama de Amenazas de la ENISA

Sinopsis

Una *botnet* es una red de equipos conectados infectados por programas de *malware*. Estos equipos los suelen usar atacantes para lanzar ataques distribuidos de denegación de servicio (DDoS). Las *botnets* operan en modo *peer-to-peer* (P2P)[1] o desde un centro de mando y control (C2)[2], y las controla de forma remota un agente malintencionado que opera de forma sincronizada para obtener un resultado determinado.[3]

Los avances tecnológicos en la informática distribuida y automatización han creado una oportunidad para que los atacantes exploren nuevas técnicas y mejoren sus herramientas y métodos de ataque. Gracias a ello, estas *botnets* operan de formas mucho más distribuidas y automatizadas, y se pueden conseguir a través de distribuidores de autoservicio y listas para usar.

Estas *botnets*, a las que en inglés también llaman «*bad bots*» no solo evolucionan constantemente sino que tanto el conocimiento de las personas como el nivel de desarrollo de las «bots» se están especializado mucho en determinadas aplicaciones, como las de los proveedores de defensa o incluso técnicas de evasión.[4] Desde una perspectiva distinta, las *botnets* proporcionan un vector que permite a los ciberdelincuentes lanzar varias operaciones, desde estafas de banca electrónica a programas de *ransomware*, minería de criptomonedas y ataques DDoS.[5]

Conclusiones

*7,7*_millones de dispositivos IdC se conectan todos los días a Internet

De ellos, se estima que 1 de cada 20 está detrás de un cortafuegos o de herramientas de seguridad de red similares.[6]

*57 %*_es el porcentaje de aumento del número de variantes Mirai detectadas durante 2019

Aunque se sabe que las variantes Mirai usan ataques por fuerza bruta predominantemente para comprometer dispositivos IdC, durante 2019 hubo un aumento tanto de los intentos por fuerza bruta (51%) como de los de explotación *web* (87%).[7]

*300 000*_es el número de notificaciones de tráfico de la *botnet* Emotet observadas durante 2019

Esto se traduce en más de 100 000 alertas más de víctimas que en el mismo período de 2018. Los investigadores creen que hubo un aumento de un 913 % en el número de variantes Emotet comparando la segunda mitad de 2018 con la de 2019.[7]

*60 %*_de la actividad de nuevas *botnets* rivales va asociada al robo de credenciales[9]

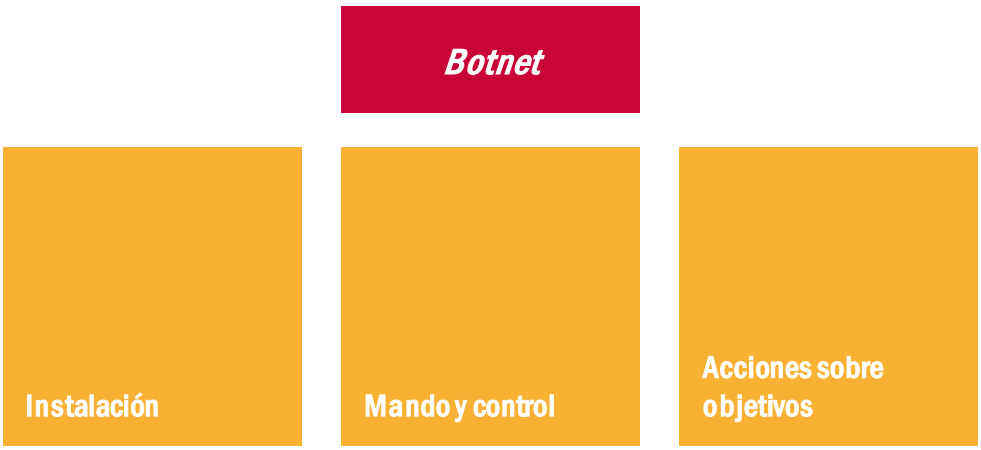
*17 602*_en 2019 se encontró este número de servidores C2 de *botnets* completamente funcionales

Un aumento del 71,5% con respecto a 2018.[5]

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

Tendencias

Las *bots* representan mucho dinero

Las *bots* están facilitando las capacidades de fuerza bruta al hacer que las víctimas compren artículos de edición limitada o artículos de ofertas de promoción para, a continuación, revenderlos a un precio más alto. Esta práctica se identificó al analizar un anuncio de trabajo en el que el anunciante buscaba un programador informático con experiencia en evadir las defensas de seguridad, en la creación de *bots* con técnicas de evasión (como *web scrapping*, sortear los reCAPTCHA, generar *cookies*, etc.) y estaban dispuestos a pagar 15 000 dólares estadounidenses (aprox. 12 750 EUR) por la persona adecuado.[4]

