Ransomware 2021

Los ataques mediante ransomware llevan más de 30 años entre nosotros. Sin embargo, desde que el primer malware de este tipo fue programado en 1989 y se lanzó el primer ataque informático mediante un troyano, **conocido como PC Cyborg**, el escenario de la ciberseguridad ha evolucionado mucho. Las amenazas se han multiplicado, los malwares son cada vez más sofisticados y **las técnicas de ransomware**, más complicadas.

Tras la aparición de bitcoin, los ciber delincuentes vieron en las criptomonedas una nueva oportunidad para solicitar rescates imposibles de rastrear a cambio de frenar el ataque. Es por eso que en la última década los incidentes de secuestro de datos o ransomware han **crecido de forma exponencial.** Analizamos qué ha sucedido en 2020 y qué nos espera para este nuevo año.

¿Qué es ransomware?: la amenaza que no cesa

Los ataques por ransomware han pasado de ser algo anecdótico a convertirse en una amenaza recurrente que genera crisis profundas en las empresas o sistemas atacados.

Leer más

Tendencias emergentes en ransomware

El primer año de pandemia supuso, al margen de los problemas sanitarios y sociales, multitud de nuevas ventanas de oportunidad para los ciber criminales. Los cambios tecnológicos que la mayoría de organizaciones tuvieron que implementar a marchas forzadas para que todos los empleados pudiesen teletrabajar **multiplicaron las vulnerabilidades** de los sistemas y los riesgos asociados. Además, el COVID-19 y la situación incierta que ha provocado fueron usados de gancho para multiplicar los ataques de ransomware y phishing.

Solo durante la primera mitad de 2020 se registraron más ataques de ransomware que en todo 2019, según **los datos de Hiscox's CyberClear Centre y Kibu.** Además, la cuantía de los rescates pagados por las empresas atacadas creció un 200% en los primeros seis meses de 2020 en comparación con el año anterior. **Lloyd's confirma la tendencia**, asegurando que el **importe de los rescates se duplicó** entre enero y junio de 2020. En este escenario expansivo, destacan cuatro tendencias relevantes para cualquier organización.

Willis Towers Watson

1 Doble extorsión: Ransomware y whistleblowing

El ataque por ransomware más habitual consiste en infectar un sistema informático con un malware que es capaz de encriptar datos valiosos para la organización. Los atacantes solicitan un pago, normalmente en criptomonedas**, a cambio de desencriptar la información** y permitir que la entidad siga funcionando con normalidad. Sin embargo, durante 2020 se detectó un aumento de los ataques de doble extorsión, una tendencia que se cree continuará en 2021.

Este nuevo tipo de ataque combina el ransomware con el whistleblowing. De acuerdo con **los datos de Willis Towers Watson**, los atacantes no solo encriptan la información, sino que también la descargan. De esta manera, el incidente se produce en dos fases. En primer lugar, se solicita un rescate para liberar los datos encriptados. Si esta primera fase no funciona como los atacantes esperaban, se amenaza con **filtrar o publicar la información,** habitualmente sensible (whistleblowing).

Este tipo de ataque doble va más allá de la organización y las autoridades de protección de datos, ya que **implica también a las personas,** sean clientes o individuos relacionados con clientes, ajenas a la entidad. El primer grupo que lanzó un ataque de este tipo fue Maze. Disponen de un portal en la dark web en la que publican la información sustraída. Aunque recientemente han anunciado sus intenciones de cerrarlo, otros grupos han seguido sus pasos.

2 Ataques de ransomware dirigido

Los ataques por ransomware no afectan en exclusiva a ningún tipo de empresa. De hecho, más de un 70% de los incidentes de este tipo registrados tienen como objetivo pequeñas y medianas empresas, según los datos de la plataforma de soluciones de ciberseguridad **Panda.** Sin embargo, durante los últimos meses se ha experimentado **un auge de los llamados ransomwares dirigidos:** ataques desarrollados con el único objetivo de atacar a una empresa concreta y en un momento específico.

Los sectores que más sufrieron este tipo de ataques durante 2020 fueron la industria manufacturera, la construcción, la salud y la industria tecnológica. Esta última fue utilizada, en gran medida, como puerta de entrada a otras organizaciones. Según el informe de Hiscox's CyberClear Centre y Kibu, un ataque bien dirigido a un proveedor de soluciones IT puede convertirse en **un ataque múltiple y simultáneo** a diferentes entidades.

3 Phishing y correo electrónico, puertas de entrada

Las tácticas de suplantación de identidad o phishing siguen siendo la puerta de entrada habitual para los ataques de ransomware. Sin embargo, durante 2020 y, sobre todo, con motivo de la pandemia, los ciber delincuentes se alejaron de las prácticas de phishing indiscriminado, con campañas generales, y se centraron más en la elaboración de **correos electrónicos personalizados.**

Todavía no está claro hasta qué punto las técnicas de phishing han sacado partido hasta ahora de la demanda de información relacionada con la pandemia y de la situación de incertidumbre generada por el COVID-19. Algunos informes señalan que más del **25% de los ataques utilizaron el coronavirus como gancho**, mientras otros apuntan a que su impacto ha sido residual. Sea como sea, el correo electrónico y las tácticas de phishing siguen siendo la puerta de entrada principal para los ataques por ransomware.

