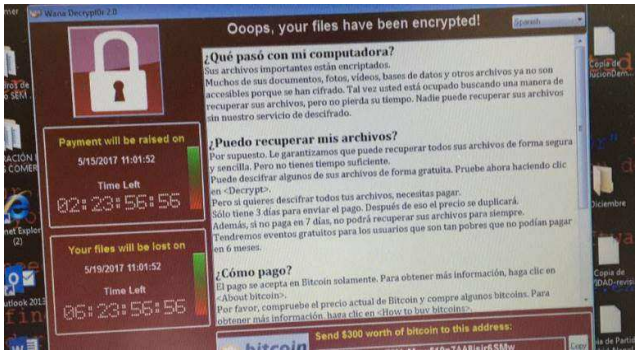
CIBERATAQUES. Amenazas globales, ensayos reales

Recientemente hemos tenido nuestro viernes negro para la ciberseguridad. Un ataque masivo de *'ransomware'* que comenzó afectando a Telefónica en España y, según la Agencia de Cooperación Policial Europea EUROPOL, eleva el número de incidencias o víctimas a más de 200.000 por el ciberataque a nivel global a 179 países y, todavía, suma y sigue.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Ha sido un ciberataque masivo con un *software* malicioso llamado *'ransomware'*, (del inglés 'ransom', rescate, y 'ware', software), en concreto con el programa conocido popularmente como *'WannaCry'* (QuieroLlorar).



El *'ransomware'* se hizo popular en Rusia y su uso creció internacionalmente en junio del 2013 y, en la actualidad, multitud de entidades se enfrentan a este tipo de virus -y a la consiguiente petición de recompensa económica de los hackers para eliminarlo- infinidad de veces al año.

El ataque informático que ahora nos ocupa, propagado a nivel internacional en 48 horas, ya ha afectado a 600 entidades españolas, según confirmó el Instituto Nacional de Ciberseguridad (INCIBE), de las que menos de diez corresponderían a empresas estratégicas u operadores críticos, como ha sido el caso reconocido de Telefónica.

El *'ransomware'* es un virus que se detecta fácilmente porque, en su propia intención de beneficio, conlleva la apertura en la pantalla del ordenador de una ventana pidiendo una cantidad por el rescate.

En esta ocasión, España ha sido el primer país, y Rusia el más afectado, seguido de Reino Unido, Estados Unidos, Canadá... así hasta más de un centenar de países. El ciberataque se inició en Telefónica por una brecha de Microsoft, detectada y 'parcheada', que se fue extendiendo como una mancha petrolera a centenares de entidades públicas y privadas y, aunque todavía no tiene autor reconocido, sí se sabe cómo se produjo, por qué se produjo y si se podía haber evitado.

"El impacto en España fue llamativo al inicio, pero un incidente que parecía local, al final se ha transformado en enorme ciberataque mundial", ha explicado el director de operaciones del INCIBE, que ha recibido informes de firmas afectadas en toda Europa, EE.UU. y Asia. *"La propagación es tremenda, jamás había visto nada*

*igual, es una locura***"**, también decía a Wired, Adam Kujawa, director de inteligencia de Malwarebytes, firma que descubrió la primera versión de *WannaCry*.

El ciberataque a nivel mundial, parece que tenía como objetivo cifrar los archivos del equipo infectado para pedir un rescate por *BitCoins*, distribuyéndose por los equipos mediante un 'dropper' (programa diseñado para instalar algún tipo de malware) enlazado a un correo electrónico que era imposible de detectar por muchos sistemas antimalware**.**

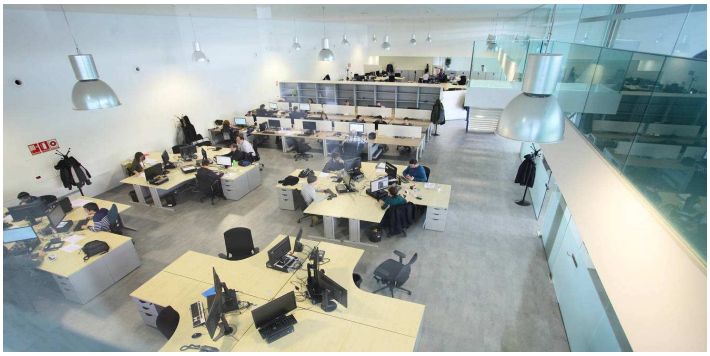
Por su lado, la unidad de emergencias del Centro Criptológico Nacional (CCN-CERT), ha confirmado en un comunicado que el ataque se ha producido utilizando una herramienta conocida como *EternalBlue,* usada por la NSA (Agencia de Seguridad Nacional de EE.UU.) para labores de espionaje, y filtrada por el grupo de *hackers 'ShadowBrokers'*.

