ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Ransomware

Panorama de Amenazas de la ENISA

Sinopsis

El *ransomware* se ha convertido en un arma popular para quienes quieren perjudicar a diario a administraciones, empresas y particulares. En estos casos, la víctima del *ransomware* podría sufrir pérdidas económicas al tener que pagar el rescate solicitado o al tener que pagar los costes para recuperarse de la pérdida si no cumple con las demandas del atacante. En un incidente ocurrido en 2019 en Baltimore, Maryland (EE. UU.), un ataque bloqueó los ordenadores municipales y para recuperarse los atacantes pedían 18,2 millones de dólares estadounidenses (aprox. 15,4 millones EUR) que las autoridades se negaron a pagar.[1] El aumento del número de incidentes deja claro que convertirse en víctima ya no es cuestión de mala suerte sino de tiempo. Sin embargo, en la lucha de la mayoría de los países contra el *ransomware* es necesario abordar varios retos, como la falta de coordinación y colaboración entre agencias y autoridades, y la falta de legislación que penalice claramente estos ataques.

Aunque las pólizas de seguros con cobertura contra ataques cibernéticos existen desde principios del año 2000[2], en los últimos 5 años los ataques de *ransomware* son una de las razones que más han impulsado el aumento del interés en este tipo de seguro. En algunos de los incidentes de 2019[7], el rescate o los costes de recuperación estaban cubiertos por este tipo de contratos. Pero, por desgracia, si se sabe que los objetivos potenciales de los ataques de *ransomware* están asegurados, los atacantes asumen que lo más probable es que les paguen. Otro inconveniente para la víctima es que los proveedores de seguros pagan el rescate por adelantado a fin de mitigar los daños y mantener intacta la reputación de la víctima. Aun así, esta conformidad a la hora de pagar rescates anima a los ciberdelincuentes y no garantiza ni la recuperación ni la protección de la reputación de la víctima.[3]

Conclusiones

10 100_ **millones EUR fue la cifra dedicada al pago de rescates durante 2019.**

La cantidad de dinero pagada en rescates fue de 3 300 millones de dólares estadounidenses más que en 2018.

365 %_ **es el aumento de las detecciones en empresas en 2019.**

La detección de ataques de *ransomware* en equipos en entornos de empresa aumentó en comparación con la primera mitad de 2018.[22]

66 %_ **de las organizaciones sanitarias sufrieron un ataque.**

Más del 66 % de las organizaciones sanitarias sufrieron un ataque de *ransomware* en 2019.[23]

45 %_ **de las organizaciones atacadas pagaron el rescate.**

Este es el porcentaje de organizaciones atacadas en 2019 que pagaron el rescate, y aun así la mitad de ellas perdieron sus datos.[37]

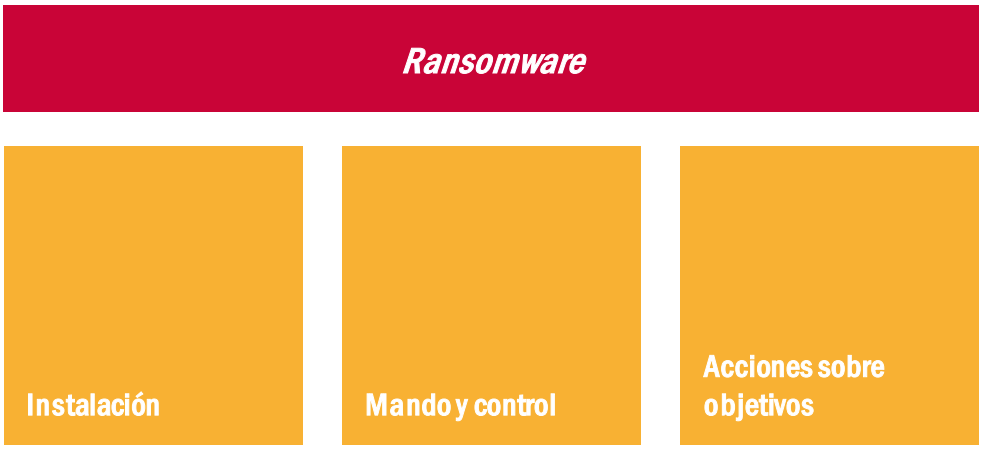
28 %_ **de los incidentes de seguridad se atribuyeron al *malware*.**

Los ataques de *ransomware* fueron el segundo tipo de ataque más común después del *malware* C2 y se asociaron a un tercio (28 %) de los incidentes de seguridad.[32]

