Malwarebytes Endpoint Security contra el ransomware

Suprimir la creciente amenaza del ransomware

El ransomware se ha hecho notar por lo difícil que resulta ponerle freno. Una vez que infecta los dispositivos, sus víctimas se enfrentan a la difícil decisión de pagar a los atacantes por una clave con la que desbloquear los datos o perder para siempre sus archivos.

Una encuesta global patrocinada recientemente por Malwarebytes en la que participaron ejecutivos del campo de la informática[1] demuestra la importancia de esta amenaza para las empresas. El 39 % de las organizaciones incluidas en el estudio se han visto afectadas por un ataque de ransomware en los 12 meses anteriores. Entre los sectores encuestados, aquellos en los que hubo más ataques de ransomware fueron en el de la atención sanitaria y en los sectores relacionados con los servicios financieros, entre ellos el de la banca y el de los seguros.

> El 39 % de las organizaciones incluidas en el estudio se han visto afectadas por un ataque de ransomware en los 12 meses anteriores.

Los costes en los que se incurrió a causa del ransomware son considerables, ya sea por que se perdieron activos digitales o por verse obligados a desembolsar una suma cuantiosa. Casi el 20 % de todas las víctimas de ransomware que participaron en la encuesta declararon que les habían exigido pagos superiores a 10 000 USD. A nivel global, casi el 40 % de las víctimas de ransomware pagaron el rescate. En Canadá, el 82 % de las organizaciones que optaron por no pagar el rescate perdieron archivos como consecuencia.

Una solicitud de información dirigida por el senado estadounidense al Fiscal general del estado y al Secretario del Departamento de Seguridad Nacional en diciembre de 2015 sobre ataques de ransomware reveló que aproximadamente 234 000 ordenadores fueron infectados con un tipo concreto de ransomware denominado Cryptolocker.[2] Tan solo algo más de un 1 % de las víctimas pagó el rescate, pero en dos meses los extorsionadores sustrajeron cerca de 27 millones de USD a los usuarios infectados. Con otra variante copiada de Cryptolocker se embolsaron más de 18 millones de USD de aproximadamente 1000 víctimas entre abril de 2014 y junio de 2015.[3]

Es más, el índice de ataques de ransomware en los Estados Unidos está aumentando. En 2015, el FBI recibió quejas relacionadas con cerca de 2500 ataques de ransomware que costaron 24 millones de USD a las víctimas. En cambio, tan solo en el primer trimestre de 2016, las extorsiones de ransomware sumaron otros 209 millones de USD a ese saldo.[4] Y lo que es peor, aunque las víctimas paguen el rescate, los delincuentes no siempre descodifican los archivos. Además, según el Instituto de Tecnologías de Infraestructuras Críticas, un vivero de ideas para el sector de las infraestructuras críticas, no hay ninguna garantía de que el sistema no sea asaltado de nuevo después del pago[5].

El coste humano de las extorsiones cibernéticas

Además de crear un problema económico grave, el ransomware también puede perturbar importantes servicios sociales. En mayo de 2016 el FBI advirtió de una considerable intensificación de la actividad relacionada con el ransomware que incluía una serie de incidentes de alto perfil contra hospitales.[6] Según un informe publicado en eWeek.com, en febrero de 2016 el Centro Médico Presbiteriano de Hollywood admitió que había pagado un rescate de 17 000 USD para que descodificaran datos infectados con ransomware.

Atacar a organizaciones de atención sanitaria es dinero fácil para los delincuentes que se sirven del ransomware. Los hospitales se juegan mucho cuando se trata de proteger la atención al paciente y puede que no tengan otra opción que pagar para recuperar sus datos. Aunque gran parte de la actividad relacionada con el ransomware no se denuncia, una

declaración de la Alianza para la Confianza de la Información de la Salud (HITRUST) indica que aproximadamente el 18 % de los hospitales de tamaño medio han sido infectados con criptoransomware (ransomware de cifrado).[7]

Por qué a los ciberdelincuentes les gusta tanto

Nada triunfa tanto como el propio éxito, y detrás del triunfo del ransomware hay un cúmulo perfecto de factores de éxito. Como señala Adam Kujawa, director de Recopilación de Información sobre Malware de Malwarebytes, «el nivel de atención que el ransomware ha estado recibiendo por parte de los medios de comunicación supone la relación peligro-exposición más peligrosa que hemos experimentado nunca». En otras palabras, la elevada incidencia del ransomware y la amenaza real que supone no son actualidad en los medios de comunicación. Basándose en el análisis estadístico de los ataques de ransomware a través de publicidad maliciosa realizado por la propia Malwarebytes, Kujawa afirma que «los malos están renunciando a otros tipos de malware y pasándose al ransomware».

