El preocupante avance del ransomware

El *ransomware*, los virus que secuestran la información del usuario para exigir un rescate, es una ciberamenaza de importancia creciente que causa pérdidas millonarias a las empresas afectadas.

El 8 de noviembre, la cadena MediaMarkt informó que había sufrido un ciberataque que afectó directamente a las tiendas de Alemania, Holanda y Bélgica, y que trajo consecuencias entre las de otros países, como es el caso de España. Se estima que en torno a 3 000 servidores Windows fueron afectados, así como numerosos servidores web. Según se supo por la propia empresa, el ataque fue de tipo *ransomware*, es decir, la introducción en los sistemas de un programa malicioso que "secuestra" los datos de la víctima –generalmente, encriptándolos-, para posteriormente exigir un rescate por su liberación, de ahí el nombre. En concreto, el *malware* utilizado en este caso fue HIVE, un virus que ha sido utilizado en el pasado para infectar los sistemas informáticos de centros sanitarios. Los delincuentes habrían solicitado a MediaMarkt más de 200 millones de euros a modo de rescate. La misma semana sufrió una ciberagresión similar la empresa cervecera Estrella Damm, que se vio obligada a parar la producción de su fábrica de El Prat. El método fue el mismo, los

delincuentes cifraron los archivos informáticos de la compañía y pidieron un rescate por su desencriptación.

Los casos de MediaMarkt y de Damm no son excepcionales, sino parte de una tendencia de crecimiento en todo el mundo del *ransomware* como modalidad preferida por los ciberdelicuentes. El poder de esta clase de ciberamenaza quedó patente en 2017, cuando el virus WannaCry infectó en un día 230 000 ordenadores de 150 países. En aquella ocasión los *hackers* explotaron una vulnerabilidad de un puerto SMB, y el *malware* fue difundido a todos aquellos equipos que no habían recibido la actualización de un software de seguridad de Microsoft. Los costes globales que supuso el ataque se estiman entre cientos y miles de millones de dólares.

Nadie está libre del *ransomware* y cualquiera puede convertirse en víctima del chantaje. El pasado octubre, la empresa de televisión estadounidense Sinclair Broadcast Group, que gestiona unos 600 canales, recibió un ataque que inhabilitó sus comunicaciones, en concreto, el teléfono y el correo electrónico, lo que impidió que pudiese retransmitir determinados programas y espacios publicitarios, con la consecuente pérdida económica derivada.

El daño financiero que puede producir un ciberataque de este tipo es incalculable. La multinacional escocesa Weir Group se vio afectada por uno en septiembre, y tuvo que apagar sus servidores informáticos, lo que le supuso una pérdida de beneficios de 55 millones de dólares, además de un coste directo de casi 7 millones por los perjuicios producidos. A veces los ataques repiten víctima, como le sucedió también en septiembre a la firma japonesa de tecnología médica Olympus, que en cinco semanas sufrió dos acciones de *ransomware* centrados en la encriptación de sus redes, con la consecuencia de que quedó paralizada su actividad comercial en Norteamérica. Los *hackers* reinciden cuando pueden seguir explotando una vulnerabilidad informática no resuelta por la empresa objeto del ataque, o cuando esta última paga el rescate exigido, de forma que deciden seguir chantajeándola.

El mayor ataque *ransomware* registrado hasta la fecha tuvo lugar en julio de 2021 y afectó directamente a 60 empresas, aunque indirectamente hasta 1 500. El grupo ciberdelincuente conocido como REvil contaminó el *software* de gestión informática de la compañía Kayesa, de forma que todos sus clientes usuarios de sus servicios quedaron infectados. Las víctimas recibieron un mensaje de rescate que ofrecía un programa de desencriptación a cambio de 45 000 dólares, a pagar en criptodivisas.

El mayor ataque ransomware registrado hasta la fecha tuvo lugar en julio de 2021 y afectó directamente a 60 empresas, aunque indirectamente hasta 1 500

El *ransomware* no es una amenaza solamente para las empresas. Las Administraciones públicas son igualmente objetivos apetecibles para los *hackers*, y ya en 2019 el ayuntamiento de Jerez sufrió el cibersecuestro de sus equipos informáticos por el virus Ryuk, después de que unos meses antes hubiera ocurrido lo mismo en veintidós consistorios del Estado de Texas, Estados Unidos. En Italia, un ciberataque a la Società Italiana degli Autori ed Editori (SIAE) –la entidad encargada de gestionar los derechos de autor- dejó en manos del grupo delincuente Everest hasta 60 GB de datos privados de personalidades públicas, que los

malhechores intentaron vender al mejor postor al no conseguir que la SIAE pagase el rescate exigido.

La osadía del *hacker* no conoce límites, y puede llegar a sabotear infraestructuras, como sucedió el mayo pasado cuando secuestraron los sistemas de la Colonial Pipeline Company, la empresa que gestiona el mayor oleoducto de Estados Unido, causando el caos en estaciones de servicio de todo el país.

La principal característica del *ransomware* frente a otros tipos de ciberataques es la demanda de un rescate a la víctima para devolverle el control sobre su información y sus equipos, que el asaltante ha bloqueado o encriptado. Generalmente, tras el ataque, se recibe un correo electrónico anónimo que establece la cantidad a pagar y el método para hacerlo, que suele ser a través de criptomonedas, como Bitcoin. El pago del rescate no garantiza la devolución del acceso a la información. De hecho, algunas acciones criminales que se hacen pasar por *ransomware* tienen como objetivo la destrucción de los datos de la víctima, independientemente de que pague o no la cantidad pedida (*wiper malware*).

