ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Ciberespionaje

Panorama de Amenazas de la ENISA

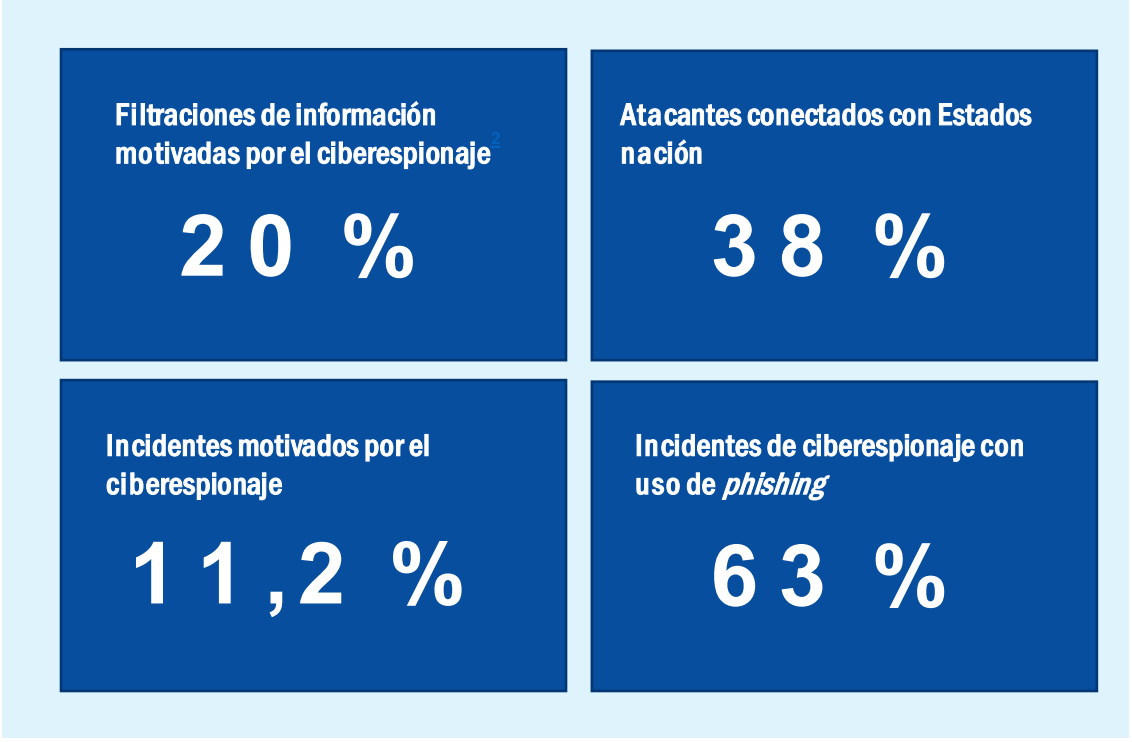
Sinopsis

En el manual de estrategia del ciberespionaje, este se considera tanto una amenaza como un motivo. Se define como «el uso de redes informáticas para obtener acceso ilícito a información confidencial», por lo general perteneciente a un gobierno u organización».[1]

En 2019 muchos informes revelaron que las organizaciones globales consideran el ciberespionaje (o el espionaje promovido por Estados nación) una amenaza en aumento que afecta a los sectores industriales, así como a infraestructuras vitales y estratégicas, incluidas administraciones públicas, ferrocarriles, proveedores de servicios de telecomunicaciones, empresas energéticas, hospitales y bancos. El ciberespionaje se centra en impulsar geopolíticas y en robar secretos de Estado y de comercio, derechos de propiedad intelectual e información de dominio privado en campos estratégicos. También moviliza a agentes de los campos de la economía, la industria y los servicios de inteligencia extranjeros, así como a aquellos que trabajan a su cargo. En un informe reciente, los analistas de la inteligencia sobre las amenazas no se sorprendieron al saber que el 71 % de las organizaciones tratan el ciberespionaje y otras amenazas como una «caja negra» y aún siguen aprendiendo sobre ellas.

En 2019 **aumentaron los ciberataques promovidos por Estados nación dirigidos a la economía y es probable que lo sigan haciendo**. En concreto: hay más ataques promovidos por Estados nación y otros ataques dirigidos por adversarios en la Internet de las cosas industrial (IdCI) en los sectores de servicios de suministro, petróleo y gas natural, y manufacturero. Asimismo, los ciberataques ejecutados por grupos de amenazas persistentes avanzadas (advanced persistent threat, APT) indican que los ataques financieros suelen estar motivados por el espionaje. Mediante tácticas, técnicas y procedimientos parecidos a los del espionaje, grupos como Cobalt Group, Carbanak y FIN7 supuestamente han estado atacando con éxito instituciones financieras y cadenas de restaurantes.

