ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Incidentes principales en la UE y el resto del mundo

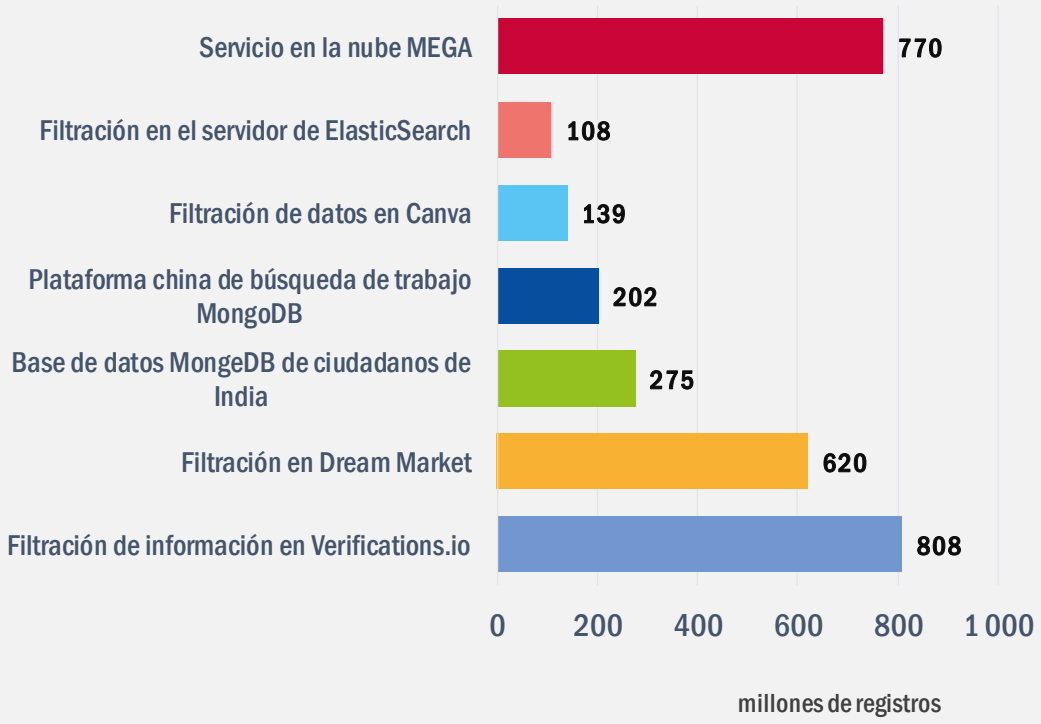
Sinopsis

La sofisticación de las capacidades de amenaza aumentó en 2019, y hubo muchos adversarios que usaron programas intrusos, robo de credenciales y ataques multietapa. El número de incidentes de filtración de datos sigue siendo muy elevado y sigue aumentando la cantidad de información financiera y credenciales de usuarios robados. En algunos casos, el no corregir una vulnerabilidad conocida que potencialmente podría afectar a programas informáticos o a las bibliotecas en uso (en un intervalo de tiempo razonable) podría tener graves repercusiones.

Durante la pasada década **el *malware* ha estado en la lista de la ENISA de las 15 amenazas principales y aun así muchos sistemas de seguridad todavía no son capaces de detectarlo**. Durante muchos años el *malware* se ha propagado principalmente a través de mensajes de correo basura malintencionados, con mensajes de *phishing* sofisticados. Las empresas tecnológicas y los proveedores de correo electrónico invirtieron en filtros de correo basura para mejorar la detección de documentos adjuntos malintencionados. No obstante **los adversarios están innovando para aumentar las posibilidades de llegar a víctimas potenciales**. Muchas de estas innovaciones han dado resultados a los atacantes durante este período.

La pandemia de COVID-19 ha sido un factor que ha ejercido mucha presión sobre las organizaciones y los profesionales de la sanidad de todo el mundo, y la salud se ha convertido en uno de los sectores más críticos que necesitan protección contra los ciberataques. El número de incidentes que implicaban un rescate (*ransomware*) dirigidos contra el sector de la sanidad ya era alto, pero durante la pandemia ha aumentado.

