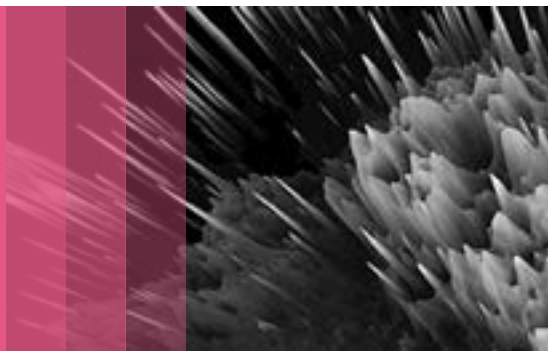
RANSOMWARE:
TENDENCIAS DE ATAQUE, PREVENCION Y RESPUESTA



RESUMEN EJECUTIVO

Durante la última década, los cibercriminales, motivados por ganancias financieras -en oposición a aquellos que robaban propiedad intelectual o que actuaban por razones políticas- volvieron sus ojos hacia los troyanos bancarios como objetivo principal. Pero la marea ha cambiado. Los troyanos bancarios han sido eclipsados por el ransomware como el arma preferida de los *hackers* en todas partes. En los últimos meses, además, los incidentes de seguridad atribuibles a ransomware han visto su crecimiento a un ritmo alarmante, tanto en empresas como en organismos públicos.

El aumento de ransomware se ha convertido en una epidemia global. Sigue acumulando víctimas en todo el mundo, obligando a las empresas a decidir entre intentar recuperar datos de copias de seguridad (y potencialmente perder datos vitales desde la última copia de seguridad) y pagar importantes sumas de rescate a los hackers. El ransomware han provocado numerosos titulares recientes, con victimas tan diversas como un hospital en Los Angeles, una iglesia en Oregón o dos hospitales alemanes. En los últimos años, todo esto ha desembocado en un volumen creciente de nuevos ataques y variantes de ransomware. Desde CryptoLocker, Locky o Kovter, hasta ataques más recientes con CryptXXX o Petya, parece que cada día conocemos casos de un nuevo ataque de ransomware, con nuevas variantes que aparecen casi cada semana.

Si bien es cierto que el ransomware existe desde hace ya tiempo, ha sido realmente en los últimos dos años cuando ha pasado a ser el protagonista de la "caja de herramientas" del hacker. El ransomware ha tomado como rehenes a miles de individuos y empresas, ha destruido datos valiosísimos y ha acumulado cientos de millones de dólares en ganancias para los *hackers*. Al mismo tiempo que los proveedores de seguridad han continuado desarrollando defensas para detectar y bloquear ataques tradicionales, el ransomware ha ido evolucionando, siendo cada vez más habitual localizarlo, oculto dentro de documentos o en sitios web aparentemente inocuos, y evitando la detección de los tradicionales antivirus y soluciones basadas en firma. Los cibercriminales atacan, cifran rápidamente archivos y luego piden un pago significativo a cambio de una clave de descifrado, que puede funcionar, o no. Luego, desaparecen sin dejar rastro.

A medida que aumenta la frecuencia de estos ataques, las empresas están cada vez más concienciadas de los riesgos que implica el ransomware. Pero muchas no están preparadas para defenderse contra las últimas evoluciones en las técnicas de ataque. Profundice en la comprensión de las amenazas del ransomware. Aprenda a proteger mejor sus activos de negocio leyendo este documento que destaca los desafíos a los que enfrentan las empresas y las mejores prácticas para prevenir ataques de ransomware y limitar su impacto en la organización.

