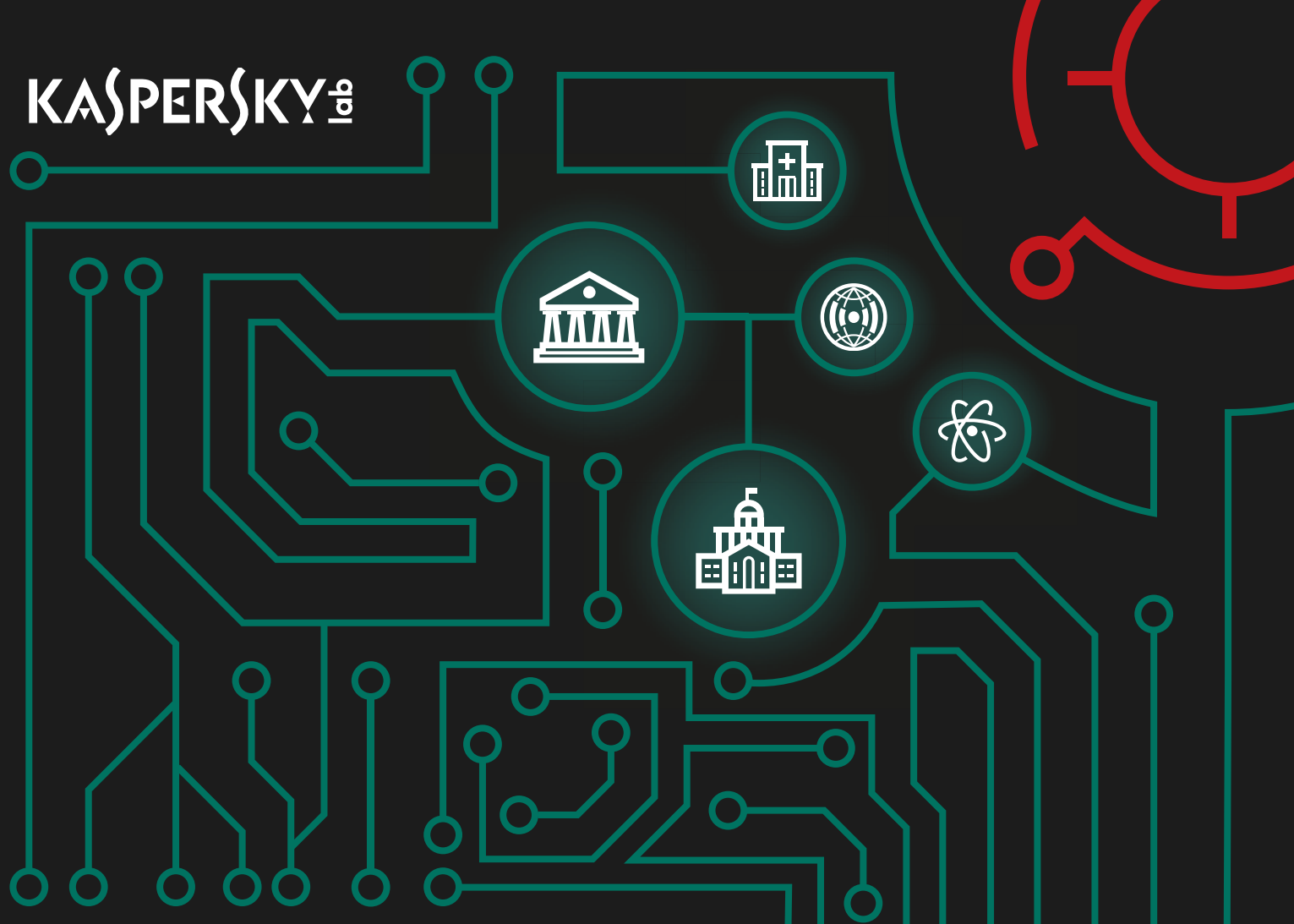
KASPERSKY lab



Kaspersky Security Bulletin:

HISTORIA DEL AÑO EN 2017

CONTENTS

NUEVA AMENAZA DE RANSOMWARE

INTRODUCCIÓN: LO QUE APRENDIMOS EN 2017

En 2017 la amenaza del ransomware de pronto se disparó de forma espectacular. Tres brotes sin precedentes transformaron, quizás para siempre, el escenario de los programas ransomware. Los ataques dirigidos contra empresas utilizaron gusanos y exploits recién filtrados para autopropagarse, cifrar datos y pedir un rescate que en realidad no querían. Los atacantes no parecen ser los ciberpiratas comunes que suelen acechar a sus víctimas con ransomware. Además, al menos uno de estos ataques contenía fallas, lo que sugiere un lanzamiento prematuro, otro se propagó mediante software corporativo infectado, dos están interrelacionados, y los dos mayores parecen estar diseñados para destruir datos. Las pérdidas para las víctimas de estos tres ataques ya han alcanzado los cientos de millones de dólares.