Principales incidentes de filtración de datos



Cronología

2019

_ Enero

MEGA cloud (Nueva Zelanda) sufrió una filtración de datos que expuso 770 millones de correos electrónicos y 21 millones de contraseñas.[1]

_ Febrero

Verification.io (EE. UU.) expuso aproximadamente 800 millones de registros.[2]

_ Marzo

Norsk Hydro (Noruega) fue víctima de un ataque de *ransomware*.[3]

_ Agosto

La agencia tributaria de Bulgaria sufrió una filtración de datos que dejó expuesta información personal identificable de todos los ciudadanos adultos.[8]

_ Septiembre

Mastercard (Bélgica) sufrió una filtración de datos que afectó a aproximadamente noventa mil clientes en Europa.[9]

_ Octubre

Sitios *web* y la cadena nacional de TV en Georgia sufrieron un ciberataque coordinado.[30]

_ Noviembre

UniCredit (Italia) fue víctima de una filtración de datos que expuso 3 millones de registros.[10]

_ Diciembre

Prosegur (España) sufrió un ataque de *ransomware* que interrumpió sus operaciones.[11]

2020

_ Enero

El Ministerio de Asuntos Exteriores de Austria fue objeto de un ciberataque.[12]

_ Abril

Facebook (EE. UU.) notificó una filtración de datos que expuso 540 millones de registros de usuarios en servidores expuestos.[4]

_ Mayo

Las empresas Thyssen-Krupp y Bayer (Alemania) fueron atacadas con *malware* de espionaje.[5]

_ Julio

City Power (Sudáfrica) fue víctima de un ataque de *ransomware* que interrumpió el suministro energético en Johanesburgo.[7]

_ Junio

Cinco hospitales de Rumanía fueron atacados por el *ransomware* Badrabbit.[6]

_ Febrero

INA Group (Croacia) fue víctima de un ataque de *ransomware*.[13]

_ Marzo

La red de ENTSO-E (Bélgica) se vio comprometida al ser víctima de una intrusión.[14]

_ Abril

Se encontraron más de 500 000 cuentas de Zoom (EE. UU.) a la venta en la *dark web*.[31]

Los sectores más atacados

En primera línea

Los sectores más atacados durante este período fueron los servicios digitales, las administraciones del estado y el sector tecnológico. Los ataques a los proveedores de servicios digitales suelen servir de intermediarios para alcanzar otros objetivos más atractivos. Por el contrario, los ataques al sector tecnológico permitieron a los atacantes comprometer la cadena de suministro o buscar vulnerabilidades para explotarlas.

La plataforma de correo electrónico **verifications.io**[18] sufrió una filtración importante de datos[2] debido a una base de datos MongoDB desprotegida. Se expusieron los datos de más de 800 millones de correos electrónicos con información sensible, incluida personale identificable.

Se expusieron más de 770 millones de direcciones de correo electrónico y 21 millones de contraseñas únicas en un foro popular para piratas informáticos alojado por el servicio en la nube **MEGA**[1]. Se convirtió en la colección de credenciales personales filtrados más importante de la historia y se denominó «Collection #1».

El proveedor de servicios en la nube y servicios de equipos virtuales **Citrix** fue víctima de un ciberataque dirigido. Para ganar acceso a los sistemas de Citrix los atacantes exploraron varias vulnerabilidades críticas del software, como la CVE-2019-19781 y emplearon la técnica denominada *password spraying* (lista de contraseñas más usadas).

El proveedor de servicios de alojamiento en la nube **iNSYNQ**[19] sufrió un ataque de *ransomware*[2] que dejó a sus clientes sin acceso a sus datos durante más de una semana, y les forzó a trabajar con copias de seguridad locales.

Los sectores más atacados

Servicios digitales_ Durante 2019 sufrieron ataques servicios como el correo electrónico, plataformas sociales y de colaboración y proveedores de servicios en la nube. Estos también se utilizaron como intermediarios para otros ataques.

Administración del Estado_ Los beneficios económicos de los rescates pagados hacen que el sector público sea uno de los objetivos más atractivos para los ataques de *ransomware*.

Sector tecnológico_ El sector tecnológico fue atacado en 2019 principalmente en ataques a la cadena de suministro que intentaban comprometer el desarrollo de *software* y que iban dirigidos a la vulnerabilidad *zero-day* y ataques por puertas traseras.

Sector financiero_ El número de incidentes sufridos por organizaciones financieras (no necesariamente bancos) aumentó sustancialmente durante el período que abarca este informe.