En pocas palabras, el ransomware es el arma preferida de los ciberdelincuentes porque:

- Es rentable, exige un pago rápido que recompensa a los ciberdelincuentes con una gratificación inmediata. Normalmente los atacantes exigen el pago en criptomonedas como, por ejemplo, las bitcoins. La mayoría de esas monedas son anónimas y prácticamente no dejan rastro, lo que permite a los ciberdelincuentes blanquear sus ganancias ilícitas cambiándolas por su moneda local. Y, exactamente igual que las grandes empresas, a veces las organizaciones de ransomware ofrecen un servicio de «atención al cliente» cuyos atentos representantes conducen paso a paso a las víctimas por el proceso de compra de una criptomoneda adecuada.
- Es fácil de usar, cada vez más. Los delincuentes experimentados están introduciendo el ransomware en el mercado en línea como un servicio, lo que se conoce como RaaS, para estafadores con menos habilidades técnicas. En la práctica, los programadores de ransomware están externalizando su malware a una red de delincuentes sin experiencia en la programación de scripts, de tal manera que distribuyen sus aplicaciones listas para usar a cambio de un porcentaje del botín para el programador original.[8]
- Protegerse del ransomware es muy difícil. Según una encuesta a ejecutivos en puestos relacionados con la informática que fue patrocinada por Malwarebytes,[9] lo que más preocupaba a los encuestados estadounidenses era la infiltración de malware a través del correo electrónico y de las visitas a sitios web. Por ejemplo, abrir un archivo adjunto que contiene un exploit permite que el malware se aproveche de cualquier punto débil que encuentre en el software comúnmente instalado en los sistemas e introduzca el ransomware. La publicidad maliciosa coloca anuncios que son trampas explosivas en sitios web de buena reputación, las cuales pueden descargar ransomware incluso aunque los visitantes no hagan clic en los anuncios infectados. Tenga en cuenta que en 2015 Google tuvo que desactivar más de 780 millones de anuncios infectados con publicidad maliciosa. De hecho, según Malwarebytes, aproximadamente el 70 % de las campañas de publicidad maliciosa entregan ransomware como carga útil.

Combatir el ransomware con Malwarebytes Endpoint Security

La mayor parte del software de seguridad de hoy en día ofrece una eficacia limitada frente al ransomware. El ransomware no actúa como el malware tradicional: algunas formas se actualizan automáticamente todos los días e incluso utilizan un código polimórfico (que cambia de forma) para evitar ser detectadas. Eso hace que sea cada vez más difícil de detectar, sobre todo porque las plataformas tradicionales y heredadas de protección de terminales utilizan tecnologías estáticas que dependen de firmas que sencillamente no pueden detectar los comportamientos cambiantes del ransomware. Además, el ransomware que se ve hoy en día es tan sofisticado que la avanzada tecnología de cifrado que utiliza hace que resulte imposible recuperar archivos sin pagar el rescate.

Lamentablemente, los sistemas de copias de seguridad en línea o conectados a redes locales pueden no ser eficaces como medida de respuesta, ya que el ransomware busca activamente diferentes tipos de sistemas de copias de seguridad y codifica las copias de los archivos. En el caso de copias de seguridad en línea, las cargas automáticas de archivos pueden dañar archivos que el usuario cree que están protegidos.

En cambio, Malwarebytes Endpoint Security es una plataforma diseñada para combatir y anular el ransomware avanzado que a otras soluciones se les escapa. Se despliega por las redes de las empresas y protege los terminales frente al malware y otras amenazas avanzadas gracias a una potente combinación de tecnologías proactivas sin firmas, heurísticas y basadas en el comportamiento dispuestas en varias capas.

Además, Malwarebytes Endpoint Security ofrece otra capa de protección frente a ataques basados en ransomware con una

nueva tecnología especialmente diseñada desde cero para detectar y bloquear todo tipo de ransomware, conocido o no, de manera que no pueda codificar los archivos de los usuarios. Esta solución de protección de terminales se diferencia de otras soluciones antiransomware, si es que existen, que normalmente consisten en un montaje hecho con una tecnología antigua que ya ha demostrado que no es eficaz.