Bienvenido al ransomware en 2017. Este es el año en que corporaciones mundiales y sistemas industriales vieron sus nombres agregados a la creciente lista de víctimas, y en el que los atacantes selectivos empezaron a interesarse seriamente en la amenaza. También fue un año de ataques cada vez más numerosos, pero con limitada innovación.

Este resumido informe destaca algunos momentos relevantes.

LOS ESTALLIDOS MASIVOS QUE NO FUERON LO QUE PARECÍAN

WannaCry

Todo comenzó el 12 de mayo, cuando la comunidad de ciberseguridad observó algo que no se había visto desde hace una década: un ciberataque mediante un gusano que se propagaba sin control alguno. En esta ocasión, el gusano estaba diseñado para instalar el cripto-ransomware WannaCry 2.0 en equipos infectados.

La epidemia de WannaCry afectó a cientos de miles de equipos en todo el mundo. Para propagarse, el gusano recurría a un exploit conocido como EternalBlue y a una puerta trasera llamada DoublePulsar; ambos habían sido publicados por el grupo "The Shadow Brokers" un mes antes del estallido. El gusano atacaba de forma automática a todos los equipos que compartían la misma subred local que el equipo infectado, así como rangos aleatorios de direcciones IP fuera de la red local, logrando así propagarse rápidamente por todo el mundo.

Para infectar un equipo, WannaCry explotaba una vulnerabilidad en la implementación del protocolo SMB de Windows. Microsoft había publicado en marzo de 2017 una actualización para reparar esta vulnerabilidad, pero la cantidad de equipos sin el parche fue tan alta que éste no pudo detener el avance de WannaCry.

Tras infectar un equipo y ejecutar una rutina para continuar con su propagación, WannaCry cifraba algunos archivos valiosos de la víctima y le mostraba una nota de rescate. Era imposible descifrar todos los archivos afectados sin pagar el rescate, aunque nuestros analistas descubrieron varias fallas en el código de WannaCry, lo que permitió a algunas víctimas recuperar parte de sus datos sin pagar el rescate.

Impacto de WannaCry

El ataque no se centró en ninguna industria, y la mayoría de las víctimas eran organizaciones con sistemas en red. El ransomware también atacó a sistemas integrados, que a menudo se ejecutan en sistemas operativos obsoletos, por lo que son particularmente vulnerables. La nota de rescate que las víctimas recibieron exigía el pago en Bitcoins. Varios informes sugieren que el número de víctimas alcanzó los tres cuartos de millón.

El fabricante de automotores Renault tuvo que cerrar su principal planta en Francia, mientras que en el Reino Unido, los hospitales afectados tuvieron que rechazar pacientes. El gigante alemán del transporte, Deutsche Bahn, la española Telefónica, la compañía bengalí occidental de distribución eléctrica, FedEx, Hitachi, y el ministerio del interior de Rusia también fueron afectados. Un mes después de haber contenido el estallido inicial, WannaCry seguía cobrando víctimas, entre ellas Honda, que se vio obligada a cerrar una de sus plantas productoras, y 55 radares de tráfico en Victoria, Australia.

Las preguntas sin respuesta sobre WannaCry

WannaCry tuvo un gran éxito como ataque devastador contra víctimas de alto perfil. Pero como ransomware con fines de lucro fue un fracaso. La propagación mediante gusanos no es lo apropiado para una amenaza con fines de lucro que busca acechar desde las sombras. Se estima que debido a su alta visibilidad, sólo obtuvo unos 55 000 USD en Bitcoins. El código tenía fallas y se sospecha que se lanzó antes de que estuviera completamente listo. También hay algunos indicadores, entre ellos similitudes con códigos previos, que sugieren que los responsables de WannaCry pertenecen al célebre grupo Lazarus de habla coreana.