Sector sanitario_ El número de ataques contra el sector sanitario sigue aumentando.

Tendencias

_Generales

- En 2019 se observó una intensa **actividad de troyanos** en todo el mundo. Emotet y Agent Tesla fueron los tipos más frecuentes y peligrosos de *malware*.
- El ***phishing*** siguió siendo una de las técnicas de más éxito para distribuir herramientas malintencionadas. Técnicas poderosas de *phishing* incluyen los engaños telefónicos, facturas falsas, pagos, presupuestos y órdenes de compra y venta.
- El ***ransomware*** sigue generando beneficios económicos sustanciales para los atacantes. Un estudio reciente identificó campañas de *ransomware* realizadas por personas[17] en las que los adversarios emplean el robo de credenciales y métodos de movimientos laterales tradicionalmente asociados a los ataques dirigidos, como los organizados por agentes Estado nación.
- **El clonaje de tarjetas** los métodos de este tipo de robo de datos de tarjetas bancarias han pasado a ser una amenaza importante en 2019 y 2020 debido al aumento en el número de compras por Internet.
- **Comprometer el correo electrónico de empresa** es una amenaza en aumento como resultado de la gran cantidad de credenciales e información personal robada durante la última década.
- Las empresas sufren una media de 12 ataques de **robo masivo de credenciales** al mes, en los que el atacante puede identificar las credenciales válidas.

Conclusiones

84 %_ de los ciberataques dependen de las técnicas de ingeniería social.

67 %_ de los programas de *malware* se distribuyeron mediante conexiones HTTPS encriptadas.[34]

230 000_ variantes nuevas de *malware* a diario.

6_ meses es el promedio de tiempo que se tarda en detectar una filtración de datos.

71 %_ de las organizaciones sufrió actividades de *malware* que se propagaron de un empleado a otro.[35]

Agentes

_Quiénes son los responsables

Saber quiénes son los responsables o atribuir responsabilidades a una persona o grupo por un incidente de seguridad sigue siendo una tarea muy difícil y en muchas ocasiones un ejercicio inútil. Aun así, desde el punto de vista de la inteligencia contra las amenazas, es esencial clasificar los comportamientos, entender las dinámicas y los *modus operandi* utilizados por determinados adversarios. Este análisis suele ayudar a los defensores a buscar pistas específicas e intentar anticiparse al siguiente ataque del adversario.

El **Lazarus Group**, por ejemplo, un grupo de amenazas persistentes y avanzadas (advanced persistent threat, APT) supuestamente promovidas por un Estado estuvo más activo durante el período que abarca este informe con ataques motivados por finanzas y espionaje. El grupo se ha asociado a varios incidentes, como la **campaña AppleJeus** dirigida a usuarios de la plataforma de compraventa de criptomoneda y sus sistemas.[22] Entre los incidentes importantes atribuidos a este grupo están:

- acceso ilegal a una planta nuclear y a una organización de investigación espacial en la India en noviembre de 2019;
- compromiso de una aplicación de transacciones de criptomoneda dirigida a los administradores de cambio en octubre de 2019;
- ataque a cajeros automatizados y bancos en la India, identificado en septiembre de 2019;
- ataque dirigido a los usuarios de Android en Corea del Sur mediante aplicaciones de la Google Play Store que contenían troyanos, identificado en agosto de 2019.

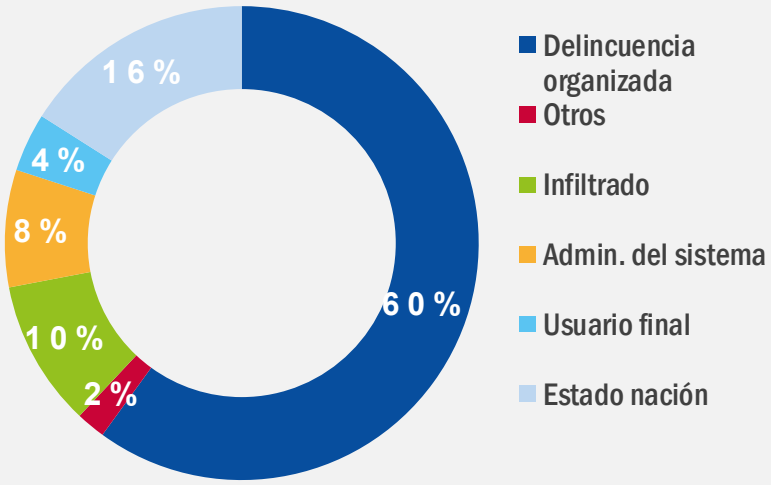
Los agentes más activos

TURLA_ Se notificó que el grupo había usado como objetivo los servidores de correo electrónico de Microsoft Exchange en los sectores de la educación, administración del Estado, militar, investigación y farmacéutico en más de 40 países en 2019.[23]