Silexbot, la red de *bots* inactivadora

En junio de 2019 un investigador especializado en temas de seguridad[17] analizó una nueva variante de *bot* desarrollada para alterar las funcionalidades de dispositivos IdC inseguros. Es decir, esta *bot* se había diseñado para usar las credenciales conocidas, o por defecto, de los dispositivos IdC para penetrar en el sistema y, seguidamente, eliminar el dispositivo borrando las configuraciones de red y añadiendo una regla de tablas IP para hacer que el dispositivo perdiera todas las conexiones. Aparte de las capacidades técnicas, un detalle interesante es la nota dejada en la muestra del *malware*. El agente de la amenaza pide disculpas por su actividad y explica que sus acciones se deben a querer evitar la explotación en masa de dispositivos IdC para crear *botnets* con fines malintencionados.

_Echobot y su creciente vector de amenaza

Durante el mes de junio de 2019 un investigador especializado en temas de seguridad identificó una versión actualizada de Echobot. En este análisis, el investigador observó una muestra compilada de equipos con arquitectura x86 que llevaron a vectores de ataque utilizados por esta variante de Mirai en 26 incidentes distintos.[10] Durante el mes de agosto, otro investigador de este campo encontró una ampliación de Echobot que explotaba 50 vulnerabilidades diferentes, incluida la de «command injection over HTTP» (CPAI-2016-0658).[25,26] En diciembre de 2019 otro equipo detectó una versión mejorada de Echobot con 71 programas intrusos (*exploits)* dirigidos a vulnerabilidades antiguas y nuevas, y presentaban también la importante capacidad de dirigirse a dispositivos de sistemas de control industrial (Industrial Control System, ICS). Afectaba a empresas y dispositivos como Mitsubishi, los controles de distribución de aplicaciones de Citrix NetScaler, la aplicación *web* cortafuegos Barracuda y las herramientas de administración de puntos terminales.[27]

_Necurs baja y Emotet vuelve a subir

Durante enero de 2019 se observó que Necurs pasaba a realizar una campaña de correo basura poco profesional que hizo pensar a los investigadores que los agentes responsables habían sufrido una reducción importante de sus capacidades.[20] Por el contrario, la actividad de Emotet aumentaba de forma sustancial desde septiembre de 2019 y seguía subiendo a finales de 2019, plantando archivos binarios compilados únicos que representaban mecanismos de vectores de penetración y comunicaciones persistentes.[7] Un análisis reveló un pronunciado aumento en la distribución de Emotet por correo electrónico.[22]

Tendencias

_Retadup, la *botnet* responsable de Monero-Mining, ha caído

Retadup actuaba principalmente como el gusano de minería de Monero que desarrolló capacidades polimórficas.[23] Había infectado equipos Windows en Latinoamérica. Esta *bot* presentaba capacidades que iban desde la minería hasta la instalación de código personalizado y descargaba archivos en los equipos de las víctimas (también se detectó que distribuía el *ransomware* STOP[24]). Un investigador especializado en temas de seguridad empezó a vigilar la actividad de Retadup en marzo de 2019 y observó que el protocolo C2 se había diseñado de una forma simple. El equipo identificó un punto débil en el protocolo que les permitió eliminar las infecciones en los equipos de las víctimas al hacerse cargo del servidor C2. La infraestructura de esta actividad malintencionada se encontraba ubicada mayoritariamente en Francia. La *botnet* se desmanteló con la colaboración de la Gendarmería Nacional francesa y se pudieron «desinfectar» unos 850 000 ordenadores.

_Mirai ha muerto, larga vida a Mirai

El que Mirai y sus variantes aún dominen en las familias de *botnets* puede deberse a la falta de capacidades y funciones en el código original, y durante el primer semestre de 2019 se observaron más de 20 000 muestras únicas al mes. Estas variantes utilizan distintas técnicas para comprometer dispositivos IdC, desde el uso de fuerza bruta para descifrar contraseñas predefinidas hasta la explotación de vulnerabilidades.[6] Y, según dos investigadores, estas variantes también van dirigidas a una amplia diversidad de arquitecturas de sistemas. En la Figura 1 se presentan más datos estadísticos sobre la actividad de Emotet.[7,18]

