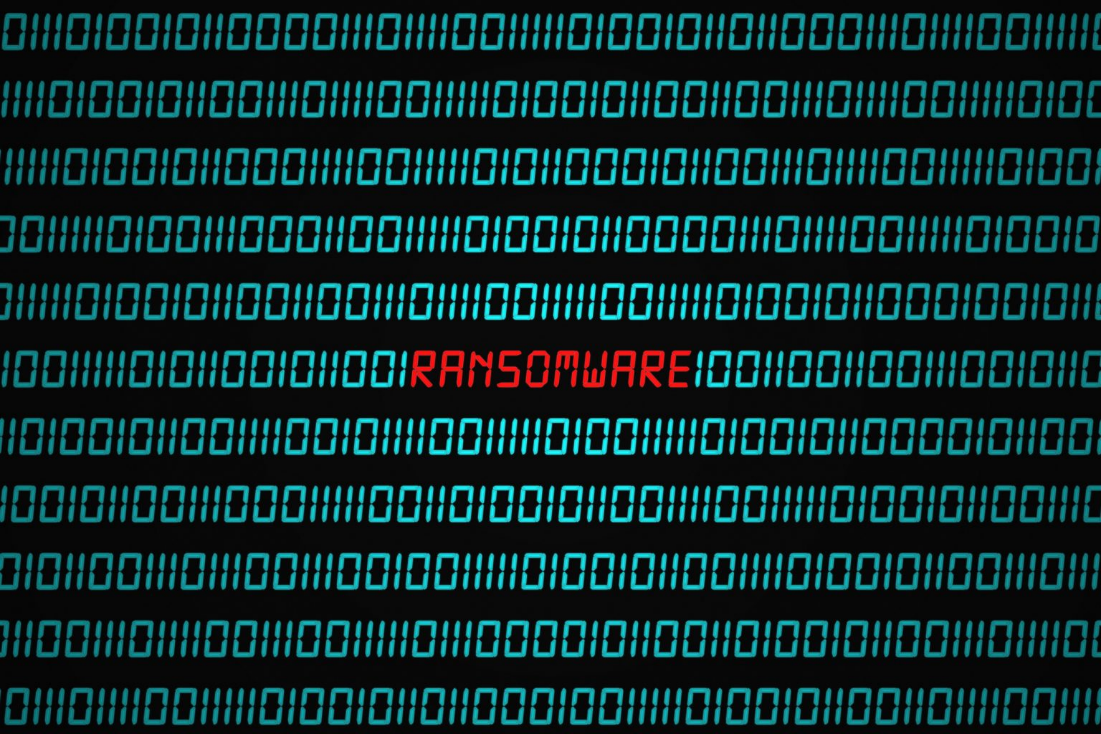
ANÁLISIS DEL RANSOMWARE, SU FUNCIONAMIENTO Y SU IMPACTO



©FERNANDO PÉREZ HOLGUÍN 1ºN BACH

TUTOR: JESÚS

COTUTORA: PAZ ABARCA ORTEGA

IES ALKALA NAHAR

BACHILLERATO 2021/2023

Tabla de contenido

[**0: Introducción: ciberseguridad y ransomware** 3](#_Toc114685857)

[**1: ¿Qué es el ransomware?** 4](#_Toc114685858)

[**1.1.** **Definición de ransomware** 4](#_Toc114685859)

[**1.2. Historia del ransomware** 5](#_Toc114685860)

[**1.3. Tipos de ransomware** 7](#_Toc114685861)

[**1.4. Impacto del ransomware** 9](#_Toc114685862)

[**2. ¿Cómo funciona el ransomware?** 12](#_Toc114685863)

[**2.1. ¿Quiénes generan el ransomware? (cibercriminales)** 12](#_Toc114685864)

[**2.2. ¿Cómo actúa técnicamente el ransomware?** 15](#_Toc114685865)

[**2.3. Análisis de una familia de ransomware** 19](#_Toc114685866)

[**3: ¿Cómo luchar contra el ransomware?** 20](#_Toc114685867)

[**3.1. ¿Cómo prevenir los ataques?** 20](#_Toc114685868)

[**3.2. ¿Cómo reaccionar en caso de ataque?** 24](#_Toc114685869)

[**3.3. Algunos dilemas planteados por el ransomware** 26](#_Toc114685870)

[**3.4. Ejemplos reales de ataques de ransomware** 28](#_Toc114685871)

[**4.** **Conclusiones** 29](#_Toc114685872)

[**Bibliografía** 33](#_Toc114685873)

# **0: Introducción: ciberseguridad y ransomware**

En las sociedades modernas, la digitalización es una de las principales prioridades, junto con la reforma energética. En esas sociedades modernas, las empresas con más beneficios y mayor cotización en bolsa son las que, gracias a la digitalización, manejan de forma más eficiente la información.

La expansión de los servicios digitales ha generado una gran dependencia de los mismos, de manera que ahora la continuidad de los servicios informáticos es fundamental para que funcione bien la sociedad. Sin esas tecnologías, ya no se podrían prestar servicios básicos como el suministro de energía, la atención hospitalaria, o la gestión del tráfico y la logística, o no se podrían realizar transacciones bancarias.

En este entorno, se observa con cada vez más preocupación el crecimiento del cibercrimen, ya sea con motivaciones políticas (ataques fomentados por Estados, como parte de las ciberguerras) o por motivos económicos: ciberdelincuentes que han visto la oportunidad de cometer ahora sus delitos en estos entornos tecnológicos, en los que actúan de forma global y con un alto grado de opacidad. Se estima el coste de la cibercriminalidad en más de 300.000 millones de euros al año[[1]](#footnote-2), y las cifras se están incrementando con el impulso que ha tenido la digitalización de la sociedad a raíz de la pandemia.

Los ciberdelincuentes llevan a cabo distintos tipos de actividades maliciosas: difusión de malware (programas de software para usos ilegítimos); ataques a las páginas de Internet; correo electrónico no deseado o spam (más del 70% de los mensajes); *phising* (mensajes falsos que intentan engañar a los usuarios para que accedan a ficheros o enlaces maliciosos); ataques de denegación de servicio (“*Distributed Denial of Service attacks*” o DDoS), con los que se intenta saturar un servicio para dejarlo inoperativo; robo de identidad digital; o ransomware, modelo criminal en el que el ciberdelincuente toma control de sistemas o dispositivos, y exige el pago de un rescate al dueño si quiere poder volver a acceder a ellos.

Las consecuencias de los ciberataques son múltiples, y, en el caso del ransomware, son particularmente graves. Algunos casos destacados ocurridos recientemente han dejado inoperativos servicios públicos o la distribución de bienes esenciales, además de afectar a millones de empresas. En este trabajo se analizará qué es el ransomware, qué tipos hay, quiénes y cómo lo difunden, qué medidas se pueden adoptar para intentar evitarlo o para reaccionar cuando hay un ataque, y qué dilemas se plantean en este ámbito.

**Objetivos:**

Con este proyecto de investigación, pretendo informar al lector sobre lo que es el ransomware, pues conocer su existencia es un paso fundamental para defenderse de este. Para ello, expondré su definición, su historia, su impacto, su funcionamiento, tanto a nivel técnico como organizacional, las medidas para prevenirlo y reaccionar ante él, y presentaré ciertos dilemas relacionados a este.

A su vez, con la parte práctica pretendo comprender el funcionamiento de un programa de ransomware y el papel de un cibercriminal por medio de la experiencia, así como ampliar mis conocimientos de programación en general.

# **1: ¿Qué es el ransomware?**

## **1.1.** **Definición de ransomware**

Ransomware (palabra que proviene de “ransom”, rescate, y “ware”, sufijo relacionado con la informática - vendría a ser “programa de rescate”) es el término empleado para referirse a un tipo de software malicioso cuyo objetivo es impedir a un usuario acceder a su dispositivo y/o a sus archivos, exigiéndole un pago para recuperar el control. Para ello, suelen encriptarse los contenidos, aunque no siempre: el ransomware no define un tipo específico de código, sino un modelo de negocio[[2]](#footnote-3).

Se considera que un caso de ransomware se define por los siguientes elementos[[3]](#footnote-4):

*a)* *El ciberdelincuente toma el control de un equipo o sistema.* Puede tratarse de un ordenador, de un teléfono móvil, de un programa o de cualquier elemento que funcione en base a software. Por ejemplo, en el caso de Colonial Pipeline, atacaron el software operativo específico que permitía gestionar la distribución de gasolina en una parte importante del mercado estadounidense, dejando sin combustible a millones de personas: la empresa acabó pagando 5 millones de dólares para recuperar el control de sus sistemas.

Una tendencia relevante para el futuro del ransomware es que los cibercriminales no ataquen directamente los sistemas o equipos de la víctima, sino los de empresas proveedoras que le prestan servicio, y que pueden tener también el efecto de impedir el correcto desarrollo de la actividad de la víctima[[4]](#footnote-5).

Para tomar el control, los ciberdelincuentes suelen usar técnicas de ingeniería social con las que logran que los usuarios abran un fichero o usen un enlace que permite instalar malware y controlar el equipo o sistema, aunque en algunos casos usan vulnerabilidades para controlar los equipos (ataques sin interacción del usuario).

*b)*  *Impide que el dueño acceda a ese equipo o sistema.* Puede ser a través de encriptación de contenidos, de pantallas que impiden al usuario acceder a los servicios que desea, o haciendo creer que tiene ese tipo de control sobre el acceso.

*c)* *Alerta al dueño de que no tiene acceso al equipo y sistema, y le pide un rescate.* Puede parecer un paso obvio, pero hay que tener en cuenta que atacantes y víctimas a menudo hablan distintos lenguajes, viven en distintas partes del mundo, y tienen capacidades técnicas muy distintas (por ejemplo, para poder formalizar el pago).

El atacante puede pedir dinero a la víctima si ésta quiere volver a acceder a sus archivos y no perderlos; y puede además amenazar con la publicación de datos confidenciales (doble extorsión); o con que el atacante se comunique con los contactos de la víctima (triple extorsión). Para aumentar la presión, puede lanzar ataques de denegación de servicio (DDoS) contra la víctima (cuádruple extorsión).

