Ciberseguridad: en el corazón de la industria del ransomware

LIBRO BLANCO



STORMSHIELD

Los ataques de ransomware van en aumento y amenazan el equilibrio económico y la sostenibilidad de numerosas empresas y organizaciones. Rara es la semana en que una empresa o una administración no sufre un ataque de este tipo y recibe la petición de rescate correspondiente.

En 30 años, hemos pasado de los programas de malware en disquete en los que se reclamaba un pago de unos cien dólares a una industria criminal estructurada, que recauda varios millones cada año mediante extorsión. ¿Cuál es el modus operandi actual de los grupos de ransomware? ¿Cómo llevan a cabo los ciberdelincuentes estos ataques contra las organizaciones? Interrupciones o incluso el cese de la actividad, la divulgación de datos... ¿qué medios de presión utilizan? Y, sobre todo, ¿cómo podemos protegernos?

Este libro blanco repasa la evolución del ransomware y los actores que lo convierten en una amenaza de primer orden. Descifra el funcionamiento de este tipo de software malicioso y proporciona buenas prácticas para mitigar sus consecuencias. Sin ocultar la pregunta central que se hacen la mayoría de estructuras que afrontan el problema: ¿pagar o no? ¿Se debe ceder?

01. Del chantaje a un particular al Big Game Hunting: el ransomware de ayer a hoy

08 — Orígenes previos a Internet (1989-2006)
10 — Una difusión que navega por la Red (2007-2013)
12 — Las primeras revoluciones tecnológicas (2013-2016)
14 — Primeros ataques a nivel estatal globalizados (2017-2018)
16 — La era del Big Game Hunting (2019-2021)
18 — Hacia la estructuración de la ciberdelincuencia (2021-2022)

02. Costes y daños: ¿cuáles son las consecuencias de un ataque de ransomware?

22 — ¿ A quién benefician los ataques de ransomware?
26 — ¿Quiénes son las víctimas?
28 — ¿Qué efectos tienen en las estructuras afectadas?
30 — Pagar o no: ¿se debe ceder?

03. En los engranajes del ransomware: una mecánica fluida

36 — Itinerario de un ransomware
38 — Hincapié en el acceso inicial

04. ¿Qué estrategias pueden establecerse para frenar estas máquinas de hacer dinero?

44 — Protegerse antes del ataque de ransomware
44 — Limitar los daños durante un ataque de ransomware
44 — Recuperarse de un ataque de ransomware

05. ¿Cuál es el futuro del ransomware?

48 — ¿Cómo será el ransomware en el futuro?
50 — ¿Qué soluciones deberían surgir?



01.

Del chantaje a un particular al *Big Game Hunting*: el ransomware de ayer a hoy

La herramienta más mediatizada de los ciberdelincuentes, el ransomware, puede poner en jaque a cualquier empresa u organización, con independencia de su tamaño y nivel de protección. ¿Cómo ha evolucionado esta amenaza en los últimos treinta años? Repasamos un fenómeno en cambio constante.

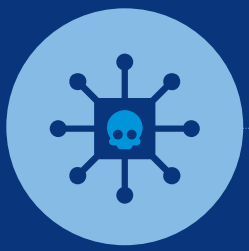
La evolución del ransomware a lo largo del tiempo



1989-2006

ORÍGENES PREVIOS A INTERNET

AIDS TROJAN, PGPCODER



2007-2013

UNA DIFUSIÓN QUE NAVEGA POR LA RED

WINLOCK



2013-2016

LAS PRIMERAS REVOLUCIONES TECNOLÓGICAS

CRYPTOLOCKER, SYPENG



2019-2021

LA ERA DEL BIG GAME HUNTING

MAZE



2017-2018

PRIMEROS ATAQUES A NIVEL ESTATAL GLOBALIZADOS

WANNACRY, NOTPETYA.



2021-2022

HACIA LA ESTRUCTURACIÓN DE LA CIBERDELINCUENCIA

RANSOMWARE-AS-A-SERVICE.

1.1 Orígenes previos a Internet (1989-2006)



1989

Los primeros ataques de ransomware surgieron a finales de la década de 1980. Este software malicioso tenía una sola misión: bloquear el funcionamiento del puesto de trabajo en el seno de las empresas y entre los (pocos) particulares equipados con microordenadores.

Sin embargo, era relativamente fácil rastrear a los atacantes en ese momento gracias a la información de pago. Quince años después, con la aparición de las monedas digitales, el ransomware proliferó a pasos acelerados.
Entre los primeros programas de ransomware distribuidos en Internet, PGPCoder, o «el ransomware de 20 USD», estaba destinado ya en 2005 a infectar los sistemas Windows dirigiéndose a archivos con las extensiones más comunes, como .rar, .zip, .jpg, .doc o .xls. —

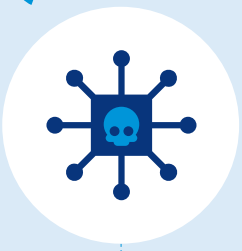
FECHA CLAVE

El primer ransomware, «AIDS Trojan», se envió en 1989 a través de disquetes. Cifra los archivos de las máquinas que infecta después de un cierto número de reinicios e insta a las víctimas a pagar un rescate de 189 USD para recuperar sus datos.

2007-2013

Una difusión que navega por la Red

1.2 Una difusión que navega por la Red (2007-2013)



Scareware

Con la adopción de la mensajería instantánea, las redes sociales, los foros o las redes *peer-to-peer*, el ransomware adquiere nuevos canales de distribución. WinLock, por ejemplo, tenía la particularidad de no cifrar los datos del ordenador infectado. Este bloqueaba el acceso a la máquina mostrando una ventana que contenía una foto pornográfica y una solicitud de pago a través de un servicio de SMS con recargo.

Esta primera evolución del funcionamiento del ransomware se denomina «locker» para reflejar su objetivo: bloquear el inicio del sistema operativo.

En la misma época, aparecieron variantes que usurpaban la imagen de los cuerpos de seguridad, como el ransomware Reveton en 2012. Distribuido en las plataformas *peer-to-peer* o los sitios web de pornografía, se hacía pasar por el FBI bloqueando el ordenador de sus víctimas y exigiendo el pago de una «multa» de 200 USD.

A partir de entonces, las peticiones de rescate pasaron a ser cada vez más creativas para aumentar sus posibilidades de éxito. —



PALABRA CLAVE

Scareware: método de chantaje que simulaba un antivirus muy popular en la década de 2010.

2013-2016

Las primeras revoluciones tecnológicas

1.3 Las primeras revoluciones tecnológicas (2013-2016)



El ransomware CryptoLocker marca un punto de inflexión tecnológica en 2013 con su servidor de comando y control, que permite chatear con la víctima y ejercer aún más presión. Es también uno de los primeros programas de ransomware que exigía un rescate enBitcoin.

Ya que las criptomonedas marcarán un nuevo hito en la evolución del ransomware. Con ellas, y en particular con la llegada del Bitcoin, la anonimización de los destinatarios de los fondos permitirá que la petición de rescate sea imposible de rastrear. Mientras tanto, algunos programas de ransomware como Sypeng encabezaron los primeros ataques a tabletas y móviles Android en 2014 a través de mensajes falsos de actualización del software Adobe Flash. En 2016, comienza la era de los ataques de phishing con Petya, que se dirige a las direcciones de correo electrónico profesionales y se esconde en el interior de un documento Word o PDF. —



27 millones de USD

CIFRA CLAVE

Esta es la cantidad generada por CryptoLocker en sus dos primeros meses de uso.

2017-2018

Primeros ataques a nivel estatal globalizados

1.4 Primeros ataques a nivel estatal globalizados (2017-2018)



Tras la publicación de vulnerabilidades de día cero robadas a un organismo público estadounidense, los ataques de ransomware adquirieron entonces la capacidad técnica de propagarse: así, se extienden masivamente de una empresa a otra cuando coexisten varias redes.

WannaCry se lanzó en 2017 y suscitó una gran cobertura mediática. En pocas semanas, afectó a 300 000 ordenadores en 150 países al propagarse a los sistemas operativos Microsoft Windows a través de la vulnerabilidad EternalBlue.

Unos meses después, el ransomware NotPetya reutilizará algunos de los elementos fundadores de WannaCry (explotación de EternalBlue, desplazamiento lateral) en el contexto del conflicto entre Rusia y Ucrania. Este programa, una auténtica arma de destrucción digital, también camufló los intentos de sabotaje del metro ucraniano[1], el aeropuerto de Kiev, la central nuclear de Chernóbil[2], el banco central y el operador nacional de energía.

Incluso en la actualidad, actores como el grupo chino Bronze Starlight siguen utilizando campañas de ransomware para disimular operaciones de espionaje.

En 2018, el mundo de la ciberseguridad descubrió el ransomware Ryuk, dirigido especialmente a las grandes empresas, un hecho que no augura nada bueno para el futuro... —

«El ransomware era solo fachada. El verdadero objetivo de NotPetya no era la extorsión económica, sino la destrucción de datos a muy gran escala al dirigirse a todo un país ».

PIERRE-OLIVIER KAPLAN — CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

1.5
La era del Big Game Hunting (2019-2021)



Leakware

A finales de 2019, el número de incidentes de ransomware aumentó un 365%. Para evitar el riesgo de detección por las herramientas de seguridad, los ciberdelincuentes abandonan las campañas a gran escala (como WannaCry) y **se centran en las grandes empresas**.

