RANSOM... ¿QUÉ?

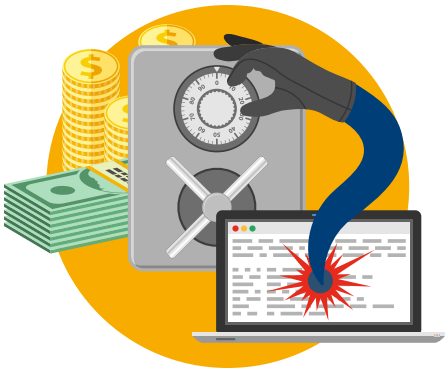
El Cibersecuestro De Datos Con el Código Malicioso Ransomware

SEPTIEMBRE 2019

LOCKTON®

** Basado en el artículo original de Imani Barnes*

La ciberdelincuencia ha expandido en los últimos años –en todo el mundo y México no es la excepción– un modelo ilícito de negocios que aún muchos desconocen: el ransomware. Se trata de un tipo de malware (código malicioso) diseñado para instalarse en un equipo de cómputo, infiltrarse en el sistema informático de una empresa privada o institución pública y encriptar datos sensibles. El objetivo es pedir una cantidad de dinero –en criptomonedas como el bitcoin– a cambio de liberar esa información y devolver los accesos seguros a las redes. Es, literalmente, un cibersecuestro de datos.



Debido a la evolución de la digitalización y la interconectividad, las amenazas cibernéticas han dejado de ser sólo una preocupación de seguridad y privacidad personal para constituirse en un auténtico peligro para plataformas de información que involucran datos de grupos de personas o comunidades enteras.

A través del despliegue del ransomware, los ciberdelincuentes ya no sólo buscan robar información de tarjetas de crédito y otros datos sensibles de identificación personal, sino que han mejorado sus tácticas para manipular a los responsables de organizaciones o instancias, públicas o privadas, para que paguen grandes sumas de dinero a cambio de la liberación segura de sus datos y el control de sus sistemas.

En México –el tercer país de Latinoamérica con más ataques de ransomware– el escenario es complicado porque los criminales han esparcido familias de malware muy diversas. De acuerdo con el Eset Security Report, de la firma especializada en seguridad cibernética Eset, en 2018 más de 200 variantes de ransomware se propagaron en territorio mexicano. Las dos familias que concentraron mayores detecciones fueron Crysis y TeslaCrypt.

Los delincuentes cibernéticos están ampliando sus alcances de posibles víctimas para incluir objetivos de oportunidad[1] en una multitud de industrias.

Esta extorsión cibernética o cibersecuestro de datos ha generado importantes ganancias a los grupos delictivos. Se estima que los costos globales de ransomware alcancen los 12 mil millones de dólares para fines de 2019.

Este documento proporciona información sobre la evolución del ransomware como un instrumento de extorsión cibernética, identifica cepas notorias y explica cómo las empresas pueden protegerse.

Autores:

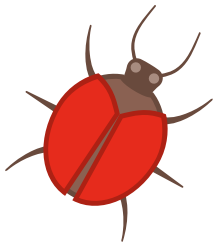
Ricardo Alvarado
Director Ejecutivo de Riesgos
ralvarado@mx.lockton.com

Karla Castro Tepale
Placement Daños
Responsabilidad Civil | Líneas Financieras
kcastro@mx.lockton.com

1 WIRED. "Meet LockerGoga, the Ransomware Crippling Industrial Firms" March 25, 2019; https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/