Es posible que nunca se llegue a conocer el verdadero propósito del ataque de WannaCry: ¿Se trató de un ransomware fallido o de un ataque deliberadamente destructivo camuflado como ransomware?

ExPetr

El segundo gran ataque se produjo apenas seis semanas después, el 27 de junio. Su principal medio de propagación fue una infección en la cadena de abastecimiento y sus principales blancos eran equipos en Ucrania, Rusia y Europa. La telemetría de la compañía indica que hubo más de 5000 usuarios atacados. Las víctimas recibieron una nota de rescate exigiendo unos 300 dólares a pagar en Bitcoins, aunque no lograron recuperar sus archivos a pesar de haber pagado.

ExPetr fue un ataque complejo que incluía varios vectores de infección. Entre ellos figuran los exploits modificados EternalBlue (también utilizado por WannaCry) y EternalRomance, la puerta trasera DoublePulsar, que sirve para la propagación dentro de la red corporativa, el software de contabilidad infectado MeDoc que se usa para propagar el malware a través de sus actualizaciones, y un sitio de noticias infectado dedicado a la región ucraniana de Bajmut que los atacantes usaron como abrevadero.

Además, ExPetr podía infectar hasta equipos debidamente parchados que se encontraban en la misma red local que el primer equipo infectado. Para ello, recopilaba credenciales desde el sistema infectado a través de una herramienta similar a Mimikatz y procedía con movimientos laterales mediante los instrumentos PsExec o WMIC.

El componente cifrador de ExPetr operaba en dos niveles: cifraba los archivos de las víctimas con el algoritmo AES-128, para después instalar un gestor de arranque modificado de otro programa malicioso, GoldenEye (sucesor del original Petya). Este gestor de arranque malicioso cifraba el MFT, una estructura crítica de datos del sistema de archivos NTFS, evitando su reinicio, y exigía un rescate.

El impacto de ExPetr

Entre las víctimas de ExPetr se cuentan grandes organizaciones, como puertos, supermercados, agencias publicitarias y bufetes de abogados, por ejemplo Maersk, FedEx (TNT) y WPP. Un mes después del ataque, las entregas de TNT seguían afectadas, y los clientes de SMB fueron los más afectados. Otra de las víctimas, el gigante de bienes de consumo Reckitt Benckiser, perdió acceso a 15 000 computadoras portátiles, 2 000 servidores y 500 sistemas informáticos en apenas 45 minutos tras sufrir el ataque, y se estima que las pérdidas causadas ascienden a más de 130 millones de dólares. Por su parte, Maersk anunció pérdidas en sus ingresos por unos 300 millones de dólares ocasionadas por el ataque.

Las preguntas sin respuesta sobre ExPetr

Los expertos de Kaspersky Lab han descubierto similitudes entre ExPetr y las variantes iniciales del código KillDisk de BlackEnergy, pero el verdadero motivo y propósito detrás de ExPetr siguen siendo un misterio.

BadRabbit

Más tarde, a fines de octubre, otro gusano cifrador apareció en escena: BadRabbit. La infección inicial comenzó como una descarga al paso realizada desde varios sitios web infectados, bajo la apariencia de una actualización de Adobe Flash Player. Cuando se ejecuta en el equipo de la víctima, el componente gusano de BadRabbit procede a autopropagarse mediante el exploit EternalRomance y emplea una técnica de movimiento lateral similar a la que utiliza ExPter. La mayoría de las víctimas de BadRabbit se encuentra en Rusia, Ucrania, Turquía y Alemania.

El componente ransomware de BadRabbit cifra los archivos de las víctimas y luego procede a dividir el disco entero a través de los módulos de DiskCryptor, una utilidad legítima. El análisis del código de muestras y de las técnicas de BadRabbit revela una notable similitud entre este programa malicioso y ExPetr. Sin embargo, a diferencia de ExPetr, BadRabbit no parece ser un limpiador, ya que su esquema criptográfico técnicamente permite que los responsables de la amenaza puedan descifrar el equipo de la víctima.

EXPLOITS FILTRADOS USADOS EN NUMEROSAS NUEVAS OLEADAS DE ATAQUES

Los ciberpiratas responsables de los brotes de ransomware arriba mencionados no fueron los únicos que usaron códigos de exploits filtrados por Shadow Brokers para causar estragos.