> "SABER NO EQUIVALE A COMPRENDER. HAY UNA GRAN DIFERENCIA ENTRE SABER Y COMPRENDER: PUEDES SABER MUCHO SOBRE ALGO, PERO NO ENTENDERLO REALMENTE"
>
> CHARLES KETTERING

Enero 2017

EL AUGE DEL RANSOMWARE

En los últimos años, el ransomware se ha convertido en una herramienta muy atractiva para aquellos hackers que buscan una alternativa al tradicional "troyano bancario", ya que ofrece muchas ventajas a los desarrolladores. Es más fácil de implementar, no requiere una gran personalización, facilita un acceso más sencillo a los fondos y no requiere un canal "vivo" o una comunicación constante con los servidores de control (C&C) para ejecutarlo. Para el atacante, esto hace más fácil y más rentable la actividad, y se puede extorsionar más dinero.

Hackear por dinero: el paso de los "troyanos bancarios" al ransomware

Durante más de una década, los troyanos bancarios han sido una de las ciberamenazas más importantes. Un tipo de malware enormemente rentable para los *hackers*, pero con sus limitaciones. Hubo un tiempo, en efecto, que era sencillo para un *hacker* crear un "espejo" de la web del banco, capturar credenciales de usuarios e incluso transferir fondos. A medida que la detección del fraude fue mejorando, y la autenticación de dos factores se convirtió en la norma, a fecha de hoy el atacante, por lo general, necesitará algo más que credenciales para conseguir sus objetivos. Además, han de aprovechar para sus ataques, dispositivos que hayan sido previamente autenticados por el usuario. En definitiva: para ser eficaces, los troyanos bancarios, tales como el utilizado en la campaña de *Zeus*, han de estar dirigidos a públicos específicos, deben ser personalizados para la web de cada entidad y deben traducirse para atender en diferentes idiomas. Este tipo de ataque, en definitiva, requiere mucho más esfuerzo, y las campañas "genéricas" ya no son una opción.

Para complicar aún más las cosas, está la logística propia de obtener los fondos de la víctima. Dichos fondos deben ser transferidos desde la cuenta objetivo a una cuenta "mula", lo cual requiere que el malware bancario mantenga un canal de comunicación activo durante el ataque. Si el servidor *Command & Control* (C&C) se cierra durante el proceso, el atacante fracasará en su intento. Incluso si logra con éxito hacer frente a estos desafíos, aún correrá el riesgo de que la transferencia sea bloqueada por el banco (mediante alguna tecnología de detección de fraude, por ejemplo) o que la transacción desencadene una alerta silenciosa para atrapar al atacante cuando vaya a retirar los fondos en persona. La capacidad de rastrear la retirada física o el movimiento electrónico de fondos supone un riesgo real para el atacante. Todo esto afectará, además, a los costes asociados, el tiempo requerido y la probabilidad relativa de éxito del troyano bancario, lo que ha llevado a los *hackers* a reemplazar esta técnica con metodologías alternativas.

Ransomware: vectores de ataque

En su forma más simple, el ransomware es un malware que encripta los archivos de la víctima y luego exige un rescate por su recuperación. El método de infección más común utilizado es el spam o los emails de *phishing*. El email, por lo general, contiene adjunto un documento de Word (u otro formato) que incorpora una macro maliciosa. Cuando el usuario abre el archivo, la macro se activa y ejecuta un script que descarga el archivo ejecutable del malware, lo instala en el ordenador de la víctima, analiza los archivos del sistema y los encripta. Otros vectores son el malware "*drive-by*" o la promoción de descargas de contenido infectado a través de "abrevaderos" (*watering holes*), esto es, sitios web diseñados para atraer visitantes desde la empresa o sector industrial objetivo del ataque.

Ejecución del ataque: simple y directo

Una vez cifrados los archivos, se muestra a la víctima una "nota de rescate", reclamando a la víctima el pago de una cantidad a cambio de la clave para descifrar y recuperar el acceso a los archivos. A diferencia de un troyano bancario, el ransomware requiere poca personalización: para traducir una campaña de ransomware, los desarrolladores solo necesitan traducir la nota de rescate al idioma local, e incluso pueden "saltarse" este paso refiriendo a los usuarios al traductor de Google. La nota de rescate proporciona instrucciones de pago a las víctimas y un plazo para efectuar el pago. Si no, los archivos se perderán permanentemente.