Malwarebytes Endpoint Security rompe la cadena de ataque del ransomware con un enfoque de cuatro capas:

1. La capa antiransomware de Malwarebytes Endpoint Security supervisa constantemente los sistemas terminales y pone automáticamente fin a procesos asociados con actividades de ransomware. Cuenta con un motor que está específicamente dedicado a detectar en tiempo real ese tipo de actividad, no utiliza firmas ni requiere ser actualizado. Además, ocupa poco espacio en el sistema y es compatible con soluciones de seguridad de terceros.
2. La capa antiexploit bloquea exploits activamente antes de que puedan entregar su carga útil de malware. Envuelve las aplicaciones vulnerables y los exploradores web con capas defensivas diseñadas para detener ataques de día cero desde el primer momento. Empleando tecnología sin firmas que identifica comportamientos característicos de un exploit, la capa antiexploit puede incluso proteger frente a malware y ransomware no identificados que otras tecnologías no pueden percibir porque no han sido expuestas a ellos con anterioridad.
3. La capa antimalware de Malwarebytes Endpoint Security aplica reglas heurísticas y de comportamiento para detectar y eliminar malware general en tiempo real, de manera que no pueda ejecutar su código.
4. La capa que bloquea sitios web maliciosos detiene el acceso a servidores de comando y control conocidos y sospechosos, de manera que el ransomware no pueda obtener claves de cifrado ni acceder a su archivo .exe para descargarlo.

Romper la cadena de ataque del ransomware con Malwarebytes

He aquí cómo las tecnologías de Malwarebytes Endpoint Security bloquean un ataque de ransomware lanzado a través de un exploit de publicidad maliciosa.

La mejor forma de explicar esto es examinando las diversas capas de la cadena de ataque del ransomware:

1. Generación de perfiles: El atacante hace un reconocimiento de su terminal a través de un banner publicitario infectado para intentar identificar su sistema operativo, su tipo de explorador web, su dirección IP y el programa de seguridad del terminal.
   Tecnología de Malwarebytes: El refuerzo de las aplicaciones reduce superficialmente su vulnerabilidad, mejora la capacidad de recuperación del ordenador y permite que se detecten activamente intentos de creación de huellas digitales mediante ataques avanzados. (sin firmas)

2. Entrega: Cómo coloca el atacante su exploit y la carga útil en el terminal.
   Tecnología de Malwarebytes: La protección web impide que los usuarios accedan a sitios web maliciosos, redes publicitarias, redes de estafadores y otros «vecindarios indeseables».

3. Explotación: El atacante se aprovecha del código vulnerable que usted pueda tener en su explorador web, Adobe Flash, Microsoft Word, etc., para entregar y ejecutar remotamente la carga útil de ransomware.
   Tecnología de Malwarebytes: Las mitigaciones de exploits detectan y bloquean activamente cualquier intento de explotación de las vulnerabilidades y de ejecución remota de código en la máquina, que actualmente es uno de los principales vectores de infección. (sin firmas) La tecnología de comportamiento de las aplicaciones garantiza que las aplicaciones instaladas se comporten correctamente e impide que se aprovechen de ellas para infectar la máquina. (sin firmas)

4. Ejecución de la carga útil: El atacante le entrega la carga útil de ransomware y lo ejecuta en su sistema.
   Tecnología de Malwarebytes: El análisis de cargas útiles está basado en reglas heurísticas y de comportamiento para identificar familias enteras de malware conocido y relevante.

5. Comportamiento malicioso: El ransomware se activa en su sistema. Se pone en contacto con un servidor de comando y control para descargar las claves de cifrado y después cifra los archivos.
   Tecnología de Malwarebytes: La mitigación de ransomware es una tecnología de supervisión del comportamiento que detecta ransomware y le impide cifrar los archivos de los usuarios. (sin firmas)
   La protección de devolución de llamada impide el acceso a servidores de comando y control (C&C) y otros sitios web maliciosos.

Resumen

A medida que aumente el número de dispositivos conectados al vasto espacio que recibe el nombre de Internet de las Cosas (IoT), el ransomware supondrá una amenaza creciente para sus víctimas; sobre todo si tenemos en cuenta que los expertos predicen que continuaremos observando múltiples y nuevas variantes por todo el espacio IoT.

