ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Robo de identidad

Panorama de Amenazas de la ENISA

Sinopsis

El robo de identidad o el fraude de identidad consiste en que un impostor utiliza de forma ilícita los datos personales de identificación de una víctima para suplantar su identidad a fin lograr un beneficio económico o de otro tipo.

Según un informe de seguridad anual, se detectaron al menos 900 casos internacionales de robo de identidad o delitos relacionados con el robo de identidad[1]. Los incidentes notificados más relevantes fueron:

- la exposición de los datos personales de casi 106 millones clientes de EE. UU. y Canadá de un banco por el incidente de filtración de datos de Capital One en marzo de 2019[2];
- la exposición de 170 millones de nombres de usuarios y contraseñas utilizados por el creador de juegos digitales Zynga en septiembre de 2019;
- el robo de 20 millones de cuentas del servicio de difusión de audio británico Mixcloud[3];
- el compromiso de los datos personales de 600 000 conductores y 57 millones de usuarios derivado del incidente de filtración de datos de Uber en noviembre de 2019;[3]
- y el robo de 9 millones de registros personales de los clientes de EasyJet, incluidos los datos del DNI y las tarjetas de crédito.

La tendencia en el robo de identidad se refleja en gran parte en las filtraciones de datos, que, en comparación con el año 2018, sufrieron el número récord de 3 800 casos públicamente divulgados; 4 100 millones de registros expuestos y un aumento del 54 % en el número de filtraciones notificadas.[4]

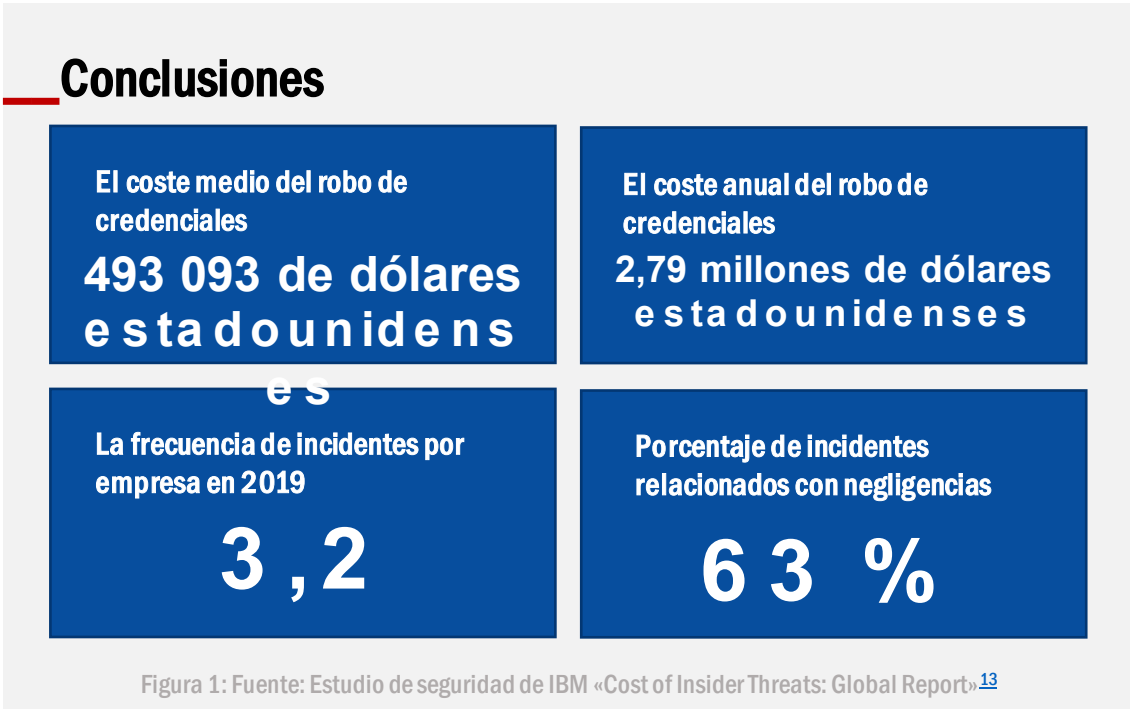


Figura 1: Fuente: Estudio de seguridad de IBM «Cost of Insider Threats: Global Report»[13]