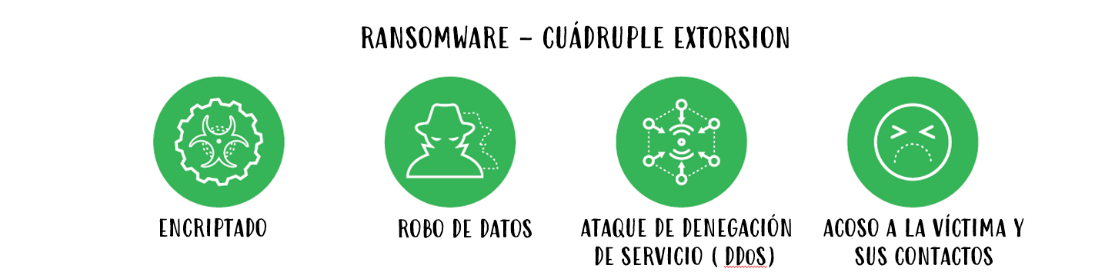


Fig. 1: Niveles de extorsión del ransomware

Llegado a este punto, el ataque puede tener éxito, y se logra el pago por parte de la víctima (normalmente en criptomonedas, que permitan la confidencialidad del pago). O el ataque puede quedar frustrado, porque la víctima logre recuperar el control de los archivos, o porque se niegue a pagar, o porque se pierda el contacto entre atacante y víctima.

Si se llega a realizar el pago, el atacante suele devolver el acceso a la víctima. Podría no devolverlo, pero a la larga, si las víctimas llegasen a estar convencidas de que pagar no serviría de nada, dejarían de hacerlo.

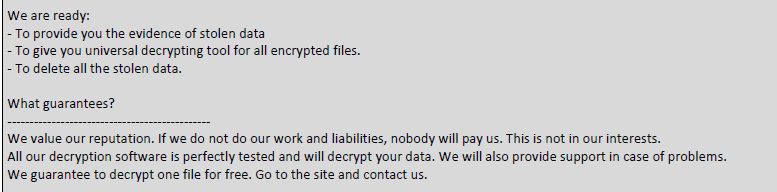
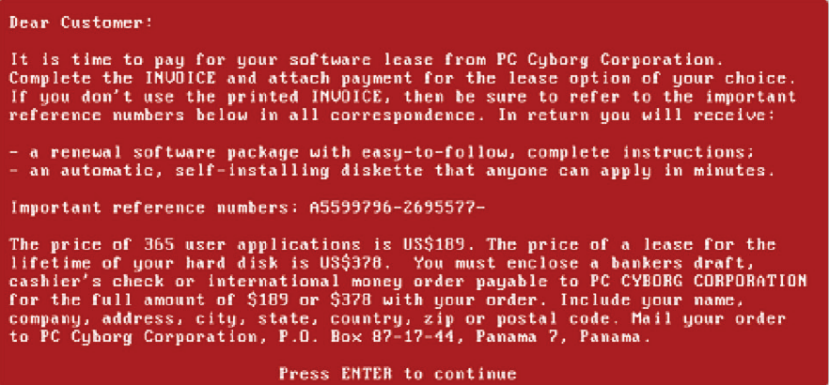
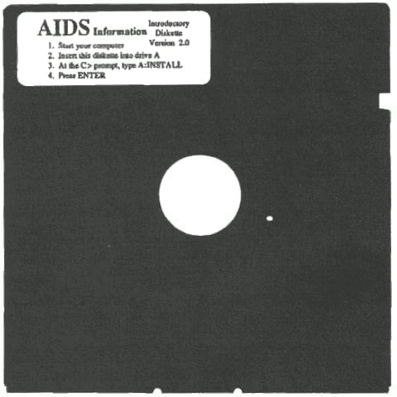


Fig. 2: Mensaje de DarkSide a una víctima

## **1.2. Historia del ransomware**

El primer caso de ransomware documentado fue en 1.989, con el programa informativo sobre el SIDA del doctor Joseph Popp, un biólogo formado en Harvard. El Dr. Popp almacenó un virus (PC Cyborg) en disquetes con un programa educativo sobre el SIDA, y lo envió por correo a múltiples destinatarios. Después de ejecutar el programa, y de apagar y encender 90 veces el equipo, se cifraban los archivos y salía una nota diciendo que era necesario mandar 189 dólares por correo a una oficina postal en Panamá para obtener la clave para desencriptarlos. El sistema de encriptado era simétrico, lo que era poco eficaz, y se lograron desarrollar dos programas (AIDSOUT y CLEARAIDS) que permitían recuperar los ficheros, aunque una organización de investigación italiana dijo que perdió los ficheros de 10 años[[5]](#footnote-6).



*Fig 3: El ransomware del Dr.Popp (PC Cyborg)*

Durante la década de los 2000, los ataques de ransomware comenzaron a ganar popularidad gracias al aumento del número de dispositivos conectados a Internet, que facilitaba la propagación del software y el cobro del rescate. En aquella época, muchos de los programas de ransomware eran sólo *scareware* (programas que usan alertas emergentes y otros trucos de ingeniería social para asustar a la víctima y hacer que pague por software falso que dice ser de seguridad). Los atacantes no tenían que desarrollar sistemas complejos, y basaban su éxito en notificaciones agresivas y solicitudes de cantidades reducidas (30$, 90$), que se podían pagar de forma sencilla.

En 2010, aparecen nuevos modelos de ransomware, como GPCode que, gracias al desarrollo del cifrado asimétrico (imposible de descifrar por fuerza bruta), suponen una amenaza real para las víctimas de esos ciberataques, que comenzaron a dirigirse hacia los equipos de las empresas, pues contienen datos más valiosos que los usuarios domésticos, y están dispuestos a pagar más por recuperarlos.

*Fig 4: pantallas de rescate de dos tipos de rasomware*

El ransomware más destacado de esta época es CryptoLocker, que surgió en 2011-2012. Este programa fue pionero en varios de los aspectos que hoy en día son comunes en los ransomwares, como el cifrado asimétrico, tener un tiempo limitado para realizar el pago, o pedir pago en criptomonedas.

A mediados de esa década, el ransomware se había popularizado tanto que surgieron grandes organizaciones criminales dedicadas a desarrollar y distribuir estos programas. Se sospecha que algunas de estas organizaciones pudieran llegar a tener apoyo de algún Estado (por ejemplo, WannaCry, una mezcla de ransomware y gusano, es un ransomware programado por un grupo de hackers que guardan una estrecha relación con Corea del Norte, con posible implicación de su Gobierno[[6]](#footnote-7)). Además, también surgió el modelo de negocio de “*Ransomware as a Service*” (RaaS)[[7]](#footnote-8). En este modelo, hackers expertos desarrollan la base de un programa de ransomware y los ponen a la venta en la *dark web*, para que sus compradores (cibercriminales menos expertos) puedan personalizarlos fácilmente para crear su propio ransomware (los desarrolladores de la base del programa se llevan un porcentaje del beneficio).

## **1.3. Tipos de ransomware**

Los dos tipos básicos de ransomware son el de cifrado de la información de la víctima, y el de bloqueo de dicha información[[8]](#footnote-9), aunque algunos expertos distinguen más tipos diferentes de ransomware, con un nivel de gravedad diferente para las víctimas[[9]](#footnote-10). Estos son :

Encriptadores (“*Filecoders*” o “*encryptors*”)

Hoy en día, este tipo de ransomware es el más popular (90% de las cepas). Su método de funcionamiento consiste en cifrar los archivos del ordenador, de forma que sean inutilizables sin una clave de descifrado, que es lo que ofrece el atacante a cambio de dinero.

El ransomware intenta acceder a todas las unidades (incluyendo unidades de red o externas conectadas), y busca sobre todo cifrar ficheros con determinadas extensiones (.docs, .xlsx, .jpg, etc.).

Normalmente, estos programas contienen un temporizador, y si la víctima no paga a tiempo, todos sus archivos se perderán para siempre.

Bloqueadores de pantalla *(“Screenlockers”)*

Este tipo de ransomware genera una ventana imposible de cerrar, de forma que el equipo sea inutilizable hasta que se envíe un pago. Para asustar a la víctima, los atacantes se hacen pasar por una institución gubernamental (policía, CNI…) y le dicen que su ordenador ha sido bloqueado por contener archivos ilegales, y que debe pagar una multa en un plazo de x horas o se adoptarán medidas más severas. A veces, para darle más credibilidad al mensaje, se incluye alguna imagen de la víctima, si el atacante se ha logrado hacer con el control de la webcam.

Ransomware de doxeo

Este tipo de ransomware hace una copia de los datos personales almacenados en el equipo de la víctima, y amenaza con publicarlos y/o reenviarlos a todos sus contactos si no paga en un plazo limitado de tiempo

Falso ransomware (“*Hoax ransomware*”)

Este tipo de ransomware es muy parecido al de cifrado, con una diferencia: el hoax ransomware no llega a cifrar los archivos (solo convence a la víctima de que los ha cifrado usando técnicas de ingeniería social).

Scareware (programas que asustan a los usuarios)

Este tipo de ransomware afirma (falsamente) que se ha encontrado una infección de virus en el dispositivo, y apremia al asustado usuario a descargar un software falso que se encargará de quitar el supuesto virus.

Los ataques de ransomware más sofisticados, y con mayores exigencias de rescate, se llevan a cabo de forma personalizada, con intrusiones a través de las cuales se estudian los sistemas informáticos de la víctima, para que el ataque de ransomware sea más eficaz.

Algunos programas de ransomware vienen asociados a otros tipos de malware, destinados, por ejemplo, al robo de credenciales de acceso, o a la instalación de *botnets*, que permiten a los atacantes controlar de forma remota el equipo, y llegar a sincronizar sus actuaciones con muchos otros, para usarlos como vectores de ataque.

## **1.4. Impacto del ransomware**

El 12 de mayo de 2.017, se lanzó un ataque de ransomware, WannaCry (un ransomware de “gusano”, que aprovechaba una vulnerabilidad del sistema operativo de Windows), y el primer día desde ese lanzamiento, se reportaron 230.000 usuarios contagiados en más de 150 países[[10]](#footnote-11). El servicio de salud británico NHS se habría visto afectado, con pérdidas de unos 100 millones de dólares y más de 19.000 citas canceladas[[11]](#footnote-12). En mayo de 2021, fue el Sistema de Salud irlandés el que, tras un ataque del ransomware Conti, se vio obligado, en plena pandemia, a volver a usar lápiz y papel, y a cancelar miles de citas[[12]](#footnote-13).

