

Por gentileza de



Defensa contra el ransomware

for
dummies[®]
A Wiley Brand

Edición especial de Cisco



Conoce las características del ransomware

Evita ataques de ransomware

Construye una nueva arquitectura de seguridad puntera

Lawrence Miller, CISSP

Acerca de Cisco

Cisco diseña y vende gran variedad de productos, proporciona servicios y ofrece soluciones integradas para desarrollar y conectar redes.

Como líder del mercado, ayudamos a nuestros clientes a conectar, digitalizar y hacer progresar sus organizaciones. Juntos, cambiamos la forma de trabajar, vivir, jugar y aprender en el mundo.

Durante más de 30 años, hemos ayudado a nuestros clientes a crear redes y a automatizar, orquestar, integrar y digitalizar productos y servicios basados en las tecnologías de la información (TI).

En un mundo cada vez más conectado, Cisco es pionero en la transformación de empresas, gobiernos y ciudades de todo el mundo gracias a una innovación diferenciadora.

Cisco Ransomware Defense:

cisco.com/go/ransomware


Cisco Ransomware Defense aprovecha la arquitectura de seguridad de Cisco para proteger a las empresas desde las redes hasta la capa DNS, correo electrónico y terminales. Última defensa contra el ransomware que es simple, automatizada y efectiva.



 <https://twitter.com/CiscoSecurity>

 <https://www.facebook.com/CiscoSecurity>

 <https://www.linkedin.com/company/Cisco-Security>

 <https://www.youtube.com/Cisco>



Defensa contra el ransomware

Edición especial de Cisco

por **Lawrence Miller, CISSP**

for
dummies[®]
A Wiley Brand

Defensa contra el ransomware For Dummies®, Edición especial de Cisco

Una publicación de
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2017 de John Wiley & Sons, Inc., Hoboken, Nueva Jersey

Ningún apartado de esta publicación se puede reproducir ni almacenar en un sistema de recuperación ni transmitir de ninguna forma ni por ningún medio electrónico, mecánico, fotocopiado, de grabación, escaneado, ni de ninguna otra manera (salvo lo permitido en los apartados 107 o 108 de la Ley de Derechos de Autor de los Estados Unidos de 1976) sin la autorización previa y por escrito del editor. Si deseas solicitar la autorización del editor, escribe a Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, o en línea en <http://www.wiley.com/go/permissions>.

Marcas comerciales: Wiley, For Dummies, el logotipo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier y cualquier otra imagen comercial relacionada son marcas comerciales o marcas comerciales registradas de John Wiley & Sons, Inc. y/o sus socios en Estados Unidos y otros países, y no se pueden utilizar sin autorización por escrito. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios. John Wiley & Sons, Inc. no tiene vinculación con ningún producto ni proveedor que se mencione en este libro.