La amenaza del robo de identidad

En 2019 se procesaron judicialmente algunos de los atacantes responsables de incidentes importantes perpetrados en los años pasados. En junio, el Departamento de Policía de Nueva York, en colaboración con el FBI, puso a disposición judicial a los miembros del grupo «Fraud Ring», que operaba en los Estados Unidos y que en 2012 robó las credenciales de los iPhones por un valor de un millón de dólares estadounidenses (aprox. 846 000 EUR) en una operación de robo de identidad a gran escala. Hasta la detención del grupo, la cantidad total robada alcanzó los 19 millones de dólares estadounidenses (aprox. 16 millones EUR)[4]. Un mes más tarde se anunció públicamente el acuerdo «Equifax»[5]. Se forzó a Equifax a compensar a la Comisión del Comercio Federal de los Estados Unidos, a la Oficina de Protección Financiera del Consumidor, a 48 Estados, al Distrito de Columbia y a Puerto Rico por la filtración de datos de 2017, cuyo coste ascendió por lo menos a 575 millones de dólares estadounidenses (aprox. 487 millones EUR). Debido a esa filtración de datos que se juzgó «completamente evitable» se filtraron casi 148 millones de direcciones y números de la seguridad social de EE. UU. A finales de ese año Brasil multó a Facebook en EE. UU. 1,6 millones de dólares estadounidenses (aprox. 1,35 millones EUR) en nombre de los ciudadanos brasileños por la filtración de datos de Cambridge Analytica.[3]

Kill chain

Robo de identidad

Reconocimiento	Uso como arma	Distribución	Explotación

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

_Ataques de suplantación de marcas

Ajustándose a la tendencia de 2018, algunas marcas son las preferidas de los suplantadores por su buena reputación. Aunque estas marcas, como Microsoft (44 %) y Amazon (17 %), siguen estando a la cabeza de las clasificaciones de 2019 de los ataques de suplantación, se han producido algunas adiciones notables, como la del IRS (Servicio de Impuestos Internos de EE. UU.).[7] La delicada información que incluye el formulario de sueldos e impuestos (W-2) siempre ha atraído a los impostores, que usaron los datos de IRS en el 10 % de los mensajes de correo electrónico basados en el fraude de identidad en el año de este informe. Como resultado, los formularios W-2 y los formularios estándar de la declaración de la renta individual de EE. UU. (1040) están disponibles en la *dark web* a un precio que oscila entre 1 y 52 dólares estadounidenses.

Este material, combinado con los números de la Seguridad Social (SSN) y las fechas de nacimiento, que también estaban disponibles, permite a cualquier pirata informático con poca experiencia invertir una cantidad de 1 000 dólares estadounidenses (aprox. 846 EUR) para acceder de forma legal a una cuenta bancaria en Estados Unidos, hacer una declaración de la renta falsa, solicitar una devolución y convertir en efectivo una inversión que se ha duplicado o triplicado. Según la investigación penal del IRS, más de 10 000 declaraciones de la renta con solicitudes de devolución de más de 83 millones de dólares estadounidenses (aprox. 70 millones EUR) fueron potencialmente fraudulentas.[9]

El ciclo de pasos para el fraude tributario "Dirty Dozen"

Figura 2 - Fuente: BDO[19]

Tendenci

_Suplantación de identidad y cambio de SIM

Esta técnica se lleva utilizando desde 2016 y va dirigida a titulares de criptomoneda. Sin embargo, en 2019 se usó la misma técnica dirigida a personas o cuentas de alto perfil con la intención de robar la identidad de la víctima. Ejemplos de víctimas del cambio de SIM fueron: Jack Dorsey (director general de Twitter), Jessica Alba (actriz), Shane Dawson (actriz), Amanda Cerny (actriz, fue víctima dos veces), Matthew Smith (actor, fue víctima cuatro veces) y King Bach (artista).[10] El cambio de SIM también se utilizó masivamente en dos casos: en el banco más grande de Mozambique, donde robaron hasta 50 000 dólares estadounidenses (aprox. 42 300 EUR) de cuentas de empresa de alto perfil; y en Brasil, donde una banda organizada pirateó las cuentas de 5 000 víctimas, principalmente políticos, ministros y gobernadores.[11]

_Uso de los cheques regalo como caballo de Troya para comprometer el correo electrónico de una empresa