- La Comisión de Asuntos Exteriores del Parlamento Europeo pidió a los Estados miembros establecer una unidad de ciberdefensa y trabajar juntos en la defensa común. Declaraba que «el entorno estratégico de la Unión se ha ido deteriorando [...] a fin de enfrentarse a los diversos desafíos que afectan directa o indirectamente a la seguridad de sus Estados miembros y sus ciudadanos; los temas que afectan a la seguridad de los ciudadanos incluyen: los conflictos armados inmediatamente al este y al sur del continente europeo y estados frágiles; terrorismo (en particular la *Jihad* Islámica), los ciberataques y las campañas de desinformación; la interferencia extranjera en los procesos electorales y políticos europeos».[42]
- Los atacantes motivados por ganancias financieras, políticas o ideológicas, irán centrando sus ataques cada vez más en las redes de proveedores con programas de ciberseguridad débiles. Los adversarios del ciberespionaje han ido cambiando gradualmente sus patrones de ataque para dedicarse a explotar a los socios de la cadena de suministro de terceras o cuartas partes.[1]



Incidentes

- El Ministerio de Defensa Nacional de Corea del Sur anunció que unos ciberdelincuentes desconocidos habían comprometido los sistemas informáticos en la oficina de aprovisionamiento del organismo.[3]
- El Departamento de Justicia de Estados Unidos anunció una operación promovida por un Estado extranjero con una *botnet* dedicada a desestabilizar mediante el ataque a empresas de los sectores de los medios informativos, aeroespacial, financiero y de infraestructuras vitales.[16]
- La firma noruega Visma reveló que había sido atacada por ciberdelincuentes que intentaron robar secretos comerciales de sus clientes.[4]
- Se interceptó a unos asaltantes en las fases iniciales de acceso a los sistemas informáticos de varios partidos políticos y del Parlamento Federal Australiano.[17]
- La empresa aeroespacial europea Airbus reveló que había sido atacada por ciberdelincuentes, supuestamente promovidos por un Estado nación, que robaron datos personales y de identificación de sistemas informáticos de varios empleados.[19]
- Tras un ataque a las fuerzas militares indias en Cachemira, los ciberdelincuentes paquistaníes atacaron casi 100 sitios *web* y sistemas vitales del gobierno indio.[5]
- La Comisión Electoral Nacional de Indonesia notificó que personas rusas y chinas habían sondeado la base de datos de votantes antes de las elecciones presidenciales y legislativas del país.[20]
- Unos ciberdelincuentes extranjeros atacaron a varios organismos oficiales europeos antes de las elecciones de la UE en mayo.[21]
- La Dirección de Señales de Defensa australiana reveló que había llevado a cabo ciberataques contra ISIS en Oriente Medio.[22]
- La policía de Finlandia detectó un ataque DoS contra el servicio de *web* utilizado para publicar los resultados de las votaciones de las elecciones finlandesas.[6]
- La oficina de Amnistía Internacional de Hong Kong anunció que había sido víctima de un ciberataque.[23]
- Las fuerzas de defensa de Israel lanzaron un ataque aéreo contra Hamás después de que estos intentaran piratear sin éxito objetivos israelíes.[7]

- Una red iraní de sitios y cuentas *web* se utilizó supuestamente para difundir información falsa sobre Estados Unidos, Israel y Arabia Saudí.[24]
- Algunas agencias oficiales croatas sufrieron ataques perpetrados por ciberdelincuentes promovidos por un Estado sin identificar. Las cargas de *malware* fueron Empire backdoor y SilentTrinity, ninguno de los cuales se había visto antes.[26]
- Libia arrestó a dos hombres a los que se acusaba de trabajar con una «granja de troles» rusa para influir en las elecciones de varios países africanos.[27]
- Varias firmas industriales importantes alemanas, como BASF, Siemens y Henkel, anunciaron que habían sido víctimas de una campaña de piratería informática promovida por un Estado.[28]
- Un grupo promovido por un Estado realizó supuestamente una serie de ciberataques contra periodistas, profesores universitarios, abogados, activistas de derechos humanos y políticos egipcios.[8]
- Un grupo de ciberdelincuentes promovido por un Estado atacó a diplomáticos y a usuarios de perfil alto y lengua rusa en Europa del Este usando el *malware* Attor.[29]
- Se detectó que una firma de ciberseguridad israelí había vendido programas de *software* espía utilizados para atacar a altos cargos gubernamentales y oficiales militares en al menos 20 países al explotar una vulnerabilidad de WhatsApp.[32]
- Se reveló que una campaña de 7 años, llevada a cabo por un grupo de espionaje de lengua española no identificado, había resultado en el robo de archivos cartográficos sensibles a oficiales de alto rango del ejército venezolano.[10]
- Un grupo de ciberespionaje promovido por un Estado supuestamente realizó una campaña de *phishing* dirigida a organismos del Estado y empresas estatales chinas para conseguir información relacionada con el comercio económico, temas de defensa y relaciones exteriores.[33]
- El Ministerio de Asuntos Exteriores checo fue víctima de un ciberataque perpetrado por un Estado extranjero no identificado.[34]
- Un agente no estatal atacó al partido Laborista británico con un importante ataque de DDoS que desconectó temporalmente los sistemas informáticos del partido justo antes de las elecciones nacionales.[36]

