Texto
R. Contreras

EL RANSOMWARE SE PERFECCIONA CON TÉCNICAS DE GUSANO

WANNACRY
UN SHOCK GLOBAL

<< Aunque su repercusión económica no ha sido la temida, WannaCry ha mostrado sus fauces a todo el planeta, envuelto de un misterio que lo relaciona con hackers afines a servicios secretos estatales y con tintes de una ciberguerra larvada.

El 12 de mayo de 2017 pasará a los anales tecnológicos como el viernes negro del ransomware. El día que WannaCry hizo temblar como amenaza planetaria a todas las empresas e instituciones públicas. Un suceso que, por otro lado, no ha supuesto un perjuicio económico de las dimensiones de virus legendarios como Conficker o ILoveYou, pero que ha puesto sobre la mesa la debilidad de las organizaciones y una sensación de indefensión ante un ataque cuya procedencia es todo un misterio. Pero además, WannaCry viene precedido de una serie de circunstancias que lo han lanzado a las portadas de los medios informativos. Es carne de cañón para la teoría de la conspiración y se inscribe como un fenómeno de esa ciberguerra larvada que se libra a nuestras espaldas, pero de la que no se sustraen los cuerpos de seguridad del Estado y servicios secretos. Es como si hubiese asomado una zarpa de esa bestia que habita en la Deep Web, como diciendo "os he podido hacer daño, pero me reservo para futuros ataques". Ahora que las aguas se han calmado, nuevas amenazas enseñan sus dientes y surgen preguntas difíciles de contestar. El propio WannaCry viene rodeado de una aureola de marketing, deriva de la contracción WannaCrypt ('quiero encriptar') y se ha reducido a 'quiero gritar', por la frustración que genera en el usuario.

China, Rusia, EEUU, UK... los más **saqueados**

400.000 equipos **infectados** en todo el mundo

Cronología de un ataque

Pero vayamos a los hechos. Todo empezó el famoso viernes a las 10 horas, cuando pantallas de los ordenadores de los edificios bandera de Telefónica, Gran Vía y Ronda de la Comunicación, se tornaron en rojo oscuro y mostraron un mensaje característico del ransomware, un software que encripta la información y te solicita el pago de un rescate de 300 a 600 bitcoins para devolverte la información. Telefónica no tardó en reaccionar y envió a los empleados un mensaje conminando a apagar los equipos, la primera medida que hay que poner en marcha para evitar un contagio mayor.

Los empleados, entre asustados y perplejos, se lanzaron a mandar capturas de pantalla y comentarios a las redes sociales. Los medios informativos online se pusieron en marcha y empezó una ceremonia de confusión. De pronto, los rumores salpicaron a Vodafone, BBVA y otras grandes del Ibex; parecía que nadie estaba libre de los ciberterroristas que 'al parecer' provenían de China. Se produjo un tira y afloja de noticias sin confirmar y desmentidos oficiales. Algunas grandes compañías, en prevención, ordenaron apagar sus equipos y evitar así males mayores.

Lo que parecía un ataque a la línea de flotación del Ibex 35, era solo una parte de un ciberataque global que ha alcanzado con mayor virulencia a Reino Unido y Rusia. También se hablaba en ese momento de Ucrania, India y Portugal. CheckPoint afirma que han sido infectados el sistema de salud de Gran Bretaña (NHS), Fedex en EEUU, Renault, Nissan, el sistema ferroviario alemán, y el Ministerio del Interior, bancos y ferrocarriles rusos, entre otras organizaciones críticas. El ciberatentado tiene tales proporciones que la propia Interpol lo ha calificado como "un ataque a un nivel sin precedentes".

El sábado 13, WannaCry alcanza la popularidad; este tipo de malware cifra los archivos con la extensión WCRY. El ataque aprovecha una vulnerabilidad de Windows (Eternalblue), mediante la ejecución remota de código de SMBv2. Una vulnerabilidad que, por cierto, descubrió la propia Agencia Nacional de Seguridad (a través del Equation Group), que a su vez fue hackeada por el grupo Shadow Brokers. El gran problema es que muchas empresas todavía no han aplicado el parche que Microsoft publicó el pasado mes de marzo, lo que las pone en situación de fragilidad.

En un fin de semana frenético, se pasó del desconcierto a la esperanza. El mundo respira el sábado aliviado cuando saltó la noticia de que un joven británico de 22 años había conseguido desactivar el ransomware. Marcus Hutchins detuvo el ciberataque global consiguiendo infectar su propio equipo y descubrir que el gusano llamaba a un dominio gwea.com que no estaba registrado. Lo registró pagando unos 11 dólares y redirigió el tráfico a un servidor de los Ángeles hasta conseguir que se desactivara.