En 2.019, el ayuntamiento de Maryland sufrió un ataque del ransomware SamSam que dejó inaccesibles sus servicios TIC durante semanas, obligando a los ciudadanos a realizar las gestiones manualmente, y generando pérdidas estimadas en más de 15 millones de euros (el ayuntamiento se negó a pagar el rescate solicitado, pese a que hubiera supuesto un coste sensiblemente inferior)[[13]](#footnote-14).

En mayo de 2.021, el ataque a la empresa Colonial Pipeline con el ransomware DarkSide dejó sin suministro de gasolina a millones de personas en la costa este de Estados Unidos[[14]](#footnote-15).

Y en España, destacó el ataque sufrido, en plena pandemia, por el Servicio Público de Empleo (SEPE), que en marzo de 2.021 fue atacado por el ransomware Ryuk[[15]](#footnote-16), y estuvo inaccesible durante días, y con restricciones operativas durante semanas, necesitándose más de 19.000 horas extras de trabajo para la recuperación y protección del sistema[[16]](#footnote-17).

Esos son solo unos pocos ejemplos visibles de una tendencia muy extendida y generalizada. Según los expertos, hay un ataque de ransomware a empresas cada 11 segundos, y se calculan las pérdidas globales anuales generadas por el ransomware en unos 20.000 millones de dólares[[17]](#footnote-18).

Según una encuesta hecha por la compañía especializada en ciberseguridad Sophos, 30% de las grandes empresas encuestadas habían sufrido algún ataque de ransomware, y el 54% de esos ataques habría tenido éxito[[18]](#footnote-19). Otra encuesta similar, de Keeper, indicaba que el 77% de los que sufren ataques no pueden acceder a sus sistemas (el 28% durante más de una semana)[[19]](#footnote-20). De nuevo Sophos indica que, cuando se pagó rescate, éste fue de 170.000 $ de promedio, y en esos casos solo se habría recuperado el 65% de la información. El perjuicio de esos ciberataques, incluyendo el tiempo de indisponibilidad de servicios, tiempo de personal para resolver el problema, coste en equipos, ingresos perdidos, pago de rescate, etc, fue de 1,8 millones de dólares[[20]](#footnote-21). Y eso no incluiría necesariamente ciertos costes menos visibles (“bajo la superficie”), como devaluación de marca o pérdida de confianza de los clientes[[21]](#footnote-22).



*Fig 5: Costes ocultos del ransomware*

Los expertos distinguen varias fases en el ciclo de vida de la respuesta a incidentes de ciberseguridad: la fase inicial reactiva (continuidad de las operaciones, comunicación al exterior); gestión del impacto (la tarea, en las semanas o meses posteriores, para hacer frente a las consecuencias directas del incidente); y recuperación de negocio (los meses o años necesarios para reparar todo el daño sufrido por la empresa e implementar las medidas necesarias para evitar daños similares en el futuro).

El desarrollo de todo eso proceso tiene elevados costes para las empresas, incluso si recuperan los datos, por haber pagado por ello (un 32% de los casos, en la encuesta de Sophos) o si los recuperan por tener copias de seguridad (lo que no evitaría la doble extorsión de que se pueda filtrar indebidamente información confidencial a la que hayan tenido acceso los atacantes, o la triple extorsión de ponerse en contacto con los clientes a cuyos datos han accedido). Como indican los expertos, el coste de este tipo de ataques puede perseguir a una empresa durante años después de sufrirlo[[22]](#footnote-23).

# **2. ¿Cómo funciona el ransomware?**

## **2.1. ¿Quiénes generan el ransomware? (cibercriminales)**

En la actualidad, el ransomware ha alcanzado un nivel de complejidad que requiere que sea generado y operado por bandas de cibercriminales (“*criminal syndicates*”)[[23]](#footnote-24).

Están formadas normalmente por hackers que mezclan profesionalismo con postureo adolescente (p.ej., en sus mensajes incluyen referencias a video juegos y a la cultura on-line que consumen). Los grupos más grandes establecen centros de atención a usuarios (“*call centers*”) para asesorar a las víctimas en el complejo proceso para pagar en criptomonedas, e incluso prometen descuentos por pronto pago.

Hay bandas criminales, como REvil, que intentan crear “franquicias” en las que otros hackers usen su software, a cambio de un porcentaje de los beneficios que se obtengan (REvil no se limita a facilitar el *Ransomware-as-a-Service*, sino que también se implican en las negociaciones si sus asociados consiguen víctimas).

Muchas de las bandas están establecidas en Rusia o en antiguas repúblicas soviéticas - a veces su malware no ataca a ordenadores que tengan habilitados como lenguaje el ruso o el ucraniano.

Algunas de las bandas emplean antiguos miembros del ejército, pero suelen importarles más el dinero que maquinaciones geopolíticas, si bien hay algún caso, como el antes mencionado de Wannacry, en el que se habría involucrado el Gobierno norcoreano, como respuesta a una película considerada como difamatoria contra su líder. Wannacry, aprovechando una vulnerabilidad de Windows, infectó a unos 300.000 ordenadores, afectando incluso a hospitales, pero fue poco exitoso como negocio: sólo pedían de 300 a 600 dólares por el rescate, y habrían conseguido solo unos 140.000 dólares, lo que fue criticado por otras bandas (un representante de REvil lo calificó como “un experimento muy estúpido”).

Esas bandas se concentran en sectores que tienen malas medidas de seguridad y baja tolerancia a la inactividad generada por los ataques (servicios de distribución, procesos industriales intermedios, sector público...) e intentan concentrar los ataques en momentos críticos (a escuelas en el periodo de matrícula, a asesores fiscales en el periodo de liquidación de los impuestos...). Algunas bandas grandes como Hades, se especializan en “caza mayor” (empresas con más de 1.000 millones de facturación). En esos casos, a veces acosan a los directivos, con llamadas y con mensajes en sus redes sociales, como LinkedIn. En 2.021, directivos del grupo Campari intentaron minimizar públicamente el impacto de un ataque, y los hackers hicieron una campaña en Facebook, en perfiles de celebridades que también habían hackeado, publicitando en ellos información robada a Campari, diciendo que era mentira que fuese un ataque menor, y que tenían enormes cantidades de datos confidenciales. En esos esfuerzos por añadir presión a las víctimas, los hackers han amenazado con publicar información sobre las webs ilegales que habrían visitado las personas a las que extorsionan, o con publicar información sobre sus familias.

Algunas de estas bandas ofrecen información poco fiable sobre sí mismas: la banda Prometheus se presentaba como miembros de grupos de élite en el sector como REvil, pero los expertos consideraban que no era cierto, que su malware era en realidad “un revoltijo hecho con retales de otros virus”, e investigadores de IBM Security X-Force encontraron un fallo en su sistema de cifrado que permite recuperar los archivos infectados sin necesidad de contraseñas[[24]](#footnote-25).

Incluso los grupos potentes tienen un alcance limitado en el tiempo. A finales de julio de 2.021, la banda de cibercriminales REvil, a la que IBM atribuía un 23% de los ataques de *ransomware* mundiales en el año anterior, se desvaneció de la red. De un día para otro se borró su presencia del internet oscuro (“*Dark Web*”). Según algunas informaciones, estos hackers podrían haber sido a su vez hackeados por fuerzas de seguridad[[25]](#footnote-26).



*Fig 6: Revil*

EJEMPLO DE BANDA DE RANSOMWARE: DarkSide

Un mes antes, en junio de 2.021, los piratas de DarkSide habían anunciado en sus propios canales de este medio que cerraban sus operaciones. DarkSide había llegado a ser un referente en este entorno[[26]](#footnote-27), ya que, por ejemplo, cobró 4,4 M$ de rescate a Colonial, gestora de oleoductos en Estados Unidos (aunque luego se habrían recuperado 2,3 M$[[27]](#footnote-28)). DarkSide intentó dotarse de un perfil más amigable, afirmando en su mensaje original que “No queremos matar tu empresa”. En sus mensajes hablaban de sí mismos como expertos de ciberseguridad que cobraban por su asesoramiento, que permitiría identificar debilidades de los sistemas de las empresas atacadas, y se presentaba en su página de la internet oscura ­ como una especie de Robin Hood: solo atacaría aquellas empresas capaces de asumir el pago del rescate de sus datos, y evitaría dirigir sus programas de secuestro informático a hospitales, colegios, empresas sin ánimo de lucro o agencias gubernamentales.

A esta promesa se sumaban acciones pretendidamente altruistas, como la donación de parte de sus beneficios a proyectos solidarios. Según proclamó la banda en un comunicado difundido en octubre de 2020, su intención era entregar parte de los rescates a organizaciones benéficas. “No importa lo malos que pienses que somos, nos satisface saber que ayudamos a cambiar la vida de alguien”, afirmaban en el anuncio de sendas donaciones de 10.000 dólares a Children International y The Water Project. José Rosell, socio director de la empresa de ciberseguridad especializada en infraestructuras críticas S2Grupo, se muestra especialmente escéptico con estas proclamas: “Mentira podrida. Esto es puro negocio. No olvidemos que son delincuentes como la copa de un pino”[[28]](#footnote-29). Y como delincientes muy buscados eran perseguidos por el FBI, como se ve en el anuncio en el que ofrecían una recompensa de 10 M$ por pistas que llevasen a su detención[[29]](#footnote-30).



*Fig 7: Cartel del FBI en el que se ofrecen 10 millones de dólares por información para encontrar a los miembros de DarkSide*

La pérdida de actividad de REvil y DarkSide dio paso a la aparición en escena de nuevas bandas como LockBit 2.0, HelloKitty, Hive o AvosLocker. Los expertos de seguridad estudian estos grupos, sus virus y sus comportamientos para intentar ayudar a detenerlos, o para poder prevenir y reaccionar mejor ante sus eventuales ataques[[30]](#footnote-31).

## **2.2. ¿Cómo actúa técnicamente el ransomware?**

2.2.1. Vectores de entrada



*Fig 8: Vectores de entrada de los ciberatacantes*

Para introducir el ransomware en los equipos de las víctimas, los hackers se sirven de múltiples formas de ataque[[31]](#footnote-32), que pueden clasificarse en dos grandes grupos.

**a: Ataques de ingeniería social**

Este tipo de ataque es el más común en el mundo del ransomware. De toda la infraestructura de un dispositivo, normalmente el componente más peligroso es el ser humano a cargo. Los ciberdelincuentes pueden engañar fácilmente a un usuario inexperto para que realice acciones que pongan a su equipo en un estado vulnerable, o incluso para que introduzca y ejecute el propio ransomware en el equipo.