> "EL MÉTODO DE INFECCIÓN MÁS COMÚN EN LAS CAMPAÑAS DE RANSOMWARE ES EL SPAM O LOS EMAILS DE PHISHING"

Las modalidades de pago del ransomware son más fiables

Los cibercriminales han encontrado maneras de superar los retos derivados de la transferencia de fondos que implican los troyanos bancarios. La mayoría de los ransomware actuales usan los bitcoins como moneda para el pago, en detrimento de otras monedas respaldadas por los gobiernos. Esto ofrece varias ventajas: a diferencia de las tarjetas o las transacciones bancarias, en bitcoins se pueden transferir fondos sin la opción de cancelar la transacción posteriormente. Las "carteras" Bitcoin permiten al atacante permanecer anónimo, y que las transacciones fuera del alcance de las autoridades. Además, cambiar bitcoins en cualquier moneda es tan fácil como usar un cajero automático.

¿No hay comunicación? No hay problema

El último factor que impulsa el cambio hacia el ransomware está relacionado con las comunicaciones. El ransomware no requiere una línea abierta de comunicación tras la infección. Una vez cifrados los archivos, la pelota está en el lado de la víctima, que tendrá que decidir si seguir las instrucciones de la nota de rescate para localizar al atacante, anonimizado en alguna red TOR, y completar la transacción. No se requiere ninguna otra acción por parte del atacante, ya que la motivación para completar el pago será enteramente de la víctima, si es que desea recuperar sus archivos. Las variantes recientes de ransomware ni siquiera requieren comunicación para obtener las claves necesaria para cifrar y bloquear los archivos del usuario, ya que vienen embebidas en una clave pública predeterminada, lo que hace innecesario incluso establecer conexión "en vivo" con un servidor C&C para generar ingresos.

Estas ventajas, así como los ingresos resultantes, han propiciado la creciente popularidad del ransomware en los últimos meses, como puede apreciarse en el siguiente gráfico, basado en datos de investigaciones de Check Point.

> "HACER EL PAGO EN BITCOINS PERMITE TRANSFERIR FONDOS SIN LA OPCIÓN DE IMPUGNAR O CANCELAR LA TRANSACCIÓN CON POSTERIORIDAD"