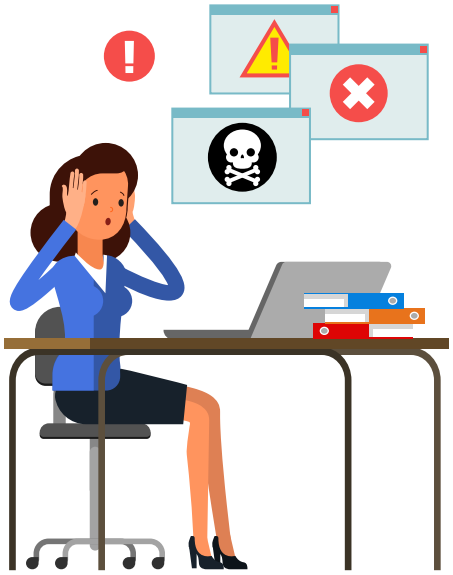
Una a breve historia del ransomware

Los primeros signos de ransomware aparecieron en 1989 en la industria de la salud. Un atacante usó disquetes infectados para encriptar archivos de computadora, alegando que el usuario estaba "violando un acuerdo de licencia"[2], y exigió 189 dólares a cambio de una clave de descifrado. Si bien el intento de extorsionar no tuvo éxito, este ataque se conoció comúnmente como PC Cyborg y puso en marcha el arquetipo para futuros hackeos. En los años siguientes, los ataques de ransomware estuvieron presentes, pero todavía no eran un problema significativo porque a los cibercriminales les faltaban tres elementos clave:



1. Una estrategia clara para desencriptar o destruir los archivos y datos por los que exigieron dinero.
2. La capacidad de comunicarse de forma anónima.
3. Un método imposible de rastrear para que la víctima pague el rescate.

2 Edith Cowan University. "Ransomware: Emergence of the cyber-extortion menace" 2015; https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1179&context=ism



Con esas limitaciones, los ciberdelincuentes se conformaron con aprovechar vulnerabilidades explotables en software y errores humanos para instalar malware en dispositivos a través de estafas de antivirus. De esta manera pudieron robar credenciales confidenciales e información personal para vender a extraños.

Años más tarde, en 2006, el virus troyano Archiveus cambió el ámbito del ransomware. Cuando se descarga, encripta todos los archivos encontrados en la carpeta "Mis documentos" de la computadora del usuario. Para que las víctimas pudieran recuperar el acceso a estos archivos, debían dirigirse a sitios web específicos –indicados por el propio Archiveus– para realizar compras y pagar así el rescate[3].

La introducción del bitcoin en 2008 fue un punto de inflexión significativo en el mundo de la ciberextorsión. Esta nueva moneda digital permitió a los cibercriminales llevar a cabo ataques y recibir pagos de rescate prácticamente imposibles de rastrear. Ahora los ciberdelincuentes tenían la libertad de ser creativos con sus ataques y subir la apuesta.

Después de varias réplicas de cepas de ransomware (los llamados CTB-Locker o CryptoLocker), en 2013 los maleantes cumplieron con los otros dos elementos faltantes. Ahora podrían ejecutar tramas poderosas de extorsión de ransomware.

En el lenguaje cibernético, "CTB" son las siglas de Curve (por la tipografía de curva elíptica), TOR y Bitcoin. Ahora, ¿qué es "TOR"? Son las siglas del protocolo The Onion Routing. Así, el CTB proporcionaba a los piratas cibernéticos un cifrado rápido y seguro del contenido del archivo, un medio para la comunicación anónima a través del protocolo TOR, y el bitcoin permitía transacciones cripto-efectivo seguras e imposibles de rastrear. Era, pues, la evolución del delito cibernético.

Dado que las organizaciones y las cadenas de suministro dependen cada vez más de las redes y de la conexión de dispositivos, la escala y el efecto de un ataque de ransomware es también cada vez mayor.

3 Computer Business Review. "The History of Ransomware" Feb. 23, 2018; https://www.cbronline.com/news/the-history-of-ransomware.

La prevalencia del ransomware

El FBI lanzó el Internet Crime Complaint Center (IC3) para rastrear los ataques de cibercrimen y ransomware y proporcionar información a personas y organizaciones sobre cómo protegerse contra estos delitos. Desde su lanzamiento en 2000, el IC3 ha recibido informes de más de 4 millones de eventos de delitos cibernéticos, con un aumento de la ciberextorsión.