No obstante, aunque Microsoft solucionó esta vulnerabilidad el pasado mes de marzo, las entidades que no han actualizado sus sistemas estaban expuestas.

Este ciberataque masivo muestra una terrible consecuencia de un presunto beneficio que hemos aceptado sin muchos comentarios, y es la de que una herramienta desarrollada supuestamente para protegernos en realidad nos puede destruir.

Realmente este maléfico *EternalBlue*, usado y desarrollado por la NSA para infectar ordenadores en remoto y espiar a sus propietarios, fue publicado en Internet por los *'hackers' 'ShadowBrokers'*. Sin mucho esfuerzo, el autor del *'ransomware' 'WannaCry'* pudo por tanto utilizarla como mecanismo para infectar y secuestrar cientos de miles de ordenadores.

Por otro lado, el CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) y el INCIBE (dependiente del Ministerio de Energía), han confirmado que, por el momento**,** "no más de diez" empresas españolas se han visto verdaderamente afectadas por el ciberataque.



Esta debacle informática que ha supuesto la acción de *'WannaCry'*, ha creado una alarma social que algunos ya califican de “ciberapocalipsis”.

Alarma social. Ciberapocalipsis

El ciberataque también ha sido ratificado por el Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), que informa que la oleada de *'ransomware'* que ha afectado a multitud de equipos, ha sido producida por la infección masiva con el virus *'WannaCry'* que, una vez instalado, bloqueó el acceso a los ficheros de cada ordenador afectado.

Igualmente, los expertos avisan que, seguidamente, puede haber una segunda oleada de *'hackeos'* masivos.

Según EUROPOL, la amenaza puede escalar e ir a más inmediatamente, y lo que no está claro es qué magnitud tendrá. Puede haber un repunte, dado que muchos sistemas ya han sido vacunados, o *'WannaCry'* nos puede sorprender con una nueva versión que vuelva a afectar a medio planeta, dado que muchos expertos califican a este virus de “extraño”.

Así, aunque ya podemos dejar de imaginar cómo sería una “ciberapocalipsis”, la situación que acabamos de vivir, el ciberataque masivo mundial de *'ransomware'* afectando a empresas y organismos públicos e infraestructuras críticas como los ferrocarriles rusos, los hospitales en Reino Unido o las comunicaciones en España, pasando por fabricantes de coches en Francia o Turquía, es uno de los mayores ataques informáticos de las últimas décadas y el mayor usando *'ransomware'* que ha ha generado semejante alarma social.

Y, todo, como consecuencia de que la Agencia de Seguridad Nacional de EEUU (NSA) que lo puede saber todo, absolutamente todo, de nuestra vida privada y de la de cualquier ciudadano en el mundo, sin pedir permiso y con total impunidad, ha creado esta herramienta bajo el argumento de combatir el terrorismo, lo que hace posible espiar de forma indiscriminada a cualquiera.

El conocimiento de este agujero de seguridad se lo debemos a Equation Group, uno de los grupos de *hackers* de élite de la NSA, quienes 'disfrutaron' de la herramienta durante años, hasta que otro grupo de *hackers*, el llamado Shadow Brokers, les robó esta información y la difundieron al mundo.

En solo cinco años, estos virus se han situado en el top 3 de las peores amenazas informáticas, y esta alarma social, todavía no apocalipsis cibernético, se veía venir y acaba de suceder, convirtiendo un *'ransomware'* en un 'gusano' que se propaga solo por las redes de forma automática.

Espionaje, terrorismo, delincuencia

El mapamundi de la piratería digital se presenta como escalofriante, y no vale pensar que es un problema de otros. La empresa de ciberseguridad Kaspersky Lab calcula que ya algunas regiones del planeta son víctimas de 12 ataques por segundo.

Bajo la amenaza de “paga o destruimos tus datos”, este formato delictivo ha encontrado un caldo de cultivo extraordinario en la sociedad de la comunicación y la información, que ha revelado así su extrema vulnerabilidad.