4 El endurecimiento del mercado asegurador

Más allá del ransomware, los **ataques a la cadena de suministro** son sin duda una amenaza emergente que desafortunadamente contribuirá al endurecimiento de los mercados. Incidentes como el caso **Solarwind** que ha afectado a empresas que proporcionan soluciones y servicios de ciberseguridad como FireEye o Malwarebytes, a diferentes agencias gubernamentales de Estados Unidos o incluso al propio Microsoft y a empresas asociadas a los servicios que este proporciona como Mimecast, impactarán directamente en los precios y condiciones de los seguros.

Durante el último año, las primas se han encarecido, las condiciones de las pólizas se han vuelto más duras y se han establecido algunos **límites a las indemnizaciones**, según un análisis reciente de **Insurance Insider**.

Además, las pólizas de ciberseguridad han continuado evolucionando para adaptarse a las nuevas amenazas, como la publicación de los datos robados en el ataque. Por otro lado, cada vez más compañías aseguradoras apuestan por llevar a cabo **controles exhaustivos previos a la contratación de las pólizas** para así poder delimitar los ciberriesgos específicos a los que se enfrenta la organización.

Principales malwares utilizados en 2020

A la hora de señalar nombres propios, Maze ha sido el grupo de ransomware más sonado durante 2020. En un único ataque a una compañía del sector salud, los ciber delincuentes lograron robar más de 10 GB de datos personales y acabaron publicando información de 1500 pacientes. El ataque, perpetrado a través del email de un empleado, supuso un coste superior a los **12 millones de dólares** para la organización. Más allá de Maze, estos son algunos de los otros nombres destacados en el panorama ransomware.

- **AKO.** Este grupo ha tenido como objetivo, sobre todo, entidades de Estados Unidos de los sectores gran consumo e industria.
- **Cl0p.** Grupo centrado en la industria manufacturera y en el sector tecnológico, aunque más internacional en su campo de acción, con ataques detectados en Alemania, Estados Unidos, Reino Unido, España, Austria y la India.
- **DoppelPaymer**. Este grupo es responsable de uno de los mayores rescates solicitados en 2020, superando los 1800 bitcoins (unos 45 millones de dólares a precios actuales). Los ataques se centraron, sobre todo, en el sector financiero y en el industrial.
- **Mespinoza**. También conocido como Protect Your Systems Amigo (PYSA), este grupo tiene como objetivo el sector consumo, el sector salud y el sector público. Sus ataques se han registrado en multitud de países alrededor del globo.
- **Nephilim.** Junto a Maze, fue uno de los primeros grupos en filtrar los datos robados. Sus objetivos principales fueron empresas de los sectores energético e industrial.
- **REvil.** También conocido como Sodinokibi, este grupo ocupó los titulares durante semanas tras perpetrar el robo de 756 GB de datos privados de un gran bufete de abogados de la industria del entretenimiento. Como en el caso anterior, utilizaron el whistleblowing para aumentar la presión sobre la organización.

La solución pasa por reforzar la estrategia de ciberseguridad

A medida que el panorama de ciberriesgos en general, y de ransomware en particular, se complica, las herramientas para combatirlos deben también ganar en sofisticación. De acuerdo con los expertos en ciberseguridad de Willis Towers Watson, las organizaciones deben desarrollar **una estrategia de defensa en profundidad**, que establezca procedimientos de backup, refuerzo de la autenticación, planes de actualizaciones, monitorización de la red y una estrategia clara de gestión de riesgos humanos.

Mantener **copias de seguridad actualizadas** de todos los datos y archivos críticos es clave para minimizar el impacto de un ataque por ransomware. Un backup debidamente protegido permite restaurar los sistemas a un punto reciente el tiempo con pérdidas mínimas de información y evitar así pagar un rescate. Estas copias de seguridad deben estar almacenadas al margen de la red de la organización, tanto en la nube como en sistemas físicos.

Muchos de los ataques mediante ransomware utilizan sistemas de acceso remoto a la red de la organización infectando el equipo de algún empleado. Por ello es importante establecer **sistemas de doble autenticación** o utilizar redes privadas virtuales (VPN, por sus siglas en inglés) para establecer un muro que dificulte el acceso a los atacantes.

Además, los expertos de Willis Towers Watson subrayan que, por muy sofisticados que sean los ataques, el elemento humano sigue siendo fundamental. Las estrategias de ciberseguridad deben estar **centradas en las personas,** tanto a la hora de tener en cuenta el comportamiento de los empleados y los riesgos que puede generar como para desplegar planes de formación e información en ciberriesgos.