De nuevo la Interpol salió a escena, lo que daba una idea de las dimensiones del ataque, el domingo se hablaba de 200.000 víctimas

RADIOGRAFÍA DE WANNACRY

- Esta variante de malware incorpora código para realizar la explotación de la vulnerabilidad publicada por Microsoft el día 14 de marzo descrita en el boletín MS17-010 y conocida como Eternalblue.
- WannaCry escanea tanto la red interna de una empresa como la externa, realizando conexiones hacia el puerto 445 (SMB), en busca de equipos no debidamente actualizados, para propagarse a través de ellos e infectarlos, lo que le confiere a la muestra funcionalidad similar a la de un gusano.
- Para realizar este movimiento dentro de la red, utiliza una variante del 'payload' Doublepulsar.
- Para descifrar los ficheros, los autores de 'WanaCrypt' han desarrollado una herramienta propia denominada Wana Decrypt0r 2.0.
- Esta herramienta se conecta vía Tor (Deep Web) a una serie de servidores (TLD. onion) de forma que, los responsables del cifrado, puedan ponerse en contacto con los usuarios afectados.
- Para ello, Wana Decrypt0r 2.0 dispone de un chat, se entiende que necesario, ya que se han de comprobar los pagos oportunos antes de proporcionar cualquier clave de descifrado.

Fuente: Panda Labs

LOS VIRUS MÁS DAÑINOS DE LA HISTORIA

CHERNOBYL (1998)
Los expertos estiman un daño de entre 20 a 80 millones de dólares, el que provocó este virus procedente de Taiwan que hizo estragos en archivos ejecutables de Windows 95, 98 y Millennium.

MELISSA (1999)
Un virus de oscuros recuerdos, utilizó Microsoft Outlook para enviarse a sí mismo a 50 direcciones de la lista de contactos un mensaje ladino: "Este es el documento que me pediste, no se lo muestres a nadie".

ILOVEYOU (2000)
De gran repercusión, se trataba de un script de Visual Basic con una ingeniería social 'amorosa'. Fue detectado en Hong Kong y transmitido vía email con 'I love you' en el asunto. Sobreescribió archivos de imágenes y de música.

CODE RED (2001)
Un virulento gusano cuyo objetivo era atacar los ordenadores que tuvieran el servidor Microsoft Internet Information Server para aprovecharse de una vulnerabilidad. En menos de una semana, infectó a 400.000 servidores.

SQL SLAMMER (2003)
Mostró sus garras un sábado, lo cual atenuó el daño económico aunque atacó a medio millón de servidores. El virus era un archivo de 376 bytes que generaba una dirección IP a la que se autoenviaba.

BLASTER (2003)
Se calcula un daño próximo a los 10.000 millones de dólares y causó auténticos destrozos, cientos de miles de ordenadores infectados. También conocido como MSBlast, atacó a sistemas Windows 2000 y Windows XP.

MYDOOM (2004)
Otro de los históricos. Era capaz de ralentizar Internet en un 10% y un 50% la carga de páginas. Dio la vuelta al mundo con un supuesto mensaje de error y estaba programado para detenerse después del 12 de febrero de 2004.

CONFICKER (2008)
Este gusano aprovechaba una vulnerabilidad en el servicio de Windows Server. Microsoft ofreció una recompensa de un cuarto de millón de dólares para quien facilitase información que permitiera encarcelar a los creadores del malware.

STUXNET (2010)
Descubierto por la firma bielorrusa VirusBlokAda, es el primer gusano conocido que espía y reprograma sistemas industriales de control (SCADA) y estuvo 'implicado' en la paralización de una planta nuclear iraní.

"En lugar de apuntar a Windows XP, WannaCry apuntó a Windows 7 y Windows Server 2008, según Kaspersky"

España, la 16ª con **1.200 PC** infectados

en 150 países, aunque los cálculos de las autoridades chinas eran más desalentadores: 179 países y unos 230.000 ordenadores infectados. Sigue la histeria; en India el Ministerio de Home Affairs ordena apagar cientos de cajeros automáticos para eludir un potencial ataque e insta a los bancos a actualizar el parche de seguridad.

Nadie las tiene consigo, el lunes 15 muchas empresas cruzan los dedos y otras prefieren dejar sus equipos en cuarentena. Se habla de nuevas mutaciones del virus, pero afortunadamente las cosas no van a mayores. A finales de la semana los expertos consideran que el huracán ya ha pasado, pero quedan frentes por mitigar. "Yo creo que está todo bajo control, el problema

Rastreados pagos en **Bitcoin** por 77.000 $

es que no hay una recuperación total de los servicios. No significa que todo esté normalizado", explica Eusebio Nieva, director técnico de CheckPoint. Los destrozos no han sido todo lo graves que parecían. Se ha podido rastrear el pago de 77.000 euros a través de bitcoins, cifra aparentemente irrisoria para la amenaza que se cernía sobre el mundo.