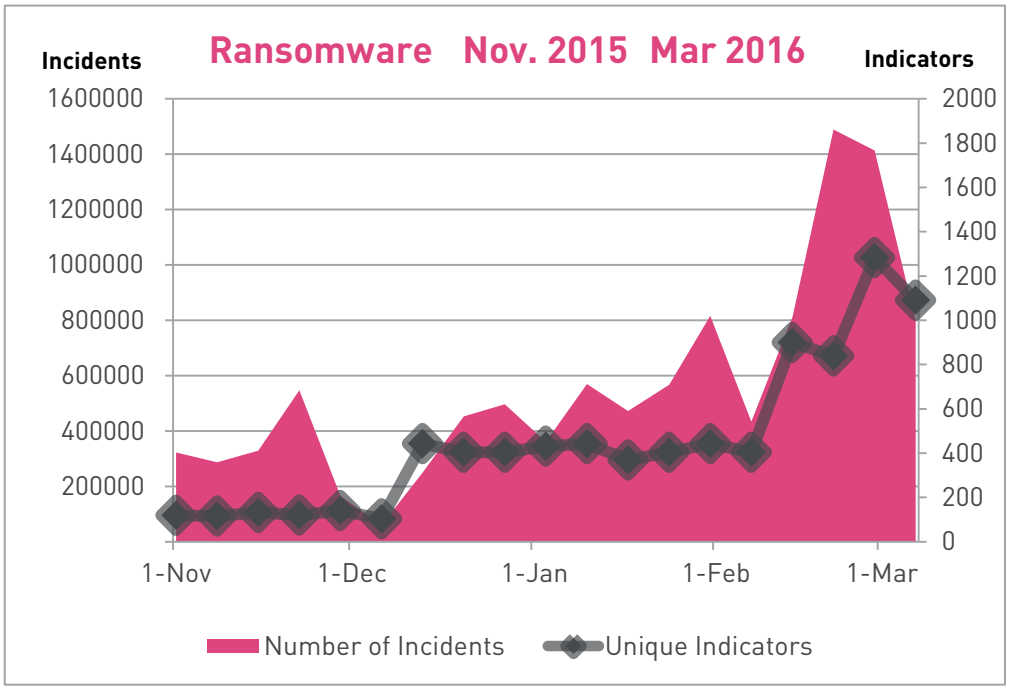


Imagen 1. Crecimiento en los ataques de ransomware (noviembre 2015 - marzo 2016)

EVOLUCIÓN EN LOS OBJETIVOS: DEL CONSUMIDOR A LA EMPRESA

Individuos

A primera vista, atacar a usuarios individuales puede no parecer rentable, especialmente si se contempla un único particular. Los atacantes que apuntan a individuos tienden a mantener exigencias de rescate relativamente bajas, esperando que, de esta manera, las víctimas paguen rápidamente en lugar de enfrentarse al ataque. El pago de un solo ataque puede variar entre 100 y 1.000 dólares (aunque actualmente el pago suele ser en bitcoins). Pero, para el atacante, este es un juego de cantidades, ya que los ataques se transmiten a múltiples víctimas potenciales, y cada vez que uno paga, se animan a seguir jugando. En lugar de atrapar a una sola víctima, un atacante puede lanzar fácilmente una amplia red de ataques contra decenas de blancos utilizando una misma estafa de *phishing* o contenido web malicioso. Incluso aunque piquen sólo unos pocos, la rentabilidad respecto al esfuerzo realizado sigue siendo enorme.

Además, los usuarios individuales siguen siendo un objetivo viable. Pocos de ellos, a nivel particular, cuentan con los recursos de TI necesarios para combatir un ataque de ransomware. En su caso es más probable que sus soluciones de protección estén desactualizadas, y a menudo no tendrán *backups* recientes desde los que restaurar. Cuando son atacados, en vez de arriesgarse a perder fotografías familiares, listas de música y otros documentos personales valiosos, es más probable que los individuos paguen el rescate si éste se establece a un nivel razonable.

Objetivos empresariales

En el pasado, el ransomware solía apuntar sobre todo a usuarios privados[1]. En los últimos tiempos, diversos factores han llevado a los atacantes a cambiar su enfoque, dirigiéndose a grandes organizaciones en un amplio abanico de sectores. Las víctimas incluyen departamentos de policía, organizaciones sin ánimo de lucro, escuelas, universidades y hospitales. Las empresas han demostrado ser un objetivo muy lucrativo para los extorsionadores por varias razones: en primer lugar, dependen mucho más de los datos para operar, lo que proporciona un mayor incentivo al pago del rescate; además, las empresas suelen tener una mayor capacidad financiera que los individuos, lo que implica que los atacantes pueden extorsionar grandes sumas de dinero atacando a menos víctimas.

Las organizaciones altamente distribuidas, con un elevado uso de dispositivos móviles o con empleados remotos son especialmente vulnerables ante ataques de ransomware. Las organizaciones con múltiples oficinas tendrán dificultades para mantener una formación, una política y unos procedimientos consistentes en sus diferentes ubicaciones. Los sitios remotos y los sitios más pequeños pueden no tener recursos locales de TI o de seguridad para apoyar a los usuarios en la recuperación de sus datos. A medida que aumenta el número de empleados, la cantidad de instalaciones y la diversidad de lugares, el desafío se multiplica.