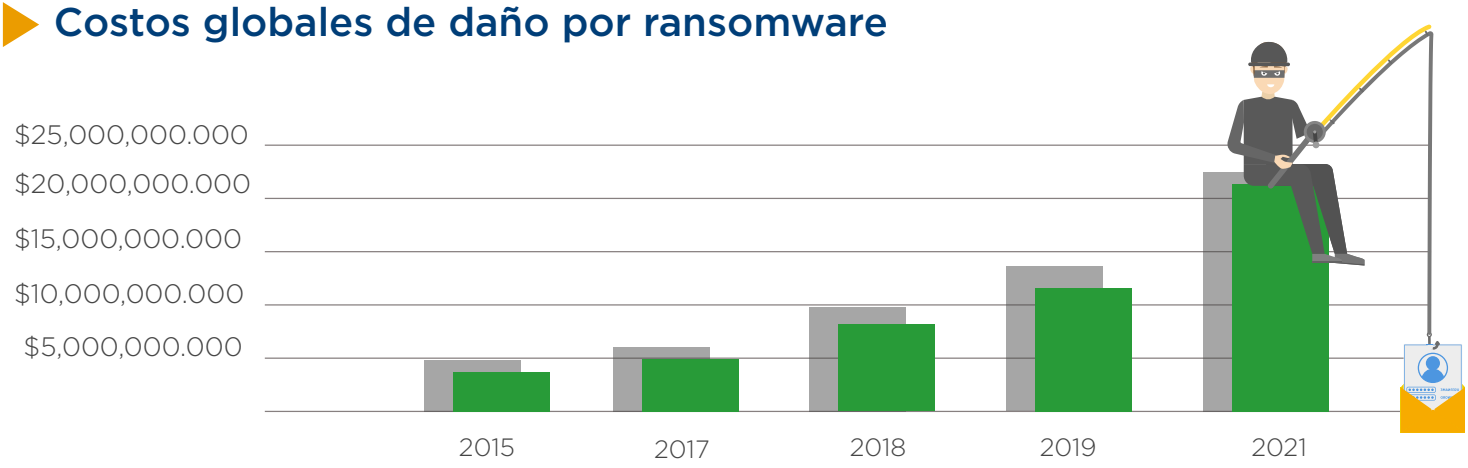
En 2018, los ataques de ransomware informados directamente al IC3 representaron aproximadamente 3.6 millones de dólares en pérdidas para las víctimas[4]. Si bien la pérdida financiera informada puede parecer baja, es importante tener en cuenta que es común que muchas organizaciones paguen rescates sin dar a conocer que han sido víctimas de ataques de ransomware.

Los ataques de ransomware también se están volviendo más agresivos. Los ciberdelincuentes duplican e incluso triplican la demanda si el rescate no se paga dentro del plazo especificado. Este método de ciberextorsión se ha convertido en un negocio multimillonario para los ciberdelincuentes, y se espera que los costos globales de ransomware alcancen aproximadamente 12 mil millones de dólares para fines de 2019 y 20 mil millones para 2021.

Estos ataques están aumentando a un ritmo tan rápido que los investigadores de Cybersecurity Ventures predicen que "una nueva organización será víctima del ransomware cada 14 segundos en 2019 y cada 11 segundos para 2021"
(Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021" Oct. 19, 2018).

4 Federal Bureau of Investigation. "2018 Internet Crime Report" 2019; https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

Costos globales de daño por ransomware



Fuente: Cybersecurity Ventures para datos de costos de daños de ransomware global.

¿Qué papel juega el Seguro de Riesgos Cibernéticos?

Es recomendable que toda organización o instancia, ya sea pública o privada, tenga una protección adecuada contra los ataques de ransomware. Esto se extiende más allá de contar con antivirus y software anti-malware y copias de seguridad.

Los escenarios de phishing (fraude electrónico) se aprovechan mucho para iniciar ataques de ransomware y comúnmente están "diseñados para engañar a un usuario para que proporcione las credenciales de la cuenta de Office 365"[5] para violar un sistema. Estos ataques van más allá de exigir rescates y a menudo vienen con varios daños y gastos asociados, que incluyen:

"Daño y destrucción (o pérdida) de datos, tiempo de inactividad, pérdida de productividad, interrupción posterior al ataque al curso normal de los negocios, investigación forense, restauración y eliminación de datos y sistemas de rehenes, daño a la reputación y capacitación de los empleados en respuesta directa a ataques de ransomware"[6] .