Conclusiones y preguntas

En su opinión, WannaCry tiene toda la pinta de un ataque dirigido a grandes compañías. "Probablemente habrán cogido una base de datos de corporaciones ya que los vectores de infección han sido a través del correo", observa. También se especula con que el ciberataque proviene del grupo norcoreano Lazarus (conocido por su acción contra Sony), al tiempo que Putin y la propia Microsoft señalan con el dedo acusador a la Agencia de Seguridad de EEUU. "Para este ataque se ha utilizado una vulnerabilidad de Windows con fecha de marzo, revelada por Wikileaks en uno de los documentos del caso Vault 7", relata Nieva. Por ello, Nieva explica que se están dando nuevas variantes de WannaCry que pueden ser letales. WannaCry es una pieza de ingeniería muy bien construida: "Tiene métodos diseñados para saltarse el sandboxing (detonar el software en un entorno virtual aséptico). Es lo que se denomina Kill Switch, que direcciona a un dominio que no existe y no llama la atención dentro del sandboxing, por lo que puede saltar la barrera corporativa".

Nieva afirma que "las empresas tienen que tener mucho más cuidado con la seguridad. Las compañías en general han sido laxas en este sentido. Ha habido países en los que el impacto ha sido mínimo, por ejemplo Israel, y no porque no haya sido atacado, sino porque su concienciación y protección son mayores". Al experto no le sorprende que países como Rusia o Reino Unido hayan sido los más 'saqueados', porque la puerta de entrada es el usuario. "El usuario tiene demasiado poder, y decide en los procedimientos de seguridad. Este modelo no se sostiene, hay muchas medidas que son incómodas para el usuario, pero se ha demostrado que son válidas en situaciones como esta". Las empresas que tienen menos segmentación de redes han sido las que más equipos han tenido infectados. "Si tienes muy separadas las redes, aisladas entre ellas, las empresas siguen funcionando con normalidad. Hay que segmentar para contener".

De cara al futuro, se temen nuevas y sofisticadas amenazas. The Shadow Brokers va a poner en marcha un Marketplace (pago por suscripción) de nuevas amenazas hackeadas a Equation Group, lo que promete diversión para los próximos meses. ■

> **Marcus Hutchins adquirió por 10 dólares el dominio señalado en el código y desactivó el gusano**

Vinculan **WannaCry** con Corea del Norte

Equation Group son los hackers de la **NSA**

CIBERSEGURIDAD: UNA CUESTIÓN DE ESTADO

Hace dos años, la conclusión de un encuentro con responsables de seguridad de las grandes empresas de nuestro país era tan cruda que no podía publicarse por no ser políticamente correcta. "Estamos jodidos", esa era la sensación de estos directivos que tienen que bregar con las amenazas que tratan día a día de invadir su coto corporativo, ya sea mediante ataques de denegación de servicio, el 'scan CEO' (una suplantación de los ejecutivos de las compañías) o el propio ransomware, que si ya venía siendo la gran estrella mediática del cibermal, acaba de consagrarse como el arma preferida para desestabilizar a nuestras empresas, a nuestros sistemas de salud, a nuestros bancos, nuestras infraestructuras críticas…

Internet es el cuarto escenario de guerra, y así lo institucionalizó Barak Obama durante su primera legislatura. Donald Trump ha firmado, el mes pasado, una orden ejecutiva para fortalecer la ciberseguridad en Estados Unidos. Si la mayor potencia occidental está concienciada y preparada para combatir el que va a ser el enemigo número uno del siglo XXI, no resulta comprensible que en España, nuestros mandatarios vivan en el limbo en torno a este asunto tan grave.

Si como tantas veces se ha denunciado desde Computing, la clase política parece vivir al margen de las Tecnologías de la Información, resulta sonrojante ante la seriedad de la situación que ningún portavoz del Gobierno haya salido a la palestra para informar y tranquilizar sobre un hecho al que tarde o temprano nos podemos ver abocados de nuevo. Las TI y la ciberseguridad deben ser una cuestión de Estado. El ataque del 'viernes negro del ransomware' ha sido global y tiene todas las trazas de haber sido un ataque coordinado. A qué esperan nuestros gobernantes para saber que la cosa les concierne muy directamente. Y que todos nos la jugamos en el envite.