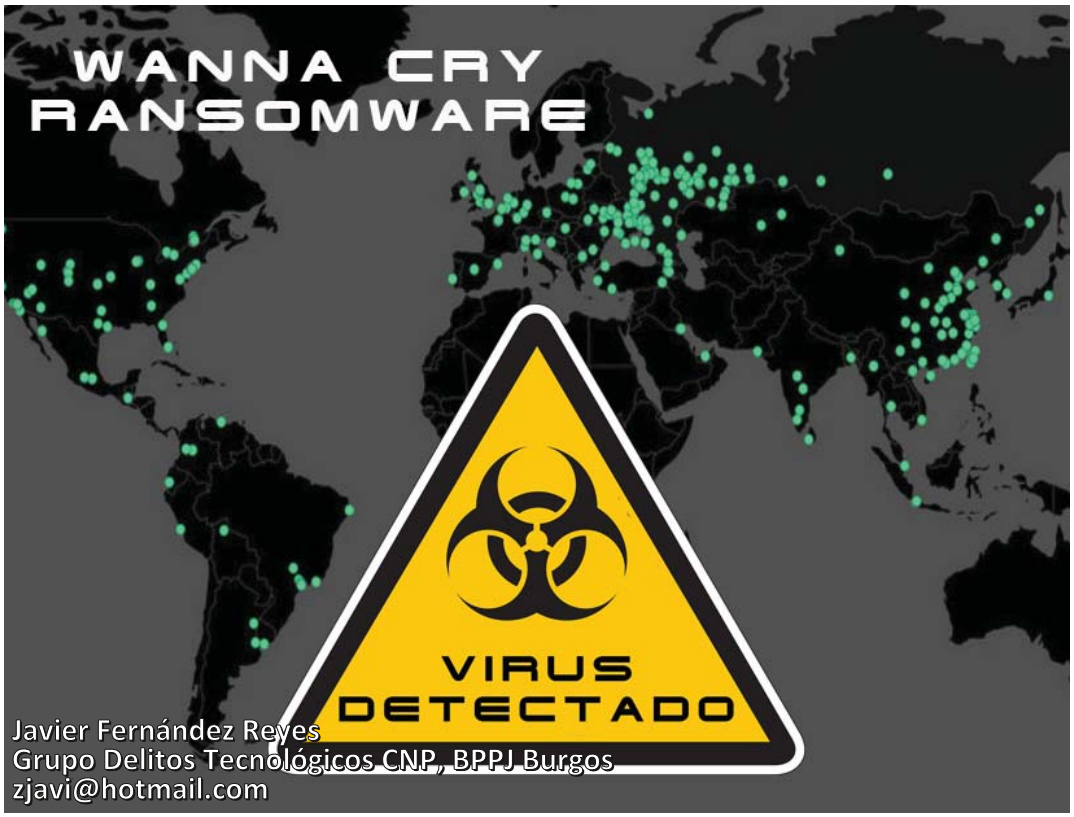

Javier Fernández Reyes
Grupo Delitos Tecnológicos CNP, BPPJ Burgos
zjavi@hotmail.com

Mucho se ha hablado del virus *WannaCry* del tipo *Ransomware* estos últimos meses, y que ha afectado a muchas empresas a nivel mundial como Telefónica, Gas Natural, Iberdrola, etc. pero ¿qué es exactamente el *ransomware Wanna Cry*?

Un virus es un programa creado por una persona, con un fin concreto, robar datos, recopilar información, dañar el sistema u otros intereses. Lejos quedó aquella época en la que se decía que los creadores de los virus eran las propias casas de antivirus para obtener así un beneficio económico vendiendo su producto.

La creación de este tipo de programas dañinos (*malware*), es usado por empresas, países, ciberdenlicuentes o simplemente, por usuarios para demostrar su habilidad tras una pantalla, si bien, los objetivos finales que promueven dicho comportamiento son muchos y variados, y serán objeto de otro artículo.