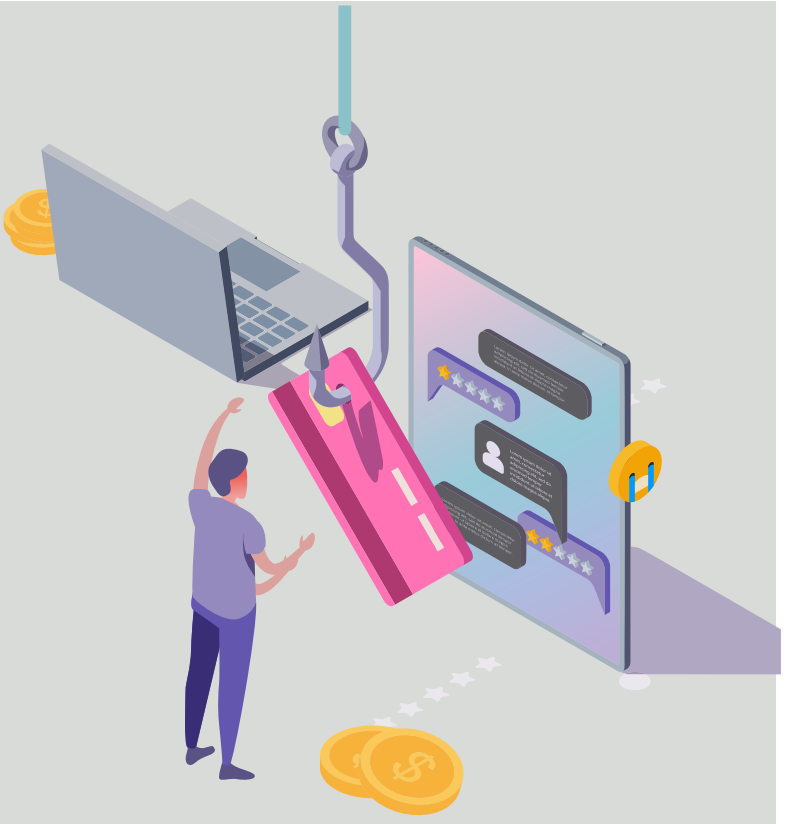
Por último, toda estrategia de ciberseguridad debe contar con un **plan de respuesta** que permita actuar de forma ágil y efectiva ante la mínima señal de ciberataque. Además de ayudar a contener la infección, estos planes deben servir para que los principales responsables sepan cómo actuar y qué pasos seguir para minimizar el impacto financiero, operacional y reputacional del incidente.

Los costes de un ciberataque son elevados. Desde los precios de contar con expertos para defenderse (sean internos o externos) hasta los costes de recuperar la continuidad del negocio, pasando por cualquier gasto legal o el impacto en la reputación de la compañía, un incidente mediante ransomware puede acabar teniendo **un peso elevado en la cuenta de resultados**. Por ello, el último pilar de la estrategia de ciberseguridad pasa por estar correctamente asegurado frente a los ciberriesgos.

¿Cómo mitigar y transferir la amenaza del ransomware?

Conoce cómo nuestras soluciones pueden ayudarte a mitigar y a transferir el ciberriesgo asociado a la brecha de datos.

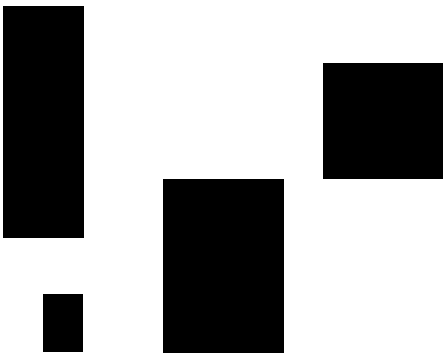
Leer más



Más información

Carolina Daantje
Head Cyber Risk Iberia
+34 608 22 04 19
carolina.daantje@willistowerswatson.com

Fernando Sevillano Ph.D.
Head of Cyber Risk Consulting Western Europe
+34 654 519 235
fernando.sevillano@willistowerswatson.com



Sobre Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW), empresa líder en consultoría global, broking y soluciones, ayuda a los clientes de todo el mundo a convertir el riesgo en un camino hacia el crecimiento. Con una historia que se remonta a 1828, Willis Towers Watson cuenta hoy con 45.000 empleados en más de 140 países. Diseña y ofrece soluciones que gestionan el riesgo, optimizan los beneficios, desarrollan el talento y potencian la capacidad del capital, para proteger y fortalecer a instituciones y particulares. Su punto de vista le permite conocer la conexión entre el talento, la experiencia y el conocimiento – una fórmula dinámica que potencia los resultados y el futuro crecimiento del negocio.

Copyright © 2021 Willis Towers Watson. All rights reserved.

willistowerswatson.com

Willis Towers Watson