Malwarebytes Endpoint Security es una plataforma de protección de terminales que protege activamente sus ordenadores frente a amenazas conocidas o desconocidas. Malwarebytes Endpoint Security tiene una capa adicional de protección frente a ataques basados en ransomware con una tecnología antiransomware sin igual que supervisa, detecta y bloquea automáticamente el ransomware incluso antes de que toque los archivos de los usuarios. Además de hacer frente a amenazas conocidas como Cryptolocker, CryptoWall o CTBLocker, acaba con nuevo ransomware en el momento en que es distribuido, protegiendo activamente a los usuarios de ransomware que ni siquiera ha sido visto antes.

Las empresas clientes se benefician de Malwarebytes Endpoint Security porque:

- Reduce la vulnerabilidad a ataques de ransomware. Detecta y bloquea automáticamente ransomware conocido o desconocido, en vez de limitarse a alertar al usuario de que hay un ataque enviándole por correo electrónico un mensaje automatizado, que es lo que hacen otros productos de seguridad.
- Bloquea el cifrado en tiempo real. Detiene el ransomware antes de que pueda empezar a actuar, eliminando la necesidad de complicadas, y a menudo ineficaces, herramientas de descifrado.
- Trabaja contra ransomware de día cero (no identificado previamente) empleando una tecnología especializada de supervisión del comportamiento que protege de nuevo ransomware que otras tecnologías no pueden detectar porque no han sido expuestas a él con anterioridad.
- Emplea un diseño único realizado desde cero para derrotar al ransomware con mayor rapidez y eficacia. Malwarebytes creó esta tecnología desde cero para defender frente al ransomware. Otras soluciones o capacidades antiransomware dependen de tecnologías obsoletas o de una colección de tecnologías retocadas que originalmente fueron creadas para hacer otra cosa.
- Utiliza tecnología sin firmas en la capa antiransomware y la capa antiexploit, gracias a lo cual es eficaz incluso frente a nuevo ransomware que todavía no tiene una firma.
- Preserva la reputación de la empresa al permitir que evite la pesadilla que un ataque o un problema de seguridad suele conllevar en lo que se refiere a las relaciones públicas.
- Protege los ingresos de la empresa que habría que dedicar a pagar el rescate de los datos cifrados.

Sitios web de consulta

Para obtener más información sobre Malwarebytes Endpoint Security y la nueva tecnología de ransomware, visite: malwarebytes.com/business/endpointsecurity/
Últimas novedades: blog.malwarebytes.com/
Solicitud de una versión de prueba: malwarebytes.com/business/licensing

Referencias

[1]Encuesta realizada en junio de 2016 y publicada en agosto de 2016 por Osterman Research, Inc.
[2]https://www.hsgac.senate.gov/media/minority-media/senators-carper-johnson-seek-information-on-threat-of-ransomware-to-our-nations-cyber-defenses-and-to-the-american-public
[3]Ibid.
[4]http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746
[5]http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf
[6]https://blog.malwarebytes.com/101/2016/06/malvertising-and-ransomware-the-bonnie-and-clyde-of-advanced-threats/
[7]http://www.eweek.com/security/ransomware-poses-a-rising-threat-to-hospital-operations.html
[8]http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/
[9]Encuesta realizada en junio de 2016 y publicada en agosto de 2016 por Osterman Research, Inc.

Acerca de

Malwarebytes es la compañía de seguridad informática de última generación en la que confían millones de personas de todo el mundo. Malwarebytes protege de manera proactiva a usuarios particulares y empresas frente a peligrosas amenazas, como el malware, el ransomware y los exploits que no son detectados por las soluciones antivirus habituales. El producto estrella de la empresa combina la detección heurística de amenazas avanzadas con la tecnología sin firmas para detectar y detener ciberataques antes de que se produzcan daños. Más de 10 000 empresas de todo el mundo usan y recomiendan Malwarebytes como software de confianza. Fundada en 2008, la empresa tiene su sede principal en California y oficinas en Europa y Asia, y cuenta con un equipo global de investigadores y expertos en seguridad.

Santa Clara, CA

malwarebytes.com

corporate-sales@malwarebytes.com

1.800.520.2796