Una nueva amenaza para su empresa: Ransomware

IGNACIO JIMENEZ PI
ÁLVARO TRIGO MARTÍN DE VIDALES
Subdirección General de Seguridad y Medio Ambiente MAPFRE

El 12 de mayo de 2017, un ransomware llamado Wannacry infectó a empresas de más de 70 países, afectando a bancos, hospitales, aseguradoras, gobiernos y empresas tecnológicas de primer orden en todo el mundo en el mayor ataque cibernético conocido hasta la fecha.

¿QUÉ ES EL RANSOMWARE Y POR QUÉ DEBERÍA PREOCUPARME?

El pasado 2016 ha sido el año en el que hemos visto cómo el Ransomware se convertía en la principal amenaza para los usuarios, manteniéndose su continuidad en este 2017. Las infecciones por Ransomware están alcanzando índices de pandemia global, y la rápida monetización del ataque y rentabilidad obtenida indica que el fenómeno irá en aumento, cada vez será más difícil de contrarrestar, y los perfiles a los que irá dirigido serán de mayor nivel, llegando incluso a buscar la afectación de grandes corporaciones y gobiernos (como vaticinaba Mr. Robot).

Pero ¿qué es el Ransomware? ¿En qué afecta a los usuarios? La explicación parece casi tan antigua como la existencia de los ordenadores domésticos: Un virus que no permite al usuario acceder al sistema y/o sus archivos y que, y aquí radica su principal amenaza, nos solicita el pago de una cantidad a cambio de poder acceder (de aquí el término "ransom", en inglés, rescate). El precio de la restauración del acceso varía entre los 300 y los 1500€, y su pago no siempre garantiza la recuperación de los mismos. La clave de su éxito radica en la reducida complejidad que supone desarrollar la infraestructura necesaria para iniciar una campaña y la facilidad y rapidez para monetizar dichos ataques.

Para entender los efectos de este programa malicioso es interesante comprender su historia. Su origen fueron los conocidos como "bloqueadores". Estos virus bloqueaban el acceso al sistema operativo o al navegador del usuario hasta que la víctima pagaba un rescate, utilizando SMS o transferencias a monederos electrónicos. En España fue muy conocido el "virus de la policía", mediante el cual, se engañaba al usuario para que creyera que debía pagar una multa a raíz de una infracción cometida. Este tipo de virus sufrió un duro golpe cuando cambió la ley de pagos electrónicos, haciendo muy difícil el cobro de los rescates.

La segunda derivada, los "cifradores", implica dos cambios básicos e imprescindibles. Por un lado, la proliferación de las divisas virtuales (Bitcoin), permiten pagos de forma prácticamente indetectable, lo cual modifica de nuevo las reglas del juego y permite el repunte de este tipo de estafas. Por otro lado, en lugar de bloquear el acceso al equipo, que podría solucionarse eliminando el virus o, reinstalando el sistema operativo, el software malicioso se dedica a cifrar todos los archivos privados existentes en el equipo, que son únicos, y la reinstalación no permite recuperarlos. En el caso de cifrados lo suficientemente robustos, se convierte en técnicamente imposible la recuperación de la información sin que los delincuentes nos faciliten la operación.

Por último, desde 2014 se ha empezado a detectar la existencia e incremento constante de "cifradores" en dispositivos móviles con sistemas operativos Android, y su funcionamiento es muy similar al descrito anteriormente, dado que las aplicaciones que realizan este "secuestro", cifran imágenes, vídeos, música y documentos existentes en el dispositivo.

Una cifra que ejemplifica la magnitud de la realidad que tratamos de exponer: el FBI estima en 206 millones de dólares las pérdidas ocasionadas por el Ransomware en el primer trimestre de 2016.

¿CÓMO PUEDE ATACARME UN RANSOMWARE?

Una vez hemos comprendido la amenaza a la que estamos expuestos como usuarios, así como el posible impacto de que nos infecte un virus del tipo Ransomware, nos preguntaremos, ¿cómo puedo infectarme?