APT27_ Se notificó que el grupo había comprometido los servidores SharePoint de organizaciones gubernamentales en dos países de Oriente Medio.

VICIOUS PANDA_ En abril de 2020, la Administración Pública de Mongolia fue supuestamente atacada por este grupo.[24]

GAMAREDON_ El grupo aparentemente empezó a atacar al Ministerio de Defensa de Ucrania con una campaña de *phishing* muy dirigida (*spear-phishing*) en diciembre de 2019.[25]



Motivaciones

_Porqué

Aunque es difícil determinar la motivación principal subyacente a un ataque cibernético, sí se pueden categorizar estos ataques basándose en el resultado del incidente.

Financiero: El número de incidentes observados que se han producido como resultado del robo de información, datos y credenciales de usuarios ha sido el más alto durante el período que abarca este informe. En la mayoría de los casos la intención es robar datos o información y venderlos en la *dark web*. También se pueden identificar otros usos de estos datos o información para ayudar a que se produzcan otros tipos de ataques con un resultado completamente distinto, como el espionaje o el fraude financiero. En el popular sitio Dream Market de la *dark web* se vendían más de 620 millones de datos de cuentas robados de 16 sitios *web* pirateados.

Espionaje: Es el motivo detrás de un número en aumento de ataques notificados, debidos principalmente a tensiones geopolíticas y comerciales. El número de incidentes no es sustancial, pero su tamaño y magnitud hacen que la ENISA los clasifique en el segundo puesto de las 5 motivaciones principales. Algunos incidentes destacables incluyen el notificado en abril de 2019, en el que un empleado de General Electric y un hombre de negocios chino fueron imputados por el Departamento de Justicia de los Estados Unidos por espionaje económico y robo de secretos comerciales de General Electric.[20] La Agencia France Presse (AFP) informó de que Airbus había sido víctima de una sofisticada campaña de ciberespionaje. Los atacantes supuestamente penetraron los sistemas informáticos de varios proveedores de Airbus y, desde ahí, entraron en los sistemas informáticos de la empresa.[21]

Los cinco motivos principales: económico, espionaje, trastorno, político y venganza.

Los motivos principales

La cifra de más abajo demuestra que el motivo **económico** sigue siendo la principal causa de la mayoría de los ciberataques. En algunos casos confluyen varios motivos en un ataque individual. Por ejemplo, el espionaje, los motivos políticos, económicos y la generación de trastornos suelen ser motivos combinados. Muchos incidentes se originan a partir de sistemas automatizados y se suministran «como un servicio» pagado en criptomoneda. Estos servicios incluyen la distribución de *ransomware*, los ataques de mando y control (c2), los ataques distribuidos de denegación de servicio (DDoS), el envío de correo basura y otras actividades ilícitas.

Vectores de ataqu

_Cómo

Los ciberataques utilizan tres pasos para llegar a los activos de valor de la víctima. Al revisar los vectores de ataque más utilizados hemos tenido que priorizar el punto de entrada, el plan de acción y la acción sobre los activos. Estas son las tres etapas más críticas que deben constituir enfoques distintos en una estrategia de defensa.

Punto de entrada: En 2019 las técnicas utilizadas con más frecuencia para iniciar un ciberataque fueron la fuerza bruta con credenciales robadas, la ingeniería social, la configuración de errores y la explotación de aplicaciones *web*. La explotación de aplicaciones *web*, por ejemplo, se utilizó con frecuencia como punto de entrada debido al aumento en el uso de este tipo de aplicación para transferir datos a la nube. Los errores en la configuración de la nube y el mal uso de los sistemas fueron el punto de entrada principal en un gran número de incidentes. El uso de ingeniería social para planificar un ataque se basa en utilizar herramientas como las de *phishing* y comprometer el correo electrónico de empresa[16]. Otras técnicas menos frecuentes, pero de la misma importancia, son la explotación de vulnerabilidades (de sistemas sin actualizar y *zero-days*) y las puertas traseras de programas informáticos, que se usan con frecuencia en ataques más complejos y sofisticados.