Incidentes

El caso de General Electric

Xiaoqing Zheng, un ciudadano americano de ascendencia china, fue acusado de espionaje contra la empresa General Electric (GE). El señor Zheng había robado supuestamente los secretos de la tecnología de la turbina de GE y se los había entregado a un hombre de negocios chino que, supuestamente, se los había entregado a su vez a funcionarios chinos. El señor Zheng había trabajado para GE del 2008 al 2018.[15]

El Departamento de Justicia de Estados Unidos acusó a los dos hombres de robar información para utilizar en sus intereses comerciales en dos empresas de investigación y desarrollo de turbinas: Liaoning Tianyi Aviation Technology Co Ltd y Nanjing Tianyi Avi Tech Co Ltd.[47]

El *modus operandi* de este agente infiltrado consistió en:

- copiar secretos en un dispositivo de memoria USB hasta que GE bloqueó el uso de estos dispositivos;
- cifrar los secretos y usar esteganografía para ocultar archivos de datos con el código binario de archivos de fotos digitales;
- conectar un iPhone al ordenador del trabajo para copiar la imagen;
- enviar los archivos a su dirección personal de correo electrónico.

Medidas de mitigación

Dada la naturaleza exhaustiva de esta amenaza, se podrían emplear varias de las medidas de mitigación recomendadas para otras amenazas en este informe como parte de los siguientes controles de mitigación iniciales[2]:

- Identificar los trabajos con las funciones más importantes en la organización y estimar su exposición a los riesgos de espionaje. Evaluar dichos riesgos basándose en información de empresa (inteligencia empresarial).
- Crear políticas de seguridad que acomoden recursos humanos, controles de seguridad de empresa y operativos para satisfacer la mitigación del riesgo. Entre ellos se deberían incluir reglas y prácticas para concienciar sobre el riesgo, de gobernanza corporativa y operaciones de seguridad.
- Establecer prácticas corporativas para la comunicación y formación del personal en lo que respecta a las reglas desarrolladas.
- Desarrollar un criterio de evaluación para tener indicadores de referencia para la operación y adaptarlo a los cambios futuros.
- Crear una lista blanca para los servicios de aplicaciones vitales dependiendo del nivel de riesgo evaluado.
- Evaluar las vulnerabilidades y parchear o actualizar el *software* periódicamente, especialmente en los sistemas que están en el perímetro.
- Implementar el principio de «necesidad de saber» para definir los derechos de acceso y establecer controles para vigilar el mal uso de perfiles privilegiados.
- Establecer filtros de contenido para todos los canales de entrada y salida (correo electrónico, *web*, tráfico de red, etc.).

Bibliografía

1. "Cyber Threatscape Report. 2019." IDefense - Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

2. "Data Breach Investigations Report 2020" DBR & Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

3. Catalin Cimpanu. "Hackers breach and steal data from South Korea's Defense Ministry". 16 de enero de 2019. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/

4. Jack Stubbs. "China hacked Norway's Visma to steal client secrets: investigators". 6 de febrero de 2019. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

5. Kate Fazzini. "In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides". 28 de febrero de 2019. CNBC. https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

6. Kati Pohjanpalo. "Finland Detects Cyber Attack on Online Election-Results Service". 10 de abril de 2019. Bloomberg.

https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service

7. Lily Hay Newman "What Israel's Strike on Hamas Hackers Means For Cyberwar". 5 de junio de 2019. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

8. "Egypt Is Using Apps to Track and Target Its Citizens, Report Says". 3 de octubre de 2019. The New York Times. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html

9. Colin Lencher. "Huawei accuses the US of 'launching cyber attacks' against the company". 4 de septiembre de 2019. The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment

10. Catalin Cimpanu "A cyber-espionage group has been stealing files from the Venezuelan military". 5 de agosto de 2019. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/

11. Catalin Cimpanu. "Croatian government targeted by mysterious hackers". 5 de julio de 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

12. Michael McGowan. "China behind massive Australian National University hack, intelligence officials say". 6 de junio de 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

13. "General election 2019: Labour Party hit by second cyber-attack". 12 de noviembre de 2019. BBC. https://www.bbc.com/news/election-2019-50388879