_La *botnet* P2P Roboto

En agosto de 2019, un equipo de investigación especializado en temas de seguridad observó la actividad de Roboto como programa de *botnet* P2P. La primera muestra capturada fue un archivo ELF sospechoso. En octubre, el equipo de investigación identificó otra muestra (archivo ELF) que resultó ser el descargador de la muestra anterior. Al analizarla con más detalle descubrieron que la *botnet* Roboto puede admitir siete funciones: funcionalidad «reverse shell», autodesactivación, recopilación de información de procesos y redes, recopilación de información de *bots*, ejecución de archivos URL específicos, ataques DDoS y ejecución de ataques al sistema. Un hecho interesante es que parece que los ataques DDoS no son su uso principal, según los investigadores. A diferencia de otras *botnets*, esta se propagaba explotando la vulnerabilidad Webmin RCE (CVE-2019-1507[28]).[11]

_Mozi, otra *botnet* basada en DHT

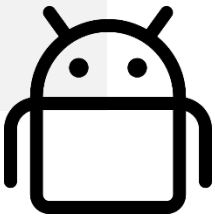
La *botnet* Mozi se llama como su archivo de propagación y se ha identificado como una nueva *botnet* basada en DHT detectada por un investigador especializado en temas de seguridad en septiembre de 2019. En un análisis inicial de la muestra realizado por otro experto en seguridad[38] se la identificó como Gafgyt. Aunque esto se hizo porque la muestra reutilizaba parcialmente el código de Gafgyt. Esta *botnet* se propaga utilizando una serie de programas intrusos y explotando las contraseñas débiles de telnet. El análisis de sus funcionalidades reveló que podía ser capaz de ejecutar ataques DDoS, recopilar información, ejecutar y actualizar muestra/carga útil utilizando una URL específica y comandos de ejecución.[29, 30]