Este modus operandi, basado en el reconocimiento del entorno y la elaboración de escenarios de ataque avanzados, recibe el nombre de «Big Game Hunting» o «caza mayor». Se trata de una estrategia lucrativa, ya que el importe medio de las peticiones de rescate se triplicó durante este periodo y pasó de 13 000 à 36 000 dólares[3].

El mecanismo de la doble extorsión también surgió en esa época. La empresa víctima no solo recibe una petición de rescate, sino también la amenaza de la reventa de sus datos en la darknet. Por si este chantaje no bastase para convencer a los más reacios de pagar el rescate, los ciberdelincuentes revelan parte de los datos críticos robados (código fuente, datos de clientes). Algunas bandas llegan a amenazar a los clientes finales o a los pacientes de estas organizaciones con revelar sus datos personales en el marco de una triple extorsión.

Entre ellos, se encuentra el grupo de los presuntos autores del ransomware Maze. ¿Su particularidad? Una comunicación continua con sus víctimas para ejercer una presión constante.

En 2020, el ataque por Darkside al gigante estadounidense del transporte y distribución de productos petrolíferos Colonial Pipeline amplió el coto de caza del *Big Game Hunting*. El ransomware, que técnicamente se parece a REvil, exige de paso un rescate de 5 millones de dólares. —

«Cuando la presión inducida por el cifrado no es suficiente, los grupos de ransomware recurren a la extorsión amenazando con divulgar los datos sustraídos. Por si no fuera suficiente, también usan ataques de tipo DDoS para obligar a sus víctimas a pagar».

EDOUARD SIMPÈRE — RESPONSABLE DE CYBER THREAT INTELLIGENCE, STORMSHIELD

PALABRA CLAVE

Módulo presente en el ransomware más reciente para robar datos.

IMPORTANTE

Una presión creciente. El grupo ALPHV/BlackCat publica los datos robados en su web .onion, así como en una web clásica cuyo nombre de dominio contiene el nombre de la empresa atacada. Esta, fácil de encontrar, incluso proporciona una función de búsqueda para que sus clientes puedan verificar por sí mismos si su información se ha filtrado.

1.6
Hacia la estructuración de la ciberdelincuencia (2021-2022)



La última revolución en el modus operandi de los ciberdelincuentes es la aparición de las plataformas de Ransomware-as-a-Service (RaaS). Los ciberdelincuentes menos experimentados encuentran allí ransomware de marca blanca para llevar a cabo campañas «llave en mano». Por un porcentaje del rescate cobrado, se benefician de la infraestructura completa de una solución maliciosa desarrollada por otros grupos de ciberdelincuentes. Se trata por tanto de un sector estructurado, donde cada uno desempeña un papel bien definido.

En 2021, aparecen los corredores de acceso inicial (Initial Acces Brokers o IAB). Estos especialistas en la intrusión venden acceso a las redes de empresa para que otros grupos maliciosos lo utilicen para sus propios ataques.

Esta creciente sofisticación de la cadena de ataques se explica por la mejora del nivel de protección de las empresas. Desafortunadamente, la industrialización del ransomware también conlleva la reducción de los plazos de ataque[5]. Hasta el punto de que algunos ya no se molestan en seguir todos los pasos: en marzo de 2022, un grupo de ciberdelincuentes iraníes[6] envió su petición de rescate a la imprenta local de una administración estadounidense sin infectar antes los puestos de trabajo. —

FECHA CLAVE

Durante dos días, la Casa Blanca reunió a decenas de países, como Francia y Alemania, en una cumbre destinada a encontrar soluciones al problema global del ransomware. ¿Una medida suficiente para tomar por fin las riendas del problema?

CIFRA CLAVE

X2

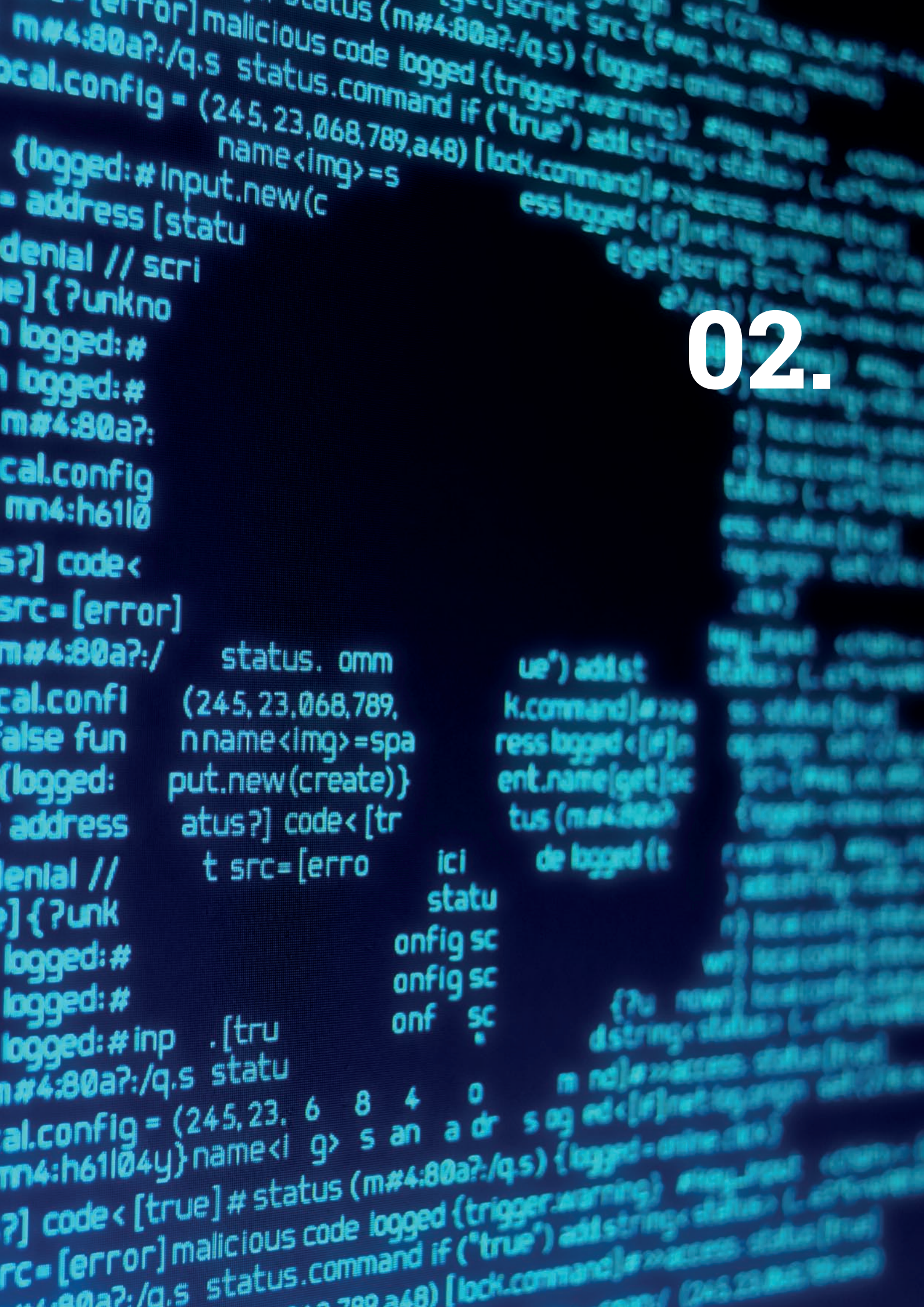
A nivel mundial, los ataques de ransomware se duplicaron en 2021[4].

PARA PROFUNDIZAR

LA HISTORIA DEL RANSOMWARE

Descubra la historia del ransomware con más detalle en nuestro artículo específico[7].

Octubre de 2022


02.

Costes y daños: ¿cuáles son las consecuencias de un ataque de ransomware?

Un ataque de ransomware rara vez carece de consecuencias para las víctimas. Más allá de las pérdidas financieras, desestabiliza toda la cadena de valor de las organizaciones. Nos adentramos en los misterios de un ataque, sus costes y daños.

2.1 ¿Quién se beneficia de los ataques de ransomware?

Durante las tres últimas décadas, el mundo del ransomware se ha estructurado. Las bandas de ciberdelincuentes van y vienen, pero su pericia creciente está más que demostrada.



Los grupos de ransomware se dividen en diferentes «familias» repartidas por todo el mundo. De las 100 familias o variantes identificadas por el FBI[8], muchas proceden de bandas con sede en Asia y Europa del Este. En Francia, hay una treintena de grupos de ransomware activos, con los nombres tristemente conocidos de LockBit, Conti, ALPHV/BlackCat o incluso Hive.

Los grupos de ciberdelincuentes, a menudo vinculados a la actualidad geopolítica, aparecen y desaparecen a una velocidad vertiginosa. Tras anunciar su apoyo a Rusia, el grupo Conti experimentó una auténtica serie de filtraciones de datos: se divulgaron los registros de chats internos, su código fuente y otros archivos utilizados por el grupo. Cerró su web insignia en 2022[9]; muy rápido para un grupo descubierto en 2020, si bien podría reaparecer adoptando otras formas, como sugieren las señales de vida de su filial Karakurt en junio[10]. Esto recuerda el ejemplo del grupo REvil, desmantelado en enero de 2022, que volvió a escena unos meses después[11].