Línea de acción: Instalar el *malware* es la técnica más usada durante la etapa del plan de acción. Una vez instalado, ayuda al adversario a explorar, moverse por los sistemas y redes de la víctima, instalar otras herramientas como programas de *ransomware*, robar datos y comunicarse con un servidor C2.

_Los cinco activos más deseados por los ciberdelincuentes

01_Secretos de empresa y de la propiedad industrial

Los secretos comerciales y de la propiedad industrial son los activos más deseados debido al alto valor que tienen para sus propietarios, para el mercado y en algunos casos para el mundo del delito.

02_Información clasificada del Estado o militar

Estos activos incluyen información sensible para un Estado. En 2019 las tensiones diplomáticas y comerciales entre varios países hicieron que esta información fuera aún más atractiva.

03_Infraestructura de los servidores

La infraestructura del servidor es el primer activo sensible después de los datos. En muchos ataques el primer objetivo es hacerse con la infraestructura del servidor de la víctima.

04_Datos de autenticación

Los datos de autenticación son activos valiosos para generar beneficios, pero también son un objetivo para respaldar un ataque.

05_Datos financieros

Los datos financieros, como la información de tarjetas de crédito, bancaria y de pago siempre tienen valor para los ciberdelincuentes.

Inteligencia estratégica

_¿Qué ha cambiado en el panorama con la pandemia de covid-19?

En 2019 la ENISA siguió catalogando el panorama de amenazas ayudando a los encargados de tomar decisiones y a los encargados de crear políticas a definir estrategias para defender a la ciudadanía, a las organizaciones y el ciberespacio. Este trabajo forma parte de la estrategia de la ENISA para proporcionar inteligencia estratégica a las partes interesadas. El tema central de 2019 fue la próxima generación de telecomunicaciones móviles, o 5G, a raíz de una solicitud de la Comisión Europea y de los Estados miembros. **La agencia seguirá produciendo estos panoramas temáticos de amenazas y en 2020** el foco se ha puesto en la inteligencia artificial.

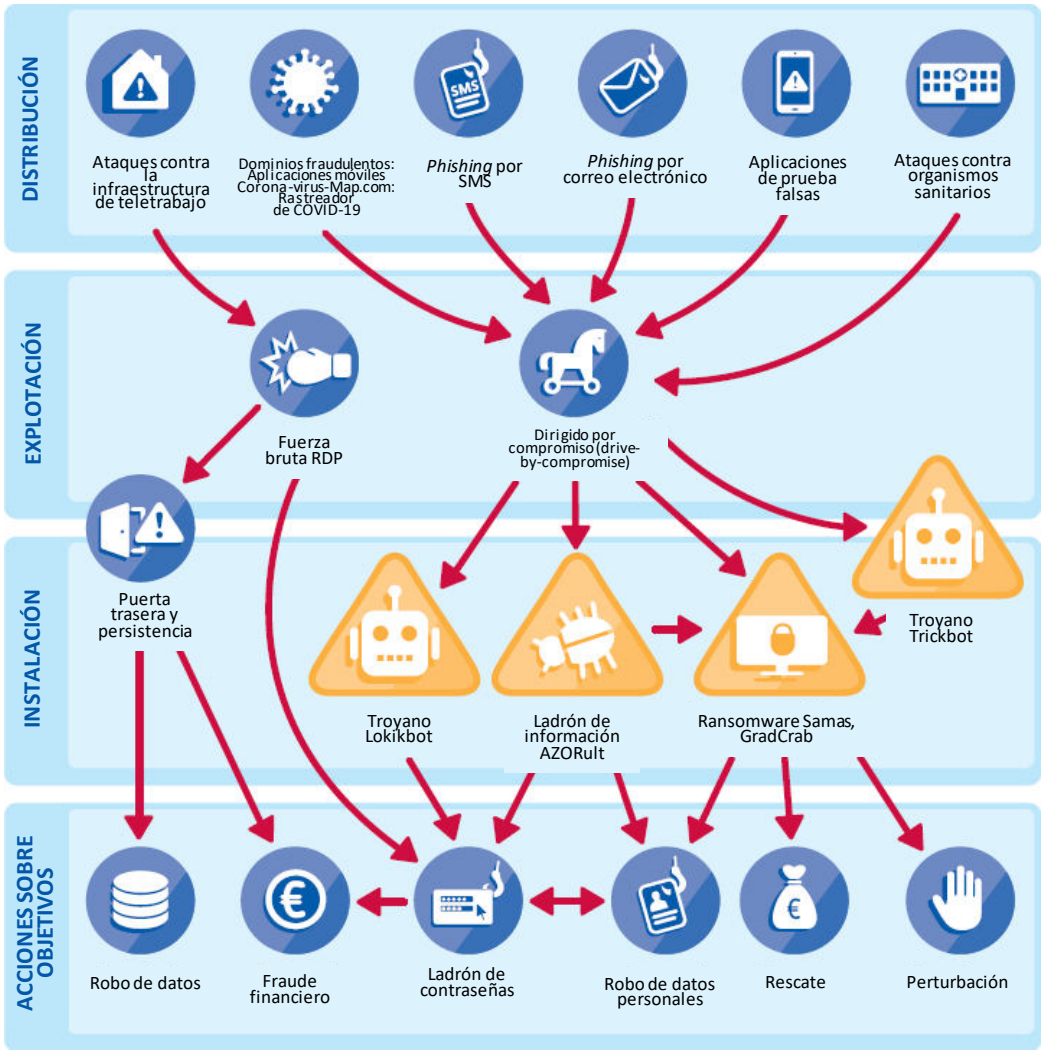
La pandemia de COVID-19 ha sido un período prolífico para los atacantes, que han lanzado ataques dirigidos contra áreas sensibles como la de los proveedores de servicios sanitarios y la de los teletrabajadores. La ENISA está trazando el mapa del panorama de amenazas sufridas durante la pandemia y proporciona asesoramiento sobre las medidas de mitigación que tratan de reducir la exposición a las amenazas.