Aunque existen multitud de métodos y variantes de los mismos por los cuales podemos infectarnos, el principal método de infección es a través de troyanos en páginas web malintencionadas o legítimas que han sido comprometidas por delincuentes con el único fin de contagiar a sus usuarios. Muchas veces no se detecta un comportamiento anómalo ni afecta a nuestra experiencia de navegación, simplemente se instala el virus en segundo plano pasando inadvertido para el usuario.

El segundo método más extendido de propagación se realiza mediante el envío de enlaces a webs comprometidas en correos masivos (spam), e incluso mensajería instantánea, redes sociales, e incluso al compartir ficheros en redes P2P (torrent, etc.).

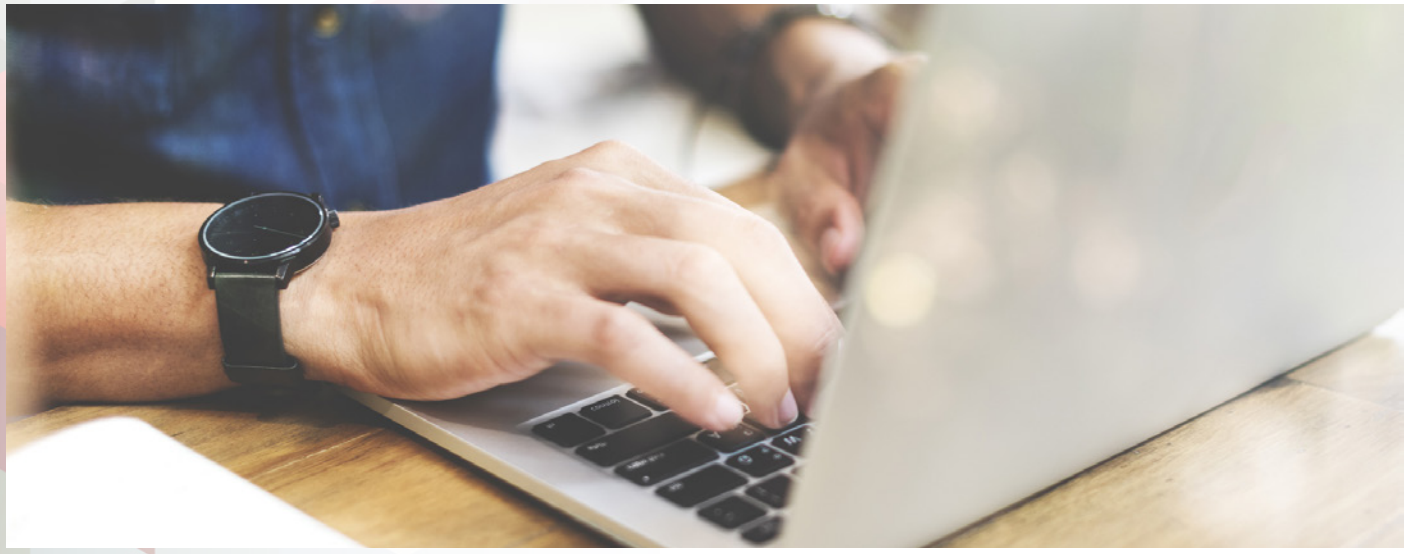
Dentro de los ataques dirigidos en empresas, aunque como usuario esto es menos habitual, también se llevan ataques dirigidos a servidores explotando vulnerabilidades conocidas en el protocolo de acceso remoto (RDP) que utilizan los administradores de sistemas para acceder a los servidores de las organizaciones.

Dado que hemos hablado del crecimiento de ataques detectados en dispositivos móviles, es importante conocer de qué forma puede introducirse un virus en nuestros dispositivos. La forma es similar, basada en engaños publicados en páginas web maliciosas, que hacen que el usuario acceda a copias de la Google Play Store con contenido malicioso, en las cuales el usuario acaba instalando una aplicación malintencionada que es la que ejecuta el "secuestro" del dispositivo. Curiosamente, muchos de estos engaños se basan en hacer creer al usuario que tiene un virus en su dispositivo, y accede a descargarse un supuesto antivirus.