En resumen, la industria del malware se está estructurando y, con ella, está surgiendo una verdadera economía paralela de amenazas cibernéticas con actividades diferenciadas. El desarrollo del mercado de los ciberataques es tal que *«hoy podemos hablar de una economía paralela»* explica Sébastien Viou, director de productos de ciberseguridad y consultor en Stormshield. —

«Ahora nos enfrentamos a la ciberdelincuencia organizada con sus foros de venta que aglutinan diferentes perfiles: los que encuentran vulnerabilidades, los que irrumpen en los sistemas, los que desarrollan el malware, etc. Estos canales también permiten captar operadores para llevar a cabo la intrusión».

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

INFORMACIÓN CLAVE

PERFILES JÚNIOR

La franquicia de ransomware Conti forma así a perfiles «júnior», les ofrece un salario fijo y un plan de participación en los beneficios.

PANORÁMICA DE LOS GRUPOS DE RANSOMWARE

El cofundador de Hackers sin Fronteras, Clément Domingo, ha identificado a poco más de la mitad de los grupos de ciberdelincuentes del planeta.

- → ALPHV
- → Ako
- → Arvin Club
- → Astro Team
- → AtomSilo
- → Avaddon
- → AvosLocker
- → Babuk
- → Babuk Locker
- → Bl4ckt0r
- → Black Shadow
- → BlackByte
- → Bonaci Group
- → CRYP70N1C0D3
- → Clop
- → Conti
- → Cuba
- → DarkLeaks
- → DarkSide
- → DoppelPaymer
- → Dotadmin
- → Egregor
- → Entropy
- → Everest
- → Exorcist
- → Grief
- → HARON
- → Hive
- → LV
- → LockBit
- → LockBit 2.0
- → LockData Auction
- → Lorenz
- → Maze
- → Medusa Locker
- → Midas
- → Mount Locker
- → Nefilim
- → Nemty
- → NetWalker
- → Night Sky
- → Pay2Key
- → payload.bin
- → Prometeus
- → Pysa (Mespinoza)
- → Qlocker
- → Quantum
- → REvil (Sodinokibi)
- → Ragnar Locker
- → Ramp
- → Ransom Cartel
- → RansomEXX
- → Ranzy Locker
- → Rook
- → Sekmet
- → Snatch
- → SunCrypt
- → Suncrypt
- → Vice Society
- → Xing

¡ATACANTES Y ATACADOS DESARROLLAN SUS COMPETENCIAS!

ENTREVISTA **FLORENT CURTET**
— ESTE ANTIGUO HACKER RECONVERTIDO SE DEDICA AHORA A LA AYUDA EN CIBERCRISIS Y ES FORMADOR DE CUERPOS DE SEGURIDAD, BUFETES DE ABOGADOS E INCLUSO DELEGADOS DE PROTECCIÓN DE DATOS EN ESTE NUEVO ARTE DE LAS NEGOCIACIONES



→ Los actores del ransomware se especializan: desarrollo, actualización, conversaciones con las víctimas, blanqueo de capitales en el medio virtual... cada uno desempeña una función específica en la era del RaaS y la afiliación. También en cuestión de seguridad están surgiendo nuevas habilidades, como lo ilustra la trayectoria atípica de Florent Curtet, director general de NeoCyber y cofundador de Hackers sin Fronteras.

¿Cuál ha sido tu mayor logro en materia de negociación?

F.C. — Mis métodos permitieron reducir drásticamente el importe del rescate desde 1 millón a 100.000 €, por ejemplo. Pude convencer a los ciberdelincuentes de que entregaran su botín en el contexto particular del ámbito médico.

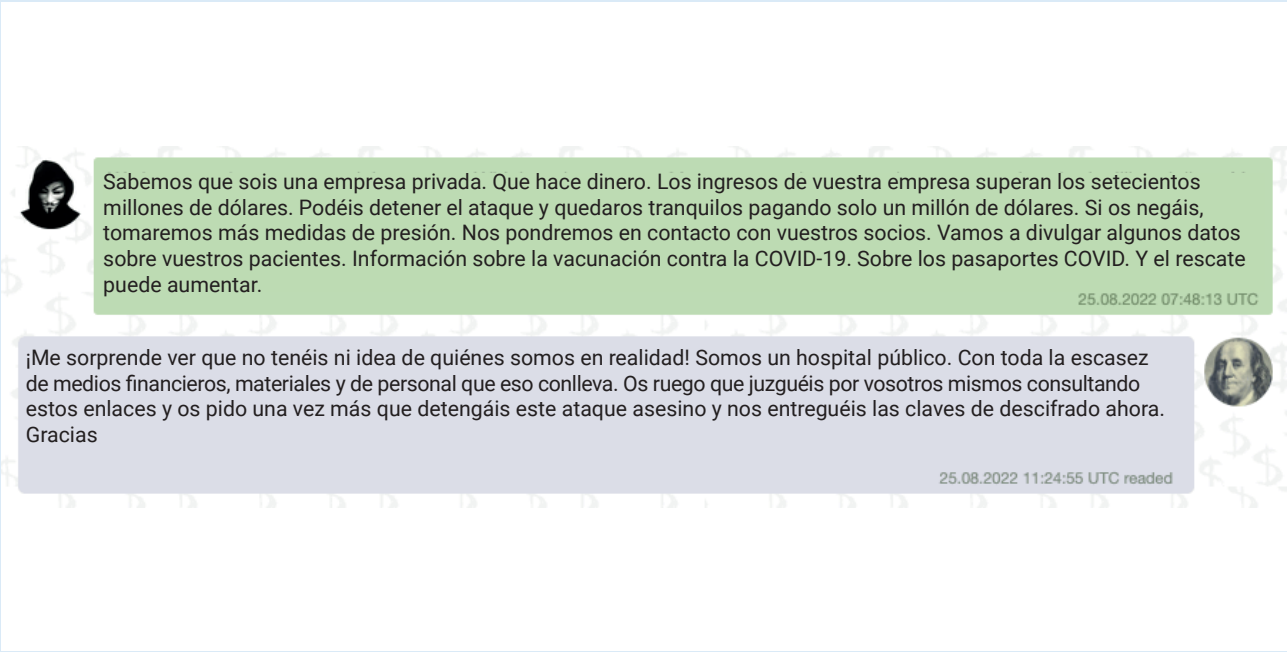
¿Qué métodos utilizaste?

F.C. — Inicialmente, el problema reside en las herramientas de comunicación. Por lo general, los ciberdelincuentes se ponen en contacto con su víctima por correo electrónico. Mi objetivo era desplazar la conversación a Tox, un servicio de mensajería en tiempo real, para establecer una relación más continuada. Esto los mantiene ocupados para ahorrar tiempo, les muestra que estamos allí y nos permite empezar a entender su estrategia.

¿Cuál es el perfil de los ciberdelincuentes con los que negocias?

F.C. — Aunque suelen estar supervisados por personas más experimentadas, en general siguen siendo perfiles bastante jóvenes e influenciables.

«Me parece que hacía falta pedagogía en ambos lados».



LEYENDA

En el caso del ataque del CHSF, el ciberdelincuente parece convencido de que está tratando con una empresa privada[14].

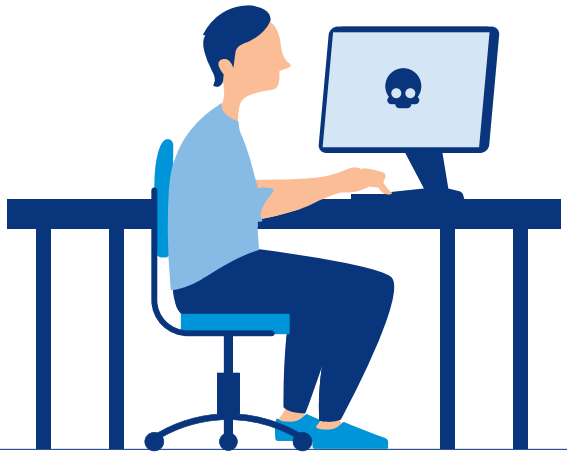
El papel de negociador puede parecer confuso, especialmente en un contexto en el que la Agencia nacional francesa de Seguridad de los Sistemas de Información (ANSSI) desaconseja encarecidamente pagar el rescate en caso de un ataque de ransomware. ¿Por qué elegiste desarrollar esta pericia?

F.C. — Me parece que hacía falta pedagogía en ambos lados. Históricamente, la negociación cibernética consistía principalmente en explicarle a la empresa víctima qué era el bitcoin, la red Tor, etc. Al chatear con ciberdelincuentes, a veces me encontraba explicando la diferencia entre ingresos y beneficios o redefiniendo la actividad de la empresa. De hecho, podemos encontrarnos rápidamente en una zona gris, de ahí la importancia de supervisar esta actividad para evitar problemas. Sin embargo, me parece que la negociación es una respuesta pragmática en un contexto en el que determinadas estructuras de menor envergadura se enfrentan a una triple sanción: bloqueo de sus actividades, divulgación de sus datos o incluso una posible multa por parte de la autoridad de protección de datos en caso de incumplimiento del RGPD. —

«Podemos encontrarnos rápidamente en una zona gris, de ahí la importancia de supervisar esta actividad para evitar problemas».