Según ha publicado The New York Times, las primeras estimaciones que los expertos cifraron es que los *'hackers'* acabarían embolsándose unos mil millones de dólares en todo el mundo, luego de que estos cientos de miles de incidencias o víctimas de más de un centenar de países se viesen afectados.

No obstante, pese a esta predicción, los investigadores consultados por el diario británico The Guardian aseguran que los atacantes habrían recibido por ahora

algo más de 56.000 dólares. Esta muy baja cifra recaudada siembra dudas sobre la verdadera intención del ataque todavía no descubierta.

Estos ataques de *'ransomware'* se integran en una conducta típica del delito de daños y sabotajes (*'cracking'*) que prevé nuestro Código Penal: el tipo actual del art. 264 CP castiga las conductas. Por ello, la prevención frente a este tipo de acciones debe tener una clara dimensión técnica, no sólo jurídica.

Pero, la Policía puede hacer poco contra estos delincuentes, escudados en el "cibercrimen internacional", atacando normalmente a particulares y empresas pequeñas que no tienen recursos propios para luchar contra ellos, excepto la consabida denuncia policial.

Lo cierto es que España se encuentra en la posición 18 del ranking por Estados, con algo menos de 600 infecciones confirmadas de esta variante del virus *'WannaCrypt.A'.* En cuanto a las del segundo tipo, las de *'WannaCrypt.B',* en España de momento "no hay datos disponibles", salvo que se trata de la variante que ha afectado a Telefónica.

Estamos ante un una importante agresión que, el exdirector nacional de inteligencia de Estados Unidos, James Clapper, ya hace un año advertía, indicando que los ataques cibernéticos suponían una amenaza incluso mayor que el propio terrorismo.

Amenazas globales, soluciones globales

Según un estudio de la empresa Panda, *"Este tipo de ataques afecta a todo el mundo, pero hemos visto cómo los delincuentes tratan de ir a por empresas, ya que poseen información valiosa por la que están dispuestos a pagar un rescate".* Así, los *malware* han dejado de ser obra de atacantes individuales para convertirse en redes de bandas organizadas internacionales para generar dinero donde los tradicionales programas de antivirus ya no son suficientes.

Por otro lado, según la empresa Check-Point, el *'ransomware'* es la estrategia más utilizada para atacar a las grandes empresas. *"Los* hackers *piden que el rescate se realice a través de un pago digital que no se pueda rastrear".* Así exigen el pago en *'BitCoins'* que es una moneda virtual no regulada por ninguna institución central cuyas transacciones son anónimas y se realizan con claves secretas, lo que convierte al *'BitCoin'* en un arma de cambio perfecta para este tipo de actividades ilícitas, difícilmente rastreable**.**

El *'ransomware'* es para un ciberdelincuente una de las formas más baratas y efectivas de ganar dinero, con un archivo adjunto infectado y el simple hecho de pedir un rescate con solo apretar un botón que es capaz de contagiar a miles de ordenadores mediante el efecto cadena que hace que las ganancias se multipliquen sin esfuerzo ni inversión.

MANUEL SANCHEZ GOMEZ-MERELO

Según la empresa Verizon, este tipo de ataques ya representan el 70% de las amenazas informáticas que se producen en el mundo, donde un 64% de las víctimas acaba pagando

No obstante, el INCIBE informa que *"se está conteniendo la propagación de la infección a nuevos sistemas informáticos y países al aplicar los mecanismos de prevención que se están publicando y difundiendo a nivel mundial".*

Como conclusión se evidencia que hace falta una estrategia de alcance global para frenar las amenazas globales de los ciberataques.

Vulnerabilidades manifiestas

Igualmente, a sabiendas de que las vulnerabilidades son importantes, en forma y dimensión, no es fácil de entender cómo es posible que hayan sido atacados y vulnerados, tanto multinacionales cómo operadores de infraestructuras críticas de comunicaciones, transporte, energía u hospitales (en las que un descuido informático puede incluso costar vidas), sin que entidades de este calibre no hayan sido más diligentes a la hora de parchear sus sistemas por amenazas ya conocidas.

Ha sido una de estas vulnerabilidades, de las que ya avisó Microsoft, la que ha permitido el ciberataque a nivel mundial. El error en su sistema fue corregido, pero la publicación de una prueba de concepto del agujero de seguridad desencadenó la campaña.