La ENISA comparte sus recomendaciones sobre ciberseguridad en la pandemia de COVID-19 dedicadas a diversos temas, como el teletrabajo, las compras en línea y los servicios de salud en línea, y proporciona asesoramiento actualizado sobre la seguridad a los sectores afectados.[32]

El **hospital de la Universidad de Brno** en la República Checa sufrió un ciberataque[33] en medio de la pandemia de COVID-19 que forzó a derivar a los pacientes y a posponer intervenciones. El incidente se considera crítico, ya que es uno de los hospitales con laboratorios de análisis de COVID-19 más grandes de la República Checa.

_El panorama de amenazas de COVID-19

La ENISA preparó varios recursos para lanzar una campaña de concienciación y compartió otros recursos internos y externos dirigidos a los expertos en ciberseguridad, que cubren temas de seguridad asociados a los problemas surgidos durante la pandemia de COVID-19. Uno de estos recursos fue el análisis de las amenazas más críticas durante este período.



Bibliografía

1. "MEGA Data Breach Exposed 773 Million Email Addresses and Passwords." 19 de enero de 2019. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

2. "Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records." 8 de abril de 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

3. "LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company." 20 de marzo de 2019. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

4. "Researchers find 540 million Facebook user records on exposed servers." 3 de abril de 2019. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

5. "Winnti: Attacking the Heart of the German Industry". 24 de julio de 2019. Web.br. https://web.br.de/interaktiv/winnti/english/

6. "Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked". 20 de junio de 2019. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

7. "Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions". 25 de julio de 2019. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

8. "Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged." 30 de agosto de 2019. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

9. "Breach Of Mastercard Loyalty Program Affected 90K Germans' Data". 23 de agosto de 2019. PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

10. "UniCredit confirms data breach". 28 de octubre de 2019. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

11. "Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware". 28 de noviembre de 2019. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

12. "Serious cyber-attack' on Austria's foreign ministry". 5 de enero de 2020. BBC. https://www.bbc.com/news/world-europe-50997773

13. "Croatia's largest petrol station chain impacted by cyber-attack". 20 de febrero de 2020. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

14. "European power grid organization says its IT network was hacked". 9 de marzo de 2020. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

15. "Fullz House hackers pivot from phishing to Magecart card skimming attacks". 26 de noviembre de 2019. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