En unos casos, los virus aprovechan los agujeros de seguridad que pueden tener algunos programas, en el caso que nos lleva, el virus *WannaCry*, aprovechó una vulnerabilidad que tenían y seguro que aún tienen algunos ordenadores con sistemas operativos Microsoft, co-

mo es el caso de Windows XP, Vista, 7, 8, 8.1, 10, así como las versiones servidor Windows Server 2003, 2008, 2012 y 2016, si es su caso, desde el centro de descargas de Microsoft Update, obtendrá el parche para su sistema, igualmenmente, la gran mayoría de las casas de antivirus, han desplegado el parche de seguridad para solucionar la vulnerabilidad.

En muchas ocasiones se utiliza el término virus para referirse a cualquier tipo de *malware*, pero hay que señalar características de lo que es un virus. El término "virus" hace referencia al programa malicioso que está en el equipo de forma latente, y se activa cuando se ejecuta el archivo que está infectado, para, a continuación, infectar el resto de archivos que se están ejecutando en el ordenador y, de esta forma, el virus intentar replicarse.

Por otro lado existe lo que se denomina "gusano", siendo igualmente un *software* malicioso, que en su caso lo que hace es contaminar a otros equipos de la red informática, siendo esta la forma de propagación de *WannaCry*, de ahí que los administradores de la red de la mercantil Telefónica como se vio en las noticias, comunicaran a sus empleados que apagaran los ordenadores, de esta forma evitarían que se contagiaran equipos limpios de la misma red, y que los contaminados no facilitaran la propagación de *WannaCry*.

Pero ¿cómo se contamina inicialmente un usuario? La forma más habitual de contagiarse junto con el uso de pendrives y descargas de *software* de sitios webs poco fiables, es a través de correos electrónicos. El abrir correos de remitentes desconocidos o cuyo remitente hace creer al destinatario que procede de una empresa o servicio de confianza, etc. hace que demos pie a que se infecten nuestros equipos.

Una vez abierto el archivo adjunto del correo de dudoso origen, éste activa lo que se llama "dropper" cuya función es aprovechar la conexión a Internet (y/o conexión de red) para descargarse Wanna Cry y es en ese momento cuando se contamina el equipo, puesto que el gusano aprovecha la vulnerabilidad MS17-10 del sistema que permite la ejecución remota de código por parte de un atacante para ejecutar una acción. Vulnerabilidad ésta, que ya fue publicada por Microsoft el 15 de mayo de 2017 y por la que comunicaba el nivel de criticidad de la misma y la actualización de seguridad correspondiente.

El virus es imparable, los equipos vulnerables se contagian de manera masiva y a velocidad de vértigo.

El virus es imparable, los equipos vulnerables se contagian de manera masiva y a velocidad de vértigo, y ¿ahora qué? Infectado el sistema, entra en funcionamiento lo que se conoce como "payload" (el cual está embebido en el propio *dropper*), siendo este *payload* la parte del código malicioso que se encarga de culminar el daño final definido por el ciberdelincuente, en el caso que nos lleva, cifrar los datos del equipo, de ahí el englobar *Wanna-*

Cry en la familia de virus del tipo "ransomware" o secuestradores, ya que se pierde el control de los archivos, ya no son accesibles por el usuario al ser ilegibles.

Si el usuario quiere acceder a sus datos, no podrá, están encriptados; si quiere recuperar su valiosa información, se le pide un rescate de unos 300 euros en divisa virtual Bitcoins, a cambio de la clave de desencriptación.

Como cualquier tipo de secuestro, jamás se debe pagar y doblegarse al chantaje, no solo porque se alienta a que se siga realizando este tipo de prácticas, sino porque recibir la clave de desencriptación no es sinónimo de que esta vaya a funcionar, ni garantía de que se vayan a recuperar los datos.

Una pregunta que puede surgir es; y si se tenía conocimiento de que existía esa vulnerabilidad ¿por qué no se implementaron las medidas de protección correspondientes? La falta de actualización de los sistemas operativos y *software* de terceros fabricantes no se debe a capricho, sino a una medida preventiva de seguridad, aunque parezca contradictorio tiene su sentido. Microsoft, de manera habitual, informa de las vulnerabilidades de sus sistemas y publica las actualizaciones correspondientes conocidas como "hotfix", coloquialmente llamados parches de seguridad, los cuales pueden jugar una mala pasada a los administradores de una red, ya que aunque no sea lo normal, ese parche no solo no puede solucionar el problema para el que ha sido destinado, sino que además puede dañar otros servicios.