Los ataques BEC (*business e-mail compromise*) causaron pérdidas de miles de millones de euros en 2019. En estos incidentes, los atacantes simulan ser una persona de confianza, normalmente perteneciente a la empresa, y se engaña a la víctima para que haga una transacción financiera o para que difunda información sensible de tipo personal o corporativa. En más de la mitad de los ataques BEC se engañaba a la víctima para que comprara un cheque regalo. Durante el proceso de compra se interceptaba información sensible como los datos de la cuenta bancaria. También se forzaba a la víctima a enviar la tarjeta regalo al atacante, como forma de opción anónima, irreversible y directa de obtener el dinero. La cantidad media robada por tarjeta de regalo era de 1 500 dólares estadounidenses (aprox. 1 269 EUR).[12]

Conclusiones

20 %_ de los ataques de suplantación de identidad usaron cuentas comprometidas.[7]

30 %_ de los ataques dirigidos a las cuentas de altos ejecutivos se llevaron a cabo utilizando la presentación del nombre como engaño.[7]

65 %_ de los ataques BEC engañaron a las víctimas para que compraran tarjetas regalo.[12]

3,32_ millones EUR es el coste medio de una filtración de datos.

95 %_ de los participantes en una encuesta del Eurobarómetro opinaban que el robo de identidad era un delito grave.

Tendencias

Dobles digitales

La técnica antifraude «máscaras digitales» salió a la luz cuando más de 60 000 identidades digitales robadas aparecieron como producto de venta en el mercado Genesis de la *dark web* en abril de 2019. Estos «dobles» estaban listos para su venta a un precio de entre 5 y 200 dólares estadounidenses cada uno. El propietario de uno de los dobles puede suplantar con más facilidad a un usuario real en una tienda de Internet o en un servicio de pago, especialmente si se combina con contraseñas y nombres de usuario robados. Además de la compra de estos dobles digitales han aparecido herramientas para ayudar al suplantador potencial, como el navegador Tenebris que incorpora un generador que permite desarrollar huellas dactilares y máscaras digitales únicas.[11]

En los últimos años se ha identificado a los responsables de robos de información de pago (con *skimmers*), de robos de información mediante la revisión de la basura de una persona u organización (*dumpster divers*), a los piratas informáticos, a los suplantadores del administrador y a los usurpadores de identidades (*phishers*) como los grupos principales culpables de los ataques de robo de identidad. Esta lista ha aumentado en 2019 con la adición de los estafadores que usan el teléfono para estafar (*vishers*) y los estafadores que usan una variante del *phishing* mediante SMS (*SMSishers*). Los *vishers* hacen *phishing* utilizando el teléfono. No suplantan una identidad, sino que simulan representar a una organización bien conocida y ofrecen ayudar a la víctima con un servicio, por ejemplo gestionar los programas de ordenador, las finanzas o una devolución de hacienda. Los *smishers* envían mensajes SMS falsos y si el destinatario responde, los estafadores piratean directamente el dispositivo o lo reenvían a un sitio *web* de *phishing*.

La figura siguiente incluye los tipos de datos principales perdidos en 2019, en los que las cuentas de datos de correo electrónico fueron las que tuvieron el número más alto de registros perdidos o robados. Estos números revelan la gravedad de la situación si se considera que los mensajes de correo electrónico pueden contener información sensible de carácter personal, corporativa o gubernamental.