2.2 ¿Quiénes son las víctimas?

El ransomware ha demostrado su capacidad de interrumpir la actividad de cualquier empresa y comunidad, con independencia de su tamaño y nivel de protección. Sin embargo, ¿hay perfiles o sectores a los que se dirige en particular? Proponemos algunas pistas.



Todo el tejido económico mundial se ve afectado por la amenaza del ransomware, desde las microempresas hasta las grandes multinacionales. En Europa, una de cada dos empresas víctimas de ransomware es una pyme o microempresa[15]. En Francia, una de cada tres pymes ya ha sufrido un ataque de este tipo[16]. Sin embargo esto es solo la punta del iceberg: ¿cuántos ataques de ransomware no declarados hay por cada ataque declarado?

Todos los sectores se ven afectados. Aunque los ataques son menos numerosos en ciertos momentos, generalmente se dirigen y concentran en ciertos sectores, en particular la fabricación, la tecnología y las finanzas[17].

Cuando no son un objetivo directo, las empresas también pueden sufrir daños colaterales como consecuencia de los ataques de ransomware sufridos por sus proveedores. —

11 millones de dólares[18]

«Nadie está a salvo de los ciberdelincuentes que llevan a cabo ataques basados tanto en la pesca de arrastre (ataques masivos a estructuras mal protegidas para interrumpir su actividad) como en la de anzuelo (acciones dirigidas a atacar la imagen de marca o el saber hacer industrial de los actores mejor protegidos)».

FLORENT CURTET — DIRECTOR GENERAL DE NEOCYBER Y COFUNDADOR DE HACKERS SIN FRONTERAS

CIFRA CLAVE

Esta es la cantidad pagada por el gigante agroalimentario brasileño JBS[19], paralizado en 2021 por un ataque de ransomware del grupo REvil.

SECTORES MÁS AFECTADOS POR ATAQUES DE RANSOMWARE EN 2022



Fuente: Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

2.3 ¿Qué efectos tiene en las estructuras afectadas?

Más allá de la pérdida de datos, las organizaciones víctimas se enfrentan a otras consecuencias que pueden prolongarse: paralización de la producción, caída de la facturación, riesgos jurídicos, pérdida de confianza de los clientes, etc.



Como su propio nombre indica, la consecuencia lógica de un ataque de ransomware es la petición de un rescate. Sin embargo, esta no es la única consecuencia para las víctimas. En la mayoría de los casos, solo se darán cuenta de la interrupción de su actividad o incluso el cese de su producción. Esto a su vez conducirá a una pérdida de volumen de negocio o incluso al cierre de la empresa en los casos más extremos.

Además, los datos no se libran. Pueden verse amenazados con ser revelados, dañados o incluso destruidos. En cualquier caso, cuando los ciberdelincuentes acceden a los datos, exponen a las empresas víctimas a un riesgo jurídico si se demuestra un incumplimiento del RGPD. Finalmente, la reputación de una empresa a menudo se ve perjudicada por un ataque de ransomware.

Entre las consecuencias más indirectas, los investigadores[20] indican que la presión sobre los profesionales de seguridad informática debido a la amenaza del ransomware contribuye al aumento de la rotación en el seno de estos equipos. —

De 2.a 3 millones de euros

CIFRA CLAVE

Este es el coste estimado del ataque de ransomware que afectó a Clestra Hauserman en abril de 2022. El fabricante alsaciano de mamparas para oficinas y «salas limpias», ya en apuros por la situación económica y geopolítica, se vio sometido a un proceso de administración judicial[21] durante un periodo de seis meses.

+71%

CIFRA CLAVE

EL IMPORTE DE LOS RESCATES VA EN AUMENTO…

500 dólares en 2016, 300.000 dólares en 2020, casi 1 millón de dólares durante los 5 primeros meses de 2022 (es decir, un 71% más que en 2021).

PARA PROFUNDIZAR

EFECTOS PSICOLÓGICOS

La principal consecuencia de un ciberataque de ransomware es obviamente financiera, ¿pero es realmente la única? Al afirmarlo, olvidaríamos las dimensiones social y psicológica de los ataques, que se pasan por alto (demasiado) a menudo.

2.4 Pagar o no, ¿se debe ceder?

¿Pagar o no? ¿Ceder o no ante una petición de rescate? Esta pregunta espinosa les ha quitado el sueño a un buen número de profesionales en puestos de decisión, ya que esta toma de decisiones afecta a la salud financiera de la estructura, su actividad, así como a su reputación y su ética.



CIFRA CLAVE

80%

Alrededor del 80% de las empresas que pagan el rescate exigido vuelven a ser atacadas[23].

¿Cuáles son las empresas que pagan el rescate solicitado? La respuesta es delicada porque pocas de ellas reconocen la operación. Descifrar antes que reconstruir, o incluso desaparecer: las estructuras más pequeñas no dudarán mucho, ya que de ello puede depender su supervivencia... Las empresas más grandes se doblegarán más por cuestiones ligadas a su reputación o a sus resultados financieros. Con independencia de la razón, pagar un rescate suele ser el último recurso. También es importante recordar que haber pagado ya el precio de un ataque con ransomware no protege frente a otro nuevo. Una empresa británica[22] se vio obligada a pagar un rescate dos veces con pocas semanas de diferencia.

En Francia, la luz verde otorgada por el Ministerio de Economía galo para la indemnización de rescates por parte de las aseguradoras, previa presentación de una denuncia, podría tener efectos adversos, además de incrementar la confusión en torno al mensaje de la autoridad nacional en la materia, la ANSSI[24]. —

«El texto tiene el mérito de existir y hacer que la gente hable sobre el tema en las altas esferas, pero no cambiará el problema de fondo. Un punto positivo es que debería poner fin a las operaciones de pago de rescates «encubiertas» para evitar posibles sanciones de la Comisión nacional francesa de Informática y Libertades (CNIL)[25]».

SÉBASTIEN VIOU — DIRECTOR DE CIBERSEGURIDAD DE PRODUCTOS Y CONSULTOR CIBER DE STORMSHIELD

PODCAST

RANSOMWARE: ¿HAY QUE ASEGURARSE Y PAGAR?

Sobre esta espinosa cuestión, ¿qué mejor que un podcast realizado por expertos? Valéry Rieß-Marchive, redactora jefe de MagIT, Fabrice Epelboin, Damien Douani y Bertrand Lenotre[26] se pronuncian sobre la justificación de este proyecto legislativo.

ACTUALIDAD

LA INDEMNIZACIÓN DE LAS EMPRESAS VÍCTIMAS DE RANSOMWARE: EL DELICADO TEMA DE LOS CIBERSEGUROS



Todo comenzó en junio de 2021. Bruno Le Maire, ministro francés de Economía, Finanzas y Soberanía Industrial y Digital y la Dirección General del Tesoro en Francia formaron un grupo de trabajo sobre el desarrollo de una oferta de seguros para cubrir los riesgos cibernéticos, para reunir a los servicios del Estado, los representantes de empresas, las aseguradoras y reaseguradoras y los expertos del mundo académico.

Este articuló un plan de acción en torno a 4 ejes:

- → **aclarar el marco jurídico para asegurar el riesgo cibernético;**
- → **comprender y medir mejor el riesgo cibernético;**
- → **mejorar el reparto del riesgo entre los asegurados, las aseguradoras y las reaseguradoras;**
- → **aumentar los esfuerzos en materia de sensibilización.**

A raíz de este informe, el Ministerio de Economía y Finanzas francés propuso al Consejo de Ministros, a finales de 2022, una medida dedicada a los ciber rescates en el marco del proyecto de ley de orientación y programación del Ministerio del Interior (LOPMI).

La única condición: que la empresa víctima presentara una denuncia en un plazo de 48 horas tras el descubrimiento del ataque informático. Posteriormente, el texto seleccionado por la Comisión Jurídica (en el seno de la Asamblea Nacional) prescindía de la palabra «rescate» en favor de una terminología más amplia del daño causado por un ciberataque.

Tras la publicación de esta información se alzaron numerosas voces, destacando los diversos riesgos y áreas de incertidumbre que conllevaba este enfoque. Incertidumbres sobre el rescate en sí: ¿quién pagará? ¿La empresa directamente o un intermediario, como un negociador, por ejemplo? ¿Cómo se organizan estos últimos? ¿Qué cantidades se deben reembolsar? Y las posibles consecuencias: ¿aumentará el importe de los rescates? ¿Las empresas francesas estarán más en el punto de mira? Si bien aún es demasiado pronto para responder estas preguntas, seguirán siendo cruciales en el futuro.

Al contrario, otros destacan un aspecto beneficioso del pago de los rescates (como una mejor evaluación de los flujos financieros, que pueden convertirse en pistas para la caza de los ciberdelincuentes), pero el debate sigue más abierto que nunca. —

ENTREVISTA

RESCATE: PAGAR O NO, ¿EL INTERROGANTE SE PLANTEA TODAVÍA HOY?

→ La recomendación oficial de la ANSSI es clara: no hay que pagar el rescate solicitado. Sin embargo, en Francia una de cada cinco empresas atacadas cedió en 2021. ¿Por qué?