El Seguro de Riesgos Cibernéticos puede evitar que una empresa agote todos sus recursos para hacer frente a un ataque y recuperarse. En el caso de una invasión de ransomware, este seguro cubriría la demanda de rescate y los gastos adicionales, incluidos análisis forenses e investigación, hasta el límite especificado de la póliza Cyber. El valor que proporciona el Seguro de Riesgos Cibernéticos se demuestra a través de los extensos acuerdos y mejoras de seguros centrales disponibles en el mercado, tales como:

- Responsabilidad de seguridad de la red.
- Procedimiento reglamentario de privacidad.
- Costos de respuesta por incumplimiento.
- Reembolso por ciberextorsión.
- Reemplazo de hardware (bricking).
- Recuperación de datos.
- Interrupción comercial y gastos extra.
- Interrupción de negocio dependiente.
- Daño reputacional.

5 Baker Hostetler. "2019 Data Security Incident Response Report" April 2019; https://www.bakerlaw.com/press/bakerhostetlers-5thannual-data-security-incident-response-report-highlights-collision-of-privacy-cybersecurity-and-compliance-details-efforts-to-minimize-risk

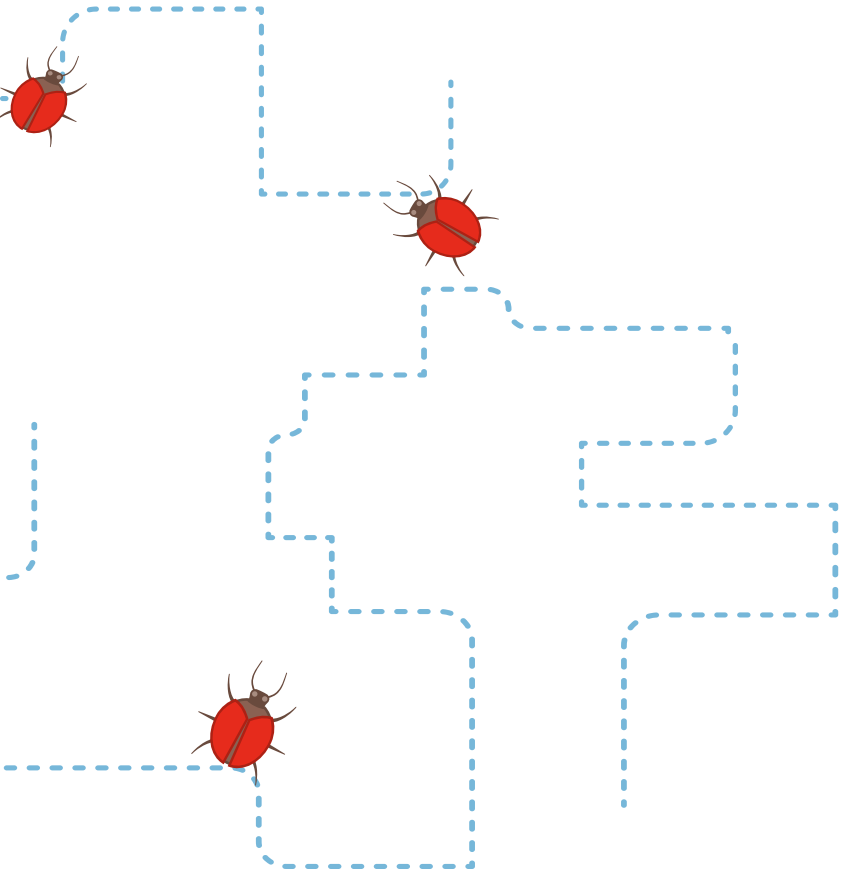
6 Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021" Oct. 19, 2018 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Hay pólizas que ofrecen cobertura a las empresas por daños causados por proveedores externos debido a un evento cibernético como el ransomware. Lockton, el corredor privado de seguros más importante a escala mundial, ve de primera mano el valor que el Seguro de Riesgos Cibernéticos ofrece a nuestros clientes contra daños y costos incurridos debido a los ataques de ransomware, como Ryuk y WannaCry, proporcionando cobertura para gastos que alcanzan más de 4.5 millones de dólares, acumulativamente.