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

Descripción

_Los ataques de *ransomware* apuntan más alto

Durante el primer y el segundo trimestre de 2019 el número de ataques de *ransomware* fue menor que el registrado en el mismo período en los 3 años anteriores. No obstante, los ataques se dirigieron contra objetivos de perfiles altos. A lo largo de 2018 se produjeron despliegues de troyanos de acceso remoto (Remote Access Trojan, RAT), descargadores y puertas traseras, pero durante ese año esos tipos de *malware*[7] permanecieron inactivos.[9,10] Ahora se piensa que ese *software* proporcionó a los atacantes la información necesaria para identificar objetivos vulnerables con perfiles altos, que podían pagar rescates más elevados. A este respecto, en el año del informe, los ataques de *ransomware* se expandieron a otros sectores distintos al sanitario, apuntando a objetivos industriales y al sector manufacturero. Recientemente se ha utilizado la familia de programas de *ransomware* LockerGoga para dañar los sistemas que controlan los equipos físicos de las plantas de producción.[11]

_Los seguros cibernéticos ganan popularidad

En el año 2019 las pólizas de seguros cibernéticos representaron un mercado de 8 000 millones de dólares estadounidenses (aprox. 6 700 millones EUR) solo en los Estados Unidos. Aunque estos productos existen desde el cambio de milenio o desde el *bug* del milenio, en los años pasados han atraído el interés de organizaciones gubernamentales, ayuntamientos, organizaciones sanitarias y otros objetivos de *ransomware* potencialmente de alto riesgo. El ataque de SamSam en Atlanta (Georgia) y el incidente de Lake City en Florida estaban cubiertos por este tipo de pólizas.[16] A medida que aumentan las demandas de rescates, las pólizas de seguros cibernéticos se están convirtiendo en algo cada vez más necesario para organizaciones y empresas. No obstante, el sentido común sugiere que las víctimas deben negarse a pagar el rescate siempre que sea posible. Cuando se acepta el pago del rescate no solo se anima al atacante a repetir el acto sino que también la víctima se arriesga a no recuperarse, ya que ha habido varios casos en los que el atacante no ha cumplido con su parte del trato.

_El protocolo de escritorio remoto abierto (Open Remote Desktop, RDP) es de alto riesgo

Varias familias de programas de *ransomware* de éxito como SamSam, BitPaymer y CrySiS se centran en servidores RDP para iniciar un ataque.[20] Lamentablemente, muchas organizaciones aún usan RDP en vez del protocolo más seguro de red privada virtual (Virtual Private Network, VPN) para el acceso remoto. El problema con el protocolo RDP es que presenta vulnerabilidades que pueden ser explotadas y el servicio RDP puede depender de servidores orientados a Internet que son de fácil acceso. Se sabe que hay más de 800 000 sistemas con servicios RDP que no se han actualizado y que son vulnerables; entre ellos, los sistemas en el intervalo IP del centro de datos Microsoft Azure.[51] Aunque Microsoft aseguró al público que estos sistemas pertenecían a terceros, aquí surge un problema relacionado con la seguridad de los proveedores de servicios en la nube.