¿POR QUÉ NO SE DEBE PAGAR EL RESCATE?

«Muchas empresas piensan que esta es la mejor manera de restaurar el servicio lo más rápido posible, pero no es necesariamente así. Muy a menudo, la herramienta de descifrado diseñada por el atacante tiene errores. Además, la falta de confianza requiere pasar por una fase de análisis antes de restaurar los datos. Hay que tener en cuenta que la restauración de datos sigue siendo el método más seguro para recuperar los datos: de media, solo el 54% de las estructuras que pagan recuperan sus datos[28]».

ARNAUD PILON —
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

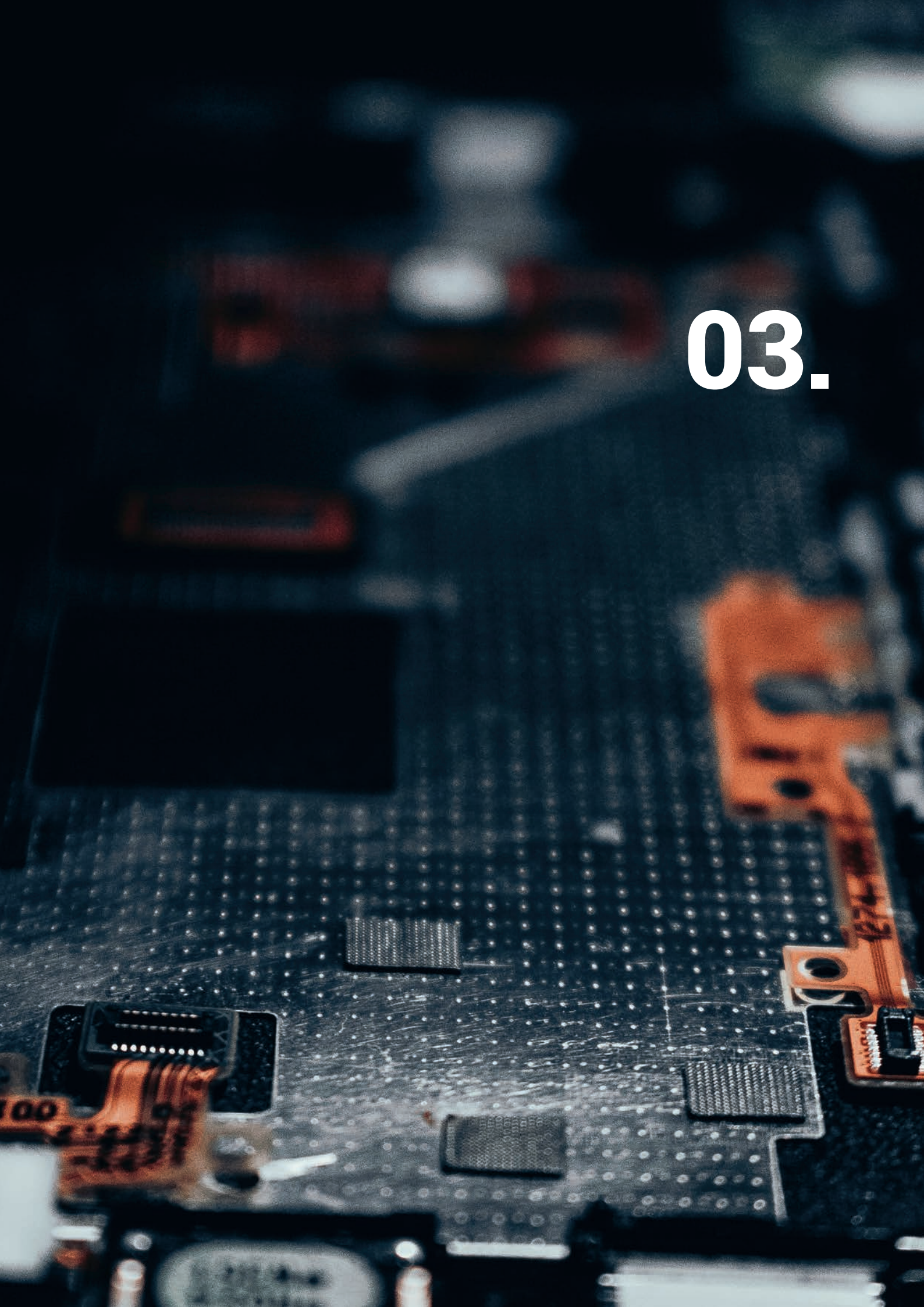
«Desde un punto de vista ético, el pago también puede verse como una validación del modelo. Aquí también surge la polémica en torno al modelo de riesgos de las aseguradoras».

NICOLAS CAPRONI —
HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

¿POR QUÉ ALGUNAS EMPRESAS NO TIENEN ELECCIÓN?

«Las víctimas a veces son empresas muy jóvenes que aún no han podido invertir en la copia de seguridad de sus datos. Para ellos, el pago es una cuestión de supervivencia. En lugar de condenar a estas estructuras acorraladas, las autoridades podrían utilizar el seguimiento de los pagos para desmantelar las bandas de ransomware y pensar paralelamente en el establecimiento de una especie de inspección técnica cibernética. ¿Por qué no introducir un crédito fiscal que permita auditar la seguridad de las empresas jóvenes?».

FLORENT CURTET —
DIRECTOR GENERAL DE NEOCYBER
Y COFUNDADOR DE HACKERS SIN FRONTERAS



03.

En los engranajes del ransomware: una mecánica fluida

Diferentes terminales pueden ser el objetivo del ransomware: un ordenador, un teléfono móvil, un autómata en una fábrica, una bicicleta conectada en un gimnasio... Pero, ¿qué sucede realmente cuando se produce un ataque de este tipo?

3.1 Itinerario de un ransomware

¿Cómo se propaga el ransomware? ¿Cuáles son sus principales recursos? Acceso inicial e infección, camuflaje, búsqueda de vulnerabilidades explotables... El proceso abarca varias fases estratégicas bien definidas.



Históricamente, el término «ransomware» se refería principalmente a los «blockers», mecanismos que bloqueaban el acceso al sistema y a los «crypto», elementos que cifraban los datos.

En la actualidad, se aplica a todos los programas que permiten la extorsión. Se trata de un tipo de ataque complejo que se basa en diferentes mecanismos y diferentes tiempos. Sin embargo, estos ataques siempre parten de una infección inicial. Esta se puede lograr mediante phishing, descargas peer to peer, descargas ocultas (drive by download), explotación de una vulnerabilidad, etc.

Luego viene la fase de ataque propiamente dicha, durante la cual, el «dropper» crea una puerta trasera en el sistema que permite instalar todas las herramientas necesarias para el ataque eludiendo los mecanismos de detección antes de que el «loader» se asegure de su correcta ejecución.

Posteriormente, el ciberdelincuente entra a la fase de evasión de defensas, durante la cual, trata de ocultar el rastro de su intrusión para que la puerta trasera sobreviva al reinicio. La siguiente etapa, el *acceso a las credenciales*, permite al atacante recuperar el acceso robando los nombres de cuenta y las contraseñas.

Entonces, comienza una fase que dura de unas horas a unos meses (*Discovery* o descubrimiento de redes), durante la cual los ciberdelincuentes buscan puntos de entrada para expandirse mediante movimientos laterales. Estas puertas de entrada pueden ser contraseñas robadas previamente, vulnerabilidades explotables o malas configuraciones de seguridad. A continuación, identifican archivos con datos de valor (*Collection*) y los cifran, a veces extrayéndolos de antemano y borrando las copias de seguridad.

El paso final consiste en presionar a la víctima mediante la publicación de elementos que demuestran el ataque, como capturas de pantalla en el sitio web de la banda, generalmente en la red Tor. En ocasiones, los ciberdelincuentes también realizan un ataque de denegación de servicio en paralelo, lo que constituye una fuente de presión adicional para incitar a la víctima a pagar más rápido y evitar que la empresa se comunique en su web institucional, por ejemplo. —

PALABRA CLAVE

Un dropper (cuentagotas en español) es un programa informático diseñado para instalar software malicioso en un sistema. El loader se encarga de su ejecución.

Dropper

¿CÓMO SE PUEDE EXPLICAR DE UNA FORMA SIMPLE EL MECANISMO DEL RANSOMWARE?

ACCESO INICIAL

↓

EJECUCIÓN
INTERFAZ DE LÍNEA DE COMANDOS

↓

PERSISTENCIA

↓

ESCALADA DE PRIVILEGIOS

↓

EVASIÓN DE DEFENSAS
ARCHIVO HTML COMPILADO

↓

ACCESO A LAS CREDENCIALES
CLAVES PRIVADAS

↓

DESCUBRIMIENTO
DESCUBRIMIENTO DEL PROCESO

↓

MOVIMIENTO LATERAL

↓

RECOPILACIÓN
SISTEMA LOCAL DEL FORMULARIO DE DATOS

↓

COMANDO Y CONTROL

↓

EXTRACCIÓN
DATOS COMPRIMIDOS

↓

IMPACTO
DATOS CIFRADOS PARA CREAR IMPACTO

Fuente: marco MITRE ATT&CK

3.2 Hincapié en el acceso inicial

Una vez identificada la empresa víctima, el ciberdelincuente comienza un minucioso trabajo para penetrar en el sistema de información de la empresa. En busca del preciado «ábrete Sésamo»; es decir, el famoso acceso inicial.