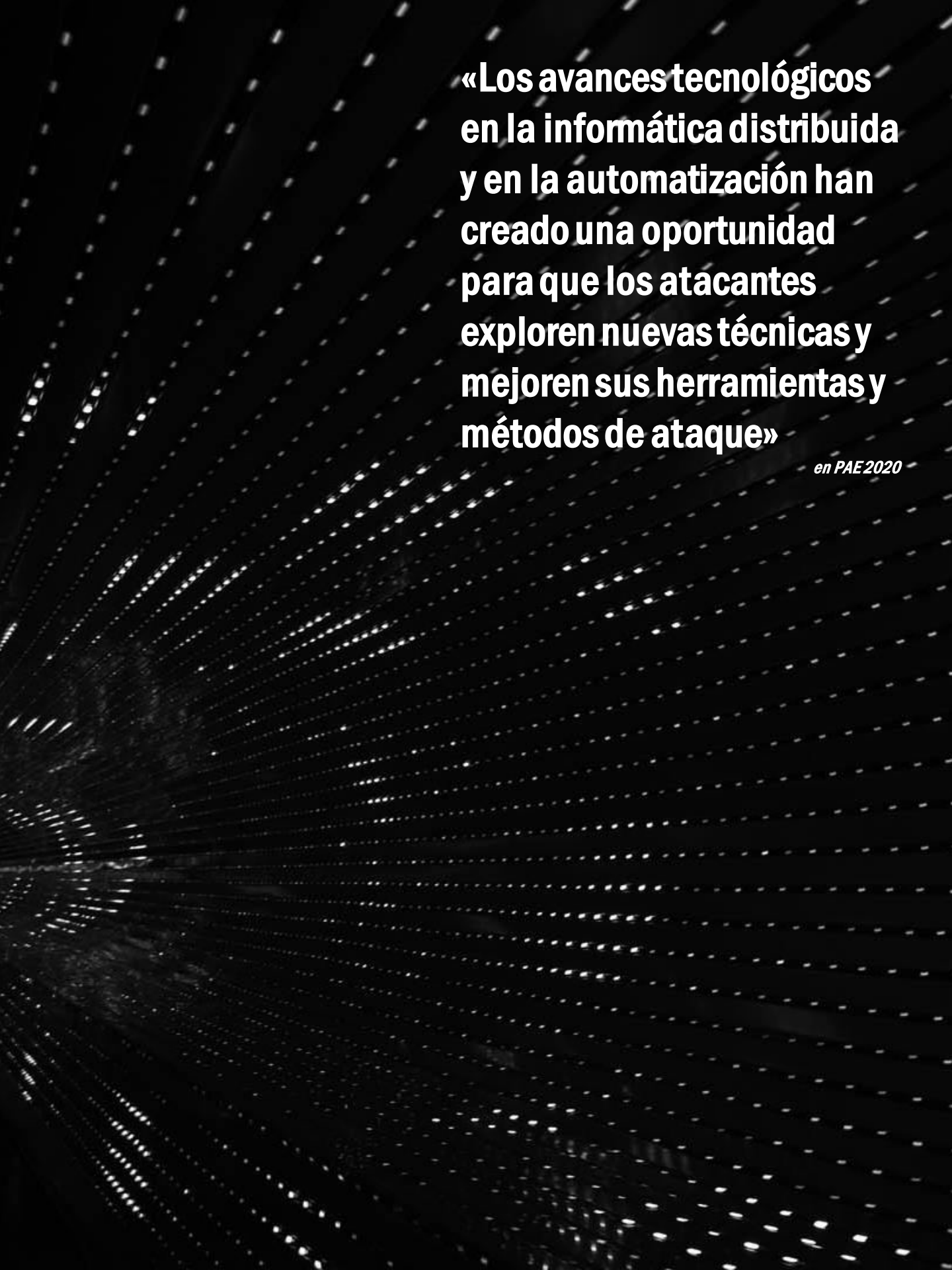
Tendencias

Estadísticas de la actividad de Emotet

Observación	Estadísticas
Número total de ASn detectados:	5 430
Número total de IP únicos detectados:	120 764
Número total de países participantes:	193
Número total de mensajes enviados por correo electrónico:	10 935 346
Número total de URL de distribución:	4 726
Número de RCPT distintos atacados:	8 052 961

Figura 1: Fuente: Spamhaus[5]





«Los avances tecnológicos en la informática distribuida y en la automatización han creado una oportunidad para que los atacantes exploren nuevas técnicas y mejoren sus herramientas y métodos de ataque»

en PAE 2020

Conclusiones

_Estadísticas y otros datos relevantes

Según un investigador experto en temas de seguridad **7,7 millones de dispositivos IdC se conectan a Internet a diario** y se estima que solo 1 de cada 20 está protegido por un cortafuegos u otra herramienta similar de seguridad de red.[6] Esta estimación revela que los **dispositivos IdC siguen siendo vulnerables y susceptibles de ser explotados** por las amenazas a la seguridad informática como Mirai.

- Durante la primera mitad de 2019, la actividad de las *botnets* y de los servidores de hospedaje C2 aumentó sustancialmente.[32] Este aumento representó un 7 % de todas las detecciones de *botnets* y un 1,8 % de los servidores C2 en todo el mundo. Los servicios financieros y sus clientes fueron el sector más atacado.
- Tailandia fue el país principal de ubicación de los servidores de hospedaje C2, con Malasia en segundo lugar, seguido por Filipinas, Singapur e Indonesia.
- Según investigaciones de la Interpol, la *botnet* Andrómeda fue la más dominante en cuanto a detección, aunque se desmanteló en 2017.[33] Conficker[34] fue la segunda, seguida por Necurs[35], Sality[36] y Gozi[37].

En 2019 el número de variantes de Mirai detectadas aumentó en más de un 57 % con respecto a 2018, como se muestra en la Figura 2.

Aunque se sabe que las variantes Mirai usan intentos por fuerza bruta predominantemente para comprometer dispositivos IdC, durante 2019 hubo un aumento tanto de los intentos por fuerza bruta (51 %) como de los de explotación *web* (87 %).

Recuento de variantes de Mirai

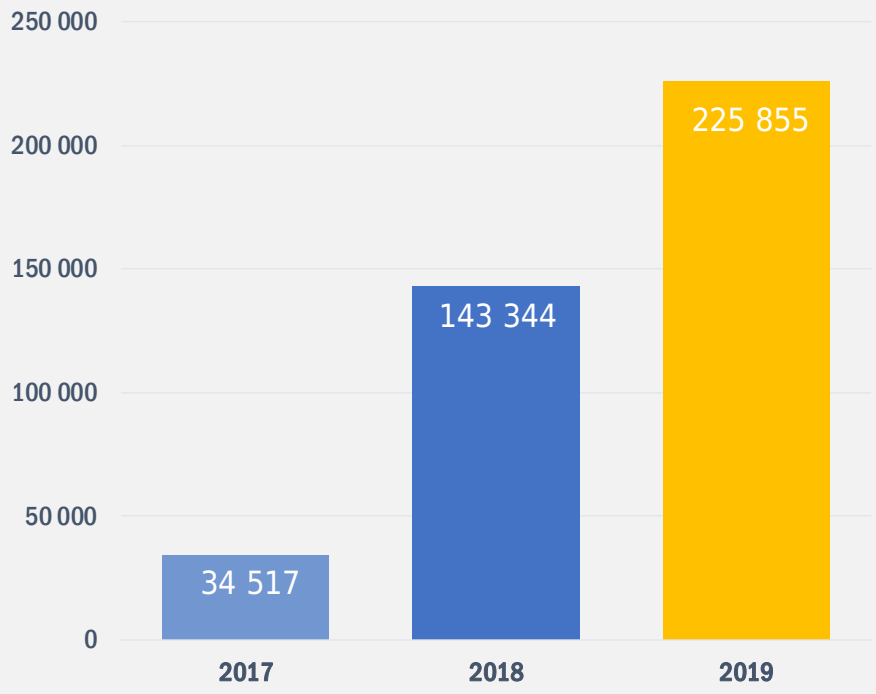


Figura 2 - Fuente: NETSCOUT[7]