Es por ello, que la principal recomendación cuando se es objeto de un chantaje de estas características es no pagar nunca, dado que nada ni nadie garantiza que los *hackers* vayan a desencriptar los sistemas afectados, y, además, pagando se alienta este tipo de delito, incluso es posible que la víctima vuelva a ser objetivo del ataque, como ocurrió con la empresa nipona Olympus. La mejor forma de minimizar el daño producido por el *ransomware* es disponer de copias de seguridad de la información estratégica y sensible, para que su posible encriptación no implique una pérdida irreparable para la organización.

Una amenaza creciente

De acuerdo con SonicWall, en los seis primeros meses de 2021, el volumen global de ataques *ransomware* alcanzó la cifra de 304,7 millones, un hito impresionante, si consideramos que en todo 2020 fueron 304,6 millones. A mediados del año, esta ciberamenaza había crecido un 151% respecto del mismo periodo del año pasado. SonicWall considera 2021 como el peor año de *ransomware* de todos los que lleva registrados.

Los picos más altos de crecimiento a mediados de año se han producido en Europa (234% más) y Norteamérica (180%), mientras que en Asia, después de un fuerte incremento en marzo, el volumen de ataques ha descendido sensiblemente. Los países que registran una mayor incidencia son Estados Unidos, Reino Unido, Alemania, Sudáfrica y Brasil. Las principales amenazas en este terreno tienen nombres propios: Ryuk, que en 2021 triplicó su cifra de ataques respecto del año anterior, Cerber, que en mayo quintuplicó los niveles de incidencia que presentaba en enero, y Samsam, que ha mitad de este año ya duplicaba su volumen de todo 2020.

Los picos más altos de crecimiento del ransomware a mediados de año se han producido en Europa (234% más) y Norteamérica (180%)

Hay varias razones que explican esta tendencia al alza. Por una parte, se constata que muchas organizaciones en el mundo están recurriendo a los ciberseguros como forma de protegerse de las pérdidas económicas derivadas de los ataques, y esta figura contempla a menudo el pago del rescate, lo que alienta al delincuente

a seguir utilizando esta modalidad de extorsión. De hecho, el haber cobrado el rescate con frecuencia invita a realizar un nuevo ataque a la misma víctima. Otro factor a tener en cuenta es que los ciberdelincuentes han diversificado sus formas de obtener ingresos, de forma que, además de exigir el rescate, antes de encriptar los datos realizan una copia para luego venderlos en el mercado negro. Esto último aumenta la rentabilidad esperada de este ciberdelito.

En España, el año pasado se registraron más de 4 000 incidentes en empresas e instituciones relacionados con el *ransomware*, según la firma Ensisoft, que supusieron en torno a los 1 200 millones de dólares de costes. Sin embargo, los particulares no están exentos de sufrir este tipo de ataques, como demuestran los datos de una encuesta realizada por ONTSI en el segundo semestre de 2020. Al analizar los virus troyanos que infectan los ordenadores domésticos, casi la quinta parte corresponden a *ransomware, rogueware* y a troyanos bancarios. El *rogueware* es un tipo de *malware* que simula ser un antivirus que ha detectado una anomalía en nuestro equipo, invitándonos a pinchar un enlace para solucionarlo, momento en que descargamos el virus de verdad. Si consideramos los dispositivos que tienen Android como sistema operativo, la cifra anterior crece hasta el 37%, y el *ransomware* supone el 28,2% de todos los troyanos. Tradicionalmente, este tipo de programas maliciosos estaban más asociados a los entornos PC, pero este último dato demuestra que progresivamente se van extendiendo a terminales móviles, como los *smartphones* y las tabletas.

Una de las principales formas de luchar contra el *ransomware* es realizar copias de seguridad de los archivos, algo que, de acuerdo con ONTSI, ahora mismo solamente hace menos de un tercio de los particulares consultados. Resulta igualmente importante tratar con cautela los correos electrónicos recibidos, especialmente aquellos que pueden resultar más sospechosos y evitar pinchar enlaces o descargar archivos que no sean de absoluta confianza.

En última instancia, la seguridad está en manos del usuario, de la información de que disponga sobre las amenazas y sobre cómo evitarlas, y de su comportamiento en las redes. En la encuesta de ONTSI, el 53% de los particulares es consciente que sus acciones *online* tienen consecuencias en la ciberseguridad, y el 42% tiene confianza o mucha confianza en internet.

Foto de **kat wilcox** en **Pexels**

Emsisoft (2021) "The cost of ransomware in 2021: A country-by-country analysis". Disponible en: https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/

Fundación Telefónica (2020) "Sociedad Digital en España 2019". Disponible en: https://www.fundaciontelefonica.com/cultura-digital/publicaciones/sociedad-digital-en-espana-2019/699/

García, J. M. (2021) "Un ciberataque colapsa los servidores de MediaMarkt en varios países europeos" en *La Vanguardia*. Disponible en: https://www.lavanguardia.com/tecnologia/20211108/7847465/ciberataque-mediamarkt.html

National Cyber Security Center (2020) "Mitigating malware and ransomware attacks". Disponible en: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

ONTSI (2021) "Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España"

Pérez, E. (2021) "MediaMarkt sufre un ciberataque por *ransomware* que afecta a sus tiendas a pocas semanas del Black Friday" en *Xataka*. Disponible en: https://www.xataka.com/seguridad/mediamarkt-sufre-ciberataque-ransomware-que-afecta-a-sus-tiendas-a-pocas-semanas-black-friday

Sonicwall (2021) “SONICWALL CYBER THREAT REPORT. Cyber threat intelligence for navigating today’s business reality”

Tessian (2021) “12 Examples of Ransomware Attacks”. Disponible en: https://www.tessian.com/blog/examples-of-ransomware-attacks/