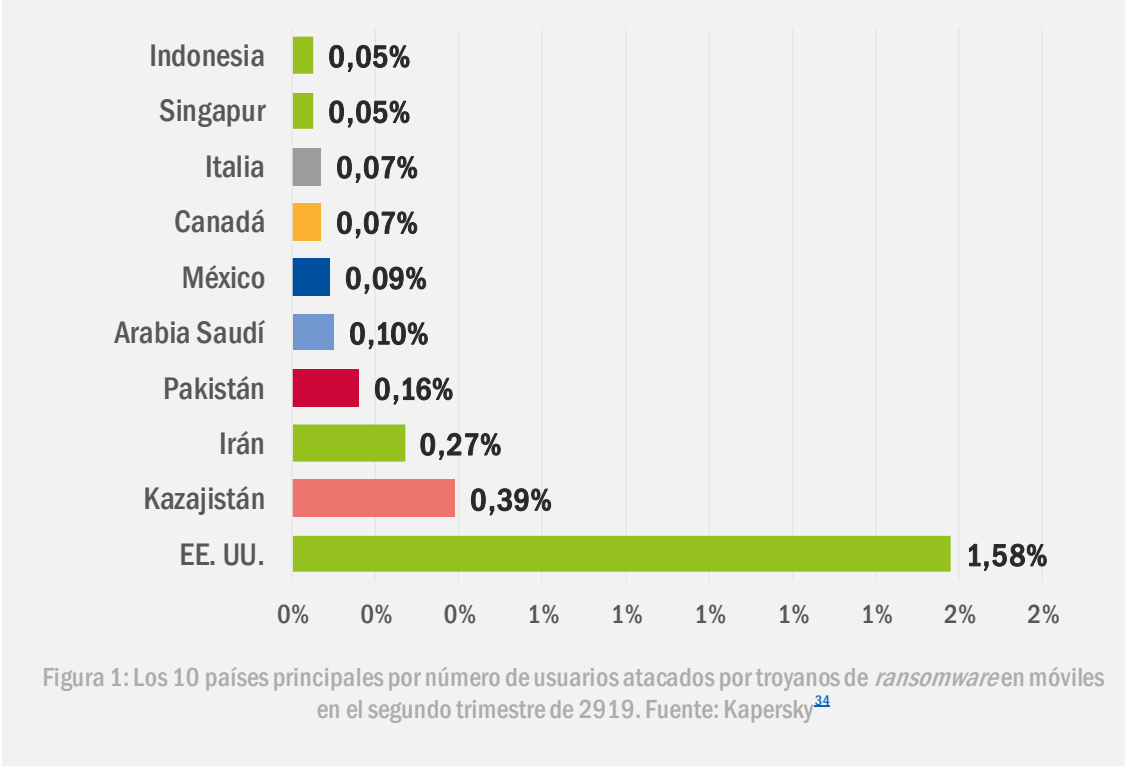


Figura 1: Los 10 países principales por número de usuarios atacados por troyanos de *ransomware* en móviles en el segundo trimestre de 2919. Fuente: Kapersky[34]

Descripción

_ Los más buscados

LOCKERGOGA_ salió a la luz por primera vez en enero de 2019 en un ataque a la empresa francesa de consultoría del sector de la ingeniería Altran Technologies.[40] El virus inactivó las redes, los sistemas informáticos y las aplicaciones de la empresa, y afectó a sus operaciones en varios países. LockerGoga es un programa plantado y ejecutado por la herramienta PsExec, que es un reemplazo de peso ligero de telnet, capaz de pasar algunas comprobaciones de seguridad como programa semiválido.[11] Cuando se instala, modifica las cuentas de usuario en el sistema atacado y obliga al sistema a desconectarse. Además, los archivos de herramientas cambian ellos mismos de nombre y de ubicación lo que hace que sea casi imposible encontrarlos. En versiones posteriores de LockerGoga, el bloqueo es tan fuerte que las víctimas ni siquiera pueden ver la nota de *ransomware* o las instrucciones para la recuperación, aun pagando el rescate. Solo unos cuantos productos *antimalware* y antivirus son capaces de detectar y defender sistemas contra LockerGoga, y no existe un descodificador específico.[10] En 2019 LockerGoga atacó a otras empresas (aparte de Altran Technologies): NorskHydro y dos compañías químicas de Estados Unidos, Hexion y Momentive.[41] Solo en el caso de NorskHydro el coste de los daños se estimó en 50 millones de dólares estadounidenses (aprox. 42 millones EUR).[21]

KATYUSHA_ es un troyano de *ransomware* que se utilizó por primera vez en octubre de 2018. Cifra los archivos de las víctimas, borra las copias instantáneas y envía adjuntos por correo electrónico. Katyusha utiliza los programas intrusos EternalBlue and y DoublePulsar para expandirse.[45] Desafortunadamente no hay herramientas o descifradores disponibles para defenderse.

JIGSAW_ no solo cifra los archivos de las víctimas, también los borra si no se paga el rescate, normalmente, en 24 horas. Es más, si la víctima intenta algo como apagar el ordenador, la velocidad de borrado aumenta. No es una coincidencia que este programa de *ransomware* lleve el nombre de un personaje de una película de terror.[45] Sin embargo, en este caso, las empresas de seguridad publican constantemente actualizaciones de descifradores de Jigsaw.[46]

PEWCRYPT_ se creó a principios de 2019 y, a diferencia de la mayoría de los programas de *ransomware*, su único objetivo es forzar a las personas a suscribirse al canal del YouTuber PewDiePie. PewDiePie competía en popularidad con T-Series, un canal indio de Bollywood, y sus seguidores decidieron usar PewCrypt para aumentar las posibilidades de que su ídolo ganara. PewCrypt es un programa de *ransomware* típico que se propaga a través de mensajes de correo basura y anuncios en línea malintencionados. Se creó con el lenguaje de programación Java. En marzo de 2019 el propio autor publicó una herramienta de descifrado.[47]

RYUK_ apareció por primera vez en agosto de 2018 y se asumió que estaba asociado a grupos de ciberdelincuentes norcoreanos. No se tardó mucho tiempo en saber que los autores de Ryuk eran los mismos que los componentes del grupo que usaba el *ransomware* de Hermes a la vez que robaba su código. Las características principales de Ryuk son que utiliza algoritmos militares y que sus ataques van dirigidos contra grandes empresas. Es más, pide a la mayoría de las víctimas que paguen el rescate en Bitcoins.[45]

DHARMA_ es un virus de cifrado que apareció por primera vez en 2016 pero del que aún se publican nuevas versiones. Dharma no solo cifra los archivos de las víctimas, también borra las copias instantáneas. En 2019 se propagaba mediante archivos contaminados con extensiones populares, legítimas o malignas como: .gif, .AUF, .USA, .xwx, .best y .heets. En septiembre de 2019 un investigador especializado en temas de seguridad publicó Rakhnidecryptor[42] para ayudar a las víctimas de Dharma a descifrar sus archivos.