Hemos descubierto otras familias de ransomware menos conocidas que en algún momento utilizaron los mismos exploits. Entre ellas están AES-NI (Trojan-Ransom.Win32.AecHu) y Uiwix (una variante de Trojan-Ransom.Win32.Cryptoff). Estas familias de programas maliciosos son ransomware 'puro', en el sentido de que no contienen capacidades de gusano, es decir, no pueden autoreplicarse, por lo que no suelen propagarse, como es el caso de WannaCry. Sin embargo, los autores detrás de ellas explotaron las mismas vulnerabilidades en los equipos de las víctimas durante las infecciones iniciales.

PUBLICAN LLAVES MAESTRAS PARA VARIAS FAMILIAS DE RANSOMWARE

Aparte de las epidemias a gran escala que sacudieron al mundo, en el segundo trimestre de 2017 apareció una tendencia interesante: varios grupos de delincuentes responsables de diferentes tipos de cripto-ransomware pusieron fin a sus actividades y publicaron sus llaves secretas para descifrar los archivos de las víctimas.

A continuación mostramos la lista de familias cuyas llaves se publicaron en el segundo trimestre:

- Crysis (Trojan-Ransom.Win32.Crusis);
- AES-NI (Trojan-Ransom.Win32.AecHu);
- xdata (Trojan-Ransom.Win32.AecHu);
- Petya/Mischa/GoldenEye (Trojan-Ransom.Win32.Petr).

La llave maestra Petya/Mischa/GoldenEye se publicó poco después del brote de ExPetr y puede haber sido un intento de parte de los autores de Petya para demostrar que no eran los responsables de ExPetr.

LA REAPARICIÓN DE CRYSIS

A pesar de que el ransomware Crysis pareció extinguirse en mayo de 2017 tras la publicación de todas las llaves maestras, no lo estuvo por mucho tiempo. En agosto comenzamos a descubrir numerosas muestras nuevas de este ransomware y resultaron ser copias casi idénticas de las muestras anteriores con apenas algunas diferencias: tenían nuevas llaves maestras públicas, nuevas direcciones de correo electrónico para que las víctimas se pongan en contacto con los ciberpiratas, y nuevas extensiones para los archivos cifrados. Todo lo demás se mantuvo inalterado, incluso las marcas de tiempo en los encabezados PE. Tras un profundo análisis de las muestras antiguas y nuevas, nuestros analistas llegaron a la conclusión de que era muy probable que las nuevas muestras se hubieran creado a partir de los parches binarios para las muestras antiguas mediante un editor HEX. Una razón para ello puede ser que los ciberpiratas responsables de las nuevas muestras no tuvieran el código fuente para este programa malicioso y se limitaran a aplicar ingeniería inversa en este ransomware para resucitarlo y usarlo para sus propios fines.

LAS INFECCIONES RDP SIGUEN EN AUMENTO

En 2016 notamos una nueva tendencia emergente entre los programas ransomware más expandidos. En lugar de intentar engañar a la víctima para que ejecute un código malicioso o de usar paquetes de exploits, los ciberpiratas recurrieron a otro vector de infección. Aplicaron fuerza bruta en inicios de sesión con RDP (Protocolo de Escritorio Remoto) y contraseñas en equipos que tenían RDP activado y a los que era posible acceder desde Internet.

En 2017, este enfoque llegó a ser uno de los principales métodos de propagación para varias familias expandidas, como Crysis, Purgen/GlobeImposter y Cryakl. Esto significa que para proteger una red, los especialistas de seguridad informática deberían tomar en cuenta este vector y deshabilitar el acceso RDP desde fuera de la red corporativa.

RANSOMWARE: EL AÑO EN CIFRAS

Es importante no concentrarse sólo en los números absolutos ya que reflejan cambios en la metodología de detección y en la evolución del escenario. Dicho esto, vale la pena mencionar algunas tendencias marcadas:

Al parecer, el nivel de innovación está declinando: en 2017, 38 nuevas cepas de ransomware criptográfico se consideraron interesantes y lo suficientemente diferentes para designarlas como nuevas 'familias', en comparación a las 62 en 2016. Esto podría deberse a que el modelo del ransomware criptográfico es bastante limitado y a que los desarrolladores de programas maliciosos encuentran cada vez más difícil inventar algo nuevo.