La vulnerabilidad de Windows utilizada por esta versión de *'WannaCry',* conocida como *EternalBlue,* ataca al protocolo de compartición de ficheros SMB de Windows. Esta vulnerabilidad fue anunciada y corregida por Windows el 14 de Marzo de 2017, con nombre MS17-010. El 14 de Abril de 2014 Shadow Brokers filtró la información relativa a un *exploit* desarrollado por la NSA para esta vulnerabilidad.

Según la empresa de seguridad S21sec el gusano explotaba una vulnerabilidad del sistema operativo Windows para “infectar” otros ordenadores vulnerables que estén en la misma red local que la máquina afectada, consiguiendo una velocidad de propagación muy alta.

Y, tristemente, el 95% de los bancos a nivel global aun siguen utilizando Windows XP en sus terminales bancarias y cajeros automáticos.

Igualmente, el sistema de salud del Reino unido, uno de los más afectados con este ataque virulento, aún continúa utilizando en un 95% el obsoleto sistema operativo en sus servidores y terminales.

Por otro lado, en el momento de escribir estas líneas, hay en Internet 1,5 millones de dispositivos con el puerto 445 abierto, según el buscador Shodan, aunque esto engloba todo tipo de sistemas operativos, cuando solo los Windows son vulnerables.

Lo cierto es que las graves consecuencias de estos riesgos, amenazas y vulnerabilidades han sido manifestadas mediante un simple *'ransomware'*, con un cibersecuestro de datos y archivos que los encripta de manera que no se puede acceder a ellos**.** Los ciberdelincuentes o presuntos terroristas han extorsionado a los afectados, a los que han exigido un rescate económico para liberar -descifrar- sus propios archivos.

El *modus operandi* es muy sencillo. Pasa por camuflar el virus en cualquier archivo que pueda ser de interés del usuario. Basta con que un empleado haya recibido un correo electrónico infectado y lo abra -el método más común-. O que esté navegando en páginas de mala o dudosa reputación y se contamine. O simplemente que pinche en un enlace de origen desconocido y se lo inocule.

Con todo ello -y sin el parche oportuno-, no se puede hacer nada más que aislar la red o apagarla, según el caso. Esto es lo que han hecho muchas de las entidades que no llegaron a ser infectadas, pero que no tenían el parche instalado.

Pero, lo más grave es que, en la mayoría de los casos, no existen políticas rigurosas de actualización de las protecciones que es, fundamentalmente, responsabilidad no solo de los departamentos de seguridad, sino de los directivos y altos cargos en empresas y gobiernos que no entienden ni ven la importancia de toda esta amenaza global.

El CERTSI**,** el INCIBE, el CCN-CERT y otros institutos de ciberseguridad no han tardado en informar nuevamente de que la única manera de que los sistemas no resulten infectados es *"tener los sistemas de protección actualizados en su última versión o parchear, según recomienda el fabricante"**.*** Es decir, este caso, aplicado el parche del que Microsoft advirtió el pasado 14 de marzo, como ya se ha dicho.

En este sentido, igualmente lo explicó anteriormente el CCN-CERT: *"La especial criticidad de esta campaña viene provocada por la explotación de la vulnerabilidad descrita en el boletín MS17-010 utilizando EternalBlue/DoublePulsar, que puede infectar al resto de sistemas Windows conectados en esa misma red que no estén debidamente actualizados. La infección de un solo equipo puede llegar a comprometer a toda la red corporativa"*.

Y aunque, como es sabido, las iinfraestructuras críticas y grandes entidades estratégicas tienen especiales vulnerabilidades, en este caso, en España, según fuentes del Ministerio de Interior y del Ministerio de Energía, al menos cinco empresas españolas estaban entre las afectadas, pero no podían revelar los nombres (salvo el de Telefónica, por haber aclarado ella misma su situación).

Por su parte, el Director de la NSA, subraya que el *ataque "manda un mensaje muy claro: todos los sectores son vulnerables"* y ha puesto el ejemplo del sector bancario, que apenas ha sufrido consecuencias por el virus *'WannaCry'*, porque *"han*

aprendido a partir de dolorosas experiencias", invitando al resto de compañías a seguir su ejemplo en medidas de seguridad.

Vigilancia cibernética

El Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), ha ratificado que la oleada de *'ransomware'* que ha afectado a multitud de equipos, se produjo por una infección masiva de equipos con el virus *'Wannacry'* y ha insistido que *"Se recomienda aplicar los últimos parches de seguridad publicados por Microsoft"*, informaba el comunicado.