Conclusiones

_Estadísticas y otros datos relevantes

- Durante 2019 un experto en temas de seguridad detectó casi 300 000 notificaciones más en el tráfico de la *botnet* Emotet y más de 100 000 alertas de víctimas adicionales en comparación con el mismo período de 2018. El experto cree que hubo un aumento de un 913 % en el número de variantes Emotet tras comparar los segundos semestres de 2018 y de 2019.[7,22]
- Desde que Roboto y Mozi empezaron a actuar se produjo un aumento de la actividad *botnet* P2P.[8]
- Las *botnets* basadas en Linux fueron las responsables de casi el 97,4 % de los ataques.[8]
- La mayor parte de las *botnets* estaban registradas en Estados Unidos (58,33 %) en el cuarto trimestre de 2019. Aunque se trata de un aumento con respecto al tercer trimestre de 2019 (47,55 %), el número total de servidores C2 casi se redujo a la mitad. El Reino Unido se encontraba en cuarto lugar y saltó al segundo con un 14,29 %, mientras que China mantuvo la misma posición con un 9,52 %. El descenso más significativo en el número de servidores registrados C2 fue en los Países Bajos (del 45 % al ~1 %). Para obtener más información sobre la distribución de los servidores C2 por país, consulte la Figura 3.[8]
- En 2019, LokiBot permanecía a la cabeza de la lista de *bots* dedicadas al robo de credenciales, con un aumento en el número de actividad de C2 del 74 % con respecto a 2018. AZORult se encontraba en segunda posición, por detrás de LokiBot.[39]
- En 2019 estaban activos 17 602 servidores C2 de *botnets*, una cifra que representa un aumento del 71,5 % con respecto a 2018.[39]

Distribución de servidores C&C de *botnets* por país

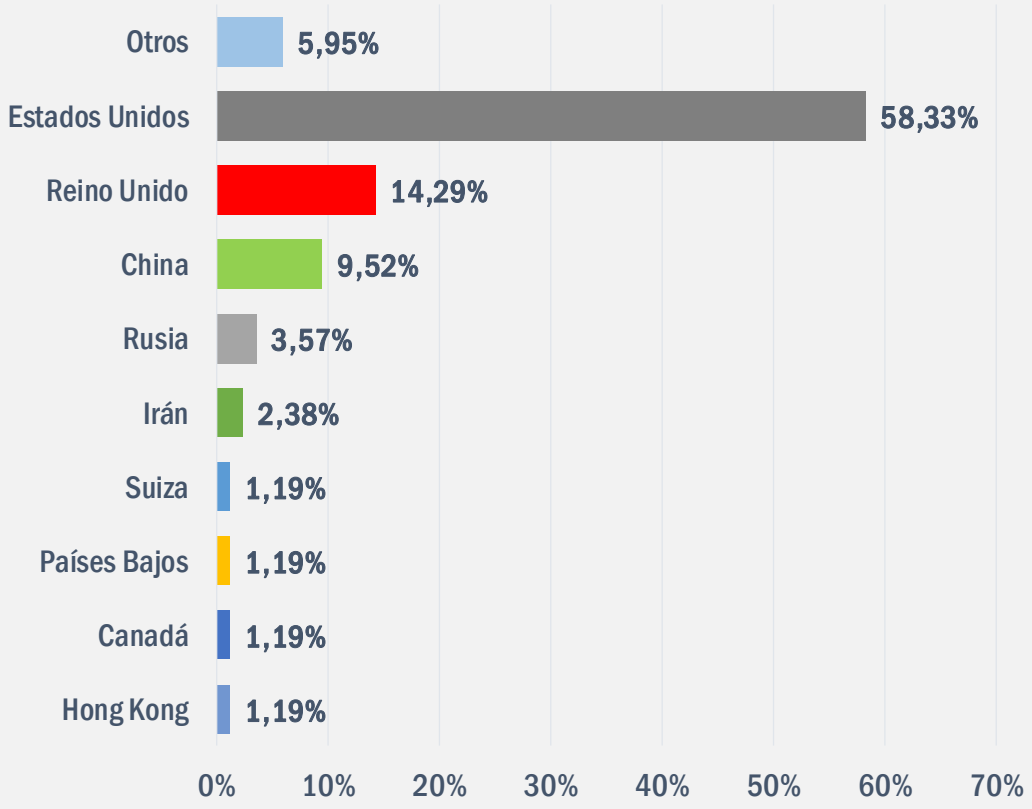


Figura 3 - Fuente: Kapersky[8]

