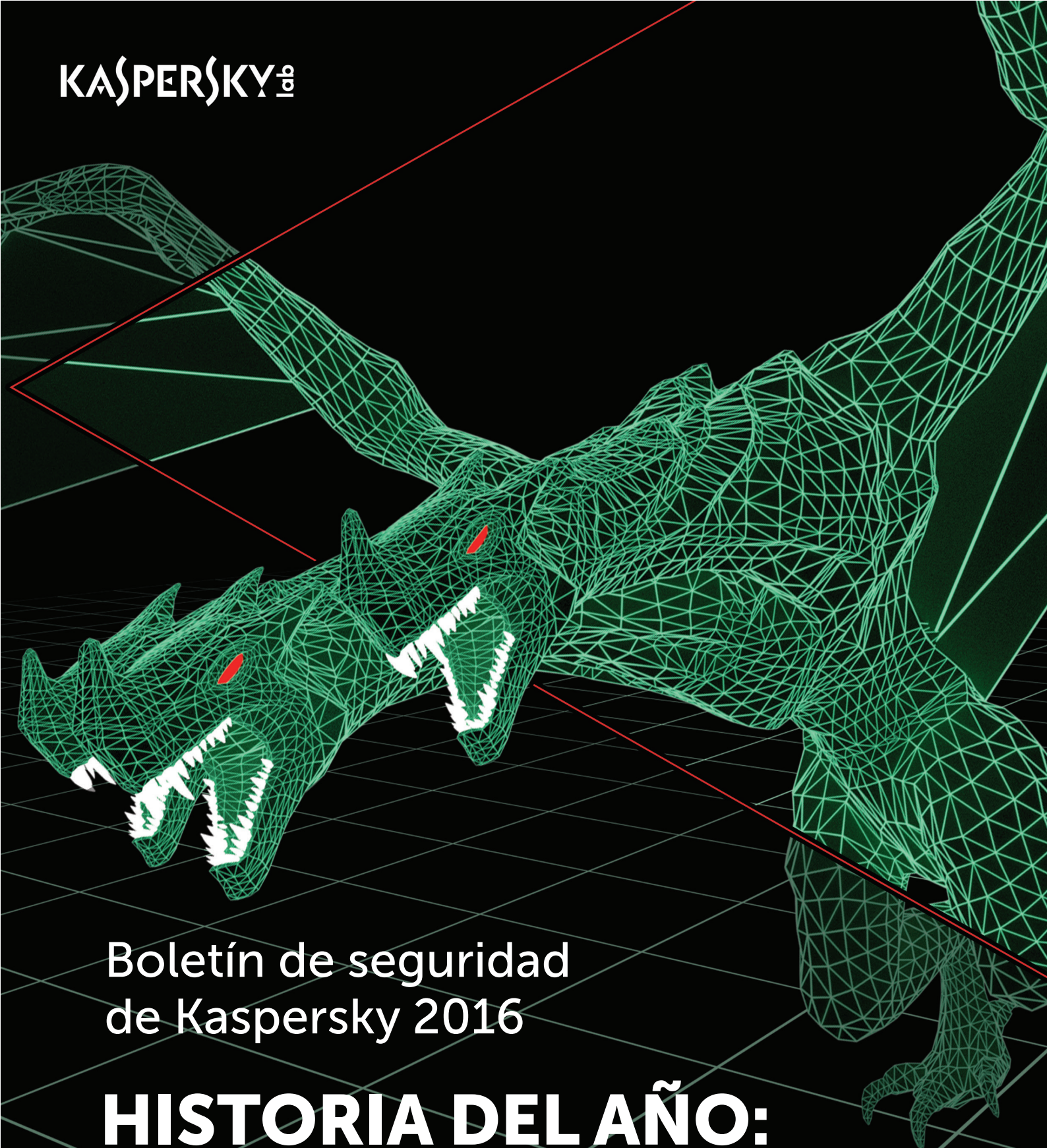
KASPERSKY lab



Boletín de seguridad
de Kaspersky 2016

HISTORIA DEL AÑO: LA REVOLUCIÓN DEL RANSOMWARE

GREAT

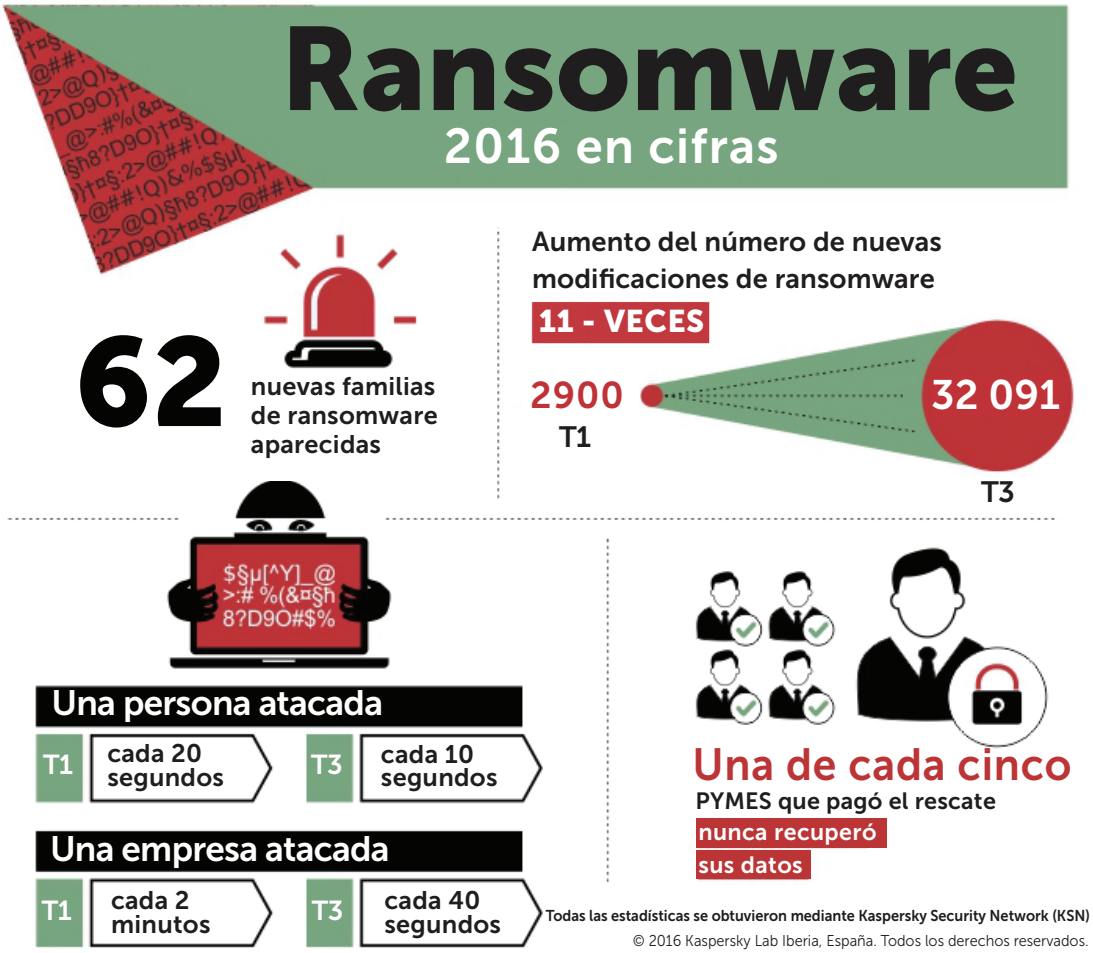
ÍNDICE

INTRODUCCIÓN

En 2016, el ransomware continuó con sus estragos en todo el mundo, afectando a los datos y dispositivos, así como a las personas y empresas.

Los números hablan por sí solos:

- Aparecieron 62 nuevas familias de ransomware.
- Se produjo un aumento de 11 veces en cuanto al número de modificaciones de ransomware: desde 2900 nuevas modificaciones en enero/marzo, hasta 32 091 en julio/septiembre.
- Los ataques a empresas aumentaron tres veces entre enero y finales de septiembre: la diferencia entre un ataque cada 2 minutos y uno cada 40 segundos.
- Para las personas, el índice de incremento pasó de cada 20 segundos a cada 10 segundos.
- Una de cada cinco pequeñas y medianas empresas que pagaron el rescate nunca recuperó sus datos.