> “LAS EMPRESAS HAN DEMOSTRADO SER UN OBJETIVO MUY RENTABLE PARA LOS EXTORSIONADORES, YA QUE TIENEN UN MAYOR INCENTIVO PARA ACCEDER A PAGAR EL RESCATE”

EL IMPACTO DE LA INGENIERÍA SOCIAL

La ingeniería social representa una vía cada vez más popular de penetración en las redes empresariales, ya que mejora las probabilidades de que un ataque tenga éxito. Es relativamente fácil para el atacante realizar una sencilla investigación sobre la empresa objetivo, para luego poder engañar a algún empleado mediante un email de *phishing* usurpando la identidad de alguien conocido por la víctima. Puede ser un pedido de un cliente, o una factura de un proveedor. Al hacer clic en el mensaje, el destinatario abre involuntariamente un archivo con la carga que se va a instalar para activar el ransomware. Combinando la ingeniería social con el malware integrado en documentos aparentemente seguros, los atacantes logran convencer incluso a sofisticados profesionales de la seguridad para abrir adjuntos maliciosos.

[1] http://blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia

UNA AMENAZA ESQUIVA

Una de las razones por las que el ransomware está superando las defensas de muchas organizaciones es que los atacantes han actualizado diferentes aspectos para hacerlo mucho más evasivo. Los productos de seguridad tradicionales, como los antivirus y las soluciones basadas en firmas, están claramente en retroceso, ya que sólo detectan malware previamente conocido, o comportamientos concretos vistos en ataques anteriores. El ransomware, por su parte, ha encontrado diversos métodos para evitar la detección e infectar con éxito las redes y los ordenadores.

Uno de estos métodos consiste en incrustar el ransomware dentro de versiones ligeramente diferentes de documentos comunes, como Word, Excel, PDF... pero cambiando el contenido empaquetado con el archivo adjunto para que no coincida con hashes (o firmas) conocidos. Un ejemplo reciente de esta técnica es el ransomware Locky[2]. Empaquetando documentos únicos con ransomware en comandos de macro, cada archivo de email es ligeramente diferente y, por lo tanto, no será detectado por las soluciones de protección tradicionales, basadas en firmas. Para convencer a los usuarios de activar las macros, el ransomware aplica técnicas de ingeniería social, con trucos que pueden engañar incluso a los usuarios más prudentes. La ingeniería social es un vector de ataque de bajo perfil tecnológico, pero con una tasa de éxito alarmantemente elevada, ya que puede sortear defensas AV tradicionales[3]. Una vez habilitada la macro, ésta extrae el programa malicioso y lo lanza[4], lo que hará que el ransomware se active y comience a cifrar tantos archivos como le sea posible.

El ransomware moderno es capaz de llegar más allá del sistema de un usuario individual. Puede dañar grandes volúmenes de datos de una organización con una sola infección, y puede alcanzar un impacto más amplio al cifrar el contenido disponible en un determinado sistema en toda la red. El infame ransomware CryptoLocker, por ejemplo, intenta acceder a todas las unidades de red que puede encontrar para cifrarlas[5]. Además, algunos tipos de ransomware, como CTB Locker, apuntan directamente a sitios web específicos. Dado que en el caso de las empresas es más probable tengan presencia en la web, este método de operación pone más en riesgo a aquéllas que a los usuarios privados[6].

ESTRATEGIAS PARA LUCHAR CONTRA EL RANSOMWARE

Medidas preventivas

En la guerra contra el ransomware, hay una serie de medidas que se pueden tomar para evitar convertirse en víctima. Seguir estas prácticas puede ser un elemento crítico para evitar ataques de ransomware, y puede ayudar a minimizar el daño causado por una campaña de ransomware con éxito contra su organización.