Para lograr que el usuario haga lo que le pidan, los ciberdelincuentes utilizan una amplia variedad de técnicas. Una de las más famosas es el “phishing”, o suplantación de identidad, en la que los cibercriminales se hacen pasar por un contacto confiable (un banco, una empresa, el gobierno, la policía) y contactan con la víctima, pidiéndole que realice una acción insegura (por medio de engaños o amenazas), confiando en que, por miedo o ignorancia, esta cumpla la petición, inyectando el ransomware (al hacer click en un link o fichero malicioso), o exponiendo su equipo al atacante.

Otra técnica similar es el malvertising, publicidad engañosa (normalmente en forma de pop-ups) que, al pinchar en ella, se accede a una página web que trata de explotar vulnerabilidades en el navegador de la víctima para inyectar el ransomware.

Un vector de entrada adicional es a través de la compra de credenciales en la “dark web”, para intentar por esa vía tener acceso al sistema, incluyendo la posibilidad de acceder ilegítimamente a redes privadas virtuales (VPNs) que permiten operar desde fuera de la organización como si se estuviese dentro de la red de la misma[[32]](#footnote-33).

**b: Explotación de vulnerabilidades “zero-click”**

Si bien los ataques de este tipo son menos comunes, son los más codiciados por los cibercriminales. Estos aprovechan vulnerabilidades críticas en componentes esenciales del sistema operativo para lograr controlar el equipo de la víctima sin que esta haga nada (basta con que el dispositivo esté conectado a internet). Debido a la peligrosidad que conllevan, existen múltiples equipos especializados en encontrar este tipo de vulnerabilidades críticas y avisar a las compañías encargadas del software vulnerable para que lancen un parche lo antes posible.

Una forma de explotar estas vulnerabilidades es por medio de los *web exploit kits* o *drive-by downloads*, páginas web maliciosas que aprovechan las vulnerabilidades para infectar a la víctima tan solo con entrar en ellas

En los ataques de ransomware a grandes empresas, los atacantes suelen querer tener acceso al dispositivo, para poder coordinar mejor el ataque, recabar datos interesantes y abrir puertas traseras que dificulten la mitigación. Para ello, se sirven de las mismas técnicas usadas para inyectar los programas de ransomware, obteniendo un reverse Shell (consola de comandos con la que controlan el equipo de la víctima) o acceso al RDP (“Remote Desktop Protocol”, protocolo de control remoto del equipo, con el que pueden controlar el escritorio de la víctima como si estuvieran físicamente delante del ordenador), que les confiere un control total sobre el dispositivo

2.2.2. El ataque (cifrado o bloqueo de los sistemas)

Una vez en el equipo, la práctica más común en los programas de ransomware es el **cifrado de archivos**, que consiste en encriptar todos los archivos personales del ordenador, de forma que sean inutilizables hasta que sean desencriptados. El ransomware encripta cada archivo “desordenando” los bytes de los que está compuesto, siguiendo un patrón concreto dictado por una serie de caracteres conocidos como “claves”[[33]](#footnote-34).

Existen dos tipos de claves, dependiendo del algoritmo de encriptado[[34]](#footnote-35):

* Claves simétricas
  + En los algoritmos de encriptado en los que se utilizan claves simétricas, los archivos se desencriptan con la misma clave que con la que fueron encriptados, siendo tan solo necesario realizar el mismo proceso a la inversa. Este tipo de claves es considerado inferior, pues profesionales especializados pueden obtener la clave sin necesidad de pagar el rescate.
* Claves asimétricas
  + En los algoritmos de encriptado con claves asimétricas, se generan dos claves: la clave pública (con la que se encriptan los archivos) y la clave privada (con la que se desencriptan). Estas dos claves están relacionadas matemáticamente, pero no son la misma, de modo que se pueden encriptar archivos sin necesidad de guardar la clave para desencriptarlos. Por lo tanto, aun obteniendo con ayuda de profesionales la clave pública utilizada por el ransomware para el encriptado de los ficheros, los archivos no se pueden recuperar, pues esto solo puede lograrse con la clave privada, que se encuentra en el equipo del atacante.

En ambos casos, las claves son cadenas de caracteres muy largas, de forma que si se intentara descifrar un archivo por fuerza bruta (probando todas las combinaciones de claves posibles), se tardaría millones de años con la tecnología de hoy en día.

2.2.3. Solicitud de rescate y posible recuperación de los archivos

Una vez encriptados los archivos, el atacante informa al usuario del secuestro de estos, generalmente por medio de una ventana emergente. En la mayoría de los programas de ransomware, esta ventana está compuesta por distintos elementos:



5

4

3

2

1

- **1: Un título** en el que se informa a la víctima que ha perdido el control de sus archivos. Suele tener una fuente grande y colores resaltantes para llamar la atención de la víctima.

- 2: **Un cuadro de texto** donde se explica en más detalle qué es un ransomware y cómo este impide el acceso de la víctima a sus archivos sin una clave que está en posesión del atacante, con el objetivo de que la víctima comprenda la situación, en caso de que esta no sepa lo que es un ransomware.

- **3: Unos temporizadores** que indican el tiempo del que dispone la víctima para hacer el pago antes de que el ciberdelincuente borre la clave, imposibilitando la recuperación de los archivos. Algunos programas también incluyen otro temporizador que indica cuánto tiempo tiene la víctima para pagar el rescate antes de que este aumente de precio.

- **4: Una dirección de una cartera de criptomonedas**, junto a un indicador del importe que se debe abonar en ella para obtener la clave de descifrado. Suele venir acompañado de un enlace informativo que explica cómo comprar y transferir las criptomonedas.

- **5: Un medio de contacto** con el atacante, para poder justificar el pago y solicitar la clave de descifrado, ya que el pago por criptomonedas es anónimo y el atacante no tiene manera de saber si la víctima ha pagado o no si solo mira las transacciones en su cartera de criptomonedas, sobre todo si es un ataque masivo y piden cantidades similares a muchas organizaciones.

Prácticamente todos los ciberdelincuentes piden el rescate en criptomonedas, pues es una moneda descentralizada, y no hay manera de relacionar a un usuario con la persona detrás de este, por lo que las autoridades en principio no pueden rescatar el dinero, aunque en el caso de Colonial antes mencionado sí que consiguieron recuperar 2,3 M$ de los 4,4 M$ pagados[[35]](#footnote-36) (la nota del Departamento de Justicia no explica cómo, posiblemente a través de alguna persona de la banda DarkSide que realizó ese ataque).

## **2.3. Análisis de una familia de ransomware**

# **3: ¿Cómo luchar contra el ransomware?**

## **3.1. ¿Cómo prevenir los ataques?**

Tras sufrir un ataque de ransomware no se puede volver al estado anterior del ataque, aun recuperando los archivos, la interrupción en las operaciones, la filtración de información importante, y el impacto público del ataque (en caso de ser una empresa) hacen que como mucho se pueda alcanzar una nueva normalidad. Así que, como dice la frase popular: “más vale prevenir que curar”.

A continuación, se detallan una serie de consejos orientados a la prevención de un ataque de ransomware.

***Tener el software con soporte y siempre actualizado a la última versión***

Los ciberdelincuentes están en constante búsqueda de vulnerabilidades en el software y las aplicaciones más populares. Debido a la complejidad del software y las aplicaciones que usamos diariamente, que los ciberdelincuentes encuentren una de estas vulnerabilidades es tan solo cuestión de tiempo, y en algunos casos, una vulnerabilidad puede ser tan grave que los ciberdelincuentes pueden infectar equipos tan solo con que estén conectados a internet, sin necesidad de ninguna acción de la víctima (estas son conocidas como vulnerabilidades *zero-click*). Para hacer frente a estas fallas de seguridad, las compañías desarrolladoras de software están en constante alerta, para poder parchear su software cuanto antes y evitar que los cibercriminales puedan aprovechar estas vulnerabilidades para infectar equipos (algunas empresas incluso ofrecen recompensas a los hackers que las descubran a cambio de ayudarles a parchearlas, o tienen su propio equipo de profesionales buscando vulnerabilidades en su propio software antes de que salgan a la luz).

Sin embargo, si los usuarios no realizan actualizaciones regularmente, sus equipos quedan expuestos debido a las vulnerabilidades sin parchear, facilitando trabajo de los cibercriminales y por lo tanto se convierten en un blanco fácil. En redes con muchos dispositivos conectados (como colegios o empresas), la necesidad de actualizar el software es aún más importante, pues un ciberdelincuente podría aprovechar un sistema obsoleto para infiltrarse y utilizarlo para escalar dentro de la red y obtener privilegios de administrador, pudiendo controlar así otros equipos, aunque estén actualizados (una cadena es tan fuerte como el más débil de sus eslabones).

Por supuesto, también es crucial que el software que se esté utilizando tenga soporte y siga siendo mantenido por su desarrolladora, porque si esta no lanza nuevos parches, los cibercriminales no encontrarán resistencia alguna para explotar las vulnerabilidades que encuentren, y cuanto más tiempo pase, más fácil será infectar un dispositivo con ese software (por poner un ejemplo, Windows 7, un sistema operativo que dejó de tener soporte hace dos años, ya puede ser infectado por gente tan principiante como yo, más información en el apartado práctico).

***Utilizar un antivirus***

Hoy en día, Windows (el sistema operativo utilizado por un 88,8% de los usuarios en junio de 2021) tiene incorporado un antivirus por defecto, llamado Windows Defender. Sin embargo, este solo ofrece protección básica, por lo que para evitar los ataques de ransomware se recomienda tener un antivirus de pago, que analice las aplicaciones y los archivos en el dispositivo y alerte al usuario, así como prevenir páginas web y archivos adjuntos maliciosos.

(antiransomware?)

***Restringir los permisos y segmentar la red***

Los permisos son una forma de restringir las acciones que puede realizar un programa. Normalmente, los programas son ejecutados con los permisos del usuario que los utiliza, pero los ciberdelincuentes pueden explotar vulnerabilidades en el sistema o engañar a la víctima mediante ingeniería social para obtener permisos de administrador. Aparte de que estos permisos facilitan la inyección de un ransomware, también permiten que el cibercriminal tenga un control total sobre el dispositivo y todos sus componentes, como si estuviera delante de él, por lo que el riesgo se multiplica. Además, si el dispositivo está conectado a una red, tener los permisos de administrador ayuda al ciberdelincuente a infectar otros equipos conectados.