2016 también fue testigo del crecimiento del ransomware en cuanto a sofisticación y diversidad, por ejemplo: cambio de táctica si se encontraba un software financiero, escrito en lenguajes de scripting, explotación de nuevas rutas de infección, cada vez más específicas, y la oferta de soluciones de ransomware como servicio listas para usarse para aquellos con menos habilidades, recursos o tiempo: todo a través de un ecosistema clandestino creciente y cada vez más eficiente.

Al mismo tiempo, 2016 vio como el mundo empezó a unirse para defenderse:

El proyecto No more Ransom se inició en julio, reuniendo al cuerpo policial nacional holandés, la Europol, Intel Security y Kaspersky Lab. Otras 13 empresas se unieron en octubre. Entre otras cosas, la colaboración ha dado lugar a una serie de tres herramientas de descifrado online gratuitas que hasta ahora han ayudado a miles de víctimas de ransomware a recuperar sus datos.

Esto es solo la punta del iceberg: queda mucho por hacer. Juntos podemos lograr mucho más que cualquiera de nosotros por nuestra cuenta.

¿Qué es el ransomware?

El ransomware se presenta en dos formas. La forma más común de ransomware es el cryptor. Estos programas cifran los datos en el dispositivo de la víctima y exigen dinero a cambio de una promesa de restaurar los datos. En cambio, los bloqueadores no afectan a los datos almacenados en el dispositivo. En su lugar, impiden que la víctima acceda al dispositivo. La demanda de rescate, que aparece en la pantalla, normalmente se hace pasar por un aviso de una agencia de las fuerzas del orden, que informa de que la víctima ha accedido a contenido web ilegal y le indica que debe pagar una multa en el acto. Puede encontrar una descripción general de ambas formas de ransomware aquí.

RANSOMWARE: PRINCIPALES TENDENCIAS Y DESCUBRIMIENTOS DE 2016

"La mayoría de ransomware prospera en una improbable relación de confianza entre la víctima y su atacante: una vez recibido el pago, se devolverán los archivos rescatados. Los cibercriminales han mostrado una sorprendente muestra de profesionalidad en el cumplimiento de esta promesa".

GReAT, predicciones de amenazas para 2017

Llegadas y salidas

Llegadas: en 2016, el mundo fue testigo de la aparición de Cerber, Locky y CryptXXX, así como de 44 287 nuevas modificaciones de ransomware

El ransomware Locky se ha extendido hasta ahora en **114** países

Cerber y Locky llegaron a principios de primavera. Ambos son cepas malas y virulentas de ransomware que se propagan ampliamente, principalmente a través de archivos adjuntos de spam y kits de explotación. Se han establecido rápidamente como "principales actores", dirigidos a usuarios y empresas. No muy lejos de ellos estaba CryptXXX. Las tres familias siguen evolucionando y manteniendo el chantaje en el mundo junto con anteriores bien establecidos, como CTB-Locker, CryptoWall y Shade.

A partir de octubre de 2016, las principales familias de ransomware detectadas por productos de Kaspersky Lab fueron las siguientes:

	Nombre	Veredictos*	Porcentaje de usuarios**
1	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	25,32
2	Locky	Trojan-Ransom.Win32.Locky/ Trojan-Dropper.JS.Locky	7,07
3	TeslaCrypt (activo hasta mayo de 2016)	Trojan-Ransom.Win32.Bitman	6,54
4	Scatter	Trojan-Ransom.Win32.Scatter/ Trojan-Ransom.BAT.Scatter/ Trojan-Downloader.JS.Scatter/ Trojan-Dropper.JS.Scatter	2,85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36
7	Shade	Trojan-Ransom.Win32.Shade	1,73
8	(veredicto genérico)	Trojan-Ransom.Win32.Snocry	1,26
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90

* Estas estadísticas se basan en los veredictos de detección devueltos por los productos de Kaspersky Lab, recibidos del uso de productos de Kaspersky Lab que han dado su consentimiento para proporcionar sus datos estadísticos.

** Porcentaje de usuarios objetivo de una determinada familia de ransomware de cifrado en relación con todos los usuarios objetivo de ransomware de cifrado.

Salidas: adiós a Teslacrypt, Chimera y Wildfire, o eso parecía...