GANDCRAB_ se utilizó por primera vez en enero de 2018 e infectó más de 50 000 sistemas en menos de un mes, con lo que se convirtió en uno de los programas de *ransomware* más populares de ese año.[43] Utiliza las macros de Microsoft Office, VBScript y PowerShell para atacar sin ser detectado.[45] GandCrab es parecido a Cerber, se basa en el modelo de *ransomware* como servicio (RaaS) y permite a los programadores y a los delincuentes compartir las ganancias. Un equipo creado por Europol, la policía de Rumanía, la Oficina del Fiscal General y Bitdefender consiguieron producir una herramienta para el descifrado[44] tras el acceso a los servidores de GandCrab. Los responsables de GandCrab anunciaron su retirada en el segundo trimestre de 2019 después de haber conseguido más de 2 000 millones de dólares estadounidenses en rescates. No obstante, el programa de *ransomware* Sodinokibi, que se observa en pequeñas campañas, parece haberse convertido en el sucesor de GandCrab.[10]

Descripción

_ Los más buscados

REVIL o SODINOKIBI o SODIN_ aparecieron por primera vez en el ataque *web* a la herramienta italiana WinRAR en junio de 2019. También se sospecha que ha estado involucrado en tres ataques a MSP y en un cuarto contra la empresa estadounidense PerCSoft, con clientela principalmente del sector sanitario.[48] Sodinokibi parece ser un producto del conocido grupo de ciberespionaje FruityArmor, que lleva activo desde 2016. Sodinokibi ha afectado a varios países de todo el mundo. Taiwán ha sido víctima del 17,56 % de todos los ataques registrados de Sodinokibi hasta la fecha, lo que lo convierte en el país más atacado por este *ransomware*. En Europa, los países más atacados han sido Alemania (8,05 %), Italia (5,12 %) y España (4,88 %). Sodinokibi se distribuye siguiendo el modelo RaaS y encripta los archivos necesarios para que se produzca un ataque «por sistema». Los atacantes introducen una «clave esqueleto» en su código que les permite descifrar los archivos remotamente, independientemente del encriptado original.[49] Sin embargo, si un ordenador tiene un teclado ruso, armenio o sirio, o de otro tipo determinado, Sodinokibi no puede encriptar, algo que seguramente apunta al origen de los autores.[50]

SAMSAM_ sigue atacando infraestructuras vitales de todo el mundo por quinto año consecutivo. Los ataques de SamSam se centran principalmente en hospitales, empresas sanitarias y organizaciones gubernamentales para lograr pagos rápidos de grandes rescates. Explota las vulnerabilidades del protocolo de escritorio remoto (RDP). Hasta la fecha, el grupo responsable de distribuir SamSam ha conseguido más de 6 millones de dólares estadounidenses (aprox. 5 millones EUR) en pagos de rescates y ha costado a sus víctimas más de 30 millones de dólares estadounidenses (aprox. 25,4 millones EUR).[45] Desde el ataque de 2018 a la ciudad de Atlanta solo los costes de daños y recuperación ascendieron a 17 millones de dólares estadounidenses (aprox. 14,4 millones EUR).[43]

«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

Descripción

_Los sectores más atacados

LOS Estados nación SIGUEN EN EL PUNTO DE MIRA_ En 2018 se utilizaron programas de *ransomware* para atacar a organizaciones de Estados nación como herramienta de hacer dinero. Esta tendencia siguió en 2019, en la que algunas naciones o grupos de naciones ocultaron su identidad usando las mismas herramientas creadas por otros grupos o Estados nación. Esta manipulación de las herramientas permite ocultar el origen y la nación del atacante a fin de evitar consecuencias diplomáticas, especialmente cuando el objetivo es una organización gubernamental o estatal.

En 2019 se produjeron varios ataques contra organizaciones gubernamentales o estatales, como el de la ciudad californiana de Lodi[4] por el que pidieron pagar un rescate de 400 000 dólares estadounidenses (aprox. 340 000 EUR) para liberar el bloqueo de las líneas telefónicas de la policía, la línea de emergencia Public Works y los números del ayuntamiento, los datos de pago y los sistemas financieros de la ciudad. La ciudad se negó a pagar y se recuperó del ataque usando sistemas de respaldo. El departamento de Recursos de Información de Texas notificó un ataque de *ransomware* coordinado a 23 pequeñas organizaciones gubernamentales en agosto de 2019.[5] Se estimó que el coste para el condado de Texas fue de 3,25 millones de dólares estadounidenses (aprox. 2,75 millones EUR). Baltimore sufrió un ataque por RobbinHood que causó daños que ascendieron a 18,2 millones de dólares estadounidenses (aprox. 15,4 millones EUR); y Lake City en Florida sufrió un ataque por Ryuk que causó pérdidas por un total de 460 000 dólares estadounidenses (aprox. 389 768 EUR). La ciudad de New Bedford en Massachusetts también sufrió un ataque de *ransomware* en julio de 2019[6] por el que pedían un rescate de 5,3 millones de dólares estadounidenses (aprox. 4,4 millones EUR). El Ayuntamiento se negó a pagar el rescate pero gastó un millón de dólares estadounidenses en recuperarse.[7]