¿QUÉ PUEDO HACER PARA EVITAR INFECTARME Y/O MINIMIZAR EL IMPACTO?

Entendiendo cómo funciona este tipo de programas y las formas más comunes para ser atacado, ¿qué se debe hacer para prevenir un ataque?

- La realización de copias de backup de nuestros archivos de manera regular es el método sin duda más efectivo de combatirlos. Por desgracia, en la mayoría de casos la recuperación de los archivos o de los equipos afectados será imposible, de modo que poder recuperarlo mediante copias de seguridad es casi siempre la única vía posible.
- Utilización de sistemas antivirus en los dispositivos. Como hemos visto, una de las vías más comunes es la ejecución de determinados archivos en nuestros equipos. Si se cuenta con un antivirus reconocido y actualizado, será más fácil repeler los ataques.
- Para poder dar menos oportunidades a sufrir ataques de seguridad, tanto las aplicaciones como el sistema operativo de nuestro equipo deberán encontrarse actualizados a la última versión disponible y con todos los parches de seguridad instalados. Especialmente relevante el caso de los navegadores web (Chrome, Firefox, Internet Explorer, Safari, etc.), ya que en ocasiones las infecciones se producen al navegar por determinadas páginas web (bien porque este sea su propósito o bien porque hayan sido comprometidas previamente).
- Utilizar el sentido común y como norma general, no confiar de sitios webs, archivos o links extraños o desconocidos. Si por ejemplo, nos llega un enlace a nuestro correo electrónico en relación a un pedido que no esperamos, no hacerle caso y ante la duda informarnos antes de darle. En muchas ocasiones, con una simple búsqueda en Google del asunto o del cuerpo del mensaje de correo electrónico puede ser suficiente para percatarnos de que lo que esperábamos fuese legítimo es en realidad una amenaza.
- Tener habilitadas las extensiones de los archivos puede ayudarnos a identificar de mejor manera un intento de ataque. Si por ejemplo, en un correo electrónico esperamos recibir una imagen y sin embargo recibimos un fichero comprimido (un ".zip" por ejemplo) puede ser indicador de que algo no va bien.
- Si tenemos la sospecha de que alguno de los archivos que hemos recibido recientemente puede tratarse de algún tipo de virus, lo primero de todo deberemos desconectar el equipo de la red. Ello mitigará el riesgo, especialmente en entornos empresariales, de que este se pueda expandir al resto de equipos de la red.



¿QUÉ HACER EN CASO DE INFECCIÓN?

Si por desgracia, no se han podido implementar estos controles citados, y la infección se ha producido, ¿qué es lo que se debe de hacer entonces? En primer lugar, se recomienda no pagar el rescate pedido por los cibercriminales ya que haciéndolo no se garantiza la recuperación de los archivos y sin embargo se fomenta la realización de esta práctica criminal. Según estudios recientes de la empresa de antivirus Kaspersky, uno de cada tres usuarios paga por el rescate de sus archivos y aproximadamente un 20 % de los mismos no logra recuperarlos. En su lugar, y dependiendo de la magnitud del incidente, como primera acción se aconseja valorar la posibilidad de ponerlo en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado, especialmente si se consideran vulnerados ciertos derechos fundamentales o se pone de algún modo en riesgo la seguridad de las personas. En el particular de organismos públicos y empresas de interés estratégico para el país, esta comunicación debe canalizarse a través del CERT del Centro Criptológico Nacional, el cual es el organismo público dependiente del Centro Nacional de Inteligencia que tiene como misión velar por la seguridad de los sistemas de información en la administración pública.