Probablemente la mayor sorpresa de 2016 fue la desactivación de Teslacrypt y la versión posterior de la clave maestra, aparentemente por los propios actores del malware.

TeslaCrypt "se suicidó": mientras la policía desactivó Encryptor RaaS y Wildfire

Encryptor RaaS, uno de los primeros troyanos en ofrecer el modelo de ransomware como servicio a otros criminales cerró la tienda después de que la policía desmontara parte de su botnet.

A continuación, en julio, alguien que aseguraba estar detrás del ransomware Petya/Mischa publicó aproximadamente 3500 claves del ransomware Chimera. Sin embargo, puesto que Petya utilizaba parte del código fuente de Chimera para su propio ransomware, podía ser de hecho el mismo grupo, que simplemente actualizó su paquete de productos e hizo travesuras.

De forma similar, Wildfire, cuyos servidores se confiscaron y se desarrolló una clave de descifrado después de un esfuerzo combinado de Kaspersky Lab, Intel Security y la Europol, ahora parece haber vuelto a surgir como Hades.

Abuso de ransomware "educativo"

Investigadores bien intencionados desarrollaron el ransomware "educativo" para proporcionar a los administradores de sistemas una herramienta para simular un ataque de ransomware y probar sus defensas. Los criminales rápidamente aprovecharon estas herramientas para sus propios fines maliciosos.

El ransomware desarrollado para "educación" dio lugar a Ded Cryptor y Fantom, entre otros

El desarrollador del ransomware educativo Hidden Tear & EDA2 publicó el código fuente en GitHub. Inevitablemente, 2016 fue testigo de la aparición de numerosos troyanos maliciosos basados en este código. Esto incluía Ded Cryptor, que cambiaba el fondo de pantalla del ordenador de una víctima por una imagen de un Santa Claus malvado y exigía dos bitcoins masivos (alrededor de 1300 USD) como rescate. Otro de estos programas era Fantom, que simulaba una pantalla de actualización de Windows de aspecto original.

Enfoques no convencionales

Los atacantes tienen actualmente por objetivo copias de seguridad y discos duro, y descifran con fuerza bruta las contraseñas

- ¿Para qué preocuparse por un archivo cuando se puede tener el disco?

  Entre los nuevos enfoques de ataques de ransomware que se observaron por primera vez en 2016 se incluía el cifrado de discos, en el que los atacantes bloquean el acceso, o cifran, todos los archivos a la vez. Petya es un ejemplo de esto, que cifra el índice maestro del disco duro de un usuario y realiza un reinicio imposible. Otro troyano, Dcryptor, también conocido como Mamba, iba un paso más allá, bloqueando todo el disco duro. Este ransomware es especialmente desagradable, ya que cifra todos los sectores del disco, incluidos el sistema operativo, las aplicaciones, los archivos compartidos y todos los datos personales: mediante una copia del software DiskCryptor de fuente abierta.

- Técnica de infección "manual"

  La infección de Dcrypter se lleva a cabo de forma manual, con los atacantes descifrando las contraseñas con fuerza bruta para el acceso remoto al equipo de una víctima. Aunque no es nuevo, este enfoque se ha vuelto mucho más notorio en 2016, a menudo como una forma de dirigirse a los servidores y obtener acceso a un sistema corporativo.

  Si el ataque tiene éxito, el troyano se instala y cifra los archivos en el servidor y, posiblemente, incluso en todos los recursos compartidos de red accesibles desde él. Hemos descubierto TeamXRat que adopta este enfoque para distribuir su ransomware en servidores de Brasil.

Shade descargaba spyware si encontraba software financiero

- Infección dos en uno

  En agosto descubrimos una muestra de Shade que tenía una función inesperada: si un ordenador infectado pertenecía a servicios financieros, descargaba e instalaba en su lugar una parte de spyware, posiblemente con el objetivo a largo plazo de robar dinero.

Ransomware en lenguajes de scripting

Otra tendencia que atrajo la atención en 2016 fue el creciente número de cryptors escritos en lenguajes de scripting. Solo en el tercer trimestre, nos topamos con varias familias nuevas escritas en Python, incluidos HolyCrypt y CryPy, así como Stampado escrito en AutoIt, el lenguaje de automatización.