LAS INSTITUCIONES EDUCATIVAS SE UNEN A LA FIESTA_ Durante 2019 se observó un cambio en los ataques a instituciones educativas. Según un informe presentado por la empresa de seguridad Emsisoft, 1 051 colegios y facultades fueron víctimas de 62 incidentes de *ransomware*. En 2018 solo hubo 11 incidentes que afectaron a instituciones educativas. El informe declara que los centros educativos americanos fueron el segundo tipo de víctima más común, por detrás de los ayuntamientos.[8]

EL SECTOR SANITARIO SIGUE SUFRIENDO_ Las organizaciones sanitarias fueron el objetivo preferido de los ataques de *ransomware* durante los años anteriores, y la tendencia se mantuvo en 2019. El proveedor de servicios médicos californiano Wood Ranch Medical sufrió un ataque durante el verano que destruyó por completo los historiales médicos electrónicos de la empresa (también las copias de seguridad) al negarse a pagar el rescate. El incidente obligó a Wood Ranch Medical a anunciar que dejaría de operar a finales de ese año.[12] En abril de 2019, exactamente la misma secuencia de eventos afectaron a otro proveedor de servicios médicos, el centro de audiología y otorrinolaringología Brookside de Michigan[13] que también se vio obligado a cerrar. Asimismo, en Australia dos grupos hospitalarios, GippslandHealth Alliance y South West Alliance of Rural Health, sufrieron un ataque. Como resultado, hospitales de varias ciudades, como Warrnambool, Colac, Geelong, Warragul, Sale y Bairnsdale, no pudieron realizar las intervenciones habituales porque hubo que desconectar los sistemas para limitar la exposición.[14] En este sector las pérdidas de datos son tan dañinas como las pérdidas económicas. Por ejemplo, en junio de 2019 un ataque de *ransomware* contra el grupo Premier Family Medical de Utah provocó la filtración de datos médicos protegidos de más de 300 000 pacientes.[15]

MSP INACTIVAS_ Muchos sectores dependen de los proveedores de servicios gestionados (MSP) y de los proveedores de servicios en la nube (CSP) para albergar la información sensible esencial para sus operaciones. También dependen de estos servicios para la integridad de los datos y la prevención de accesos no autorizados.[17] Aun así, los programas de *ransomware* GandCrab y Sodin atacaron las vulnerabilidades de los MSP que exponen sus infraestructuras y los datos que albergan y, en un momento dado, permiten que el ataque se propague por toda la clientela del MSP. El Webroot2FA, una herramienta habitual de los MSP, presenta estas vulnerabilidades y se ha usado en varias ocasiones en 2019.[18] Este año varios MSP sufrieron ataques en un período de tan solo tres meses (PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. y IT By Design).[19]

Vectores de ataque

_ Cómo

Un nuevo tipo de *ransomware* llamado Sodinokibi explota la vulnerabilidad CVE-2019-2725 recientemente anunciada del servidor Oracle WebLogic para obtener capacidades remotas de ejecución de código. La víctima se infecta sin emprender acciones. También se han publicado los parches oficiales para las versiones 10.3.6.0 del 12.1.3.0 del servidor Oracle WebLogic.[51] El mismo ataque explota la vulnerabilidad CVE-2018-8453 para ganar más privilegios de usuario (elevarlos), terminar procesos de listas negras, eliminar archivos de listas negras y filtrar información del anfitrión.[48]

También se utilizó otra vulnerabilidad, la CVE-2019-0708, para plantar el *ransomware*. Esta vulnerabilidad permite establecer una conexión no autorizada a través del protocolo de escritorio remoto (RDP) de Microsoft. En mayo de 2019 Microsoft publicó los parches para las versiones del sistema operativo actual así como los de las versiones para las que ya no se ofrece servicio.[51]