Los ataques de ransomware implican severas mermas económicas, además de interrupción del negocio en muchas ocasiones. Durante los últimos 30 años, el ransomware se ha adaptado a las estrategias defensivas una y otra vez, pues los cibercriminales explotan numerosas vías para llevar a cabo ataques.

Desde los intentos de ingeniería social y phishing hasta sitios web infectados, la amenaza se vuelve más sofisticada a cada minuto. Su avance está afectando a un número creciente de industrias. La pregunta ya no es si estoy expuesto a un ataque, sino cuándo ocurrirá. Las organizaciones deberían cambiar su enfoque de una postura de recuperación a una proactiva, y desarrollar los planes de prevención y contingencia apropiados.

Lockton ha asegurado endosos complementarios exclusivos con muchas de las grandes compañías de Seguros de Riesgos Cibernéticos para garantizar que nuestros clientes cuenten con condiciones de cobertura óptimas.



LÍNEA DE TIEMPO

Ataques más grandes de ransomware y malware a la fecha.

FECHA	TIPO	EVENTO	INDUSTRIA
2012	Reveton	Troyano que afirmaba de manera fraudulenta que hacía cumplir la ley y excluía a los usuarios de sus dispositivos hasta que se pagara la demanda o "multa".	SECTOR PÚBLICO Servicio de Policía Metropolitana (Londres)
Septiembre 2013	CryptoLocker	Troyano que solía apuntar a dispositivos que ejecutan Microsoft Windows, utilizando el virus Gameover Zeus entregado a través de mensajes de spam. El virus logró infectar aproximadamente 500 mil computadoras en todo el mundo. Los ciberdelincuentes pudieron obtener, vía extorsión, aproximadamente un millón de dólares en un periodo de seis meses.	AEROESPACIO Y DEFENSA – GOBIERNO - LA NASA - Salud y Servicios Humanos COMPUTACIÓN, JUEGO Y SOFTWARE
Febrero 2015	TeslaCrypt	Una variante de CryptoLocker, conocida por infectar a los jugadores de computadora, se descargaba de una página web HTML infectada y no sólo encriptaba los datos de los jugadores y los archivos auxiliares, sino también otros archivos encontrados en sus dispositivos, a cambio de un rescate. Los pagos de extorsión sumaron 76 mil 522 dólares.	COMPUTACIÓN, JUEGO Y SOFTWARE
2015	SimpleLocker	Dirigido a los usuarios de dispositivos con sistema operativo Android de Google, para cifrar las tarjetas SD con el pretexto de que el usuario había cometido un delito. El virus demandó el pago a cambio del acceso a los datos del usuario, además exigió no informarlo a las autoridades.	SERVICIOS DE COMUNICACIÓN - Google