LÍMITE DE RESPONSABILIDAD/EXCLUSIÓN DE GARANTÍAS: EL EDITOR Y EL AUTOR NO OFRECEN NINGUNA REPRESENTACIÓN NI GARANTÍA SOBRE LA PRECISIÓN O INTEGRIDAD DE LOS CONTENIDOS DE LA MISMA Y ESPECÍFICAMENTE RENUNCIAN A TODAS LAS GARANTÍAS, INCLUIDAS, A TÍTULO MERAMENTE INFORMATIVO, LAS GARANTÍAS IMPLÍCITAS DE APTITUD PARA UN PROPÓSITO PARTICULAR. NINGUNA GARANTÍA PODRÁ CREARSE NI EXTENDERSE MEDIANTE MATERIALES DE VENTA O PROMOCIONALES. LOS CONSEJOS Y ESTRATEGIAS QUE SE INCLUYEN EN LA PRESENTE OBRA PUEDEN NO SER APTOS PARA TODAS LAS SITUACIONES. ESTA OBRA SE VENDE CON LA PREMISA DE QUE EL EDITOR NO SE DEDICA A INTERPRETAR ASUNTOS LEGALES, CONTABLES NI PROFESIONALES. SI SE NECESITA AYUDA PROFESIONAL, DEBERÁN BUSCARSE LOS SERVICIOS DE UN PROFESIONAL COMPETENTE. NI EL EDITOR NI EL AUTOR SERÁN RESPONSABLES DE POSIBLES DAÑOS DERIVADOS DE LA PRESENTE OBRA. EL HECHO DE QUE SE HAGA REFERENCIA A UNA ORGANIZACIÓN O SITIO WEB EN ESTA OBRA O SE MENCIONEN COMO POSIBLES FUENTES DE INFORMACIÓN ADICIONAL NO SIGNIFICA QUE EL AUTOR O EL EDITOR ESTÉ DE ACUERDO CON LA INFORMACIÓN QUE LA ORGANIZACIÓN O SITIO WEB PUEDA PROPORCIONAR NI CON LAS RECOMENDACIONES QUE PUEDA HACER. ASIMISMO, LOS LECTORES DEBEN SABER QUE PUEDEN EXISTIR SITIOS WEB QUE SE MENCIONEN EN ESTE LIBRO QUE HAYAN CAMBIADO O DESAPARECIDO ENTRE EL MOMENTO EN QUE SE ESCRIBIÓ ESTA OBRA Y EL MOMENTO DE LEERLA.

ISBN 978-1-119-37845-7 (pbk); ISBN 978-1-119-37853-2 (ebk)

Producido en los Estados Unidos de América

10 9 8 7 6 5 4 3 2 1

Para obtener información general sobre nuestros productos y servicios, o sobre cómo crear un libro *For Dummies* personalizado para tu empresa u organización, ponte en contacto con el Departamento de Desarrollo Empresarial en EE. UU. en el teléfono 877-409-4177, envía un correo electrónico con info@dummies.biz, o visita www.wiley.com/go/custompub. Para obtener información sobre cómo otorgar licencias a la marca *For Dummies* para productos o servicios, ponte en contacto con BrandedRights&Licenses@Wiley.com.

Reconocimientos del editor

Entre algunas de las personas que contribuyeron a lanzar este libro al mercado se incluyen las siguientes:

Editora de desarrollo: Elizabeth Kuball

Redactora: Elizabeth Kuball

Editora de adquisiciones: Amy Fandrei

Director editorial: Rev Mengle

Representante de desarrollo editorial:
Karen Hattan

Editor de producción: Siddique Shaikh

Colaboración especial: Rachel Ackerly,
Mary Briggs, Dan Gould, Aivy
Iniguez, Kate MacLean, Ben
Munroe, Mark Murtagh

Índice

INTRODUCCIÓN	1
Acerca de este libro.....	1
Algunas suposiciones obvias	1
Iconos utilizados en este libro	2
Más allá del libro	2
CAPÍTULO 1: ¿Qué es el ransomware?	3
Definición de ransomware.....	3
Cómo reconocer el ransomware en el entorno actual de amenazas	4
Cómo funciona el ransomware	7
CAPÍTULO 2: Prácticas recomendadas para reducir los riesgos de ransomware	9
Antes del ataque: descubre, aplica y refuerza.....	9
Durante el ataque: detecta, bloquea y defiende.....	14
Después del ataque: campo de acción, contención y reparación.....	15
CAPÍTULO 3: Construcción de una nueva arquitectura puntera de seguridad	17
Los límites de los diseños de seguridad actuales	17
Definición de la nueva arquitectura de seguridad	19
CAPÍTULO 4: Implementación de Cisco Ransomware Defense	25
Uso del DNS como primera línea de defensa en la nube	25
La seguridad en los terminales y las amenazas por correo electrónico.....	30
Protección de la red con firewalls y segmentación de próxima generación	34
Agilización de las implementaciones y refuerzo de la respuesta ante incidentes	36

CAPÍTULO 5: Diez recomendaciones clave para la defensa contra el ransomware..... 39