En este caso, la estrategia de recuperación debe de ser, primero la eliminación del archivo que produce el cifrado de los archivos en nuestro dispositivo y segundo la obtención de la clave, la llave, con la que han sido cifrados. Por suerte para nosotros, existen organismos y entidades privadas que trabajan activamente en esta tarea ofreciendo aplicaciones y recursos gratuitos que pueden servirnos para tal fin. Especialmente conocido en el mundo de la ciberseguridad es el proyecto "No More Ransom", liderado por Europol y la unidad de crimen tecnológico de la policía holandesa junto con alguna de las empresas privadas más importantes del sector. A través de esta organización, se ofrecen un conjunto de herramientas gratuitas que permiten descifrar los archivos atacados por una gran mayoría de Ransomware, así como consejos o guías para abordar un incidente de esta naturaleza.

¿EXISTE ALGUNA FORMA DE ASEGURAR UN POSIBLE INCIDENTE INFORMÁTICO?

Con el aumento de la incidencia de nuevas ciber amenazas, han proliferado en nuestros mercados la existencia de productos aseguradores cuyo fin es dar cobertura a las empresas. Un reciente informe remitido por la consultora PwC sostiene que cerca del 30 % de organizaciones norteamericanas tienen en la actualidad algún tipo de cobertura que les permite protegerse frente a las consecuencias de un ciberataque (la mayoría de los sectores de sanidad, tecnología y retail). En España la cifra es menor y hoy por hoy parecen concienciadas únicamente las empresas del Ibex 35 donde cerca de la mitad tienen algún tipo de póliza o están en proceso de contratación. Es importante señalar que este tipo de pólizas no se encuentran a menudo estandarizadas, sino que se adaptan individualmente permitiendo personalizar a las empresas las coberturas a aplicar, de modo que puedan escogerse aquellas que sean más adecuadas a las particularidades del negocio.

Dado que los ciberataques suelen impactar directamente contra la operativa de las compañías, los seguros de ciberriesgos deben estar preparados para cubrir las posibles pérdidas económicas, junto con los gastos relacionados con la investigación forense o el proceso de comunicación a los clientes (cabe recordar que el futuro reglamento europeo UE 2016/679 obligará a las compañías a informar sobre las brechas de seguridad y notificar a terceros las violaciones de sus datos). Particularizando el caso de los ataques de Ransomware, el elemento principal que

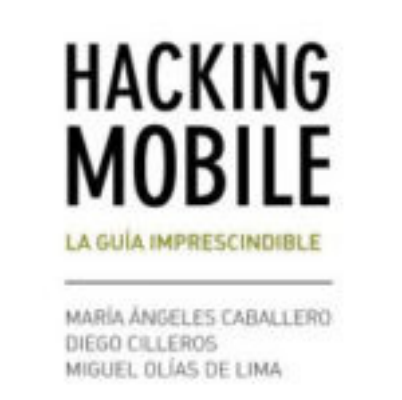
distingue el tipo de póliza a aplicar frente a otras es la cobertura en relación a los costos de extorsión.

En la actualidad, MAPFRE dispone de un Seguro de Ciberriesgos con el fin de proteger a sus clientes, PYMES y autónomos, ante este tipo nuevo de amenazas:

- Gastos de restauración de imagen.
- Multas y sanciones derivadas del ataque.
- Gastos de defensa jurídica.
- Robos de información confidencial.
- Daños a los sistemas informáticos.
- Pérdidas económicas como consecuencia de la interrupción del negocio.

Puede consultar más información en: https://www.mapfre.es/seguros/empresas/seguros-de-responsabilidad-civil/seguro-ciberriesgos/

BIBLIOGRAFÍA RELACIONADA



Dado que el Ransomware en dispositivos móviles es uno de los vectores en los que el crecimiento se prevee exponencial, si está interesado en conocer y explorar el mundo de la ciberseguridad en dispositivos móviles, le recomendamos a modo de bibliografía básica el libro "Mobile Hacking" de la editorial ANAYA donde se abordan éste tipo de cuestiones. http://www.anayamultimedia.es/libro.php?id=4312499