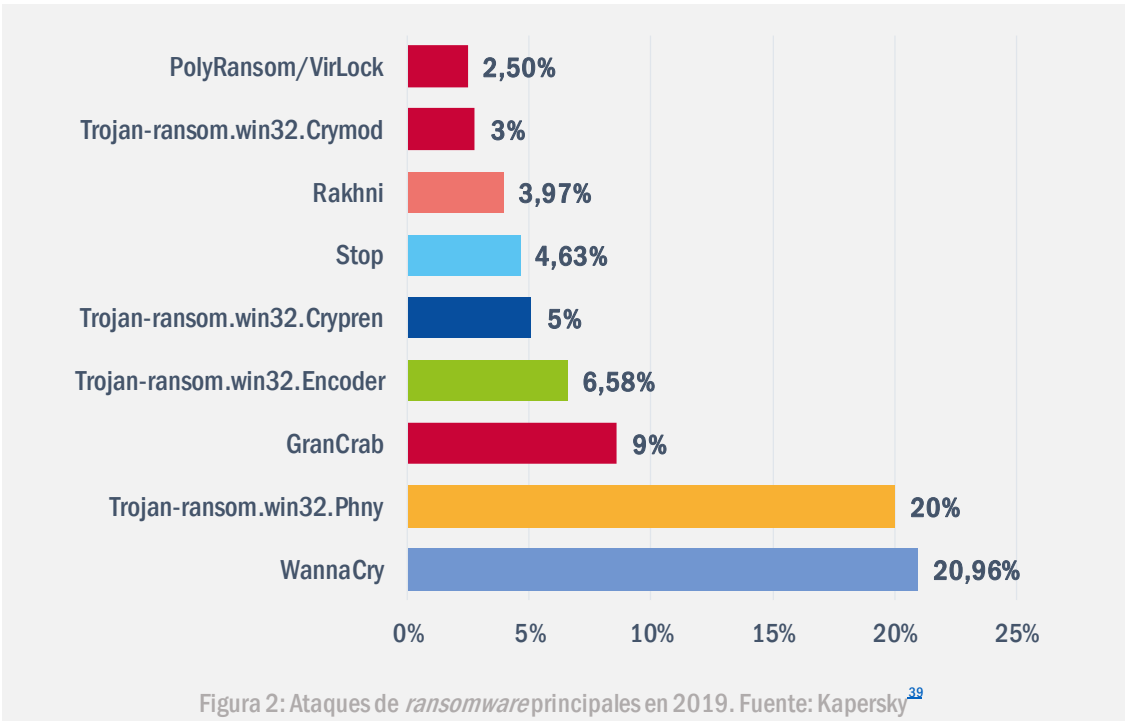


Figura 2: Ataques de *ransomware* principales en 2019. Fuente: Kapersky[39]

Incidentes

- Incidente en el condado de Baltimore[1]
- Ataque a los hospitales de Alabama[7]
- Incidente en la ciudad californiana de Lodi[4]
- Incidente en Texas (Departamento de Recursos de Información de Texas)[5]
- Ataque del *ransomware* Ryuk en Lake City (Florida)[7]
- Incidente en New Belford (Massachusetts)[6]
- Ataques de *ransomware* en más de 500 centros educativos y universidades[8]
- Incidente en el centro médico Wood Ranch Medical (California)[12]
- Incidente del centro de audiología y otorrinolaringología Brookside (Michigan)[13]
- Incidentes en los hospitales de Gippsland Health Alliance y South West Alliance of Rural Health (Australia)[14]
- Incidente en el grupo Premier Family Medical (Utah)[15]
- Incidentes en MSP PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. y IT By Design[19]
- Incidente en el centro de datos Microsoft Azure[51]
- Ataque de LockerGoga a Altran Technologies[40]
- Ataque de LockerGoga a Norsk Hydro[7]
- Ataques de LockerGoga a Hexion y a Momentive[41]
- Incidente en Albany IT[60]
- Incidente en el condado de Jackson (Georgia)[61]
- Incidente en Riviera Beach (Florida)[62]
- Incidente en Nueva Orleans[63]
- Atraque al fabricante de audífonos danés Demant[64]

Mitigación:

_Acciones propuestas

- Mantener copias de seguridad fiables que sigan la regla 3-2-1 (es decir, mantener por lo menos tres copias, en dos formatos distintos y una de las copias en otra ubicación).[5]
- Invertir en una póliza de seguros que cubra los daños por ataques de *ransomware*.[21]
- Usar segmentación de la red, cifrado de datos, control de acceso y refuerzo de políticas para garantizar una exposición mínima de los datos.
- Utilizar métodos como el de monitorización para identificar las infecciones con rapidez.
- Monitorizar el acceso y el estado de la infraestructura pública utilizada.
- Crear un centro de operaciones de seguridad con personal experto en seguridad dentro de cada organización o empresa.
- Usar las herramientas adecuadas y actualizadas para la prevención de los ataques de *ransomware*.
- Definir exactamente e implementar el nivel mínimo de derechos de acceso a datos para minimizar el impacto de los ataques (menos derechos, menos datos cifrados).
- Implementar la gestión robusta de vulnerabilidades e instalación de parches.
- Implementar 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.
- Instalar protección de punto final con programas antivirus, pero también bloquear la ejecución de archivos (p. ej., bloquear la ejecución en la carpeta de archivos temporales).
- Usar políticas para controlar los dispositivos externos y la accesibilidad de los puertos.
- Usar listas blancas para evitar que ejecutables desconocidos se ejecuten en los puntos terminales.
- Invertir en el aumento de la concienciación de los usuarios en materia de *ransomware* especialmente en lo que se refiere al uso seguro de los programas navegadores.