Vectores de ataque

_ Los ataques de las *botnets*

Según un investigador experto en temas de seguridad, en 2019, casi un 60 % de la actividad de las nuevas *botnets* rivales iba asociada al **robo de credenciales**. Como ya se ha mencionado anteriormente, LokiBot es la más activa en esta área. Aparte de la actividad de robo de credenciales, la **banca electrónica y el fraude financiero** son otras áreas en las que la presencia de las *botnets* es muy alta. Emotet y TrickBot son dos buenos ejemplos de esta actividad, ya que presentan un modelo actualizado que no solo cubre las estafas en la banca electrónica sino también las estafas de pago-por-instalación (PPI).[9]

Además, los **troyanos de acceso remoto** (Remote Access Trojans, **RAT**) fueron una de las herramientas más utilizadas en las actividades de los servidores C2 de *botnets*. Durante 2018, la mayoría de estas actividades estaban asociadas a Adwind, pero en 2019 su actividad se redujo y fue reemplazada por NanoCore.[5]

En 2019 **se adoptaron vectores de ataque específicos**. Las *botnets* usan varios vectores de ataque para conseguir sus objetivos. Las máquinas infectadas o redes zombi se crean al explotar vulnerabilidades comunes utilizando fuerza bruta y otras técnicas de infección habituales.[10,11,12] A continuación, el controlador de las *bots* es capaz de proporcionar una plataforma para distintos ataques, incluida la propagación de campañas de correo basura y de *malware*, el robo y la reutilización de credenciales, actividades de *cryptomining* y ataques DDoS.

Otro ejemplo de vector de ataque utilizado por una *botnet* es la técnica **«amenaza triple»**. Con esta técnica la organización atacada se infecta primero con el *malware* Emotet[7]. A continuación, el *malware* Emotet introduce el troyano TrickBot, que busca y explora información sensible. Si encuentra la información y el entorno o red atacado está en la lista del atacante, se introduce el *ransomware* Ryuk.[13]

Número de servidores C2 de *botnets* observados entre 2014 y 2019

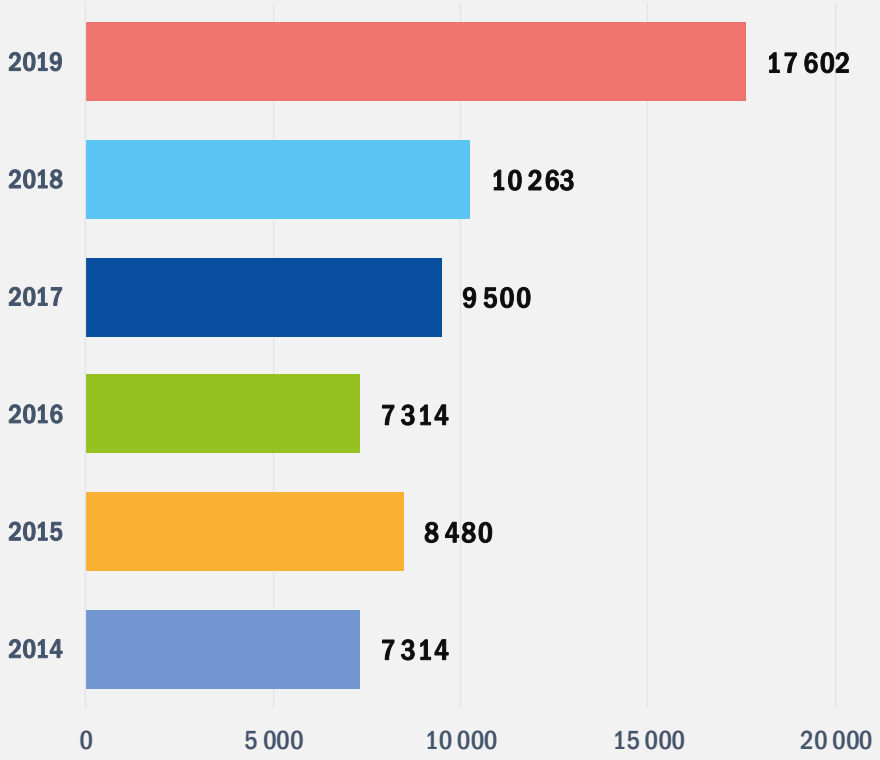


Figura 4 - Fuente: Spamhaus[5]

Mitigación

_ Acciones propuestas

Uno de los aspectos clave para tener una defensa sólida es el concepto de conocimiento del entorno. Esto ayudará a identificar actividad malintencionada en el tráfico basándose en un posible punto de referencia inicial (p. ej., detecciones de comportamiento)[14] medido a través de una herramienta de monitorización del tráfico.[4] Si se considera que el tráfico sustancial de *botnets* va asociado a la actividad DDoS, las técnicas de mitigación para las amenazas DDoS también son aplicables.