Realice backup de sus archivos importantes, de forma consistente, utilizando preferiblemente almacenamiento en espacios aislados (redes "*air-gap*")[7]. Si es posible, programe backups automáticos para sus empleados -no confíe en que todos ellos recuerden realizarlas por sí mismos-. En caso de un ataque de ransomware, podrá utilizar estas copias de seguridad en lugar de pagar un rescate, o al menos podrá decidir si el coste de la restauración es mayor o menor que el rescate solicitado.

La educación de los empleados ha sido clave, típicamente, para prevenir las infecciones de malware, y esto también es aplicable al ransomware. Los fundamentos de considerar de dónde vinieron los archivos, o si se puede o no confiar en el remitente, siguen siendo elementos dignos de tener en cuenta por los usuarios[8].

Otro aspecto clave es garantizar que los usuarios sólo acceden a la información y los recursos que necesitan para ejecutar su trabajo, ya que reducirá significativamente la posibilidad de "movimiento lateral" de los ataques y minimizará el impacto potencial en su organización. Si abordar un ataque de ransomware en un solo host puede ser una molestia, el impacto potencial de un ataque en toda la red puede ser mucho más dramático.

LUCHANDO CONTRA EL RANSOMWARE

Medidas preventivas

- ✓ *Haga copias de seguridad de sus datos y programe backups automáticos*
- ✓ *Eduque a los empleados para reconocer amenazas potenciales*
- ✓ *Limite el acceso y evite "movimientos laterales"*
- ✓ *Mantenga actualizados los antivirus y otras protecciones basadas en firmas*
- ✓ *Implemente extracción avanzada de amenazas y tecnologías de sandboxing*

[2] http://blog.checkpoint.com/2016/03/02/locky-ransomware/, http://arstechnica.com/security/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro/
[3] https://medium.com/@networksecurity/it-s-time-to-secure-microsoft-office-be50ec2797e3#.9y7xkrheq
[4] http://thehackernews.com/2016/02/locky-ransomware-decrypt.html
[5] http://krebsonsecurity.com/2013/11/how-to-avoid-cryptolocker-ransomware/
[6] http://www.pcworld.com/article/3038207/security/ctb-locker-ransomware-hits-over-100-websites.html
[7] http://blog.checkpoint.com/2015/08/17/what-you-can-and-cant-do-against-ransomware/
[8] http://blog.checkpoint.com/2015/08/17/what-you-can-and-cant-do-against-ransomware/

Pasando al papel de la seguridad de la Información en la prevención de ataques, es ciertamente beneficioso mantener los antivirus y otras soluciones de protección basadas en firmas, y que todo esté actualizado. Pero tenga en cuenta que estas protecciones basadas en firmas, por sí solas, no son suficientes para detectar y evitar ataques de ransomware sofisticados, diseñados para evadir las protecciones tradicionales. Un enfoque multi-capa ofrecerá la mejor oportunidad para defenderse del ransomware y el daño que podría causar. Dos componentes clave en un enfoque de este tipo son la extracción de amenazas (desinfección de archivos) y el *sandboxing*. Cada uno de estos elementos proporciona una protección distinta, y si se usan juntos, ambos ofrecen una solución completa para la protección a nivel de red y en los dispositivos end-point.

Los documentos que contienen macros o *exploits* integrados son un medio eficaz para desencadenar la infección inicial. La mejor manera de prevenir este tipo de infección es filtrar el contenido malicioso de los documentos mediante la extracción de amenazas (*Threat Extraction*). Despojando a estos archivos de todos sus elementos activos, la organización puede neutralizar los ataques mediante la entrega rápida de versiones limpias y saneadas, minimizando así el riesgo para los usuarios. Y, a diferencia de los humanos, esta herramienta es completamente inmune a la ingeniería social.