En 2017 se detectaron muchas más modificaciones de ransomware nuevo y conocido, con un total de 96 000 en comparación a las 54 000 en 2016. El aumento de las modificaciones puede reflejar los intentos de los atacantes por ofuscar sus programas ransomware ante soluciones de seguridad que cada vez son mejores para detectarlos.

La cantidad de intentos de ataque contra los clientes de Kaspersky Lab se mantuvo bastante constante. De hecho, los notorios picos alcanzados en 2016 han sido reemplazados por una distribución mensual más consistente. En general, casi 950 000 usuarios únicos fueron atacados en 2017, en comparación a los casi 1,5 millones en 2016. Sin embargo, estos datos incluyen a los programas cifradores y a sus descargadores; si nos enfocamos sólo en la cantidad de cifradores, entonces los números de 2017 son similares a los de 2016. Esto tiene sentido si consideramos que muchos atacantes están comenzando a propagar sus programas ransomware a través de otros medios, como la aplicación de fuerza bruta para averiguar contraseñas y los lanzamientos manuales. Estas cifras no incluyen los numerosos equipos en todo el mundo que no están protegidos por nuestras soluciones y que fueron víctimas de WannaCry; se estima que se trata de unas 727 000 direcciones IP únicas.

Aparte de WannaCry, ExPetr y BadRabbit, el número de ataques selectivos contra corporaciones apenas se incrementó: un 26,6% en 2017 contra un 22,6% en 2016. Solo un poco más del 4% de las víctimas en 2017 eran pequeñas y medianas empresas.

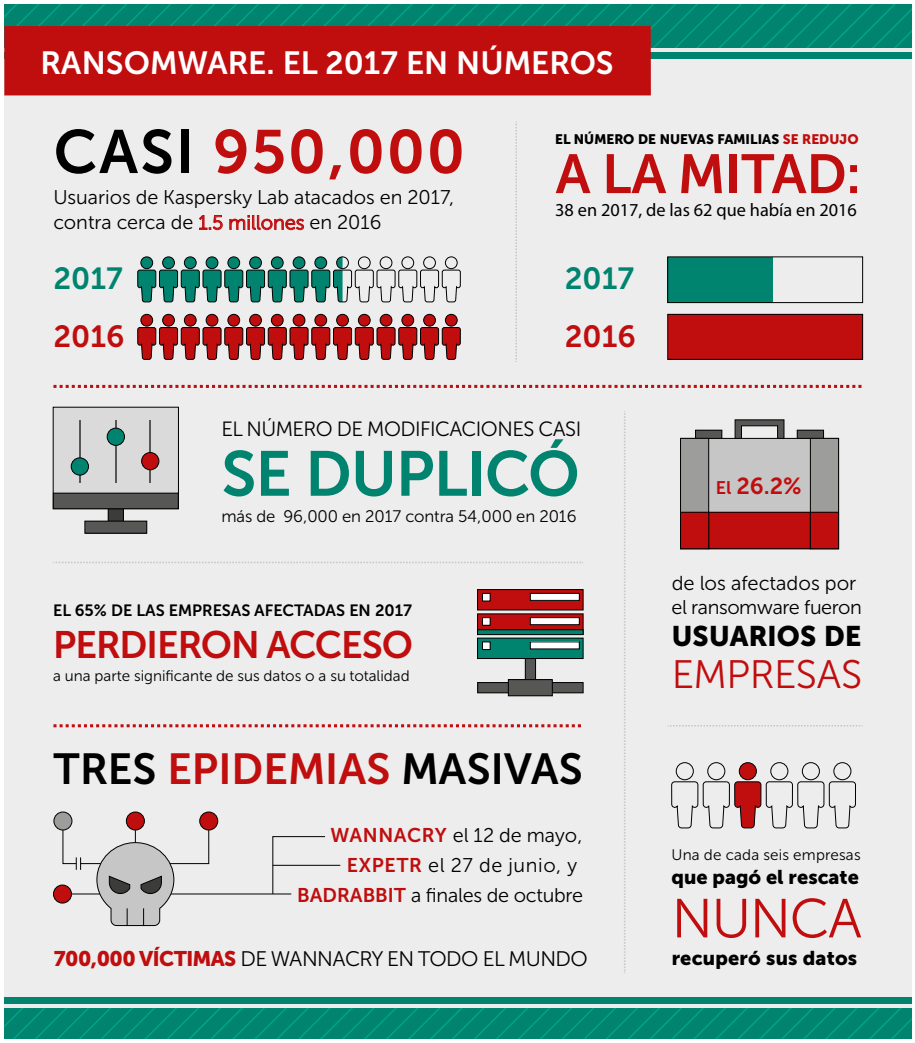
El Informe estadístico 2017 de Kaspersky Security Bulletin contiene más detalles sobre estas tendencias, incluyendo los países más afectados y las principales familias de ransomware.