El ransomware está evolucionando..... 39

El ransomware como servicio es una amenaza emergente 40

El pago de un rescate no soluciona tus problemas de seguridad 40

Construcción de una arquitectura de seguridad por capas basada en estándares abiertos 41

Implementa soluciones integradas y punteras 42

Integra la seguridad en el entorno de red 42

Reduce la complejidad de tu entorno de seguridad..... 42

Haz uso de la inteligencia de amenazas en la nube y en tiempo real..... 42

Automatiza las acciones de seguridad para reducir el tiempo de respuesta..... 43

Si ves algo, informa de ello 43

Introducción

El aumento del ransomware en los últimos años es un problema cada vez mayor que se ha convertido rápidamente en un negocio delictivo sumamente lucrativo. Las organizaciones víctimas de este delito piensan a menudo que pagar el rescate es la forma más rentable de recuperar sus datos; algo que, desgraciadamente, podría ser cierto. El problema es que cada empresa que paga para recuperar sus archivos está financiando directamente el desarrollo de la próxima generación de ransomware. Como resultado, el ransomware está evolucionando a un ritmo alarmante con variables nuevas y más sofisticadas.

El ransomware debe prevenirse siempre que sea posible, detectarse cuando trate de traspasar una red y contenerse para limitar los posibles daños que pueda causar cuando infecte sistemas y puntos de conexión. La defensa contra el ransomware necesita un enfoque arquitectónico nuevo y puntero que cubra toda la organización, desde el límite de la capa del sistema de nombres de dominio (DNS) hasta el centro de datos, pasando por los dispositivos de puntos de conexión, independientemente de dónde se utilicen.

Acerca de este libro

Defensa contra ransomware For Dummies contiene cinco breves capítulos que analizan cómo funciona el ransomware y cuáles son las características que lo definen (Capítulo 1), prácticas recomendadas de seguridad para reducir los riesgos de ransomware (Capítulo 2), una «nueva y puntera» arquitectura de seguridad (Capítulo 3), la solución de defensa contra el ransomware de Cisco (Capítulo 4) e importantes recomendaciones para la defensa contra el ransomware (Capítulo 5).

Algunas suposiciones obvias

Se ha dicho que la mayoría de las suposiciones han sobrevivido a su inutilidad, pero aun así yo doy por supuestas algunas cosas.

Sobre todo, doy por supuesto que tienes nociones sobre seguridad de la información. Quizá seas un ejecutivo informático de alto nivel, el director de TI, un arquitecto de TI sénior, un analista o jefe, o un administrador de seguridad, redes o sistemas. Como tal, este libro se ha escrito principalmente para lectores técnicos que saben algo sobre redes, infraestructuras y sistemas empresariales informáticos.

Si tu caso se encuentra entre alguno de estos supuestos, este libro es para ti. Si no es así, puedes seguir leyendo de todas formas. Es un libro excelente y, cuando termines de leerlo, sabrás lo suficiente sobre ransomware como para ser un peligro (para los malos).

Iconos utilizados en este libro

En todo el libro utilizo iconos especiales para llamar la atención sobre información importante. Esto es lo que encontrarás:



RECUERDA

Este icono señala la información que debes almacenar en tu memoria no volátil, tu materia gris o tu cabeza –junto a las fechas de aniversarios y cumpleaños.



CUESTIONES
TÉCNICAS

Aquí no encontrarás un mapa del genoma humano, pero si quieres alcanzar el séptimo nivel de FRIKI-vana, ¡ánimo! Este icono explica la jerga que se esconde tras la jerga, y es de lo que están hechos los expertos, bueno, los frikis.



CONSEJO

Gracias por leer, espero que disfrutes del libro y que no te olvides de los autores. Ahora, en serio. Este icono resalta sugerencias y datos útiles.



ADVERTENCIA

Este icono te indica las cosas de las que te advirtió tu madre. Vale, no exactamente. Pero debes estar atento, ya que podrías ahorrarte algo de tiempo y frustración.

Más allá del libro

Con solo 48 páginas, no puedo abarcar todo lo que quiero, así que, si terminas el libro pensando «Qué libro tan bueno. ¿Dónde puedo seguir aprendiendo?», visita www.cisco.com/go/ransomware.