_Descifradores

EUROPOL[7] y 163 socios han conseguido un progreso significativo con el proyecto «No more ransom» (no más rescates)[7]. El portal ha añadido 28 herramientas en 2019 y ahora puede descifrar 140 infecciones distintas de *ransomware*.[65] El equipo ha desarrollado una serie de descifradores de *ransomware* y ha actualizado otros. A continuación se citan algunos ejemplos.

RANSOMWARE	DESCIFRADOR
Aurora[52], **Muhstik**[53], **Ryuk**[54]	Emsisoft
Rakhni, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Democry, TeslaCrypt, Chimera, Crysis, Jaff, Dharma, Cryakl, Yatron, FortuneCrypt,[55,56]	Kaspersky Lab
GandCrab[44]	Europol, la policía de Rumanía, la Oficina del Fiscal General y Bitfender
Jigsaw[46]	Avast
Mira[57]	F-Secure
Nemty[58]	Tesorion
PewCrypt[47]	PewCrypt (autor)

Bibliografía

1. "Washington idle as ransomware ravages cities big and small" 28 de septiembre de 2019. Politico. https://www.politico.com/news/2019/09/28/ransomware-cities-washington-007376

2. "What you — and your company — should know about cyber insurance". 20 de agosto de 2019. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

3. "The State of Ransomware in 2019". 17 de junio de 2019. IT Pro Today. https://www.itprotoday.com/threat-management/state-ransomware-2019

4. "California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware". 2 de agosto de 2019. Trend Micro. https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware

5. "Coordinated Ransomware Attack Cripples Local Government Organizations in Texas". 19 de agosto de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coordinated-ransomware-attack-cripples-local-government-organizations-in-texas

6. "The State of Ransomware in the US: Report and Statistics 2019". 12 de diciembre de 2019. EMSISOFT blog. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

7. "Alabama hospitals have been hit by a massive ransomware attack". 3 de octubre de 2019. https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

8. "500+ Schools Have Been Affected by Ransomware in 2019". 4 de octubre de 2019. Campus Safety, https://www.campussafetymagazine.com/safety/500-schools-ransomware-2019/

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

10. "Proofpoint Q2 2019 Threat Report - Emotet's hiatus, mainstream impostor techniques, and more". 19 de septiembre de 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques

11. "6 of the Biggest Cybersecurity Crises of 2019 (So Far)". 24 de septiembre de 2019. EC-Council Blog. https://blog.eccouncil.org/6-of-the-biggest-cybersecurity-crises-of-2019-so-far/

12. "Ransomware Attacks Double in 2019: Medical Providers Can't Recover and Shut Down". 3 de octubre de 2019. https://www.natlawreview.com/article/ransomware-attacks-double-2019-medical-providers-can-t-recover-and-shut-down

13. "Michigan's Brookside ENT and Hearing Center forced to close due to a Ransomware Attack". 23 de abril de 2019. SPAM Fighter. https://www.spamfighter.com/News-22154-Michigans-Brookside-ENT-and-Hearing-Center-forced-to-close-due-to-a-Ransomware-Attack.htm

14. "Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack". 1 de octubre de 2019. https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

15. "Ransomware Attack Affects 300,000 Patients in Utah". 12 de septiembre de 2019. CISO Mag. https://www.cisomag.com/ransomware-attack-affects-300000-patients-in-utah/

16. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks". 27 de agosto de 2019. ProPublica. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

17. "CYBER THREATSCAPE REPORT". 2019. Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

18. "Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread". 2019. Coveware. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

19. "Armor Identifies 15 New Ransomware Victims in the Last 2 Weeks, All of them Educational Institutions – Threat Intelligence". 20 de septiembre de 2019. Armor. https://www.armor.com/resources/armor-identifies-10-new-ransomware-victims-in-the-past-9-days/

20. "4 Ransomware Trends to Watch in 2019". 13 de febrero de 2019. https://www.recordedfuture.com/ransomware-trends-2019/

21. "BDO Cyber Threat Insights - 2019 2nd Quarter Report". Julio de 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

22. "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

23. "Healthcare Cyber Heists in 2019". 3 de octubre de 2019. VMWare. https://www.carbonblack.com/resources/threat-research/healthcare-cyber-heists-in-2019/

24. "Australia | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/australia-global-threat-report-defender-power-on-the-rise/

25. "France | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/france-global-threat-report-defender-power-on-the-rise/

26. "Italy | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/italy-global-threat-report-defender-power-on-the-rise/

27. "Japan | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/japan-global-threat-report-defender-power-on-the-rise/

28. "Canada | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/canada-global-threat-report-defender-power-on-the-rise/

29. "Singapore | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/singapore-global-threat-report-defender-power-on-the-rise/

30. "UK | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/uk-global-threat-report-defender-power-on-the-rise/