(En redes jerárquicas (en las que una cuenta controle todos los equipos, como en algunos colegios o empresas), obtener la clave de administrador de un equipo puede ayudar al hacker a “escalar” privilegios dentro de la red, hasta conseguir la clave maestra y así controlar e infectar todos los equipos conectados.)

Por lo tanto, se recomienda que la clave de administrador sea conocida por el mínimo número de personas posible y no se utilice a no ser que sea estrictamente necesario.

A su vez, se recomienda segmentar las redes grandes, es decir, filtrar la red para evitar que se pueda acceder a todos los dispositivos de una red desde un equipo (que es la opción por defecto), para que en caso de que un ciberdelincuente haya logrado hacerse con la clave de administrador, este no pueda escalar privilegios tan fácilmente y atacar a todos los dispositivos a la vez.

IMPORTANTE: APRENDER MÁS SOBRE CÓMO FUNCIONA LA SEGMENTACIÓN Y AÑADIR MÁS DEL FIREWALL

***Cerrar la conexión con el exterior lo máximo posible***

La mayoría de los ataques de ransomware vienen de fuera de la red local, por lo que es esencial limitar toda conexión con la red externa que no sea necesaria. Se recomienda instalar un *firewall* para bloquear las conexiones entrantes o salientes no deseadas, junto a un filtro de spam y de URL que bloquee las páginas web y los correos que puedan ser maliciosos. Si es necesario acceder a servicios de la red local desde fuera, se puede instalar una VPN, con la que mediante un usuario y una contraseña se pueda “fingir” que un equipo está dentro de la red local.

***Activar sistemas de detección y vacunas***

En grandes redes, se recomienda instalar un EDR (Endpoint Detecion Response), un sistema que se encarga de monitorear tanto la red como los equipos con algoritmos de inteligencia artificial, para detectar una intrusión o un programa malicioso antes de que actúe.

A su vez, también se recomienda usar las vacunas desarrolladas por el CERT, programas diseñados para detectar ciertas variantes de ransomware para destruirlas en el momento que entren en el dispositivo.

[CCN-Cert bp]

***Evitar la suplantación de un usuario***

Para evitar que el ciberdelincuente se haga con el control de la red, las cuentas (especialmente las de los administradores) deben guardarse celosamente, y sus contraseñas deben cumplir unos estándares de seguridad (generalmente, tener ocho o más caracteres, tener mayúsculas, minúsculas, números y símbolos y evitar ser usadas en más de un sitio). Además, se recomienda tener activada la autenticación multifactor (MFA), que requiere de una confirmación por teléfono/correo y/o comprobación de medidas biométricas para conceder el acceso a una cuenta.

***Deshabilitar las macros y los scripts de Powershell***

Los archivos de los programas de ofimática, como Microsoft Office o LibreOffice, pueden contener un pequeño script conocido como macro, aparte del propio contenido, que se abre junto al archivo. Los macros fueron ideados como una manera de dar libertad a los usuarios para ampliar las funcionalidades de estos programas, automatizando tareas y otorgando más interactividad a los archivos. Sin embargo, los ciberdelincuentes pueden aprovechar las macros para escribir código malicioso que infecte los dispositivos en los que sea ejecutado. Para evitar esto, los programas de Microsoft Office no ejecutan las macros si el origen del archivo es sospechoso, pero pulsando el botón de “habilitar edición” para editar un archivo, las macros maliciosas pueden ejecutarse, por lo que se recomienda desactivar su ejecución desde los ajustes.

Otra de las tácticas más utilizadas para ejecutar código malicioso es el uso de scripts de Powershell, que suelen utilizarse para automatizar tareas, pero también pueden utilizarse para infectar un dispositivo, con el añadido que, al no ser aplicaciones convencionales, ciertos antivirus no los detectan como maliciosos. Afortunadamente, al igual que con las macros, existe una manera de deshabilitar la ejecución de los scripts de Powershell en el equipo.

***Tener copias de seguridad de la información***

Esta es posiblemente la medida más importante, ya que, si por alguna razón todas las precauciones no son suficientes para evitar un ransomware, tener una copia de seguridad garantiza la recuperación completa y gratuita de los datos, siempre que esta se realice apropiadamente.

Se recomienda que no se pueda acceder a la copia de seguridad desde la red, ya que si no esta corre el riesgo de ser encriptada también por el programa de ransomware. Además, esta debe realizarse con asiduidad, aunque depende de la importancia de los datos y los medios disponibles. Por ejemplo, para un ordenador de uso personal, guardar una copia de seguridad de los archivos en un medio offline (como un disco duro) cada ciertas semanas es suficiente, pero para otros casos donde haya un gran tráfico de datos importantes, se recomienda tener un equipo dedicado a almacenar copias de seguridad del resto de equipos de la red cada día (equipado con medidas de protección para evitar intrusiones) y hacer una copia de seguridad en un medio offline cada más tiempo, para estar protegidos en caso de que el atacante haya logrado encriptar los archivos de la copia de seguridad diaria. En el caso de organismos con más medios, también se recomienda copiar las propias copias de seguridad y guardarlas en distintos equipos o medios.

Además se recomienda activar las “shadow copies” en el equipo

***Habilitar la visión de la extensión de los archivos***

En Windows, el explorador de archivos no muestra la extensión de los archivos por defecto. Esto ayuda a los atacantes, que pueden cambiar el icono de un archivo para engañar a las víctimas, por ejemplo, haciéndoles creer que un programa ejecutable .exe es una fotografía o un documento, por lo que la abren pensando que es inofensiva y se infectan. Por lo tanto, activar la opción de ver las extensiones de los archivos es una medida sencilla pero útil para prevenir la ejecución de un programa malicioso.

***Seguir buenas pautas para evitar los ataques de ingeniería social***

Puesto que los ciberdelincuentes se sirven frecuentemente de la ingeniería social para introducir su ransomware en los equipos, se recomienda seguir una serie de pautas para evitar sus engaños:

* Al utilizar el correo electrónico:
  + Comprobar la dirección de correo del remitente (puede ser parecida, pero diferente)
  + Comprobar que no se esté realizando “spoofing” (técnica con la que los hackers pueden enviar un correo cuyo remitente sea otra dirección)
  + Tener un filtro antispam
  + Comprobar los enlaces antes de abrirlos
  + Si un remitente es sospechoso, no abrir su correo (puede tener un exploit zero-click o confirmación de lectura)
  + En empresas, se recomienda realizar pruebas de phishing (enviar correos que simulen un ataque de ingeniería social para instruir al personal)
  + Desactivar la carga automática de imágenes y HTML en los correos
* Al navegar por internet:
  + Intentar navegar solo por páginas https (con el “candadito”)
  + Si una página web descarga un fichero automáticamente, eliminarlo
  + Al descargar un archivo de una página web no confiable, es mejor escanearlo con un antivirus antes de abrirlo
  + No dar permisos a las páginas web no confiables

***Realizar auditorías***

En redes a gran escala, es muy recomendado realizar auditorías de vez en cuando, es decir, pruebas realizadas por expertos para determinar el nivel de protección de la red y los equipos, y los puntos débiles de esto. Afortunadamente, el desarrollo de sistemas de automatización ha hecho que las auditorías sean sencillas y asequibles [INCIBE guía de aprox]

***Informarse sobre el ransomware y los ataques de ingeniería social***

La mayoría de los ataques de ransomware son exitosos gracias a un elemento clave: la ignorancia. Según una encuesta de ¿???, un xx% de los usuarios no sabe qué es el ransomware, ni tampoco saben reconocer un intento de ingeniería social. Los cibercriminales aprovechan esto para realizar sus ataques, sabiendo que la víctima no se percatará del peligro hasta que sea demasiado tarde. Por lo tanto, la principal prioridad para prevenir los ataques de ransomware es ser consciente de su existencia e instruir a la mayor cantidad de personas posibles sobre cómo prevenirlos y cómo actuar en caso de sufrir un ataque.

Aparte, también se recomienda desarrollar un plan de respuesta a un ataque, en caso de que todas las medidas de prevención no fueran suficientes, ya que cuando el atacante consigue hacerse con el control de un equipo, el tiempo de respuesta de la víctima es clave.

ACABAR 3.1 CON:

PONER PORCENTAJE

PONER LAS FUENTES DEL STICKNOTE AL TEXTO Y PONER LAS MEDIDAS EN ORDEN

AÑADIR DETECCIÓN Y SHADOW COPIES

Pegado del sticknote:

Baseideas:

- Prepararse contra emails/webs falsas (INCIBE)

- Actualizar a la última

- Usar antivirus (incluso antiransomware) (INCIBE)

- Mínimo privilegio (uclm)

- Guardar celosamente las claves (uclm)

- MFA (uclm)

- Segmentación de la red

- Cerrar puertos (aka firewall) (CCN-bp)

- Fuera macros, powershell etc (CCN bp)

- Extensión de archivos (10 recomm)

- Copia de seguridad (CCN)

- Antingenería social

## **3.2. ¿Cómo reaccionar en caso de ataque?**

Por muchas medidas que se tomen para tratar de prevenir un ransomware, siempre existe una posibilidad de que el atacante sea capaz de sortearlas y encriptar los archivos. Si desgraciadamente esto llegara a ocurrir, las decisiones tomadas por la víctima tras percatarse del ataque pueden alterar drásticamente las consecuencias de este. A continuación, detallaré una serie de pautas a seguir:

***Inmediatamente después de percatarse del ataque***

***No pagar el rescate***

Si los archivos encriptados son muy importantes y no se ha realizado una copia de seguridad, uno puede verse tentado a pagar el rescate. Sin embargo, esto no es recomendable por una serie de razones:

* No se garantiza la recuperación de los archivos. Tan solo un xx% de las víctimas que pagan recuperan parcialmente sus archivos, de media un 65%. Es necesario recordar que se está tratando con criminales, y su palabra no es confiable. Además, en ataques a gran escala, es posible que el ciberdelincuente ni siquiera tenga la capacidad de desencriptar los archivos de todas las víctimas que pagan, debido a su gran número y el hecho de que los pagos por criptomonedas son anónimos
* Al pagar, se contribuye a convertir el desarrollo de ransomware en un negocio viable, atrayendo así a más hackers dispuestos a llevarse un botín

***Apagar la red***

Lo primero que se debe hacer inmediatamente es desconectar todos los equipos de la red, infectados o no, para evitar que el ciberdelincuente siga teniendo control sobre esta y pueda infectar más equipos. Se recomienda desconectar los equipos físicamente (tirando del cable) para evitar que el atacante pueda restablecer la conexión. [incibe empresas]

***Identificar la variante de ransomware***

Si es posible, se recomienda realizar una búsqueda en internet sobre la variante de ransomware que ha infectado el equipo, basándose en el mensaje del rescate. Si es una variante conocida, se puede encontrar en internet información que ayude a combatirla.