Tipos principales de datos perdidos en 2019

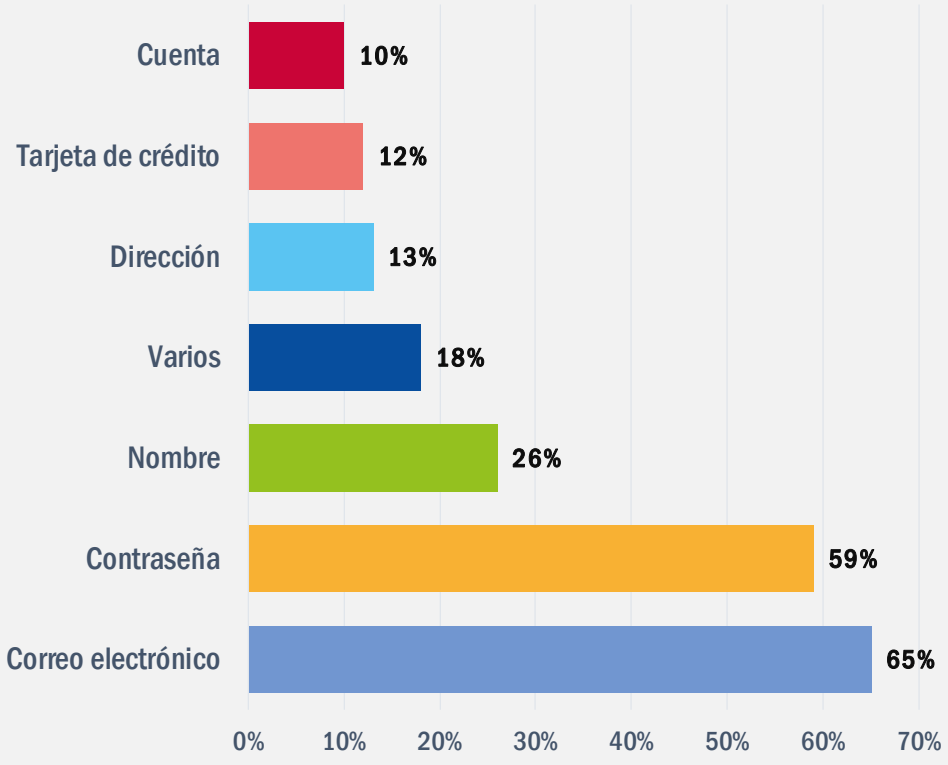


Figura 3 - Fuente: RiskBased SECURITY[8]

Vectores de ataque

Cómo

- **LA NUBE COMO INTERFAZ DE ATAQUE PARA OBTENER LOS DATOS DE LOS CLIENTES**. En el año de este informe, un ataque de este tipo afectó a Amazon CloudFront, una red de distribución de contenido (content delivery network, CDN).[14] Se expusieron los sitios *web* que albergaban o estaban vinculados a bibliotecas en la infraestructura de Amazon revelando contenido cargado externamente, incluidos los datos de tarjetas de crédito.
- **URL de PHISHING**. En 2019 se volvieron a utilizar las técnicas habituales de URL de *malware*[16] de acaparamiento de dominios (*domain squatting*), de toma del control de un dominio registrado (*domain shadowing*) y de reducción de la longitud de las direcciones URL. En el último trimestre de 2019, se observó que el 26 % de los dominios malintencionados utilizaban un certificado seguro y uno de cada tres de esos certificados era SSL. Este truco afectaba a la confianza del visitante, que al ver el icono de sitio seguro (el candado) pensaba que se trataba de un sitio seguro.[15]
- **Engaño W2**. El engaño W2 es otro ataque dirigido a los registros de empresas y organizaciones para tener acceso a información sensible. El engaño se produce al embaucar a un miembro ejecutivo del Departamento de Recursos Humanos o Finanzas para obtener los registros de los empleados. Estos registros se usan luego para el robo de identidad. El engaño se llama W2 por el formulario de la hacienda de Estados Unidos W2, que se utiliza para notificar el sueldo de un empleado. Este engaño de ingeniería social, aunque es antiguo (el IRS lo notificó por primera vez en 2016), ha aumentado en los últimos años sistemáticamente un 10 % por año.[9,17]
- **NIMCY**. En 2019, el grupo responsable de la familia de *malware* Zebrocy introdujo una herramienta de suplantación de identidad muy dirigida (*spear-phishing*) llamada Nimcy. La herramienta se desarrolló usando el lenguaje de programación Nim (antes Nimrod) creado por el mismo grupo de piratas informáticos. Este nuevo programa descargador y de puerta trasera se utilizó para robar las credenciales de inicio de sesión, pulsaciones de teclas, comunicaciones y archivos de diplomáticos, oficiales de las fuerzas armadas y personal del Ministerio de Asuntos Exteriores. Parece que los atacantes se centraban en los gobiernos de Asia Central, prefiriendo Pakistán y la India.[14]