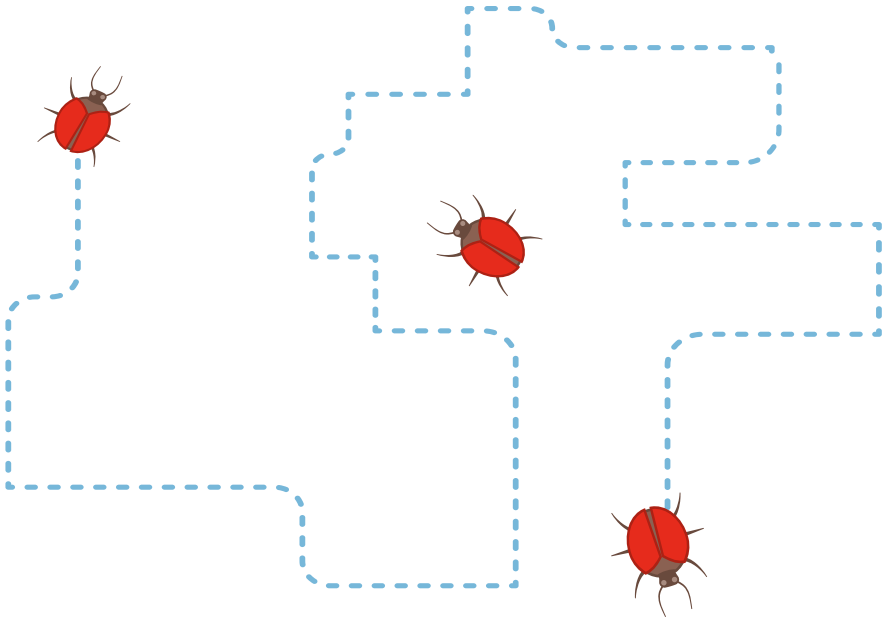
Febrero 2016	**Locky**	Un ataque dirigido que entregó código malicioso a través de un correo electrónico de phishing con un documento de Microsoft Word o un archivo adjunto de JavaScript. Una vez descargado, atacó agresivamente los sistemas y archivos críticos de respaldo, lo que dificultó el éxito de los métodos de recuperación de datos. El virus cifró todo el sistema y exigió un rescate por la devolución de los archivos informáticos del hospital y el acceso a los sistemas.	SALUD – Hollywood, Centro médico presbiteriano
Noviembre 2016	**HDDCryptor**	Cifró todas las unidades locales y en red mediante la modificación de los registros maestros de arranque (MBR) de todo un sistema de transporte. Esto dejó las puertas de la estación de tren abiertas y las máquinas de boletos fuera de servicio, incluso mostrando mensajes de que los pasajeros podían viajar gratis.	TRANSPORTE MUNICIPAL - Autoridad de Transporte Municipal de San Francisco
Mayo 2017	**WannaCry**	Explotó un código desarrollado por la NSA llamado EternalBlue y brechas en el parche del Protocolo de Bloqueo de Mensajes del servidor (SMB, utilizado para impresoras, uso compartido de archivos y acceso remoto). Esto en dispositivos que ejecutan el sistema operativo Windows 7. El ransomware se distribuyó por correo electrónico y, una vez en el sistema, el virus cifró los archivos en el disco duro, evitando el acceso del usuario a ese dispositivo y a cualquier otro dispositivo conectado a la red a cambio de que se pagara el rescate en bitcoin. Este ataque logró afectar a más de 300 mil computadoras en total y se cree que está relacionado con el Grupo Lazarus, con conexiones con el gobierno de Corea del Norte	SALUD Servicio Nacional de Salud de Gran Bretaña AEROESPACIO Y DEFENSA - Boeing TELECOMUNICACIONES - MegaFon en Rusia FLETE AÉREO Y LOGÍSTICA - FedEx FABRICANTES DE AUTOMÓVILES Nissan, Renault EDUCACIÓN - Universidades en China SECTOR PÚBLICO - Autoridades policiales en India y China AGENCIAS GUBERNAMENTALES - Ministerio del Interior Ruso ELECTRÓNICA

Junio 2017	**NotPetya**	Una nueva versión de Petya que fue lanzado en marzo de 2016, el cual cifraba el disco duro y la información que contenía la computadora al correr el sistema operativo de Windows. El virus mostraba un mensaje al usuario explicando que se requería pagar un rescate para poder liberar la información. Fue esparcido a través de un archivo adjunto en un correo electrónico, con apariencia de un curriculm vitae, para hacer que el usuario diera click en él, abriera el PDF y aceptara dar acceso a los controles de usuario de Windows. El virus tomó su nombre del filme de James Bond de 1995, GoldenEye. NotPetya, una nueva y más poderosa versión, cuyo objetivo es encriptar todo, no sólo el disco duro del dispositivo. Este virus se propagó sin la asistencia de spam o ingeniería social. El virus sobrescribió el registro de arranque maestro, bloqueando con éxito a los usuarios fuera de sus dispositivos. Se cree que fue un ataque dirigido por Rusia y es conocido como un “ataque de pozo de agua”, que infecta un sitio web que utiliza un accounting software en común con el utilizado en Ucrania en combinación con EternalBlue. Este ataque es notable por las siguientes razones: No sólo cifró todo el dispositivo, sino también destruyó los datos y el hardware, dejando éste “bloqueado”. Mientras se exigía un rescate, no había forma tangible de pagarlo. El mayor ataque de malware por impacto. Los daños totales hasta la fecha se estiman en 10 mil millones de dólares o más.	TRANSPORTE Y LOGISTICA Maersk FARMACÉUITICAS — Merck CONSTRUCCIÓN — Saint-Gobain GIRO ALIMENTOS — Mondelez International, Inc. AEROLÍNEAS Y LOGÍSTICA — TNT Express (FedEx) ENERGÍA NUCLEAR — Planta nuclear de Chernobyl MANUFACTURA, SERIVICIOS PROFESIONALES