***Detener el ransomware***

A continuación, se debe tratar de cerrar el programa de ransomware, para que no continúe ejerciendo actividades maliciosas en el sistema. Para ello, se puede terminar el proceso buscándolo desde el administrador de tareas. Conocer la variante del ransomware puede ayudar a encontrar el programa. Si no se puede encontrar el proceso malicioso, se recomienda apagar completamente el equipo. Si se necesita volver a encender el sistema, siempre debe acceder desde el modo seguro para que los programas ajenos al sistema(en especial, el ransomware) no puedan volver a ejecutarse

En caso de que el ransomware advierta que se borrarán los datos si se intenta detenerlo o apagar el equipo, se recomienda alterar el orden de esta pauta con la siguiente [ccn bp]

***Realizar una clonación***

Aunque los archivos estén encriptados, se recomienda realizar una clonación del disco duro, ya que dependiendo de la variante del ransomware es posible que estos se puedan desencriptar sin pagar al ciberdelincuente (se hablará en detalle sobre este asunto más adelante).

[Incibe empresas]

***A corto plazo después del ataque***

***Comprobar las “shadow copies”***

Si las shadow copies estaban habilitadas en el sistema, se recomienda encender el equipo (en modo seguro para evitar que el ransomware vuelva a habilitarse) y comprobar si se ha realizado un punto de restauración. Puesto que las shadow copies se realizan con más frecuencia que las copias de seguridad y están ocultas en el disco duro, estas pueden ayudar a recuperar archivos recientes. Desafortunadamente, algunas variantes de ransomware también encriptan las shadow copies, aun estando ocultas.

***Utilizar un disco duro nuevo, instalar un sistema operativo desde cero y comprobar que este esté limpio***

Tras infectar un equipo, algunos programas de ransomware pueden instalar puertas traseras en el disco duro o en otros componentes del equipo para que el atacante pueda volver a atacarlas tras volver a conectarse a la red. Por lo tanto, se recomienda comprar un disco duro nuevo, instalar un sistema operativo desde cero y después comprobar con un antivirus que no quede ninguna puerta trasera abierta.

***Cambiar las contraseñas***

Aparte de encriptar los archivos, es posible que el ransomware también haya extraído las claves de los equipos y se las haya mandado al ciberdelincuente, por lo que es necesario cambiar todas las contraseñas.

***Recuperar los archivos de la copia de seguridad***

Si existe una copia de seguridad, esta se puede utilizar para recuperar parte de los archivos. Antes de pasar los archivos de vuelta a los dispositivos, se recomienda escanearlos con un antivirus para asegurarse de que no haya una copia del ransomware escondida en ellos.

***Denunciar el ataque y realizar un post-mortem***

Después de sufrir un ataque de ransomware, se debe denunciar al Equipo de Respuesta ante Emergencias Informáticas (CERT). Este cuenta con personas especializadas que pueden ayudar a la recuperación de la actividad, y a descubrir la manera en la que el atacante consiguió infiltrarse y encriptar los archivos, de forma que la vulnerabilidad pueda resolverse antes de volver a conectar los equipos.

Una vez realizados todos estos pasos, se puede volver a conectar los equipos y retomar la actividad, prestando especial atención en cumplir las medidas de prevención, para evitar otros ataques.

***A largo plazo después del ataque***

A pesar de que el disco duro esté encriptado, si hay archivos importantes que no se han podido recuperar, se recomienda guardarlo, pues numerosas organizaciones, tanto gubernamentales como privadas, tratan de analizar el ransomware para encontrar algún fallo del programa o de sus autores que permita recuperar los archivos sin necesitar la clave. Si encuentran una manera de desencriptar los archivos, esta es publicada para que cualquiera pueda utilizarla y así recuperar todos sus datos.

## **3.3. Algunos dilemas planteados por el ransomware**

3.3.1. Pagar o no pagar

Al sufrir un ataque de ransomware, una de las decisiones más complicadas es pagar o no. Por un lado, si no se tiene una copia de seguridad ni forma inmediata de recuperar los archivos, pagar es una alternativa muy tentadora, pues de lo contrario se pueden perder archivos extremadamente importantes. Además, en casos en los que el ataque sea de doble extorsión o más, no hay que tener en cuenta solo la pérdida de archivos, sino la posibilidad de que los ciberdelincuentes revelen datos confidenciales o infecten contactos.

Sin embargo, al pagar se fomenta la ciberdelincuencia, pues el ransomware se convierte en un negocio rentable, por lo que varios gobiernos, como el de Estados Unidos, pueden llegar a imponer multas a aquellos que paguen el rescate, para desincentivar esas conductas[[36]](#footnote-37).

Para evitar que esos pagos sean visibles para las autoridades, las empresas (u organismos públicos) atacados contratan a veces servicios de emergencia de empresas de ciberseguridad, a través de las cuales se efectúan a veces esos pagos – como a través de las empresas que ofrecen seguros de ransomware que, además de cubrir daños causados por los ataques, llegan a incluir pagos por rescatar la información.

3.3.2. Los seguros de ransomware

Debido al creciente número de ataques de ransomware, ciertas empresas aseguradoras han comenzado a ofrecer seguros contra estos. Algunas compañías incluyen este tipo de seguro como una parte de sus servicios, mientras otras se dedican exclusivamente a vender seguros de ransomware.

Aunque este tipo de seguro mueve 8 millones de dólares anualmente tan solo en los estados unidos, menos de un 15% de las grandes empresas tienen uno de estos seguros hoy en día.

Los seguros de ransomware suelen encargarse de cubrir los daños de pagar el rescate, el daño causado a los equipos, la responsabilidad civil en caso de que se hayan filtrado datos personales y el descenso de ingresos debido a la pérdida de reputación, aunque depende de cada proveedor. Además, muchas aseguradoras también incluyen un servicio de ayuda a sus clientes para informarse sobre el ransomware y para proteger sus equipos.

A pesar de la ayuda que proveen, los ciberseguros también tienen su parte negativa, puesto que los cibercriminales tienden atacar los equipos cubiertos por uno de estos seguros, confiando en que, al estar cubiertos por este, serán más propensos a pagar el rescate. Es por esto por lo que cada vez más empresas de seguros de ransomware no solo ofrecen ayuda para proteger los equipos de estos ataques, también exigen que los equipos asegurados cumplan ciertas medidas de seguridad (cada vez más estrictas) si sus clientes quieren cobrar el seguro tras ser infectados.

[combating,enisa]

3.3.3. Persecución de los ciberdelincuentes

Por supuesto, el ransomware es una práctica ilegal en todos los aspectos. Sin embargo, los delincuentes son muy complicados de identificar debido a que estos toman múltiples medidas para volverse irrastreables, como el uso de VPNs anónimas.

Aún si los cibercriminales son localizados las consecuencias legales para los cibercriminales dependen ampliamente del país en el que se encuentran.

En España, realizar un ataque de ransomware es considerado un delito, recogido en el artículo 264 del código penal, que indica que alterar datos informáticos ajenos sin autorización será castigado con penas de prisión de seis meses a tres años, o de dos a cinco años y multa si cumple una serie de condiciones agravantes, como formar parte de una organización criminal, afectar a servicios críticos, o haber realizado el delito por medio del robo de cuentas para acceder al equipo y por medio de un programa concebido para cometer el delito

[https://www.boe.es/eli/es/lo/1995/11/23/10/con]

Sin embargo, en otros países, como en Rusia, el ransomware es solo ilegal si este afecta a personas o empresas rusas, ignorando los ataques a víctimas del resto del mundo. Por ello, un gran número de programas de ransomware están diseñados para no ejecutarse si detectan que el paquete de idioma ruso está instalado en el dispositivo (curiosamente, esto significa que instalar el idioma ruso en el ordenador y luego no utilizarlo es una medida útil para protegerse de los ataques de ransomware).

Corea del Norte va un paso más allá, puesto que no solo permite ataques de ransomware a otros países, sino que los instiga, como ya se mencionó en apartado 1.2

## **3.4. Ejemplos reales de ataques de ransomware**

# **4.** **Conclusiones**

**ANEXO**

**PARTE PRÁCTICA: CREACIÓN DE UN RANSOMWARE**

Como parte práctica de este proyecto de investigación he decidido crear mi propio programa de ransomware, empleando los conocimientos de Python adquiridos en clase y un curso sobre ciberseguridad que realicé hace unos años.

Para explicar su funcionamiento, dividiré este anexo en seis apartados: herramientas utilizadas, obtención de acceso, control de la víctima, encriptado de los archivos, la pantalla de secuestro y el desencriptado.

1. Herramientas utilizadas

Para realizar mi programa de ransomware, me he servido de tres elementos principales.

1: Metasploit

Metasploit es un set de herramientas incluido en el sistema operativo “Kali Linux”, y está orientado al hacking ético. Con este, se pueden crear aplicaciones que aprovechan vulnerabilidades en los sistemas para obtener el acceso a un dispositivo y controlarlo, escalar privilegios, obtener credenciales y archivos, y más. Estas aplicaciones son fáciles de crear e incluyen muchas opciones sencillas de usar, pues metasploit está pensado para instruir más que para realizar ataques reales, ya que la mayoría de antivirus lo detectan inmediatamente, y ocultarlo es una tarea muy complicada.

Con metasploit (en concreto la herramienta “msfvenom”) he creado el programa “noesunvirus.exe”, que al ser ejecutado otorga el control del equipo a la máquina de Kali Linux desde el que se creó.

2: Python

El resto de los programas que actúan en el ransomware los he programado yo completamente en Python.

Para que estos puedan ejecutarse en cualquier dispositivo, independientemente de que tengan Python instalado o no, los he compilado por medio de PyInstaller, un programa que convierte código de Python en código máquina.

También he usado una librería específica para el encriptado de archivos, de la que hablaré a detalle más adelante.

3: VMware

Tanto para poder ejecutar Kali Linux como para poder simular el ordenador de la víctima, he utilizado Vmware, un programa con el que se pueden simular ordenadores dentro de un ordenador, conocidos como máquinas virtuales.