El ransomware de mala calidad aumenta la probabilidad de que los datos se pierdan para siempre

Una larga fila de aficionados e imitadores

Muchos de los troyanos de ransomware nuevos detectados en 2016 resultaron ser de baja calidad; poco sofisticados, con defectos de software y errores descuidados en las notas de rescate.

Esto vino acompañado por un aumento del ransomware de imitación. Entre otras cosas, detectamos que:

- Bart copia la nota de rescate y el estilo de la página de pago de Locky.
- Un imitador basado en Autoit de Locky (AutoLocky doblado) utiliza la misma extensión ".locky".
- Crusis (también conocido como Crysis) copia la extensión ".xtbl" utilizada originalmente por Shade.
- Xorist copia todo el esquema de nomenclatura de los archivos cifrados por Crusis.

Probablemente el imitador más destacado que descubrimos este año ha sido Polyglot (también conocido como MarsJoke). Imita totalmente el aspecto y el enfoque de procesamiento de archivos de CTB-Locker.

Se espera que estas tendencias aumenten en 2017.

"A medida que la popularidad sigue aumentando y los criminales de menor grado deciden entrar en el espacio, es probable que nos encontremos con cada vez más "ransomware" que carezca de la garantía de calidad o capacidad de codificación general para sostener realmente esta promesa. Esperamos que el ransomware "infantil" bloquee los archivos o el acceso al sistema o simplemente elimine los archivos, engañe a la víctima para que pague el rescate y no proporcione nada a cambio".

GReAT, predicciones de amenazas para 2017

LA PRÓSPERA ECONOMÍA DEL RANSOMWARE

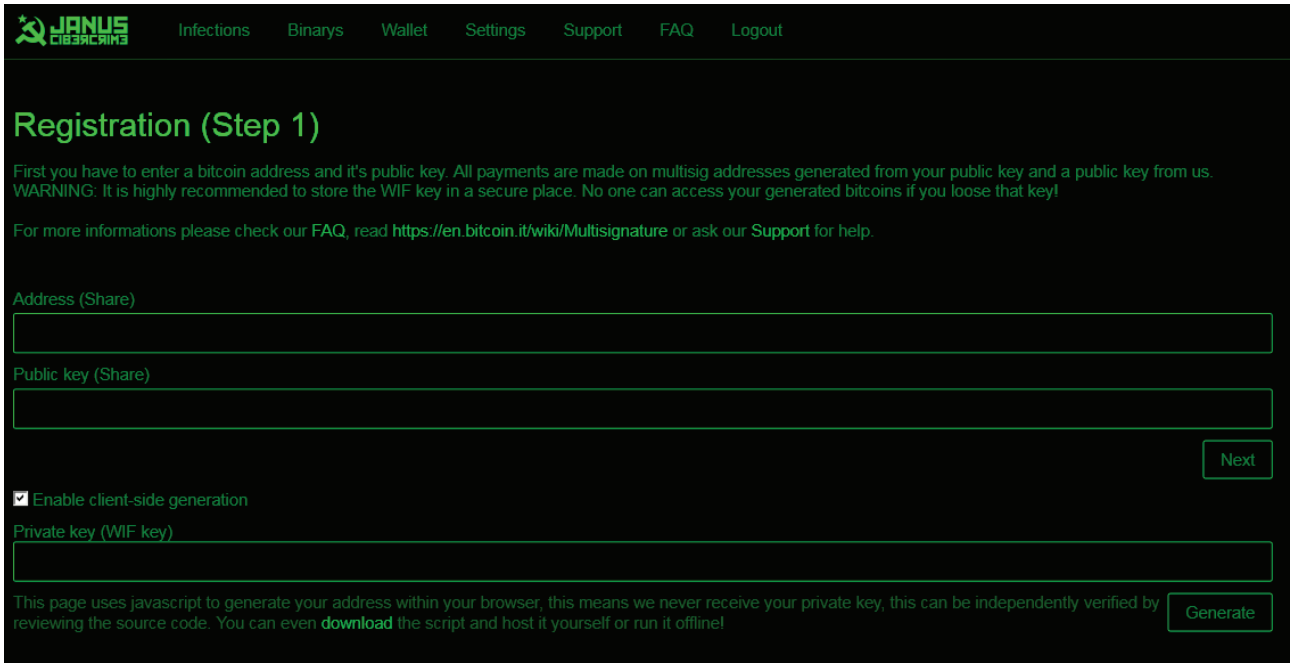
El ransomware es cada vez más de alquiler en el entorno clandestino de los criminales