16. "FBI warns of cloud based BEC attacks." 8 de abril de 2020. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

17 "Microsoft Alerts Healthcare to Human-Operated Ransomware" 1 de abril de 2020. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

18. "Verification.io suffers major data breach." 15 de marzo de 2019. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

19. "Inside the Insynq attack: 'We had to assume they were listening'". 8 de agosto de 2019. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

20. "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets". 23 de abril de 2019. USA DoJ. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

21. "Airbus supply chain hacked in a cyberespionage campaign". 27 de septiembre de 2019. CERT-EU. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

22. "Lazarus group's 'AppleJeus' sequel targets cryptocurrency traders". 10 de enero de 2020. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

23 "Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server". 7 de julio de 2019. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

24. "Vicious Panda: The COVID Campaign". 12 de marzo de 2020. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

25. "Gamaredon APT Improves Toolset to Target Ukraine Government, Military". 5 de febrero de 2020. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

26. "Virus attacks Spain's defense intranet, foreign state suspected: paper". 26 de marzo de 2019. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

27 "115 Million Pakistani Mobile Users Data Go on Sale on Dark Web". 10 de abril de 2020. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

28. "Your business hit by a data breach? Expect a bill of $3.92 million". 23 de julio de 2019. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

29. "Cyber Security Statistics for 2019". 21 de marzo de 2019. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

30. "Georgia 'I'll Be Back' Cyber Attack Terminates TV, Takes Down 15,000 Websites." 29 de octubre de 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

31. "Half a million Zoom accounts for sale on the dark web." 16 de abril de 2020. We Live Security by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

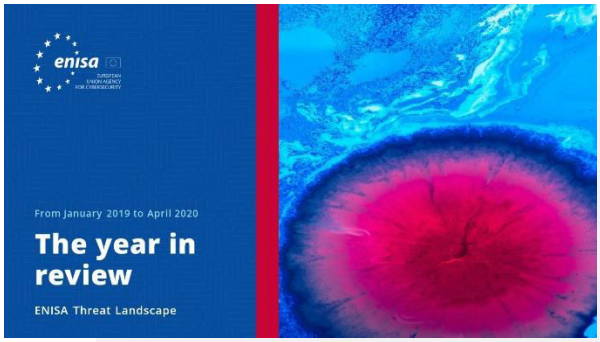
32. "ENISA COVID-19 Resources". ENISA https://www.enisa.europa.eu/topics/wfh-covid19

33. "Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak". 17 de marzo de 2020. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

34. "Most malware in Q1 2020 was delivered via encrypted HTTPS connections". 25 de junio de 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

35. "Malware statistics and facts for 2020". 29 de julio de 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

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

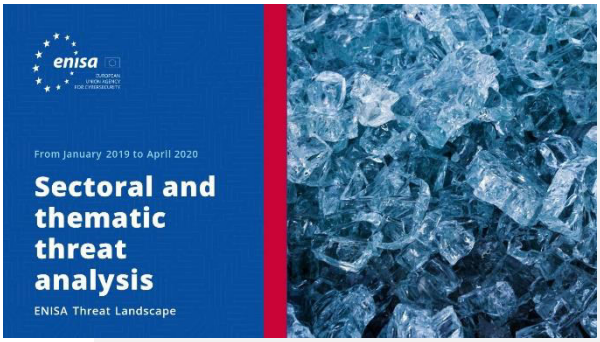
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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

Otras publicaciones

Hoja de ruta para la cooperación entre las CSIRTS y las fuerzas y cuerpos de seguridad

Una hoja de ruta sobre la cooperación entre las CSIRT, en particular entre las fuerzas y cuerpos de seguridad y las judicaturas nacionales y gubernamentales.

LEER EL INFORME

Informe sobre el estado del desarrollo de la respuesta de los Estados miembros de la UE ante incidentes

Un estudio dirigido al análisis de la configuración operativa actual de respuesta ante incidentes de los sectores de la Directiva sobre Ciberseguridad donde se identifican los cambios recientes.

LEER EL INFORME

ENISA: Modelo de evaluación de la madurez de los CSIRT

Una versión actualizada sobre los retos para los equipos de respuesta a incidentes de seguridad informática (CSIRT) en Europa en 2016: Estudio sobre la madurez de los CSIRT publicado por ENISA en 2017.

LEER EL INFORME

«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

¿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