El *sandboxing* avanzado , sistema de emulación de amenazas (*Threat Emulation*) .aporta un segundo elemento dentro del enfoque de seguridad multi-capa. Funciona en paralelo con la extracción de amenazas para proteger contra malware desconocido y ataques de día cero. A diferencia de los antivirus y otras soluciones, no está basado en firmas. El *sandboxing* avanzado de Check Point SandBlast analiza el comportamiento de los archivos en base a diferentes indicadores, incluido el análisis dinámico. Además, utiliza una técnica exclusiva de detección a nivel de CPU, resistente a la evasión, para detectar y bloquear el malware más complejo en la fase de *exploit*, antes de que tenga la oportunidad de desplegarse.

Además de proporcionar una protección de la red potente, también será necesario proteger los dispositivos *end-point* que se encuentran fuera del perímetro de defensa de la red. Los usuarios que trabajan a distancia, fuera de la protección de los *gateways* corporativos, o bien los que utilizan los empleados de subcontratas para conectarse a la red corporativa, o los dispositivos de almacenamiento extraíbles que contienen malware sin el conocimiento de su propietario... todos ellos representan puntos de entrada para un atacante experto. SandBlast Agent amplía la protección avanzada de día cero a los puestos de trabajo, protegiéndoles contra malware desconocido y amenazas avanzadas.

Respuesta post - infección

Si bien prevenir el ransomware es lo ideal, también hay que saber qué hacer en caso de que un ataque ransomware tenga éxito, con posterioridad a la infección e implementar herramientas capaces de identificar un incidente y contener las infecciones de ransomware puede suponer la diferencia entre perder un ordenador o sufrir una infección más extensa.

Si está preparado para ataques a través de canales no protegidos, detectar el ransomware dentro de su red y bloquear cualquier comunicación entre el ransomware y sus servidores de comando y control (C&C), utilizando la tecnología Anti-Bot, limitará y posiblemente bloqueará su capacidad para operar. Muchos tipos de ransomware (aunque no todos), para poder cifrar archivos, han de acceder primero una clave de cifrado de un servidor C&C[9]. Poner en cuarentena procesos y comunicaciones maliciosos de forma rápida y eficaz permitirá contener, y posiblemente mitigar, esta amenaza.

Incluso si el ransomware llega a cifrar archivos en el dispositivo infectado, la tecnología Anti-Bot puede bloquearlo automáticamente, evitando la propagación a los sistemas de almacenamiento en red u otros entornos. Los archivos cifrados del dispositivo *end-point* afectado serán automáticamente restaurados a partir de las copias de seguridad de corto plazo. Esto puede reducir drásticamente el daño causado por el ransomware y limitar el impacto posterior en el negocio.

LUCHANDO CONTRA EL RANSOMWARE

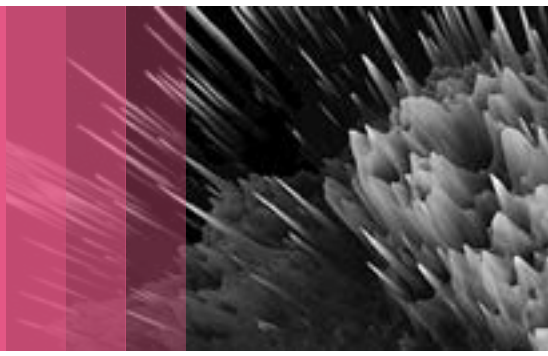
Medidas post-infección

- ✓ *Evite que el ransomware comunique con sus centros de control mediante la detección y bloqueo de bots*
- ✓ *Contenga rápidamente las infecciones de ransomware y restaure los ficheros cifrados para minimizar el impacto en su negocio*
- ✓ *Utilice datos o información de análisis forense para desinfectar totalmente el ataque y evitar daños mayores*

[9] http://blog.checkpoint.com/2013/11/14/defeating-cryptolocker-with-threatcloud-and-gateway-threat-prevention/