1. Obtención del acceso

Para obtener acceso a la computadora de la víctima, he creado un programa llamado “lanzador.docx.exe”, diseñado en Python y compilado con PyInstaller. Está preparado para engañar a la víctima por medio de ingeniería social (por ejemplo, un correo suplantando a una empresa pidiendo a la víctima que lea un documento), pues tiene un icono de documento de Word, tiene la extensión .docx.exe (confiando en el que usuario no haya activado la opción de ver la extensión de los archivos) y hasta abre un documento que tiene embebido como una cadena en base64

Cuando el usuario abre el programa, este le pide permisos de administrador. Independientemente de que la víctima se los de o no, el programa se ejecutará, pero el atacante se verá limitado en su alcance si los rechaza.

Al ejecutarse, el programa extrae dos archivos embebidos como dos cadenas en base64: un documento de Word (que sirve de distracción) y el programa “noesunvirus.exe”, creado con msfvenom, que otorga accedo al equipo desde mi sistema Kali Linux.

1. Control del dispositivo

Una vez abierto el archivo anterior, puedo controlar el ordenador afectado desde meterpreter, una consola de comandos de metasploit. Con ella puedo realizar acciones como obtener privilegios de administrador, ver la pantalla y cámara de la víctima, obtener sus credenciales, y sobre todo: enviar/recibir archivos y ejecutar programas de forma remota.

Usando estas dos últimas funciones, puedo subir dos programas más: “encrypt.exe” y “susto.exe”

1. Encriptación de archivos

Gracias a meterpreter, puedo enviar el archivo “encrypt.exe” al ordenador de la víctima y ejecutarlo remotamente.

“Encrypt.exe” es otro programa que he realizado en Python. Este utiliza el método “Fernet” de la librería “cryptography” para encriptar y desencriptar los archivos.

Al ejecutarse, el programa genera una clave simétrica aleatoria. Luego, utiliza esa clave para encriptar todos los archivos encontrados en las carpetas del usuario más comunes (Documentos, Imágenes, Descargas, Escritorio, Música y Vídeos) excepto los esenciales para que funcione el hack. A continuación, crea un archivo de texto donde se guardan detalles de la ejecución, como la hora (para calcular el tiempo restante para pagar) y si ha funcionado o no.

Después, el programa desencripta otro programa embebido, “launchersusto.exe”, y lo ejecuta. Este se encarga de comprobar en todo momento que el otro programa recibido, “susto.exe”, esté abierto. “launchersusto.exe” se copia a la carpeta del menú inicio, así que se abre aun si se reinicia el equipo.

Finalmente, desde meterpeter descargo la llave generada (que se clasifica automáticamente y se programa para borrarse tras 24 horas) y la borro del pc infectado-

1. Pantalla de ransomware

Cuando “launchersusto.exe” se ejecuta, entra en un bucle en el que comprueba si “susto.exe” está abierto. Si no, lo busca entre los archivos y lo abre.

Al abrirse, “susto.exe” descomprime dos archivos embebidos: un fondo de pantalla y un pequeño extracto musical ominoso de la 5ª sinfonía de Beethoven, que se reproduce a la vez que aparece la pantalla de rescate, hecha con tkinter. En esta se informa al usuario sobre los pasos a realizar para recuperar sus archivos, se muestran unos temporizadores del tiempo que queda para el aumento del pago/borrado de la clave, y links para más información y para contactar con el atacante, junto al “id de secuestro” (para saber cuál es la clave de encriptado).

1. Desencriptación de los archivos

SI la víctima pagase los archivos, le enviaría la llave generada junto al programa “decrypt.exe”. Este programa es casi igual a “encrypt.exe”, pero realiza los pasos inversos: utiliza la llave para desencriptar los programas y borra los archivos generados por el ransomware, aparte de restaurar el fondo de pantalla original.

# **Bibliografía**

“6 Ways to Defend Against a Ransomware Attack”, Manasi Sakpal, , Gartner, 16.11.2020 <https://www.gartner.com/smarterwithgartner/6-ways-to-defend-against-a-ransomware-attack>

”Así es Ryuk, el ransomware que ha dejado tumbado al SEPE (y que antes tumbó a otros muchos)”, Javier Pastor, Xataka, 10.03.2021 - <https://www.xataka.com/seguridad/asi-ryuk-ransomware-que-ha-dejado-tumbado-al-sepe-que-antes-tumbo-a-otros-muchos>

”Beneath the surface of a cyberattack”, Deloitte, 2017 - <https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/beneath-the-surface-of-a-cyberattack.html>

“Breaking down ransomware attacks”, Jeremy Brown & Ashlie Blanca, Unit 42 – Palo Alto Networks, 21.05.2021 - <https://unit42.paloaltonetworks.com/breaking-down-ransomware-attacks/>

“Combating Ransomware”, IST (Institute for Security + Technology) – Ransomware Task Force, 23.09.2021 - 81 pp. - <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf>

“Cyber Insurance is Supporting the Fight against Ransomware”, Marsh, <https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-supporting-fight-against-ransomware.html>

“Cyber insurance may be making ransomware worse, here’s why”, Matthew Delman, Morphisec, 01.07.2021 - <https://blog.morphisec.com/cyber-insurance-may-be-making-ransomware-worse-heres-why>

“DarkSide Ransomware” – Basque Cybersecurity Center, mayo 2021, 36 pp. <https://www.basquecybersecurity.eus/archivos/202105/bcsc-malware-darkside-ransomware-tlpwhite_v1.pdf?1>

“DarkSide Ransomware: Informe de código dañino”, CCN-CERT ID-09/21, julio 2021, 29 pp. - <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6080-ccn-cert-id-09-21-dark-side-1/file.html>

“DarkSide Ransomware Gang: An Overview”, Ramarcus Bayloer, unit 42- PaloAlto Networks, 12.05.2021 - <https://unit42.paloaltonetworks.com/darkside-ransomware/>

“Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside”, The United States Department of Justice, 07.06.2021 - <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>

“Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware”, Nik Simson & Ron Blair, Gartner, 06.01.2021 - [https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gartner.com%2Fdoc%2Freprints%3Fid%3D1-258HHK51%26ct%3D210217%26st%3Dsb&data=04%7C01%7Calberto.perez%40red.es%7C94981e0164904196c3ec08d99af05d38%7Cf9337b9a82d042bca8f3aea9991055c4%7C0%7C0%7C637711179427688370%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=6P6SupUEju%2FXtjgU4yqWxQ5bdOkF5my7tz4JrmeswRg%3D&reserved=0)

”El ciberataque al SEPE provocó que sus técnicos trabajaran 19.000 horas extras en jornadas maratonianas y festivos: así levantaron una barricada contra el 'ransomware'”, Alberto R. Aguiar, 02.12.2021, Business Insider - <https://www.businessinsider.es/vivio-ciberataque-sepe-dentro-19000-horas-extra-973861>

“Enfrentándonos al Ransomware”, Manuel López y Jesús Arnáiz, INCIBE, 15.07.2015 - <https://www.incibe-cert.es/blog/enfrentandonosransomware>

“FBI: Ransomware: What It Is & What To Do About It“, FBI (Federal Bureau of Intelligence), 02.04.2021 - <https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf>

“Four emerging ransomware groups take center stage“, Shaun Nichols, Techtarget, 24.08.2021 - <https://www.techtarget.com/searchsecurity/news/252505816/Four-emerging-ransomware-groups-take-center-stage>

“Gestión de incidentes de ransomware: Informe de buenas prácticas”, CCN-CERT, BP/21, abril 2021, 37 pp - <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5867-ccn-cert-bp-21-gestion-de-incidentes-de-ransomware-1/file.html>

“Guía esencial sobre el ransomware”, Patrick Seguin, AVAST Academy, 20.12.2021- <https://www.avast.com/es-es/c-what-is-ransomware>

“How to Negotiate with Ransomware Hackers”, Rachel Monroe, 31.05.2021, The New Yorker Magazine, June 7, 2021 Issue, <https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers>

“Informe de amenazas 2021 de Sophos”, Sophos, noviembre 2020, 36 pp. - <https://www.sophos.com/es-es/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf>

“Key Learnings Following the Ransomware Attack on Irish Healthcare”, GÉANT Connect, 07.10.2021 <https://connect.geant.org/2021/10/05/key-learnings-following-the-ransomware-attack-on-irish-healthcare>

“Maze - Informe de código dañino”, CCN-CERT ID 14/20, mayo 2020, 25 pp, <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4976-ccn-cert-id-14-20-maze-1/file.html>

“Maze Ransomware - Threat Brief”, Brittany Barbehenn & Doel Santos, unit-42 – Palo Alto Networks, 08.05.2020, <https://unit42.paloaltonetworks.com/threat-brief-maze-ransomware-activities/>

“Medidas de seguridad contra ransomware – Informe de amenazas”, CCN-CERT IA-01/16, Agosto 2016, 29 pp - <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1384-ccn-cert-ia-01-16-medidas-de-seguridad-contra-ransomware/file.html>

“Mitigating malware and ransomware attacks”, National Cyber Security Center UK (NCSC), 09.09.2021 - <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

“North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions”, US Department of Justice, 06.09.2018 - <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>

“Rançongiciels”, Fiche reflexe, Cybermalveillance.gouv.fr – 20.11.2019 <https://www.cybermalveillance.gouv.fr/medias/2019/11/Fiche-reflexe_rancongiciels.pdf>

“Ransomware and Cyberthreats Protection 2022”, Veeam, 2022 - <https://www.veeam.com/videos/webinar-ransomware-cyberthreats-protection.html?rwty&st=drip>

“Ransomware as a Service” Explained. What is RaaS?”, David Harrington, 25.02.2022, Varonis - <https://www.varonis.com/blog/ransomware-as-a-service>

“Ransomware: buenas prácticas: 10 recomendaciones clave para protegerse frente al ransomware”, Informe CCN-CERT BP-04/16 - <https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/4368-diez-recomendaciones-clave-para-protegerse-frente-al-ransomware.html>

“Ransomware: ENISA Threat Landscape”, ENISA (European Union Agency for Cybersecurity), 2020, 26 pp. - <https://www.enisa.europa.eu/publications/ransomware/@@download/fullReport>

“Ransomware Impact Report 2021” (+ Infographic), 2021, Keeper, 15 pp. - <https://www.keeper.io/hubfs/2021_Ransomware_Impact_Report/2021_Ransomware_Impact_Report.pdf>

“Ransomware Readiness Assessment”, Unit 42 – Palo Alto Networks, 2021, 4 pp. - <https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/ransomware-readiness-assessment>