- » Identificación del ransomware y de las características que lo definen
- » Análisis de las tendencias de ransomware
- » Cómo funciona el ransomware

Capítulo 1

¿Qué es el ransomware?

El ransomware es la amenaza de malware que más rápido está creciendo hoy en día, habiéndose convertido ya en epidemia. Según un informe interinstitucional del gobierno de los EE.UU., desde enero de 2016 cada día se ha producido un promedio de más de 4.000 ataques de ransomware. En este capítulo descubrirás en qué consiste el ransomware, cómo está evolucionando como amenaza y cómo funciona.

Definición de ransomware

El ransomware es un software malicioso (malware) que se usa en ataques cibernéticos para cifrar los datos de las víctimas con una clave de cifrado que solo conoce el atacante, por lo que los datos no pueden utilizarse hasta que la víctima pague un rescate (normalmente *criptomoneda*, como bitcoin).



CUESTIONES
TÉCNICAS

La criptomoneda es una moneda digital alternativa que utiliza el cifrado para regular la «impresión» de unidades de moneda (como bitcoins) y para verificar la transferencia de fondos entre diversas partes, sin que exista un intermediario ni banco central.

Las cantidades de los rescates son normalmente altas, aunque no desorbitadas. Por ejemplo, lo que se pide a personas independientes puede variar entre 300 y 600 dólares, mientras que lo normal es que las organizaciones de mayor tamaño paguen más. En 2016, el distrito de un colegio de Carolina del Sur pagó un rescate de unos 10.000 dólares, y un hospital de California pagó aproximadamente 17.000 dólares a los criminales cibernéticos. Estas cantidades se van sumando rápidamente, más de 200 millones de dólares en los primeros tres meses de 2016 según la Oficina Federal de Investigación (FBI) de los Estados Unidos. Esta es una

característica del diseño del ransomware, que hace que las víctimas simplemente paguen el rescate lo más rápido posible en lugar de ponerse en contacto con fuerzas policiales y posiblemente acabar pagando costes directos e indirectos mayores debido a la pérdida de sus datos y la publicidad negativa.



ADVERTENCIA

Las cantidades de los rescates pueden también aumentar significativamente cuanto más tiempo deje pasar la víctima. Una vez más, así es como se ha diseñado este malware, para limitar las opciones de la víctima y hacer que pague el rescate lo más rápido posible.

Cómo reconocer el ransomware en el entorno actual de amenazas

El ransomware no es una nueva amenaza (consulta la figura 1-1). El primer caso de ransomware que se conoce, llamado PC Cyborg, se remonta a 1989. Desde entonces, el ransomware ha evolucionado y se ha convertido en algo mucho más sofisticado. En la actualidad, el ransomware es también más persuasivo y lucrativo debido a los siguientes elementos:

- » **El lanzamiento del teléfono Android:** Android se ha convertido en un vector de ataque popular (macOS es también ahora un objetivo y, sin duda, Apple iOS también lo será).
- » **El aumento del bitcoin:** El bitcoin permite realizar pagos prácticamente indetectables a criminales cibernéticos anónimos de manera muy sencilla.
- » **La aparición de ransomware como servicio (RaaS):** El *RaaS* (ransomware que puede adquirirse por una pequeña tarifa o un porcentaje del pago del rescate) facilita a casi cualquiera el uso de ransomware.

A pesar de los informes en los medios de comunicación sensacionalistas sobre filtraciones indiscriminadas de datos que afectan a organizaciones y empresas, como la Oficina de Administración de Personal (OPM) de los EE. UU., Anthem Blue Cross Blue Shield, Target y Home Depot, con el fin de conseguir robos de identidad y cometer fraudes con tarjetas de crédito, el aumento del ransomware se ha convertido en una de las amenazas más generalizadas que han sufrido las organizaciones y empresas –además de los particulares– el último año.