Aumento de RaaS

Aunque el ransomware como servicio no es una tendencia nueva, en 2016 este modelo de propagación se siguió desarrollando, con cada vez más creadores de ransomware que ofrecían su producto malicioso "a petición". Este enfoque ha demostrado ser de gran atractivo para los criminales a los que les faltan habilidades, recursos o inclinación para desarrollar el suyo propio.

Algunos ejemplos destacados de ransomware que aparecieron en 2016 y utilizan este modelo son el ransomware Petya/Mischa y Shark, que posteriormente cambió su nombre por Atom.

Este modelo de negocio es cada vez más sofisticado:



Sitio de partners del ransomware Petya

El partner a menudo se registra en un acuerdo tradicional basado en comisión. Por ejemplo, la "tabla de pago" del ransomware Petya muestra que si un partner consigue 125 bitcoins a la semana, obtendrán 106,25 bitcoins después de la comisión.

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Tabla de pago de Petya

También hay un coste de uso inicial. Alguien que recurre al uso del ransomware Stompado, por ejemplo, tiene que pagar solo 39 USD.

Con otros criminales que ofrecen sus servicios en la distribución de spam, notas de ransomware, etc., no es difícil que un aspirante a atacante empiece.

De las redes basadas en comisión a la asistencia al cliente y la marca

Los criminales ofrecen asistencia al cliente para asegurarse de que más víctimas pagan

Los atacantes más "profesionales" ofrecían a sus víctimas un servicio de asistencia técnica que los guiaba por el proceso de compra de bitcoins para pagar el rescate y, a veces, incluso estaban abiertos a la negociación. Cada paso adicional animaba a la víctima a pagar.

Además, los expertos de Kaspersky Lab que estudiaron el ransomware en Brasil observaron, que para muchos ataques, la marca del ransomware era una cuestión de importancia. Los que buscan la atención de los medios de comunicación y el miedo del cliente optan por un alto perfil, tema de fama o trucos: mientras que los más preocupados por estar lejos del radar renuncian a la tentación de la fama y dejan que sus víctimas se enfrenten solo a un correo electrónico para ponerse en contacto con los delincuentes y una dirección de bitcoins para pagar.

Aún es una cuestión de bitcoins

A lo largo de 2016, las familias más populares de ransomware siguieron prefiriendo el pago en bitcoins. La mayoría de las demandas de ransomware no fueron excesivas, con una media de 300 USD, aunque a algunos se les cargó, y pagaron, muchísimo más.

Otros, especialmente operaciones regionales y artesanales, a menudo prefirieron una opción de pago local; aunque esto también significaba que ya no se podían ocultar a plena vista y mezclarse con el resto de morralla de ransomware.

EL RANSOMWARE APUNTÓ A LOS NEGOCIOS

Una empresa sufre un ataque con ransomware cada 40 segundos

En los tres primeros meses de 2016, el 17 % de los ataques de ransomware se dirigió a empresas: esto equivale a un ataque contra una empresa en algún lugar del mundo cada dos minutos*. Al final del tercer trimestre, había aumentado al 23,9 %: un ataque cada 40 segundos.

De acuerdo con la investigación de Kaspersky Lab, en 2016, una de cada cinco empresas de todo el mundo sufrió un incidente de seguridad de IT como resultado de un ataque de ransomware.

- El 42 % de las pequeñas y medianas empresas fue atacado por ransomware en los últimos 12 meses.
- El 32 % de ellas pagó el rescate.
- Una de cada cinco nunca recuperó sus archivos, incluso después de pagar.
- El 67 % de aquellas afectadas por el ransomware perdió parte o todos sus datos empresariales, y una de cuatro pasó varias semanas intentando restaurar el acceso.

* Cálculos basados en: el 17 % de 372 602 usuarios únicos con ataques de ransomware bloqueados por productos de Kaspersky Lab en el primer trimestres de 2016 y el 23,9 % de 821 865 usuarios únicos con ataques de ransomware bloqueados por productos de Kaspersky Lab en el tercer trimestre de 2016.