14. Nicole Perlroth, Matthew Rosenberg. "Russians Hacked Ukrainian Gas Company at Center of Impeachment". 13 de enero de 2020. The New York Times. https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

15. Danny Bradbury . "GE Engineer Charged for Novel Data Theft". 24 de abril de 2019. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/

16. "U.S. announces disruption of 'Joanap' botnet linked with North Korea". 30 de enero de 2019. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/

17. "The cyber attack on Parliament was done by a 'state actor' — here's how experts figure that out". 20 de febrero de 2019. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466

18. "While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US". 5 de marzo de 2019. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3

19. "Airbus hit by series of cyber attacks on suppliers". 26 de septiembre de 2019. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. "Indonesia Says Election Under Attack From Chinese, Russian Hackers". 12 de marzo de 2019. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. "Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections". 21 de marzo de 2019. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. "Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know". 18 de diciembre de 2019. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. "State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack". 25 de abril de 2019. Amnesty International. https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. "New Report Shows How a Pro-Iran Group Spread Fake News Online". 14 de mayo de 2019. The New York Times. https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. "China behind massive Australian National University hack, intelligence officials say". 6 de junio de 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. "Croatian government targeted by mysterious hackers". 5 de julio de 2019. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. "Two Russians accused of election interference arrested in Libya". 8 de julio de 2019. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. "BASF, Siemens, Henkel, Roche target of cyber attacks". 24 de julio de 2019. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. "New espionage malware found targeting Russian-speaking users in Eastern Europe", 10 de octubre de 2019. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. "Advanced Israeli spyware is targeting Moroccan human rights activists". Noviembre de 2019. The Next Web. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. "Hacking the hackers: Russian group hijacked Iranian spying operation, officials say". 21 de octubre de 2019. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. "Israeli spyware allegedly used to target Pakistani officials' phones". 19 de diciembre de 2019. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. "A phishing campaign with nation-state hallmarks is targeting Chinese government agencies". 8 de agosto de 2019. Cyber Scoop. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. "Foreign power was behind cyber attack on Czech ministry: Senate". 13 de agosto de 2019. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. "Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications.". 15 de agosto de 2019. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. "Labour suffers second cyber-attack in two days", 12 de noviembre de 2019. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. "Extensive hacking operation discovered in Kazakhstan". 23 de noviembre de 2019. ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Bibliografía

38. "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems". 20 de noviembre de 2019. Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. "Russian 'Gamaredon' Hackers Back at Targeting Ukraine Officials". 6 de diciembre de 2019. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. "Iran announced it foiled 'really massive' foreign cyber attack". 11 de diciembre de 2019. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. "Croatian government targeted by mysterious hackers". 5 de julio de 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. "Report on the implementation of the common foreign and security policy – annual report", 18 de diciembre de 2019. Parlamento Europeo. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_EN.html

43. "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent". 26 de septiembre de 2012. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. "Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack". 2 de enero de 2013. The Threat Post. https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

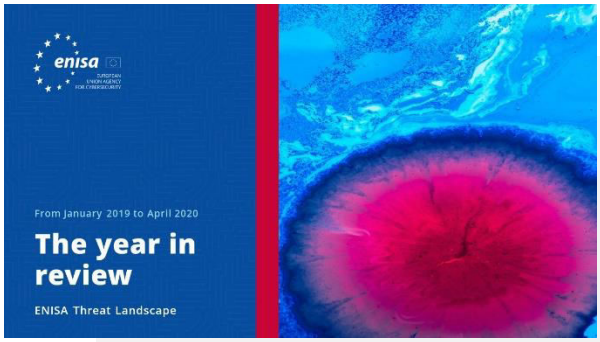
45. "The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity". 25 de febrero de 2014. CrowdStrike Blog. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

46. "Advanced Persistent Threat Groups". Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. "U.S. accuses pair of stealing secrets, spying on GE to aid China". 23 de abril de 2019. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ24O


«El número de ciberataques promovidos por Estados nación dirigidos contra la economía aumentó durante 2019».
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

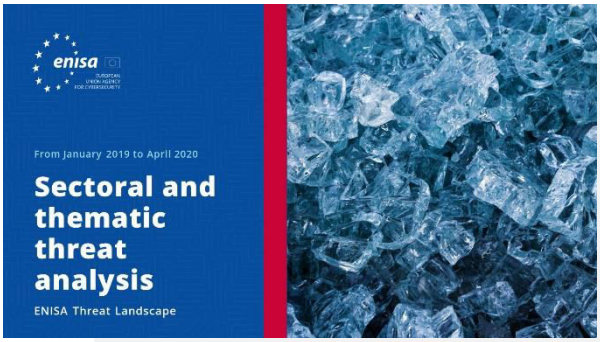
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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

LEER EL INFORME

Informe 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 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.

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.

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