ADVERTENCIA

Según un informe del Instituto de Tecnología de Infraestructura Crítica (ICIT), el año 2016 ha sido el año en el que el ransomware «ha causado estragos en la comunidad de infraestructuras críticas de los Estados Unidos».

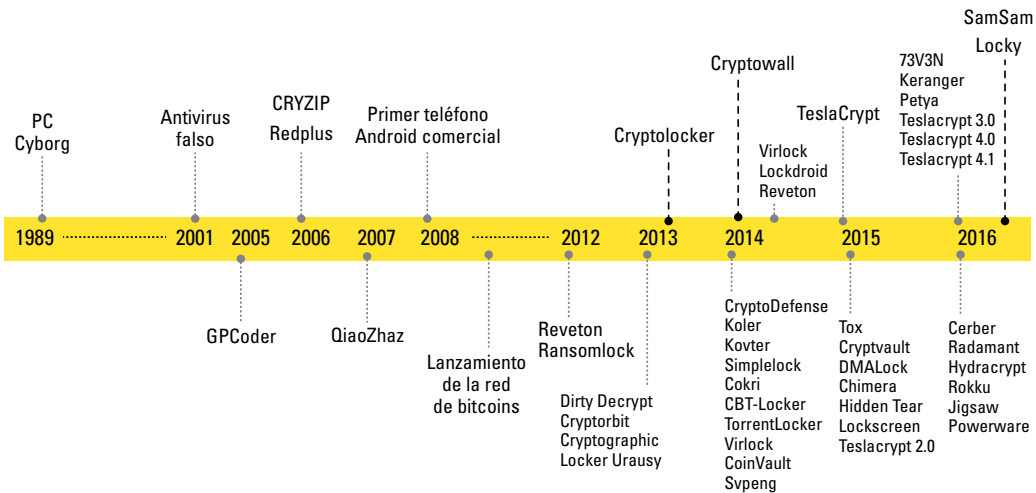


FIGURA 1-1: La evolución del ransomware.

Locky es un ejemplo de variante agresiva de ransomware que se cree que afectará a cerca de 90.000 víctimas cada día. El rescate medio que pide Locky es de 0,5-1 bitcoin. Según las estadísticas de Talos, el grupo de inteligencia de amenazas de Cisco, un 2,9 % de media de las víctimas afectadas en un ataque de ransomware pagará el rescate. Así, Locky podría infectar a 33 millones de víctimas en un periodo de 12 meses, con lo que conseguiría entre 287 y 574 millones de dólares con los pagos de los rescates (consulta la tabla 1-1).

Aunque un cálculo prudente de 287 millones de USD pueda parecer trivial en comparación con una sola filtración de datos (como la de Target,

TABLA 1-1 Pagos a Locky por rescate

Precio del rescate	1 bitcoin	0,5 bitcoins
Víctimas/día	90.000	90.000
Número de pagos/día	2.610	2.610
Precio actual del bitcoin (a 2 de octubre de 2016)	610,82 USD = 1 bitcoin	610,82 USD = 1 bitcoin
Beneficios en 1 día	1.594.240 USD	797.120 USD
Beneficios en 1 mes	47.826.206 USD	23.913.603 USD
Beneficios en 12 meses	573.926.472 USD	286.963.236 USD

que se calcula que le costó a la compañía más de 300 millones de dólares), es importante recordar que los cálculos de pérdidas por filtración de datos se basan en los costes de la organización que ha sufrido el ataque, no en las víctimas individuales a las que se les ha robado la identidad o los datos de sus tarjetas de crédito. Entre los costes para la organización se incluyen los siguientes:

- » **Multas y sanciones reguladoras impuestas** por diversos organismos reguladores, como la Industria de Tarjetas de Pago (PCI).
- » **Tasas legales** asociadas a los litigios a resultas de la filtración.
- » **Pérdidas comerciales** derivadas de la interrupción de la actividad, daños a la reputación de la marca, y pérdida de clientes.
- » **Reparación**, incluida la respuesta al incidente y la recuperación, relaciones públicas, notificaciones de la filtración, y servicios de supervisión de crédito para las personas afectadas.