Según la encuesta anual de seguridad informática de Kaspersky Lab[i]

El 65% de las compañías atacadas con ransomware en 2017 dijo haber perdido acceso a gran parte de sus datos o a todos ellos, mientras que el 29% afirmó que si bien lograron descifrar sus datos, perdieron para siempre una notable cantidad de archivos. Estas cifras son altamente consistentes con las de 2016.

El 34% de los afectados tardó varias semanas en restaurar por completo el acceso a sus datos, contra un 29% en 2016.

El 36% pagó el rescate exigido, pero el 17% de ellos nunca recuperó sus archivos (32% y 19% en 2016).



[i] Encuesta internacional de seguridad informática de B2B con Kaspersky Lab, 2017.

CONCLUSIONES: ¿QUÉ PODEMOS ESPERAR DEL RANSOMWARE?

En 2017, vimos a actores de amenazas avanzados que al parecer usaban los programas ransomware para lanzar ataques con el fin de destruir datos en vez de buscar recompensas financieras. La cantidad de ataques contra consumidores, PYMES y compañías se mantuvo elevada, pero incluían principalmente códigos existentes o modificados de familias conocidas o genéricas.

¿Comienza a hacer aguas el modelo de negocios del ransomware? ¿Existe una alternativa más lucrativa para los ciberpiratas que buscan ganancias monetarias? Una posibilidad podría ser la generación de monedas criptográficas. Las predicciones de Kaspersky Lab sobre amenazas para las monedas criptográficas en 2018 sugieren un alza en la cantidad de ataques selectivos con el objetivo de instalar generadores de monedas criptográficas. Si bien el ransomware ofrece ingresos potencialmente altos, pero no recurrentes, los generadores de monedas criptográficas pueden proporcionar ganancias menores pero a largo plazo, y esto podría ser un prospecto tentador para muchos ciberpiratas que ahora se dedican a los ataques de ransomware. Pero una cosa es segura: el ransomware no desaparecerá, ni como amenaza directa, ni como camuflaje para ataques más devastadores.

[CAN WE DO THIS IN A BOX OR SOMETHING AT THE END?]

LA LUCHA CONTRA EL RANSOMWARE CONTINÚA

Mediante colaboración: El 25 de julio de 2016, Kaspersky Lab, la Policía nacional holandesa, Europol y McAffee lanzaron la iniciativa No More Ransom. Se trata de un singular ejemplo del poder de la colaboración público-privada para luchar contra los ciberpiratas y ayudar a sus víctimas brindándoles conocimientos, consejos y herramientas descifradoras. A un año de su lanzamiento, el proyecto cuenta con 109 socios y está disponible en 26 idiomas. El portal en Internet contiene 54 herramientas descifradoras que cubren 104 familias de ransomware. Hasta la fecha se han descifrado más de 28 000 dispositivos, evitando que los ciberpiratas obtengan unos 9,5 millones de dólares en rescates.

Mediante inteligencia: Kaspersky Lab ha monitoreado desde su inicio la amenaza del ransomware y fue uno de los primeros en proporcionar actualizaciones regulares de inteligencia de amenazas sobre programas maliciosos extorsionadores con el fin de concienciar a la industria sobre este problema. Kaspersky Lab publica, a intervalos regulares, informes sobre el cambiante escenario de los programas ransomware, por ejemplo aquí y aquí.

Mediante la tecnología: Kaspersky Lab ofrece protección de múltiples capas contra esta amenaza cada vez más extendida, incluyendo una herramienta gratuita anti-ransomware que cualquier usuario puede descargar y utilizar, cualquiera que sea la solución de seguridad instalada en su equipo. Los productos de la compañía incluyen otra capa adicional de tecnología: System Watcher, o vigilante del sistema, que puede bloquear y restaurar los cambios maliciosos realizados en un dispositivo, como el cifrado de archivos o el acceso bloqueado a la pantalla.

KASPERSKY lab