La necesidad de implementar una solución urgente hace que, desde Redmond, los ingenieros de Microsoft no puedan testear con garantías suficientes las actualizaciones de seguridad, esa labor se hará a posteriori publicando los "Services Packs", lo que viene siendo una recopilación de "hotfix" ya testeados con garantías.

Cualquier red informática que se precie e independientemente del servicio que preste, no se puede permitir el lujo de que su sistema se venga abajo por una mala solución preventiva, por lo que en muchos casos, antes de implementar en la red corporativa un parche de cualquier distribuidor de *software*, éste es instalado y probado en unos equipos controlados, para una vez verificados, instalarlos en el resto de ordenadores de la red. Evidentemente en grandes redes informáticas como puede ser el caso de Telefónica, este proceso de verificación se prolonga en algunas ocasiones en exceso dado el volumen de datos a comprobar.

De todos es sabido que la seguridad total no existe y en el mundo de la informática no va a ser una excepción, motivo por el cual estas empresas suelen tener un plan de contingencia para que en caso de que suceda una incidencia, la capacidad de resiliencia sea mínima, hecho que demostró Telefónica.

Como cualquier tipo de secuestro, jamás se debe pagar y doblegarse al chantaje, no solo porque se alienta a que se siga realizando este tipo de prácticas, sino porque recibir la clave de desencriptación no es sinónimo de que esta vaya a funcionar, ni garantía de que se vayan a recuperar los datos.

¿Cómo se paró la propagación de *WannaCry*? Los creadores de éste virus tenían previsto el bloqueo de *malware* a través, pero ¿por qué dejar un "botón de autodestrucción"? Una vez sale a la luz una vulnerabilidad, ésta se intenta explotar al máximo por el ciberdelincuente ya que una vez descubierta, empresas y usuarios se apresuran en implementar las medidas de protección correspondientes. Entonces ¿qué sentido tenía dejar la posibilidad de bloquear el virus?

Rápidamente las casas de antivirus, Microsoft y sobre todo el CERTSI (Centro de Respuesta ante Incidentes Cibernéticos de Seguridad e Industria) que opera bajo INCIBE (Instituto Nacional de Ciberseguridad) y junto con la coordinación del CNPIC (Centro Nacional de Infraestructuras Críticas), publicaron los parches correspondientes para proteger los equipos no infectados, pero un joven analista de *malware* conocido como @MalwareTechBlog, empleando técnicas de ingeniería inversa, logró frenar la propagación de *WannaCry*. Para ello y, tras analizar el código del virus, descubrió que este *malware* intentaba conectarse a un dominio de Internet concreto, dominio que al no estar creado permitía seguir actuando a este *malware*. Como resultado del estudio, el analista decidió registrar dicho dominio y es esa conexión correcta entre el virus y el nombre de dominio lo que permitió frenar su propagación. ¿Qué fin tenía dejar esa puerta abierta por parte del ciberdelincuente?

Desde que comenzaron este tipo de infecciones allá por el año 2011, han salido a luz diversas variantes de *ransomware*, desde el Cryptoloker pasando por Android Koler, hasta el actual *WannaCry*, pudiendo asegurar sin ningún género de dudas, que a fecha de publicación del presente hay nuevos virus y variantes de *ransomware*.