Una de cada cinco PYMES nunca recuperó sus archivos, incluso después de pagar

Ya no existe un sector de bajo riesgo

La ingeniería social y los errores humanos siguen siendo los factores clave de la vulnerabilidad corporativa. Uno de cada cinco casos que implicó una considerable pérdida de datos llegó a través del descuido o la falta de concienciación de los empleados.

Algunos sectores industriales se ven más afectados que otros, pero nuestra investigación muestra que todos están expuestos al riesgo.

	Sector	% de atacados con ransomware
1	Educativo	23
2	IT/telecomunicaciones	22
3	Entretenimiento/medios de comunicación	21
4	Servicios financieros	21
5	Empresas de construcción	19
6	Gobierno/sector público/defensa	18
7	Industria	18
8	Empresas de transporte	17
9	Asistencia sanitaria	16
10	Minoristas/mayoristas/ocio	16

"Estamos viendo más ransomware específico, en el que los grupos de criminales escogen con cuidado y realizan spear-phishing de sus objetivos, debido a los datos que poseen y/o su confianza en la disponibilidad de estos datos valiosos".

John Fokker, coordinador del equipo digital con la Unidad Nacional de Delitos de Alta Tecnología holandesa

Ataques de ransomware que aparecen en los titulares

- **Los hospitales se convirtieron en un objetivo prioritario**: con un efecto potencialmente devastador ya que se cancelaron operaciones, se derivó a los pacientes a otros hospitales, etc.
  - El ejemplo más famoso de un ataque de ransomware tuvo lugar en marzo, cuando los criminales bloquearon los ordenadores del Hollywood Presbyterian Medical Center de Los Ángeles, hasta que el hospital pagó 17 000 USD.
  - En cuestión de semanas, una serie de hospitales de Alemania también se vio afectado.
  - En el Reino Unido, 28 servicios nacionales de salud admitieron haber sido atacados en 2016.
- **El proveedor de servicios en la nube y escritorios alojados** VESK pagó casi 23 000 USD de rescate para recuperar el acceso a uno de sus sistemas tras un ataque en septiembre.
- **Los principales medios de comunicación**, incluidos New York Times, BBC y AOL se vieron afectados por el malware que llevaba ransomware en marzo de 2016.
- **La Universidad de Calgary de Canadá**, un importante centro de investigación, confirmó que tuvo que pagar alrededor de 16 000 USD para recuperar mensajes de correo electrónico que se cifraron durante una semana.
- **Una pequeña comisaría de Massachusetts** terminó pagando un rescate de 500 USD (a través de bitcoin) con el fin de recuperar los datos esenciales relacionados con casos, después de que un agente abriera un archivo adjunto de correo electrónico malicioso.
- **Incluso las carreras de coches se vieron afectadas:** un importante equipo de carreras de NASCAR se enfrentó a la pérdida de datos por valor de millones por un ataque de TeslaCrypt en abril.

DEFENSA

Mediante la tecnología

Las versiones más recientes de los productos de Kaspersky Lab para empresas más pequeñas se han mejorado con la función de anticriptomalware. Ademas, se ha puesto a disposición de todas las empresas una nueva herramienta antiransomware gratuita para su descarga y uso, independientemente de la solución de seguridad que utilicen.

Hay disponible una nueva herramienta antiransomware independiente de AV gratuita

Anti-Ransomware Tool for Business de Kaspersky Lab es una solución "ligera" que puede funcionar en paralelo con otro software antivirus. La herramienta utiliza dos componentes necesarios para la detección temprana de troyanos: la red distribuida Kaspersky Security Network y System Watcher, que supervisa la actividad de las aplicaciones.

Kaspersky Security Network comprueba rápidamente la reputación de archivos y URL de sitios web a través de la nube, y System Watcher supervisa el comportamiento de los programas y proporciona protección proactiva contra versiones aún desconocidas de troyanos. Lo que es más importante, la herramienta puede realizar copias de seguridad de los archivos abiertos por aplicaciones sospechosas y revertir los cambios si se demuestra que las acciones realizadas por los programas son maliciosas.