- Desplegar monitoreos de protocolo BGP con la capacidad para buscar dTLD (dominios de primer nivel descentralizados) para bloquear las conexiones a las direcciones IP relacionadas con la actividad C2 de la *botnet*.[8]
- Entender y categorizar las vulnerabilidades e implementar procesos de actualización y parches robustos.[15,16]
- Restringir o bloquear las agrupaciones de minería de criptomonedas y vigilar el entorno para los usuarios requeridos.[5]
- Desplegar capacidades basadas en pruebas para que los sitios *web* requeridos comprueben el origen del tráfico (como reCAPTCHA).[16]
- Desplegar políticas de autenticación (2FA) y contraseñas robustas en servidores o infraestructuras de cara al público para evitar convertirse en víctima de la explotación de contraseñas débiles o del proceso de autenticación.[5]
- Desplegar y configurar cortafuegos de red y de aplicaciones.

«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. "Peer-to-peer (P2P)." Malwarebytes Labs https://blog.malwarebytes.com/glossary/peer-to-peer/

2. Monnappa K A. "Learning Malware Analysis." Junio de 2018. O'reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml

3. "ASEAN Cyberthreat Assessment 2020." 17 de febrero de 2020. Interpol https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

4. "State of The Internet Security - DDoS and Application Attacks Report: 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

5. "Spamhaus Botnet Threat Report 2019." 28 de enero de 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

6. "NETSCOUT Threat Intelligence Report: Powered by ATLAS - Findings from H1 2019." 2019.

7. "NETSCOUT Threat Intelligence Report - With key findings from the 15th Annual Worldwide Infrastructure Security Report (WISR) - Findings from H2 2019." 2019. NETSCOUT. https://www.netscout.com/threatreport

8. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q4 2019." 13 de febrero de 2020. Kaspersky. https://securelist.com/ddos-report-q4-2019/96154/

9. Alina Dettmer. "What is Pay Per Install.?" 26 de octubre de 2017. Aye Studios. https://www.ayetstudios.com/blog/mobile-advertising/mobile-campaign-types/pay-per-install

10. Larry Cashdollar. "Latest Echobot: 26 Infection Vectors." 13 de junio de 2019. Akamai. https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html

11. "The awaiting Roboto Botnet." 20 de noviembre de 2019. Netlab. https://blog.netlab.360.com/the-awaiting-roboto-botnet-en/

12. Asher Davila. "Home & Small Office Wireless Routers Exploited to Attack Gaming Servers." 31 de octubre de 2019. Paloalto. https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/

13. "Triple Threat: Emotet deploys Trickbot to steal data & spread Ryuk." 2 de abril de 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

14. "Bots." Imperva. https://www.imperva.com/learn/application-security/what-are-bots/

15. Rebecca Carter. "Bot Mitigation Best Practices." 19 de octubre de 2018 DYN. https://dyn.com/blog/bot-mitigation-best-practices/

16. "What is a Botnet?" Veracode. https://www.veracode.com/security/botnet

17. "SIRT Advisory: Silexbot bricking systems with known default login credentials". 26 de junio de 2019. Akamai.

18. "Mirai Botnet Continues to Plague IoT Space". 10 de septiembre de 2019. Reversing Labs. https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space

19. The Shadowserver Foundation. https://www.shadowserver.org/

20. "As Necurs Botnet Falls from Grace, Emotet Rises" 27 de enero de 2020. Publicación en FB: https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

21. "Mirai malware, attacks Home Routers". 14 de diciembre de 2016. ENISA. https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

22. "Estimating Emotet's size and reach". 12 de diciembre de 2019. SPAMHAUS. https://www.spamhaus.org/news/article/791/estimating-emotets-size-%20-and-reach

23. "Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant". 23 de abril de 2018. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/

24. "Meet Stop Ransomware: The Most Active Ransomware Nobody Talks About". 20 de septiembre de 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

25. "Command Injection Over HTTP". 26 de julio de 2016. Check Point. https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0658.html/

26. "August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices". Agosto de 2019. Check Point. https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/

27. "Echobot Malware Now up to 71 Exploits, Targeting SCADA". 18 de diciembre de 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

28. "CVE-2019-15107 Detail". NIST https://nvd.nist.gov/vuln/detail/CVE-2019-15107

29. "What is a distributed hash table?". EDPresso. https://www.educative.io/edpresso/what-is-a-distributed-hash-table