31. "Anticipating the Unknowns". Marzo de 2019. Cisco. https://ebooks.cisco.com/story/anticipating-unknowns/

32. "2020 Data Breach Investigations Report" 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

33. "IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks". 5 de septiembre de 2019. IBM. https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks

34. IT threat evolution Q2 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

35. IT threat evolution Q1 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

36. "The state of industrial cybersecurity". Julio de 2019. Kaspersky. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

37. "2019 Cyberthreat Defense Report" Cyber Edge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

38. "Evasive Threats, Pervasive Effects". 27 de agosto de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

39. IT threat evolution Q3 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

40. "What You Need to Know About the LockerGoga Ransomware." 20 de marzo de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

41. "BDO Cyber Threat Insights - 2019 2nd Quarter Report". Julio de 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

Bibliografía

42. Ransomware Decryptor Tools, Kapersky https://noransom.kaspersky.com/

43. "ENISA Threat Landscape Report 2018". 28 de enero de 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

44. "New GandCrab v5.1 Decryptor Available Now". 19 de febrero de 2019. Bitdefender LABS. https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

45. "10 Ransomware Attacks You Should Know About in 2019". 28 de abril de 2019. Allot. https://www.allot.com/blog/10-ransomware-attacks-2019/

46. Ransomware Decryptor Tools. Avast. https://www.avast.com/ransomware-decryption-tools

47. PewCrypt Ransomware Source. GitHub. https://github.com/000JustMe/PewCrypt

48. "Are the REvil, GranCrab Ransomware Families Related?" 25 de septiembre de 2019. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/revil-gandcrab-related/

49. "Threat Landscape Report", Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf

50. "Sodin Ransomware includes exploit for Windows CVE-2018-8453 bug". 4 de julio de 2019. Security Affairs. https://securityaffairs.co/wordpress/87944/malware/sodin-ransomware-cve-2018-8453.html

51. "Threat Landscape Report" 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

52. "Emsisoft Decryptor for Aurora" 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/aurora

53. "Emsisoft Decryptor for Muhstik" 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/muhstik

54. "Caution! Ryuk Ransomware decryptor damages larger files, even if you pay". 9 de diciembre de 2019. Emsisoft. https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

55. "RakhniDecryptor tool for defending against Trojan-Ransom.Win32.Rakhni ransomware". Kaspersky. https://support.kaspersky.com/10556

56. "Another two bite the dust: Kaspersky updates decryption tool to fight ransomware pair". 27 de septiembre de 2019. The Online Citizen. https://www.theonlinecitizen.com/2019/09/27/another-two-bite-the-dust-kaspersky-updates-decryption-tool-to-fight-ransomware-pair/

57. "Mira Ransomware Decryptor". 1 de abril de 2019. F-Secure. https://blog.f-secure.com/mira-ransomware-decryptor/

58. "Nemty update: decryptors for Nemty 1.5 and 1.6" Tesorion. https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/

59. "McAfee Labs Threats Report". Agosto de 2019. McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

60. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/2

61. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/3

62. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/6

63. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/7

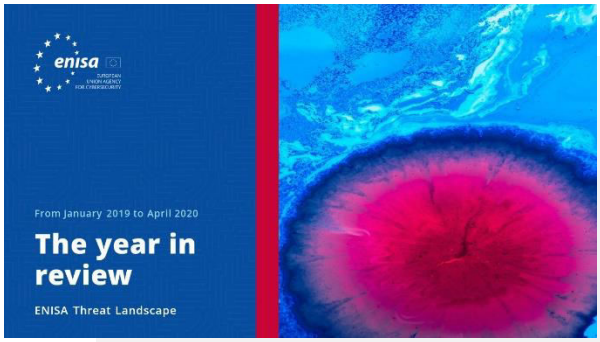
64. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/11

65. https://www.nomoreransom.org/

«La CTI se ha establecido firmemente en el dominio de la ciberseguridad como herramienta esencial para mejorar la agilidad y la eficiencia contra los ataques informáticos».

en PAE 2020

Lecturas relacionadas



LEER EL REPORTAJE

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

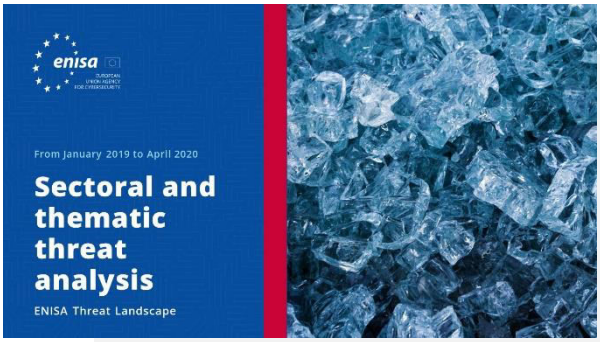
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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) n.° 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

https://www.enisa.europa.eu