Un investigador de MalwareTech, un británico de apenas 22 años, ha sido el que ha logrado dar con la solución para frenar el avance del *'ransomware'*, aunque anunciando que, pese a cierto control de la situación, "nada ha acabado", añadiendo que *"Los 'hackers' se darán cuenta de cómo lo hemos parado, cambiarán el código y volverán a empezar"*.

Hay que insistir una vez más en que la clave está en las actualizaciones mensuales de Microsoft, como la de su boletín MS17-010, en el que advertía de hasta 56 vulnerabilidades, 41 clasificadas como importantes y 15 de ellas críticas, que afectaban a productos como .NET, DirectX, Edge, Internet Explorer, Office, Sharepoint y Windows**.**

Así, la propia tecnología ofrece soluciones frente a los riesgos que genera: el software antivirus y los sistemas de seguridad y de detección de intrusos son ejemplos de este tipo de medidas, aunque, en algunas ocasiones, puede existir una incompatibilidad entre los parches que recomienda el fabricante y el software a medida del que algunas entidades disponen, lo que retrasa las comprobaciones y verificaciones que confirmen que esos nuevos parches no van a 'romper' ninguno de estos programas específicos o personalizados.

En cualquier caso, el INCIBE ha publicado unas recomendaciones para que podamos sentirnos algo más seguros, aunque próximamente sabremos si llega o no un nuevo 'ciberapocalipsis'.

Las empresas cuentan también con una defensa que el CCN-CERT puso a disposición de todo el mundo muy al principio del ataque: el programa NoMoreCry, que bloquea la ejecución del *'ransomware'*.

En resumen, este tipo de ciberataque se puede prevenir y una de las claves para no caer en la extorsión es realizar copias de seguridad y limitar a los empleados el acceso a los ficheros, para que la información de los servidores no se vea comprometida.

A modo de conclusiones

El mayor ataque de la historia realizado con *'ransomware'* comienza a dejar algunos datos para la reflexión y, además, convendría recordar que es cuestión de tiempo que un ataque similar se vuelva a repetir.

Por ello, es fundamental la prevención frente a este tipo de conductas que debe tener una clara dimensión técnica, no sólo jurídica. El software antivirus y los sistemas de seguridad y de detección de intrusos son ejemplos de este tipo de medidas, sin olvidar que, el ataque ahora sufrido infectó a aquellos ordenadores que no tenían instalado el parche recomendado el 14 de marzo por Microsoft.

En cualquier caso y, en resumen, el impacto que ha tenido este ciberataque se puede relacionar con aspectos como, en general, la escasa concienciación y, en el sector empresarial, la poca formación del personal para controlar aquellos ficheros que vienen en emails “sospechosos”, así como el diferente potencial de las empresas para detectar que están sufriendo los efectos de un ataque y ser capaces de activar mecanismos de respuesta.

Del mismo modo, es importante la velocidad de respuesta de las empresas en aplicar los parches o correcciones de Windows y otras empresas suministradoras de productos y soluciones software, pues una respuesta no inmediata en la aplicación de estos parches o correcciones puede dejar a una empresa en situación de desprotección, como así ha pasado en este ataque reciente.

Finalmente, aunque no existe la protección total o garantía de no poder ser afectado, con la permanente actualización se consigue evitar sucesos como éste o al menos aminorar el importante nivel de impacto que han tenido.

Aunque todavía quedan muchos interrogantes por resolver, algunas conclusiones ya son inevitables, como pensar si los atacantes de verdad buscaban dinero, incógnita que se despejará en breve, tras la investigación correspondiente, o cuando suframos otro ciberataque similar.

También queda un interrogante aún peor, en términos de seguridad global y es que el origen del ataque sea terrorista o haya sido orquestado desde algún Estado como una prueba para verificar la efectividad del contagio entre ordenadores.

Lo cierto es que hay un crecimiento de la amenaza (en magnitud y violencia) y un incremento notable de la ciberdelincuencia que requiere un mayor monitoreo y respuestas rápidas. No obstante, aunque, al parecer, este ciberataque ha tenido más impacto mediático en las redes sociales que en el funcionamiento interno de las entidades y países afectados, urge realizar las investigaciones y los análisis correspondientes y tratar los problemas globales con soluciones globales inmediatas.

Madrid, mayo 2017

MANUEL SANCHEZ GOMEZ-MERELO