Mediante la colaboración: El proyecto "No More Ransom"

El proyecto " No more Ransom" ha conseguido hasta ahora que 4400 personas recuperen sus datos y ha privado a los criminales de 1,5 millones USD en rescate

El 25 de julio de 2016, el cuerpo policial nacional holandés, la Europol, Intel Security y Kaspersky Lab anunciaron el lanzamiento del proyecto "No more Ransom": una iniciativa no comercial que unifica las organizaciones públicas y privadas y trata de informar a las personas sobre los peligros del ransomware y ayudarles a recuperar sus datos.

El portal online actualmente tiene ocho herramientas de descifrado, cinco de las cuales fueron realizadas por Kaspersky Lab. Estas pueden ayudar a restaurar archivos cifrados por más de 20 tipos de criptomalware. Hasta la fecha, más de 4400 víctimas han recuperado sus datos, y se han ahorrado más de 1,5 millones USD en demandas de rescate.

En octubre, las fuerzas del orden de otros 13 países se unieron al proyecto, incluidos: Bosnia y Herzegovina, Bulgaria, Colombia, Francia, Hungría, Irlanda, Italia, Letonia, Lituania, Portugal, España, Suiza y Reino Unido.

Eurojust y la Comisión Europea también apoyan los objetivos del proyecto y se espera que se anuncien pronto más partners del sector privado y de las fuerzas del orden.

"Las colaboraciones públicas/privadas son la esencia y la fortaleza de la iniciativa de NMR. Son esenciales para combatir eficaz y eficientemente el problema, lo que nos proporciona una capacidad mucho mayor que las fuerzas del orden por sí solas".

Steven Wilson, director de EC3 de la Europol

Enfrentarse al ransomware: cómo protegerse

1. Realice copias de seguridad de los datos de forma regular.
2. Utilice una solución de seguridad fiable y recuerde mantener funciones clave, como System Watcher, activadas.
3. Mantenga siempre el software actualizado en todos los dispositivos que utilice.
4. Trate los archivos adjuntos de correo electrónico o mensajes de personas que no conozca con precaución. En caso de duda, no lo abra.
5. Si es una empresa, también debe formar a sus empleados y equipos de IT; mantenga los datos confidenciales aparte; restrinja el acceso; y realice copias de seguridad de todo, siempre.
6. Si tiene la desgracia de ser víctima de un cifrador, no se preocupe. Utilice un sistema limpio para comprobar nuestro sitio No más rescate; puede encontrar una herramienta de descifrado que le ayude a recuperar sus archivos.
7. Por último, pero no menos importante, recuerde que el ransomware es un delito. Informe a las fuerzas del orden locales.

Por qué no debe pagar: consejo de la Unidad Nacional de Delitos de Alta Tecnología holandesa

1. Se convertirá en un objetivo mayor.
2. No puede confiar en los criminales: puede que nunca recupere sus datos, incluso si paga.
3. Su próximo rescate será mayor.
4. Anima a los criminales.

"Instamos a las personas a que informen sobre un ataque. Todas las víctimas tienen pruebas esenciales que proporcionan información valiosa. A cambio, podemos mantenerlas informadas y protegerlas de "ofertas" sospechosas de terceros para descifrar datos. Pero tenemos que asegurarnos de que más oficinas de las fuerzas del orden sepan cómo tratar el cibercrimen".

Ton Maas, coordinador del equipo digital con la Unidad Nacional de Delitos de Alta Tecnología holandesa

¿PODEMOS GANAR LA LUCHA CONTRA EL RANSOMWARE?

Creemos que sí, pero solo si trabajamos juntos. El ransomware es un lucrativo negocio criminal. Para detenerlo, el mundo tiene que unirse con el fin de interrumpir la cadena de ataques de los criminales y hacer que les sea cada vez más difícil implementar y sacar provecho de sus ataques.

Securelist, el recurso para la investigación técnica, análisis e ideas de expertos de Kaspersky Lab.

Síganos

Sitio web global de Kaspersky Lab

Blog de Eugene Kaspersky

Blog B2C de Kaspersky Lab

Blog B2B de Kaspersky Lab

Servicio de noticias de seguridad de Kaspersky Lab

Academia de Kaspersky Lab