Una vez que haya logrado usted contener el ransomware, será importante tratar toda la infección y remediar el ataque. Los ataques deben tratarse en su conjunto, y deben aplicarse protecciones para evitar que se repitan en otro lugar. Para tener éxito, el equipo de respuesta ante incidentes (IRT) debe analizar todos los aspectos del ataque, desde el punto de entrada y la ruta seguida hasta el alcance de los daños. La implementación y uso de herramientas automatizadas de análisis forense mejora en gran medida la capacidad del IRT para entender cómo los ataques se infiltraron inicialmente en las redes. El análisis forense automático proporciona una visión completa del ataque, y aporta orientación para su remedio. Estas herramientas reducen drásticamente el tiempo para el análisis de eventos, tomando lo que antes era un esfuerzo de horas o días y reducirlo a minutos, permitiendo al personal de TI entender y responder al ataque de una manera mucho más eficiente y eficaz.

EN CONCLUSIÓN



[LA TECNOLOGÍA BASADA EN FIRMAS] YA NO ES UNA OPCIÓN

El ransomware va en aumento. Aunque muchas organizaciones ya han protegido sus archivos, datos y sistemas mediante la implementación de software antivirus y otras soluciones basadas en firmas, estos métodos –que siguen siendo esenciales– no defienden frente a ataques avanzados de ransomware, diseñados precisamente para evadir estos métodos de detección tradicionales. Las organizaciones necesitan implementar un enfoque de seguridad multi-capa para hacer frente a los nuevos desafíos del ransomware y proteger eficazmente su red y dispositivos *end-point*.

Este enfoque debe ser integral, incluyendo tanto medidas preventivas como herramientas eficientes de respuesta y mitigación. Las capacidades avanzadas de *sandboxing* de SandBlast Zero-Day Protection combinan la detección tradicional a nivel de sistema operativo con la detección a nivel de CPU para proteger proactivamente sus activos de las amenazas persistentes avanzadas (APT) y de día cero. Al mismo tiempo, las capacidades de extracción de amenazas de SandBlast filtran los elementos potencialmente maliciosos de los documentos y proporcionan rápidamente contenido desinfectado para minimizar el riesgo para los usuarios. Estas herramientas, junto con las soluciones tradicionales basadas en firmas, son elementos críticos en la defensa de las organizaciones contra los ataques de ransomware.

La protección no puede limitarse a la red. Proporcionar un nivel equivalente de protección en el punto final es un componente crítico para una cobertura de seguridad integral. SandBlast Agent amplía las defensas de SandBlast Zero-Day Protection para defender los dispositivos *end-point* contra malware desconocido y amenazas avanzadas de día cero. Además, protege contra el ransomware mediante el uso de análisis avanzado de comportamiento, detección de cifrado e instantáneas de datos a corto plazo para los archivos activos.

Si bien la prevención es fundamental, las organizaciones también deben implementar herramientas que les permitan entender, responder y limitar el alcance de los ataques. Anti-Bot, tanto a nivel de red como en los propios terminales, permite a las organizaciones detectar rápidamente el ransomware dentro de su red y bloquear cualquier comunicación con los servidores C&C antes de que pueda causar más daños. Lo cual puede aprovecharse para poner en cuarentena procesos y comunicaciones maliciosos, y bloquear los dispositivos infectados para limitar el impacto potencial del ataque. Después del ataque se ha producido, los equipos de TI necesitarán utilizar las más avanzadas herramientas de análisis forense automatizado para entender el plano de ataque completo y remediarlo de manera adecuada, rápida y eficaz.

Si quiere saber más sobre la prevención de amenazas y sobre cómo SandBlast Zero-Day Protection y SandBlast Agent pueden ayudar a proteger su empresa contra el ransomware, visite nuestra página web www.checkpoint.com/sandblast.

> “LOS ANTIVIRUS Y OTRAS SOLUCIONES BASADAS EN FIRMAS, SI BIEN SON ESENCIALES, QUEDAN INDEFENSAS CONTRA EL RANSOMWARE AVANZADO”

CONTACTE CON NOSOTROS

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com
Email: Info_iberia@checkpoint.com • Teléfono: +34 91 799 27 14

Enero 2017