- **AMENAZAS MÓVILES.** En 2019 se observó un aumento de aplicaciones para móviles malintencionadas que continuó en 2020. Incluso las plataformas más fiables y más usadas como Google Play contenían aplicaciones cuya misión era robar credenciales (p. ej., Acesse SantaMobile, Modulo ID). No obstante, el número de descargas fue extremadamente bajo, lo que demuestra que las víctimas potenciales no se dejaban engañar.[20]
- **TROYANO BANKER.ANDROIDOS.SVPENG.AK.** Este troyano para móviles ocupa el octavo puesto en la lista de los troyanos más populares y es también el troyano bancario más popular, responsable, respectivamente, de un 1,75 % y un 16,85 % de los ataques únicos, la mayoría dirigidos a robar las credenciales bancarias de las víctimas y los códigos de autorización de dos factores. La mayoría de las víctimas de estos troyanos se encontraban en Rusia, lo que convierte a este país en el más atacado por troyanos bancarios para móviles.[21]
- ***FORMJACKING***. Los ataques por *formjacking* (copiar datos de formularios de Internet) fueron extremadamente comunes en 2018, pero parecen haber descendido considerablemente en el primer trimestre de 2019. Aun así, en mayo con el ataque a un proveedor de servicios sanitarios americano y con el robo de los credenciales de apertura de sesión, el número de ataques siguió subiendo durante el resto del año. En ese mes se registró un número récord de detecciones (1,1 millones). Los cinco países con más detecciones de ataques de tipo *formjacking* en 2019 fueron Estados Unidos (51,8 %), Australia (8,1 %), la India (5,7 %), el Reino Unido (4,1 %) y Brasil (3,5 %). El grupo de piratas informáticos Megacart está fuertemente asociado a la mayoría del desarrollo de las herramientas para esta actividad, y con los ataques a British Airways, Newegg, Feedify y Ticketmaster[22]

Mitigación

Acciones propuestas

- Evitar el uso del gestor de contraseñas del programa navegador. Si se necesita un programa de este tipo, utilizar uno que funcione fuera de línea y esté protegido con contraseña.[23]
- Comprobar la información de todo el que envía una solicitud de transferencia de dinero por teléfono o en persona.[19]
- No compartir información delicada, como las historias médicas de pacientes en notas escritas a mano para evitar su pérdida o traspapelado. Los archivos digitales son mejores para datos de corta duración y luego deben destruirse por completo.
- Utilizar la «búsqueda de amenazas» en su empresa para reforzar sus planes de seguridad. La búsqueda de amenazas la realizan miembros expertos del equipo del centro de operaciones de seguridad (security operation centre, SOC) y consiste en identificar proactivamente las vulnerabilidades y evitar que las amenazas se aprovechen de ellas.
- Utilizar políticas como las reglas basadas en la velocidad para mitigar el fraude de identidad, especialmente en las transacciones con tarjetas de pago. Los datos de máquina de las transacciones válidas pueden proporcionar información suficiente para una definición óptima de las políticas.
- Utilizar un método de autenticación única (single-sign-on, SSO) siempre que se pueda, ya que permite al usuario entrar en varias aplicaciones con el mismo conjunto de credenciales digitales. El uso de este método está altamente recomendado para minimizar el número de cuentas de usuarios y credenciales almacenadas.
- Instalar protección de punto final con programas antivirus, pero también bloquear la ejecución de archivos apropiadamente (p. ej., bloquear la ejecución en la carpeta de archivos temporales).
- La autenticación multifactor es una medida de seguridad para evitar el pirateo de contraseñas o pérdidas y para garantizar el éxito del proceso de autenticación con varias claves. La introducción de la autenticación multifactor adaptativa optimiza el proceso de autenticación basado en el comportamiento del usuario y en el contexto asociado.

- Comprobar las URL que se envían por correo electrónico o que se visitan al azar basándose en su dirección IP, el ASN asociado a la IP, el propietario del dominio y la relación entre este dominio y otros, antes de dar el siguiente paso.
- Las organizaciones que utilizan los servicios en la nube deben tener operaciones de seguridad robustas y preferiblemente utilizar una arquitectura de almacenamiento en sus instalaciones y el almacenamiento en nube privado y público simultáneamente para proteger la información personal de sus clientes.
- Hacer obligatorio el uso de métodos de cifrado robustos y actualizados, como TLS 1.3 (usa claves temporales) para los datos sensibles para evitar incidentes.
- Proteger adecuadamente todos los documentos de identidad y sus copias (físicas o digitales) contra el acceso no autorizado.
- No revelar información de identificación a destinatarios no solicitados; no debe darse curso a las peticiones de esta información por teléfono o correo electrónico o en persona.
- Hacer obligatorio el uso de dispositivos protegidos con contraseña, para garantizar la buena calidad de las credenciales y métodos seguros para su almacenamiento.
- Garantizar credenciales de buena calidad y métodos seguros para su almacenamiento en todos los soportes usados.
- Prestar mucha atención cuando se usan las redes Wi-Fi públicas porque los estafadores las piratean o las duplican. Si se usa una red de este tipo, evitar el acceso a aplicaciones y datos sensibles. Utilizar un servicio VPN de confianza para conectarse a las redes de Wi-Fi públicas.
- Comprobar las transacciones periódicamente cotejando los extractos bancarios o recibos en busca de irregularidades.
- Instalar programas de filtro de contenido para filtrar documentos adjuntos no deseados, mensajes de correo electrónico con contenido malintencionado, correo basura y tráfico de red no deseado.
- Hacer obligatorio el uso de soluciones para la prevención de la pérdida de datos (data loss prevention, DPL).