Una vez identificada la empresa víctima, el ciberdelincuente comienza un minucioso trabajo para penetrar en el sistema de información de la empresa. En busca del preciado «ábrete Sésamo»; es decir, el famoso acceso inicial.

Este es la piedra angular de los grupos de ransomware, ya que se utiliza para penetrar en el sistema de información de sus futuras víctimas y requieren una larga fase de reconocimiento. «*El estudio de objetivos va más allá del simple estudio técnico de la superficie de ataque expuesta en Internet,* detalla Valéry Marchive en un artículo[29] publicado en Le Mag IT. *Se trata en particular de obtener coordenadas que permitan contactar con cada una de las personas identificadas, probablemente para ejercer presión después de que se haya activado el ransomware* ».

Para recuperar todos estos datos, se utilizan varias técnicas. Más o menos elaborados, los **correos electrónicos de phishing** son el vector por excelencia. Al mismo tiempo, también se movilizan otros canales para utilizar técnicas de ingeniería social similares, como la mensajería de LinkedIn, por ejemplo.

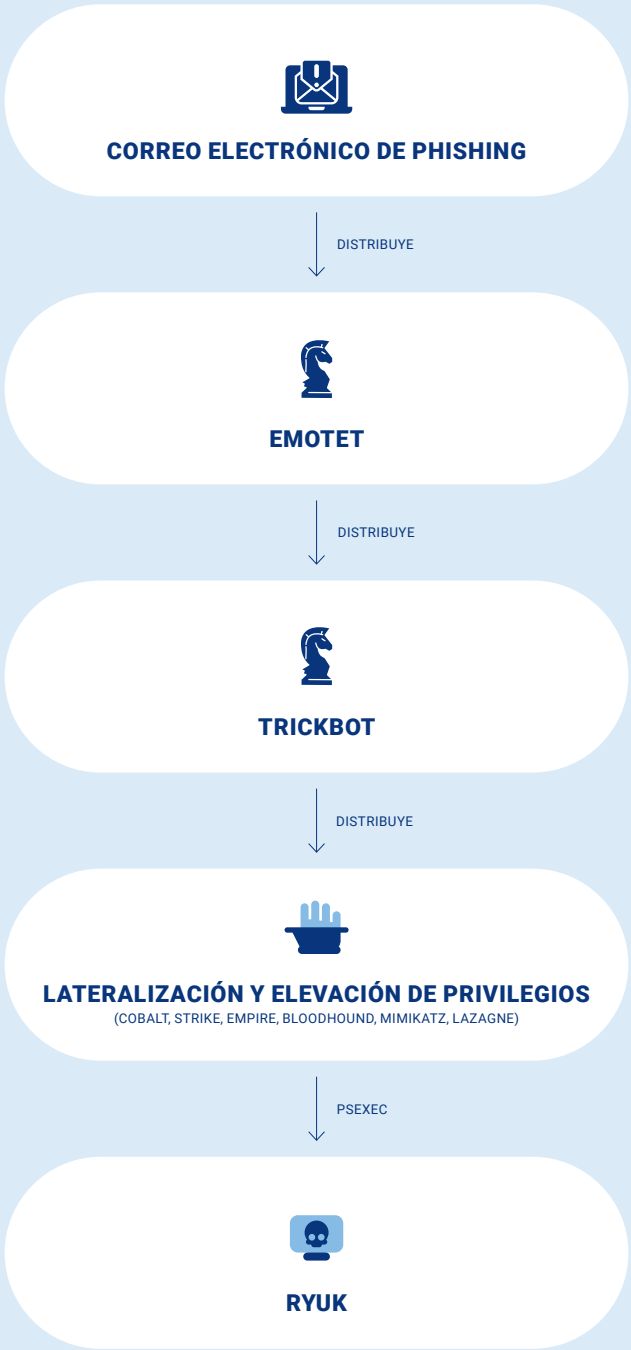
PARA PROFUNDIZAR

RANSOMWARE: CÓMO PREPARAN LOS CONTI SUS CIBERATAQUES.

Un artículo para entender cómo el grupo Conti recupera el acceso inicial a los sistemas de información de numerosas organizaciones en todo el mundo.

EL RANSOMWARE TAMBIÉN SE INTEGRA EN UNA CADENA MÁS COMPLEJA

SECUENCIA SIMPLIFICADA DE LA CADENA DE INFECCIÓN EMOTET-TRICKBOT-RYUK



Fuente: Informe «Le rançongiciel Ryuk», ANSSI, 2021

Sin embargo el software utilizado en las empresas también puede ser parte de su superficie de ataque cuando, sin saberlo, incorpora una vulnerabilidad, a menudo explotada durante la fase de replicado.

«No es raro que los ciberdelincuentes utilicen otros programas de malware como Emotet, Trickbot o el loader Bumblebee antes de su ataque».

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

«Las tecnologías funcionan cada vez más como una interfaz. Aquí, Emotet actúa como un troyano: obtiene el código que proporciona el atacante y luego se propaga como un gusano informático, así que es un medio más que un fin. Trickbot, por otro lado, es un botnet que se infiltra en el cliente, espera instrucciones de Emotet y las ejecuta».

PIERRE-OLIVIER KAPLAN — INGENIERO DE INVESTIGACIÓN Y DESARROLLO, STORMSHIELD

Otro factor que hace que los ataques sean más complejos es la proliferación a través de la cadena de suministro: los ciberdelincuentes comprometen cadenas de suministro completas al atacar las vulnerabilidades del software de gestión o los servicios en la nube. Así, en mayo de 2021, el editor de soluciones TI Kaseya fue víctima de REvil. Más de 1.500 empresas se vieron afectadas a través de las redes de 60 de sus clientes y el rescate exigido ascendió a 70 millones de dólares[30]. —

+1.500

CIFRA CLAVE

Más de 1.500 empresas se han visto afectadas tras la infección del software del editor Kaseya


04.
SYSTEM
HACKED

¿Qué estrategias pueden establecerse para frenar estas máquinas de hacer dinero?

El ransomware se ha convertido en la pesadilla de los departamentos de informática y de las empresas en general. Sin embargo, ¿son una fatalidad? Preguntamos a Sébastien Viou, director de Ciberseguridad de Producto y Consultor de Stormshield, cuáles son las medidas que deben tomarse para afrontarlo.

01

PROTEGERSE ANTES DEL ATAQUE DE RANSOMWARE

- **HACER UNA COPIA DE SEGURIDAD DE LOS DATOS... Y PROTEGER LAS COPIAS DE SEGURIDAD[31]**
  «Esta precaución por sí sola no es suficiente, porque es lo primero que el ransomware intentará destruir, incluso antes del cifrado. Hay que hacer copias de seguridad sin conexión y trabajar cuidadosamente la frecuencia de estas copias de seguridad. También es necesario probar las restauraciones para asegurarse de que las copias de seguridad se puedan utilizar».

- **MANTENER EL SOFTWARE Y LOS SISTEMAS ACTUALIZADOS**
  «Las actualizaciones deben realizarse continuamente e incluir los PC Windows, así como los sistemas Linux y Mac, que también pueden ser puntos de entrada. Esto abarca toda la ofimática, desde Microsoft Exchange hasta Active Directory, incluidos todos los servidores expuestos, aunque sean pequeños».

- **COMPARTIMENTAR EL SISTEMA DE INFORMACIÓN**
  «Se recomienda para ello aplicar reglas estrictas de flujos autorizados entre diferentes zonas según su criticidad».

- **LIMITAR LOS DERECHOS DE LOS USUARIOS Y LOS PERMISOS DE LAS APLICACIONES**
  «En este sentido, la gestión a lo largo del tiempo es decisiva: para poder mantener la seguridad, se deben planificar revisiones periódicas».

- **LLEVAR A CABO LA SUPERVISIÓN DE LOS REGISTROS**
  «La recopilación de logs es obligatoria. En los casos en que se requiera un nivel de seguridad muy alto, es posible agregar un componente de detección de intrusos a través de un SOC».

- **SENSIBILIZAR A LOS EMPLEADOS**
  «Con la ingeniería social, el principal punto de entrada al sistema de información de una empresa siguen siendo sus empleados. Por lo tanto, es importante abordar los temas de ciberseguridad, aunque la sensibilización tenga sus límites».

8%

Esta es la proporción de empleados de la Organización Europea para la Investigación Nuclear (CERN) que quedaron atrapados durante una campaña de phishing falsa, llevada a cabo después de una campaña de sensibilización[32].

- **PENSAR EN LA ESTRATEGIA DE COMUNICACIÓN DE CRISIS CIBERNÉTICA**
  «Aquí, nuevamente, es útil haber trabajado en los mensajes y contactos con anterioridad para comunicarse adecuadamente con las diferentes audiencias. Las comunicaciones deben servir para advertir de una interrupción inesperada de la producción, por ejemplo, o incluso de fugas de datos personales, tal y como establece el RGPD ».

- **ESTABLECER UN PLAN DE RESPUESTA A CIBERATAQUES**
  «Este plan es crucial, porque permite reaccionar rápidamente contactando lo antes posible, por ejemplo, con las empresas CERT identificadas de antemano. Obviamente incluye un componente técnico mediante la implantación de soluciones de protección como Stormshield Endpoint Security Evolution y Stormshield Network Security».