30. "A Look into the Gafgyt Botnet Trends from the Communication Traffic Log". 23 de julio de 2019. https://nsfocusglobal.com/look-gafgyt-botnet-trends-communication-traffic-log/

32. " ASEAN Cyberthreat Assessment 2020, Key Insights From The ASEAN Cybercrime Operations Desk" Interpol, 2020

33. "International team takes down virus-spewing Andromeda botnet". 5 de diciembre de 2017. The Register. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

34. "The odd, 8-year legacy of the Conficker worm". 21 de noviembre de 2016. WeLiveSecurity. https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/

35. "The Necurs Botnet: A Pandora's Box of Malicious Spam". 24 de abril de 2017. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

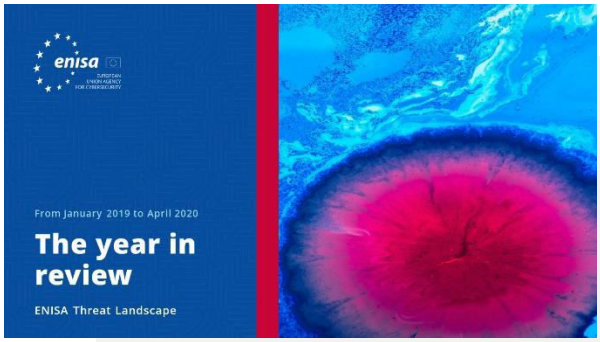
36. "WhitePaper: Sality: Story of a Peer to-Peer Viral Network". 10 de junio de 2011. Broadcom.

37. "Botnet C&C: Gozi". FortiGuard Labs. https://fortiguard.com/encyclopedia/botnet/7630489

38. Virustototal. https://www.virustotal.com

39. "Spamhaus Botnet Threat Report 2019" 2020 . Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

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

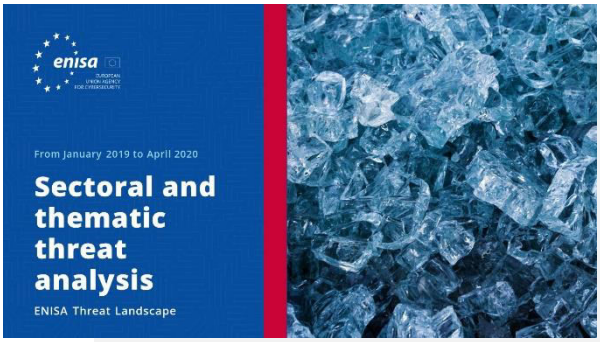
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

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 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) 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

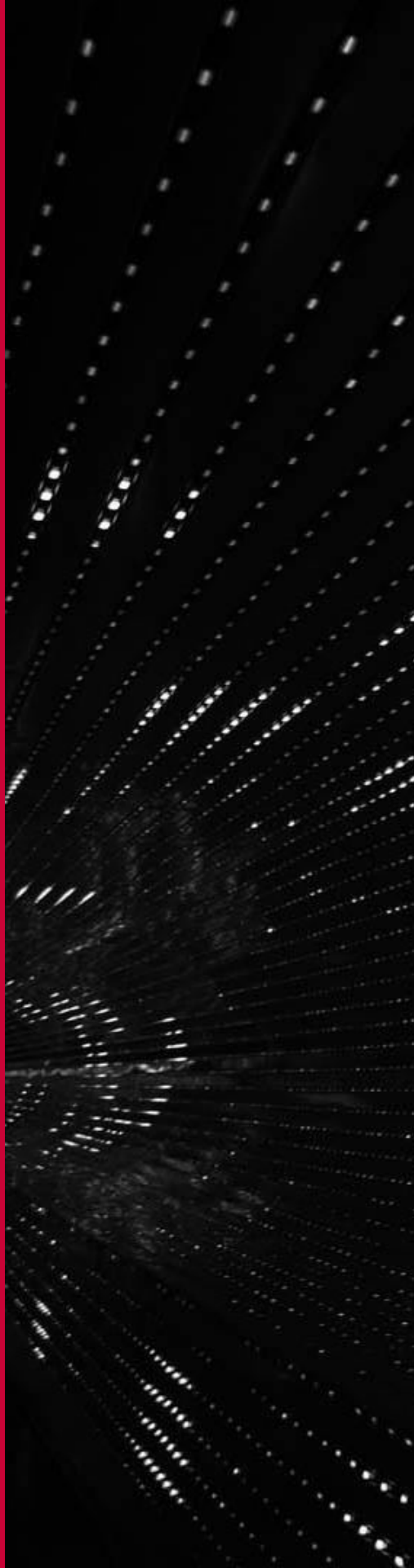
Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. Esta publicación 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.

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