Bibliografía

1. "2019 identity theft report released", 31 de julio de 2019. ITIJ. https://www.itij.com/latest/news/2019-identity-theft-report-released

2. "Capital One data breach: What you can do now following bank hack". 12 de agosto de 2019. C | Net. https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

3. "Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks". 8 de enero de 2020. Cyber crime Magazine. https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/

4. "$19 million worth of iPhones stolen in massive identity theft scam". 15 de junio de 2019. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

5. "Equifax to pay at least $575 million as part of FTC settlement". 22 de julio de 2019. C | Net. https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/

6. "2019 data breaches: 4 billion records breached so far" Norton. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

7. "Q1 2019: Email Fraud and Identity Deception Trends" Agari. https://www.agari.com/insights/ebooks/2019-q1-report/

8. "Data Breach QuickView Report, 2019 Q3 trends." Noviembre de 2019. RiskBased SECURITY. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

9. "IRS issues 2019 annual report; highlights program areas across the agency" 6 de enero de 2020. IRS. https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency

10. "Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too". 5 de septiembre de 2019. The New York Times. https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

11. "IT threat evolution Q2 2019". 19 de agosto de 2019. Kaspersky. https://securelist.com/it-threat-evolution-q2-2019/91994/

12. "Phishing Activity Trends Report". 12 de septiembre de 2019. Anti-phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

13. "The Cost of Insider Threats" IBM. https://www.ibm.com/downloads/cas/LQZ4RONE

14. "APT trends report Q2 2019". 1 de agosto de 2019. Kaspersky. https://securelist.com/apt-trends-report-q2-2019/91897/

15. "Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more" Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

16. ENISA Threat Landscape Report 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

17. "Q2 2019 Cryptocurrency Anti-Money Laundering Report" CipherTrace. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

18. "Latest Quarterly Threat Report - Q1 2019" Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

19. "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare". Octubre de 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

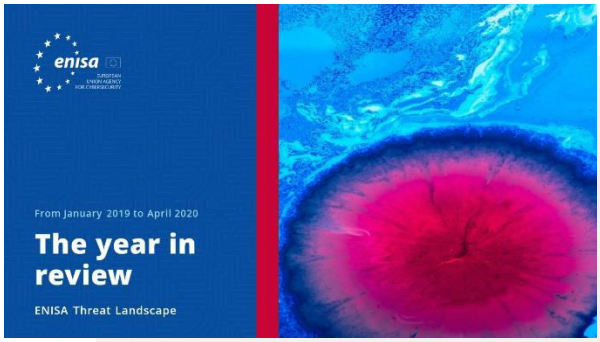
20. "IT threat evolution Q1 2019. Statistics". 23 de mayo de 2019. Kaspersky. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

21. "IT threat evolution Q3 2019. Statistics". 29 de noviembre de 2019. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

22. "FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month". Agosto de 2019. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf

23. "Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web" VMWare. https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

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

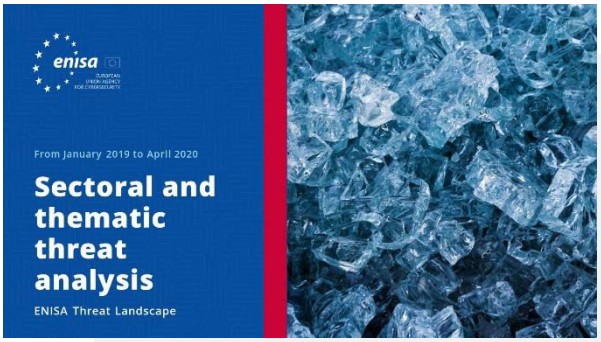
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

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.



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Análisis de las amenazas por sectores y temas**

Análisis contextualizado de las amenazas durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Tendencias emergentes**

Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Sinopsis de la inteligencia sobre las ciberamenazas**

Situación actual en materia de inteligencia sobre las ciberamenazas en la UE.

¿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