- **EVALUAR EL INTERÉS DE SUSCRIBIR UN CIBERSEGURO**
  «Algunos ciberseguros incluyen cláusulas de despliegue de soluciones de ciberseguridad; son interesantes en este sentido, porque imponen cierta protección. Sin embargo, el ciberseguro no debe considerarse como una medida de supervivencia suficiente por sí sola, y menos como una medida de protección. En otras palabras, el seguro contra el ransomware nunca constituye una estrategia de ciberseguridad».

02

LIMITAR LOS DAÑOS DURANTE UN ATAQUE DE RANSOMWARE

- **ADOPTAR LOS REFLEJOS ADECUADOS**
  «Hay que ser capaz de detectar rápidamente que algo va mal y no dudar en desconectarlo todo para mitigar el riesgo y contener la propagación al máximo. A nivel individual también hay que aprender a reaccionar, a decir «he hecho clic donde no debía» porque cada minuto cuenta».
- **LIDERAR LA GESTIÓN DE LA CIBERCRISIS DESDE EL COMITÉ EJECUTIVO**
- **COMUNICARSE AL NIVEL ADECUADO**
- **DENUNCIAR**

03

RECUPERARSE DESPUÉS DE UN ATAQUE DE RANSOMWARE

- **RESTAURAR LOS SISTEMAS DESDE FUENTES LIMPIAS**
- **INVESTIGAR LA RUTA DE ATAQUE SEGUIDA**
  «Para comprender cómo se ha desarrollado el ataque y las debilidades de su propio sistema, hay que analizar lo sucedido. De esta manera, tendremos todas las posibilidades de evitar que vuelva a suceder».
- **ELABORAR UN PLAN DE CORRECCIÓN**
  «Dependiendo del caso, ¿puede ser necesario configurar la autenticación multifactorial o mejorar las soluciones de seguridad presentes en los puestos de trabajo?».
- **COMUNICAR EL SINIESTRO AL SEGURO**
- **APLICAR EL PLAN DE COMUNICACIÓN ENTRE LOS CLIENTES AFECTADOS, LOS INVERSORES, ETC.**
- **GESTIONAR EL IMPACTO PSICOLÓGICO PARA LOS EMPLEADOS**
  «Paro técnico, culpabilidad, sobrecarga de los equipos de informática... el ransomware también tiene consecuencias en los recursos humanos y hay que tenerlas en cuenta».
- **EMPRENDER ACCIONES LEGALES SI AÚN NO SE HA HECHO**
- **ESTABLECER UN PLAN DE PRODUCCIÓN PARA PONERSE AL DÍA TRAS EL RETRASO ACUMULADO**

¿QUÉ PROPORCIONA STORMSHIELD ENDPOINT SECURITY EVOLUTION FRENTE A LOS ATAQUES DE RANSOMWARE?

→ SES Evolution comprende funcionalidades particularmente útiles en la lucha contra la amenaza del ransomware: detección del cifrado de archivos, protección de copias de seguridad automáticas y contra inyecciones de DLL, análisis conductual o bloqueo en tiempo real de procesos ante un comportamiento anómalo. —

PARA OBTENER MÁS INFORMACIÓN, CONSULTE ESTE VÍDEO


05.

¿Cuál es el futuro del ransomware?

¿Cuál será el objetivo futuro del ransomware? ¿Se centrará en los monederos de criptomonedas? ¿En los vehículos autónomos? ¿Usarán los ciberdelincuentes la IA para realizar ataques polimórficos? No, no es una distopía. Simplemente es el mundo que se perfila.

5.1 ¿Cómo será el ransomware en el futuro?

El retrato tipo del ransomware del futuro no está escrito. Sin embargo, está claro que se volverá más complejo y se adaptará a un entorno mejor protegido. También buscará empresas más maduras y contextos geopolíticos frágiles.



Si LockBit es actualmente la franquicia de ransomware más popular, la competencia es feroz. Solo en el primer semestre de 2022 aparecieron veinte nuevas bandas.

«Podemos imaginar que los ataques de ransomware se orientarán en el futuro a los monederos de criptomonedas, los NFT y los vehículos autónomos. Las tecnologías emergentes no son inmunes».

PIERRE-OLIVIER KAPLAN — CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

La situación geopolítica y las crisis económicas que se están gestando son autores están redoblando su inversión en I+D.

«Nuestras investigaciones técnicas también han revelado que un grupo poco conocido de doble extorsión de RaaS llamado Vice Society utiliza diferentes tipos de ransomware según los objetivos y los sistemas: Zepplin para Windows, HelloKitty para Linux[33]».

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

Sin embargo, estos avances son bastante caros, lo que obliga a los ciberdelincuentes a apuntar a las grandes empresas para amortizar la operación. —

NUEVAS FAMILIAS DE RANSOMWARE EN EL PRIMER SEMESTRE DE 2022

- → YourCyanide
- → Vandili
- → GoodWill
- → Vulcan Ransom Team
- → Cheerscrypt
- → NwGen
- → Axxes
- → RTM
- → Nokoyawa
- → Pandora
- → Hermetic Ransom
- → Mindware
- → Yashma
- → Onyx
- → Black Basta

Fuente: Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

¿CÓMO RASTREAR EL RANSOMWARE?

CON **ARNAUD PILON** — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ «Seguir la actualidad en materia de ransomware no es fácil. Tratamos de identificar los elementos invariables en los procedimientos, técnicas, herramientas, porque no es raro que diferentes grupos compartan «trucos», por ejemplo, sobre los métodos de propagación. También permanecemos atentos a las campañas de phishing, que no deben subestimarse. Finalmente, tratamos de identificar qué vulnerabilidades es probable que se exploten de forma masiva». —

5.2 ¿Qué soluciones deberían surgir?

Frente a una amenaza en constante evolución, las soluciones de protección de los puestos de trabajo deben seguir el ritmo. La mejora y multiplicación de los medios de detección es una vía a explorar, pero ello no debe hacernos olvidar las soluciones de protección necesarias.



Los ataques de ransomware han permitido abordar las amenazas para los sistemas de información. Esta comunicación ha captado la atención de los directores de los sistemas de información, que han aumentado los niveles de seguridad. Además de impulsar unos sistemas de información más robustos, la presión del ransomware ha generado un resurgimiento en la industria de las copias de seguridad.

Así, el mercado de las soluciones de ciberseguridad ya ofrece una serie de herramientas como EDR o XDR, que aumentan las posibilidades de detección y bloqueo de ransomware. No obstante, no hay que olvidar que estas soluciones de detección y subsanación son paliativas: a estas alturas, el ciberataque ya ha causado daños en las empresas.

«El desafío para los próximos años es lograr reducir el número de falsos positivos en los sistemas de información de gran envergadura, lo cual puede requerir el aprendizaje automático, si bien no es un fin en sí mismo. Por otro lado, ante la acumulación de capas de productos de seguridad, la mejora de la interoperabilidad de los sistemas será decisiva».

ARNAUD PILON — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

El primer paso imprescindible es poner en marcha medidas de protección (de los datos, ordenadores y redes).
La coordinación de soluciones es, por tanto, una de las pistas que debemos estudiar para reducir la fatiga del SOC.

La confianza que confieren las soluciones utilizadas será aún más estratégica de lo que es hoy, lo cual debería reforzar la importancia del sistema de cualificación a nivel europeo o francés. —

¿TENDREMOS ALGÚN DÍA UNA «VACUNA» CONTRA EL RANSOMWARE?

ARNAUD PILON — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ ***«Por desgracia, las amenazas se adaptan rápidamente a este tipo de soluciones técnicas. Mientras estos ataques generen beneficios, los ciberdelincuentes seguirán adaptándose, invirtiendo en I+D y, por tanto, progresando».***

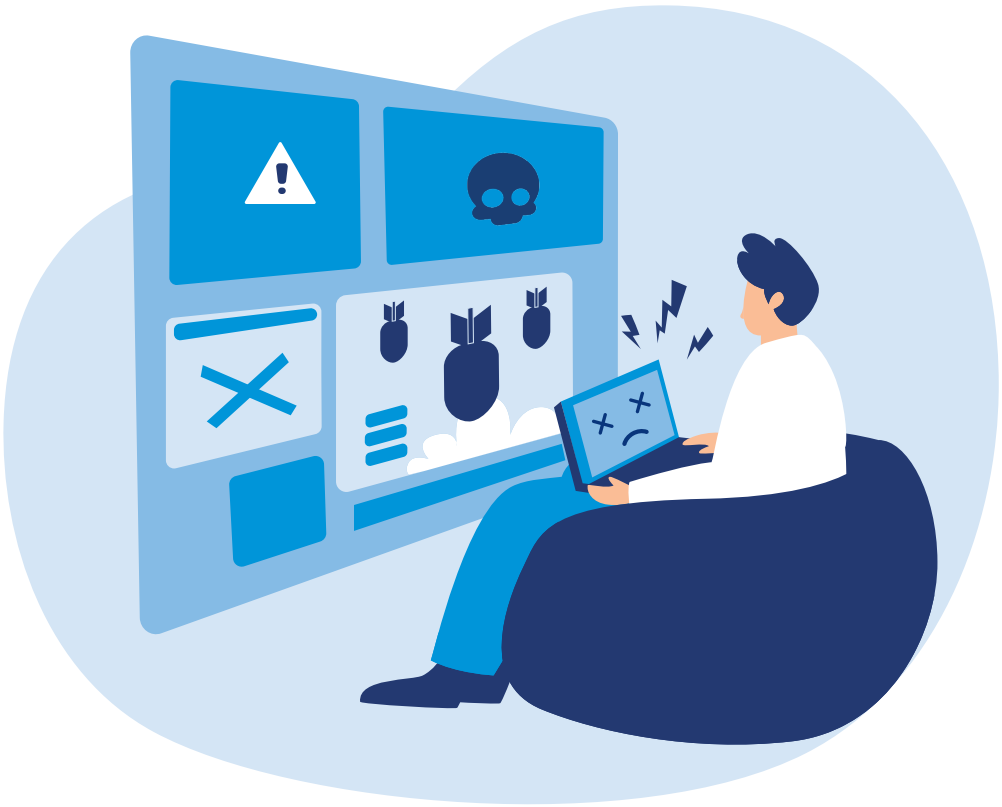
NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