Junio 2017	**Bad Rabbit**	Como NotPetya, fue considerado también como un “ataque de pozo de agua”, donde el virus utiliza un falso instalador de actualizaciones de Adobe Flash que es descargado de un sitio web infectado, visitado frecuentemente por el usuario. Una vez que se activa la descarga, el virus bloquea el acceso del usuario al dispositivo y solicita el pago del rescate en las siguientes 40 horas.	AGENCIAS DE NOTICIAS — Agencia rusa de noticias Interfax
Enero 2018	**SamSam**	Explota las vulnerabilidades en el Protocolo de Escritorio Remoto (RDP) o el protocolo de transferencia de archivos basada en Java. Asimismo, en Servidores (FTP) en dispositivos que ejecutan el sistema operativo Windows, para obtener acceso a la red y ejecutar malware en el sistema. Esta cepa cifró los sistemas y archivos y exigió un rescate para recuperar el acceso a los archivos de los pacientes, las órdenes de arresto y casos judiciales pendientes. Esencialmente, los criminales detrás de SamSam adquirieron accesos de la darkweb para poder ingresar a sistemas a través de RDP o FTP. Este ataque de ramsomware se las arregló para obtener cerca de 850 mil dólares en pagos de rescate y ocasionó daños que se calcula exceden los 30 millones de dólares.	SECTOR SALUD — Allied Physicians of Michiana, Hancock Health, Allscripts Healthcare Solutions GOBIERNOS — Ciudad de Atlanta

Agosto 2018	**Ryuk**	Ataque diseñado principalmente en Estados Unidos, único por cómo se implementó. Los cibercriminales se posicionaron dentro de la red de las organizaciones durante un año para reunir la información necesaria para ejecutar su ataque. El virus usó Emotet y Trickbot, troyanos para entregar el malware a través de un correo electrónico de phishing. Este correo electrónico adjuntaba un documento de Microsoft Office que contenía código malicioso. Una vez abierto, el código era ejecutado y descargaba el Emotet Trojan. Este troyano se esparció por la red y descargó el troyano Trickbot, el cual atacó a la memoria y robó accesos. Esta cepa de virus cifró las unidades de red, borró copias instantáneas y deshabilitó la opción "Restaurar sistema" de Windows para el usuario final. Este ataque es notable por la mayor demanda de rescate de la historia: 145 mil en bitcoin, aproximadamente 700 millones de dólares. Más víctimas están siendo descubiertas con la información sobre cómo este virus se desarrolla. Los actores detrás del ataque han cosechado aproximadamente 4 millones de dólares en pagos de rescate.	SERVICIO DE AGUAS — Onslow Water and Sewer Authority (ONWASA) CENTRO DE DATOS Y PROVEEDOR DE SERVICIOS DE NUBE — Data Resolution, LLC
Enero 2019	**LockerGoga**	Mientras la información acerca de cómo el virus se propagó aún se encuentra en investigación, esta cepa encriptó todos los dispositivos en la red de trabajo, desconectándolos y cambiando las contraseñas de usuarios y administradores, bloqueando los dispositivos. El virus atacó al Administrador de arranque de Windows, responsable de iniciar el sistema operativo del dispositivo, y se ha utilizado para detener las operaciones de fabricación. Sobre esta cepa, actualmente no se conoce forma de descifrar sistemas y archivos, y las variantes "no permiten a un sistema infectado funcionar lo suficientemente bien como para que la víctima pague el rescate o usar una herramienta de descifrado" **7.** El grado del daño generado aún está en curso, pero ya va en casi 40 millones de dólares.	

7 Trend Micro. "What You Need to Know About the LockerGoga Ransomware" March 20, 2019.; https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-locker-goga-ransomware



LOCKTON®

LOCKTON.COM.MX

Avenida Santa Fe 481, piso 19, Colonia Cruz Manca, Cuajimalpa,
Ciudad de México.C.P. 05349

Teléfono: 5980-4300