Las primeras versiones se camuflaban bajo la apariencia de mensajes procedentes de correos electrónicos de entidades públicas, como el mensaje de Correos por el que informaban de que se tenía una carta certificada e invitaban a pinchar sobre un enlace para recibir información sobre la misma, enlace que al pincharle conllevaba irremediablemente a la infección del equipo. O el famoso "virus de la policía", cuya fuente de contagio eran los malos hábitos de navegación de algunos usuarios al visitar páginas poco fiables y/o seguras, descargas de *software* pirata, etc. Una vez contaminado el equipo, se bloqueaba el acceso al sistema operativo no permitiendo el acceso mostrando una pantalla simulando ser el Cuerpo Nacional de Policía usando la imagen corporativa del referido cuerpo policial, acusando al usuario haber descargado pornografía infantil, *software* pirata o películas y música, pidiendo un pago de 100 euros a través de plataformas y pasarelas de pago como uKash o Paysafecard para así evitar la acción penal. El que fuera una cuantía mínima y junto al hecho de que saliera a la luz tal acto que dañaría la reputación e imagen de la víctima, hacía que un gran número de usuarios pagaran por el desbloqueo del equipo, desbloqueo que nunca llegaría y que conllevaba, en algunos casos, a repetir el pago y, en otros, llamaban a Comisaría quejándose porque no se les había desbloqueado el equipo tras haber pagado la multa. Este tipo de "virus de la policía" tuvo diversas variables, llegando a fotografiar a través de la webcam al usuario y mostrando su imagen en la pantalla, para que no se tuviera ninguna duda sobre la identidad del autor y coaccionar aún más a la víctima a realizar el pago.

Desde la Policía Nacional, se informó en diversas ocasiones y por distintos medios de éste virus, así como de la forma de solucionar el secuestro del virus que no permitía acceder al sistema. Y como en otros delitos monetarios, hubo una cifra negra de víctimas difícil de cuantificar.

Tiempo después y, por parte de la Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, se procedió a la desarticulación de la célula que operaba en España para el blanqueo de capitales procedente de los pagos que generaba el *ransomware*, y de la detención de un ciudadano ruso en Dubái, creador del virus.

Posteriormente nacieron otras versiones de este virus, esta vez afectaba a las versiones de Windows Server usadas en empresas, esta vez más dañino, ahora permitía acceder al sistema pero en contrapartida encriptaba los archivos de datos de las sociedades mercantiles, y dada la importancia de los mismos, garantizaba en más o menos medida cobrar por el secuestro de datos.

Pero, ¿por qué dejarlo ahí?, surgieron nuevas variantes por las que afectaban a versiones

de usuario de sistemas operativos Microsoft, Windows XP, Vista, 7,… y cómo no, si un *smartphone* es una extensión de un ordenador personal, también hay virus que afectan a sistemas Android con la misma finalidad; encriptar documentos, fotografías, etc.

Tal es la cantidad de virus de este tipo, que ya no llama la atención el oír que a una persona le han encriptado los datos del móvil u ordenador, pero llama la atención cuando las víctimas son grandes empresas.

Como la tendencia futura es un aumento de virus del tipo *ransomware*, es recomendable tomar una serie de sencillas medidas tanto preventivas como reactivas en caso de ser infectado, lo difícil es habituarse a las mismas y no dejarlas de lado como si de una dieta se tratara.

Tener los equipos actualizados con los últimos parches de seguridad del sistema operativo.

Hay antivirus con herramientas antiespía, *antimalware*, *firewall*, etc. que facilitan estas labores, pero no son del todo útiles si no se tienen buenos hábitos de navegación a la hora de ver páginas webs o realizar descargas, recordando que no se debe abrir correos de origen desconocido, mucho menos pulsar sobre los enlaces que puedan contener, ni abrir los archivos adjuntos.

En caso de que el usuario haya sido infectado por algún tipo de *malware* tendremos que recurrir a las copias de seguridad, copias de las que solo se acuerda uno cuando tiene problemas, por lo que un buen consejo es programarlas para que se hagan de manera periódica. Pero cuidado, de nada nos sirve hacer los *backups* en un disco externo y dejarlo conectado siempre al ordenador, ya que de hacer esto, también se cifrarán los datos de nuestra copia de seguridad.

Si nuestro equipo ha sido infectado y no disponemos de copia de seguridad, solo nos queda guardar nuestro disco duro y esperar a que se publiquen los algoritmos de desencriptado, evidentemente, nunca hay que pagar al ciberextorsionador.

De forma periódica se publican las claves de desencriptado de los diversos virus del tipo *ransomware* que operan cada día. Uno de estos casos, a modo de ejemplo, es www.nomoreransom.org, un proyecto de la policía holandesa desde donde facilitan la posibilidad de recuperar nuestros datos cifrados de forma gratuita, así que solo será cuestión de tiempo que implementen la solución a *WannaCry*. ■