“Ransomware: The Rapidly Evolving Trend”, Bitsight, 2021, 9 pp. - <https://www.bitsight.com/resources/ransomware-the-rapidly-evolving-trend>

“Ransomware: The True Cost to Business – A Global Study on Ransomware Business Impact”, 2021, Cybereason, 31 pp. <https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business#:~:text=THE%20IMPACT%20OF%20RANSOMWARE%20ON,the%20U.S.%20in%202020%20alone>

“Ransomware Threat Report 2021”, DarkTrace, 2021, 20 pp., <https://www.darktrace.com/ko/resources/wp-ransomware-threat-report.pdf>

“Ransomware: una guía de aproximación para el empresario”, INCIBE, 20.04.2021, 34 pp. - <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf>

“Ransomware: unlocking the lucrative criminal business model”, unit-42 – Palo Alto Networks, 2018, 21 pp. - <https://itcorporate.co.uk/Resource/Detail/43677>

“The future of ransomware: 2022 and beyond”, Daniel dos Santos, 22.11.2021, ITProPortal - <https://www.itproportal.com/features/the-future-of-ransomware-2022-and-beyond/>

“The State of the Ransom ware 2021”, Sophos, 2021, 18 pp. - <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>

”The True Cost and Impact of Ransomware: How an Attack can Haunt your Business for Years”, Stratosphere Networks, 2022 - <https://www.stratospherenetworks.com/blog/the-true-cost-and-impact-of-ransomware-how-an-attack-can-haunt-your-business-for-years/>

“Vida y muerte de las webs fraudulentas: la mayoría duran menos que una mosca”, Montse Hidalgo, El País – Tecnología, 13.12.2021 - <https://elpais.com/tecnologia/2021-12-13/vida-y-muerte-de-las-paginas-fraudulentas-la-mayoria-duran-menos-que-una-mosca.html>

“White Paper: Surviving Ransomware – what you need to know”, Palo Alto Network, 8 pp., 2022 - <https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/surviving-ransomware>

**NOTAS**

.

1. Digital Information World lo estima en más de 300.000 millones de dólares al año - <https://www.digitalinformationworld.com/2021/08/annual-cost-of-cybercrime-reportedly.html> - Steve Morgan, de Cybersecurity Ventures hablaba en 2.020 de más de 3 billones de euros al año - <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/> [↑](#footnote-ref-2)
2. “Ransomware: unlocking the lucrative criminal business model”, unit-42 – Palo Alto Networks, 2018, 21 pp. - p. 5 “Defining Ransomware”. [↑](#footnote-ref-3)
3. “White Paper: Surviving Ransomware – what you need to know”, Palo Alto Network, 8 pp., 2022 - Ransomware 101: The basics, pp. 2-3 & 4-5. [↑](#footnote-ref-4)
4. “The future of ransomware: 2022 and beyond”, Daniel dos Santos, 22.11.2021, ITProPortal [↑](#footnote-ref-5)
5. Ver “Guía esencial sobre el ransomware”, Patrick Seguin, AVAST Academy, 20.12.2021- y “Ransomware: unlocking the lucrative criminal business model”, unit-42 – Palo Alto Networks, 2018, 21 pp. [↑](#footnote-ref-6)
6. “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions”, US Department of Justice, 06.09.2018 [↑](#footnote-ref-7)
7. “Ransomware as a Service” Explained. What is RaaS?”, David Harrington, 25.02.2022, Varonis. [↑](#footnote-ref-8)
8. “Enfrentándonos al Ransomware”, Manuel López y Jesús Arnáiz, INCIBE, 15.07.2015 - “clasificación del ransomware”. [↑](#footnote-ref-9)
9. “Ransomware: una guía de aproximación para el empresario”, INCIBE, 20.04.2021, 34 pp. - “tipos de ransomware” (pp. 9-10); y “Guía esencial sobre el ransomware”, Patrick Seguin, AVAST Academy, 20.12.2021. [↑](#footnote-ref-10)
10. “Ransomware: unlocking the lucrative criminal business model”, unit-42 – Palo Alto Networks, 2018, 21 pp. - “WannaCry”, p. 14. [↑](#footnote-ref-11)
11. “Ransomware: The True Cost to Business – A Global Study on Ransomware Business Impact”, 2021, Cybereason, 31 pp. - p. 9. [↑](#footnote-ref-12)
12. “Key Learnings Following the Ransomware Attack on Irish Healthcare”, GÉANT Connect, 07.10.2021 [↑](#footnote-ref-13)
13. “Ransomware: ENISA Threat Landscape”, ENISA (European Union Agency for Cybersecurity), 2020, 26 pp. - p. 2. [↑](#footnote-ref-14)
14. “Ransomware: The True Cost to Business – A Global Study on Ransomware Business Impact”, 2021, Cybereason, 31 pp. - p. 2 [↑](#footnote-ref-15)
15. ”Así es Ryuk, el ransomware que ha dejado tumbado al SEPE (y que antes tumbó a otros muchos)”, Javier Pastor, Xataka, 10.03.2021. [↑](#footnote-ref-16)
16. ”El ciberataque al SEPE provocó que sus técnicos trabajaran 19.000 horas extras en jornadas maratonianas y festivos: así levantaron una barricada contra el 'ransomware'”, Alberto R. Aguiar, 02.12.2021, Business Insider [↑](#footnote-ref-17)
17. “Ransomware: The True Cost to Business – A Global Study on Ransomware Business Impact”, 2021, Cybereason, 31 pp. - p. 2 [↑](#footnote-ref-18)
18. “The State of the Ransomware 2021”, Sophos, 2021, 18 pp. ”Key findings”, p.3. [↑](#footnote-ref-19)
19. “Ransomware Impact Report 2021” (+ Infographic), 2021, Keeper, 15 pp. ”Ransomware recovery extracts high indirect costs“, p. 6. [↑](#footnote-ref-20)
20. “The State of the Ransomware 2021”, Sophos, 2021, 18 pp. ”Key findings”, p.3. [↑](#footnote-ref-21)
21. ”Beneath the surface of a cyberattack”, Deloitte, 2017. [↑](#footnote-ref-22)
22. ”The True Cost and Impact of Ransomware: How an Attack can Haunt your Business for Years”, Stratosphere Networks, 2022 [↑](#footnote-ref-23)
23. Sobre las bandas de ciberdelincuentes de ransomware, y sobre las personas que se dedican a negociar con esas bandas, ver “How to Negotiate with Ransomware Hackers”, Rachel Monroe, 31.05.2021, The New Yorker Magazine, June 7, 2021 Issue, <https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers> [↑](#footnote-ref-24)
24. Ver “Vida y muerte de las webs fraudulentas: la mayoría duran menos que una mosca”, Montse Hidalgo, El País – Tecnología, 13.12.2021 - <https://elpais.com/tecnologia/2021-12-13/vida-y-muerte-de-las-paginas-fraudulentas-la-mayoria-duran-menos-que-una-mosca.html> [↑](#footnote-ref-25)
25. ”El FBI atrapa a REvil, la banda de ransomware más famosa, utilizando sus mismos métodos”, Juan Antonio Pascual Estapé, Computer Hoy, 22.10.2021- https://computerhoy.com/noticias/tecnologia/fbi-atrapa-revil-banda-ransomware-952545 [↑](#footnote-ref-26)
26. Ver “DarkSide Ransomware Gang: An Overview”, Ramarcus Bayloer, unit 42- PaloAlto Networks, 12.05.2021 - <https://unit42.paloaltonetworks.com/darkside-ransomware/> [↑](#footnote-ref-27)
27. “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside”, The United States Department of Justice, 07.06.2021 - <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside> [↑](#footnote-ref-28)
28. Ver “Vida y muerte de las webs fraudulentas: la mayoría duran menos que una mosca”, Montse Hidalgo, El País – Tecnología, 13.12.2021 - <https://elpais.com/tecnologia/2021-12-13/vida-y-muerte-de-las-paginas-fraudulentas-la-mayoria-duran-menos-que-una-mosca.html> [↑](#footnote-ref-29)
29. Ver la nota de prensa “US offers 10 M$ reward in hunt for DarkSide cybercrime group”, Reuters, 04.11.2021, - <https://www.reuters.com/technology/us-offers-reward-up-10-mln-information-darkside-cybercrime-group-2021-11-04/> [↑](#footnote-ref-30)
30. Ver “Four emerging ransomware groups take center stage“, Shaun Nichols, Techtarget, 24.08.2021 - <https://www.techtarget.com/searchsecurity/news/252505816/Four-emerging-ransomware-groups-take-center-stage> [↑](#footnote-ref-31)
31. Ver ”Common attack methods” en “White Paper: Surviving Ransomware – what you need to know”, Palo Alto Network, p. 3., 2022 - <https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/surviving-ransomware;> ”Cómo infecta el ransomware un dispositivo”, en “Guía esencial sobre el ransomware”, Patrick Seguin, AVAST Academy, 20.12.2021- <https://www.avast.com/es-es/c-what-is-ransomware;> y en el curso de ransomware de la Plataforma de formación on-line Ángeles del CCN-CERT - https://angeles.ccn-cert.cni.es/index.php/es/menu-formacion-es/cursos-online-ccn-ciberseguridad-menu-es [↑](#footnote-ref-32)
32. Ver ”How ransomware infects networks” en “Breaking down ransomware attacks”, Jeremy Brown & Ashlie Blanca, Unit 42 – Palo Alto Networks, 21.05.2021 - <https://unit42.paloaltonetworks.com/breaking-down-ransomware-attacks/> [↑](#footnote-ref-33)
33. Ver “Breaking down ransomware attacks”, Jeremy Brown & Ashlie Blanca, Unit 42 – Palo Alto Networks, 21.05.2021 - <https://unit42.paloaltonetworks.com/breaking-down-ransomware-attacks/> [↑](#footnote-ref-34)
34. “Symmetric vs. Asymmetric Encryption: What are the Differences”, SSLBuy - <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences#:~:text=Symmetric%20encryption%20uses%20a%20single,and%2el0decrypt%20messages%20when%20communicating> [↑](#footnote-ref-35)
35. “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside”, The United States Department of Justice, 07.06.2021 - <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside> [↑](#footnote-ref-36)
36. Ver “Ransom Payments“, en “Combating Ransomware”, IST (Institute for Security + Technology) – Ransomware Task Force, 23.09.2021 - p. 12, y pp. 47-50 - <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf> [↑](#footnote-ref-37)