→ ***«No creo en una vacuna, pero tampoco creo en la fatalidad. La victimología revela que la mayoría de los ataques son oportunistas. Ciertamente, siempre habrá alguien que haga clic en un archivo adjunto comprometido, pero combinando el conocimiento de la amenaza con las herramientas de detección, es posible detectar el ataque antes del cifrado y la extracción de datos».***

FLORENT CURTET — DIRECTOR GENERAL DE NEOCYBER Y COFUNDADOR DE HACKERS SIN FRONTERAS

→ ***«No existen soluciones a medio plazo para detener el fenómeno, especialmente porque el modelo de negocio de los secuestradores sigue evolucionando: algunos usan fallas muy avanzadas y pagan a «infiltrados» para ejecutar el virus ».***

En última instancia, la vigilancia y la victimología son cruciales en la lucha contra el ransomware, porque nos permiten comprender mejor las organizaciones de ciberdelincuentes y, por lo tanto, combatir mejor esta amenaza, que no ha dejado de transformarse durante las últimas tres décadas. Por lo tanto, es de esperar que se descubran periódicamente nuevas cepas y nuevas variantes, más aún en el contexto actual de aparición de nuevas tecnologías y de conflictos geopolíticos.



FUENTES Y ANEXOS

[1] https://www.liberation.fr/futurs/2017/06/28/notpetya-le-logiciel-ranconneur-a-propagations-multiples_1580043/
[2] https://www.leparisien.fr/high-tech/cyberattaque-les-centrales-nucleaires-francaises-sont-elles-en-securite-28-06-2017-7094979.php
[3] https://www.insurancebusinessmag.com/asia/news/cyber/ransomware-big-game-hunting-has-major-impact-on-insurers-189773.aspx
[4] https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
[5] https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
[6] https://www.zdnet.com/article/these-ransomware-attackers-sent-their-ransom-note-to-the-victims-printer/
[7] https://www.stormshield.com/fr/actus/petite-histoire-des-ransomwares/
[8] https://www.fbi.gov/news/testimony/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks
[9] https://www.zdnet.fr/actualites/le-groupe-de-ransomware-conti-ferme-son-site-vitrine-39943928.htm
[10] https://www-lemagit-fr.cdn.ampproject.org/c/s/www.lemagit.fr/actualites/252522126/Cyberattaques-Karakurt-fait-un-retour-en-fanfare?amp=1
[11] https://www.zdnet.fr/actualites/le-site-du-groupe-revil-donne-des-signes-de-vie-39940953.htm
[12] https://www.latribune.fr/technos-medias/informatique/qui-est-lockbit-3-0-le-cyber-ranconneur-de-la-poste-mobile-925065.html
[13] https://www.linkedin.com/posts/clementdomingo_cybersaezcuritaez-ransomwares-ransomgangs-activity-6985605220269441024-ZqLc
[14] https://www.lemagit.fr/actualites/252524255CHSF-lattaquant-ne-semble-pas-comprendre-que-cest-un-hopital-public
[15] https://www.ouest-france.fr/societe/cyberattaque/cyberattaques-voici-combien-les-entreprises-francaises-ont-perdu-depuis-janvier-482ff564-dfe7-11ec-b2a8-056c7579e285
[16] https://www.channelnews.fr/une-pme-francaise-sur-trois-a-deja-ete-victime-dun-ransomware-114729
[17] https://www.zdnet.com/article/ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
[18] https://www.lemondeinformatique.fr/actualites/lire-ransomware-jbs-debourse-11-m$-pour-recuperer-son-it-83225.html
[19] https://www.zdnet.fr/actualites/le-geant-de-l-agroalimentaire-jbs-vise-par-revil-39923901.htm
[20] https://www.lesechos.fr/pme-regions/grand-est/clestra-hauserman-demande-sa-mise-en-redressement-pour-trois-mois-1778519
https://www.lemoniteur.fr/article/clestra-place-en-redressement-judiciaire.2217432
[21] https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
[22] https://securite.developpez.com/actu/313967/Victime-d-un-ransomware-une-entreprise-paie-des-millions-aux-cybercriminels-pour-restaurer-ses-fichiers-L-entreprise-se-fait-attaquer-a-nouveau-par-le-meme-ransomware-et-paie-encore/
[23] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[24] https://www.usine-digitale.fr/article/ransomwares-rembourser-la-rancon-un-jeu-dangereux-que-les-assureurs-continuent-de-jouer-sous-conditions.N2038932
[25] https://www.linkedin.com/posts/s%C3%A9bastien-viou-b0806861_cybersaezcuritaez-ransomware-activity-6973284015197827073-dAGn?utm_source=share&utm_medium=member_desktop
[26] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[27] https://www.clubic.com/antivirus-securite-informatique/actualite-442272-cybersecurite-faut-il-assurer-les-victimes-de-ransomware-le-senat-dit-oui.html
[28] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf
[29] https://www.lemagit.fr/actualites/252501084/Ransomware-ces-rancons-payees-qui-plaident-en-faveur-de-la-cyberassurance
[30] https://www.numerama.com/cyberguerre/738790-apres-deux-mois-dabsence-le-terrible-gang-revil-fait-un-retour-inattendu.html
[31] https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
[32] https://www.cio-online.com/actualites/lire-experience-de-faux-phishing-au-cern-8%C2%A0-de-compromission-14450.html
[33] https://feedback.sekoia.io/changelog/11222

https://www.lesechos.fr/finance-marches/banque-assurances/
assurance-bercy-donne-son-feu-vert-a-lindemnisation-des-cyber-rancons-1786154
https://www.usine-digitale.fr/article/assurance-un-projet-de-loi-clarifie-le-cadre-
de-l-indemnisation-des-rancons-en-cas-de-cyberattaque.N2041292
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group/
https://www.cap-com.org/actualit%C3%A9s/20h02-la-web-serie-des-hopitaux-lyonnais-sur-la-covid-19
https://www.stormshield.com/fr/actus/50-nuances-de-ransomwares/
https://www.stormshield.com/fr/actus/vers-une-nouvelle-economie-de-la-vulnerabilite/
https://www.stormshield.com/fr/zero-ransomware/
https://www.stormshield.com/fr/ressourcescenter/ask-ze-expert-ransomware-ne-payez-pas-les-rancons/
https://www.stormshield.com/wp-content/uploads/SES-FR-Ransomware-Infographics-202204.pdf
https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf
https://www.stormshield.com/fr/actus/quel-etat-des-lieux-des-ransomwares-en-2020/
https://www.stormshield.com/fr/actus/alerte-securite-snake-combattre-infection-avec-stormshield-endpoint-security/
https://www.stormshield.com/fr/actus/ransomware-robbinhood-pourquoi-baltimore-se-retrouve-sous-les-projecteurs/
https://www.stormshield.com/fr/actus/tour-dhorizon-des-ransomwares-les-plus-wtf-de-la-planete/
https://www.stormshield.com/fr/actus/les-pirates-seraient-ils-des-juillettistes/
https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
https://www.idc.com/getdoc.jsp?containerId=US48093721
https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
https://www.zdnet.com/article/
ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
https://cyware.com/news/ransomware-sprawl-fbi-finds-over-100-variants-to-be-active-88f659f6
https://youtu.be/azdrKZzyWgg
https://www.nomoreransom.org/fr/decryption-tools.html
https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf
https://www.vadesecure.com/fr/blog/ransomware-as-a-service-raas-une-activite-illicite-qui-a-desormais-pignon-sur-rue
https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
https://www.lemondeinformatique.fr/actualites/lire-4-groupes-de-ransomwares-emergents-dangereux-a-surveiller-83944.html
https://www.darktrace.com/fr/blog/les-9-stades-des-ransomwares-comment-l-ia-repond-a-chaque-etape/

LA OPCIÓN EUROPEA EN CIBERSEGURIDAD

WWW.STORMSHIELD.COM

Queda prohibida toda difusión, reproducción o representación, incluso parcial, de este estudio para fines distintos al uso individual en cualquier soporte, lo que podría comprometer la responsabilidad civil y penal de cualquier persona que no cumpla esta prohibición
Copyright © 2022 Stormshield

STORMSHIELD