CONSEJO

El Instituto Ponemon informa que el coste medio de una filtración de datos para las organizaciones afectadas es de aproximadamente 6,5 millones de dólares americanos.

Los criminales cibernéticos venden normalmente la información robada de la identidad y de las tarjetas de crédito en la web oscura –contenido web anónimo (como la venta de droga en el mercado negro, pornografía infantil, delito cibernético, u otras actividades que tratan de evitar la vigilancia o detención preventiva) para cuyo acceso se necesite un software, configuración o autorización especiales– por tan solo unos pocos céntimos o dólares por registro. Según un estudio de 2015 sobre el coste de los delitos cibernéticos llevado a cabo por el Instituto Ponemon, el precio de venta medio de los datos de una tarjeta de crédito estadounidense robada es de unos 0,25 a 60 dólares por tarjeta. En comparación, un criminal cibernético puede conseguir desde cientos a miles de dólares con los pagos directos de los rescates que hagan las víctimas y las organizaciones.

Según el *Estudio sobre el fraude de identidad de 2016* de Javelin Strategy and Research, el coste real para las víctimas de robo de identidad y fraude con tarjetas de crédito se calculó en 15.000 millones de dólares americanos en 2015. El estudio revela también que, aunque el número de víctimas de robo de identidad y fraude con tarjetas de crédito en los Estados Unidos ha permanecido relativamente estable desde 2012, con una media aproximada de 12,8 millones de víctimas particulares, las pérdidas por fraude han descendido en torno al 25 %, lo que significa que los beneficios para los criminales cibernéticos, aunque significativos, están también disminuyendo.

En contraposición a la tendencia a la baja del robo de identidad y el fraude con tarjetas de crédito, el FBI informó que el número de delitos de ransomware se había multiplicado por diez el año anterior, solo durante los tres primeros meses de 2016. El coste para las víctimas de organizaciones y empresas de los Estados Unidos se calcula moderadamente en más de 200 millones de dólares americanos, lo que hace que el ransomware se convirtiera en un delito que costó mil millones de dólares americanos en 2016.

Cómo funciona el ransomware

El ransomware llega normalmente a través de exploit kits, ataques watering hole (en los que uno o varios sitios web de los que visita una organización con frecuencia se infectan con malware), publicidad maliciosa, o campañas de phishing por correo electrónico (consulta la figura 1-2).

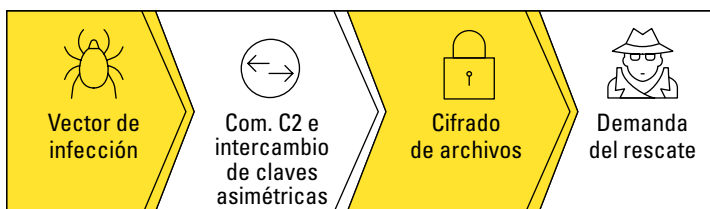


FIGURA 1-2: Cómo infecta el ransomware un terminal.



CONSEJO

Visita <https://youtu.be/4gR562GW7TI> para ver la anatomía de un ataque de ransomware.

Una vez lanzado, el ransomware normalmente identifica los archivos y datos del usuario y los cifra con algún tipo de lista de extensiones de archivo incrustada. También se programa para evitar la interacción con ciertos directorios del sistema (como el directorio del sistema de WINDOWS, o ciertos directorios de archivos de programas) para garantizar la estabilidad del sistema con el fin de que pueda pagarse el rescate después de que la carga deje de ejecutarse. Los archivos de ubicaciones específicas que coinciden con una de las extensiones de los archivos de la lista se cifran. Si no, los archivos no se tocan. Cuando ya se han cifrado los archivos, el ransomware deja normalmente una notificación para el usuario, con instrucciones sobre cómo pagar el rescate (consulta la figura 1-3).

INFECCIÓN POR CORREO ELECTRÓNICO



INFECCIÓN A TRAVÉS DE LA WEB

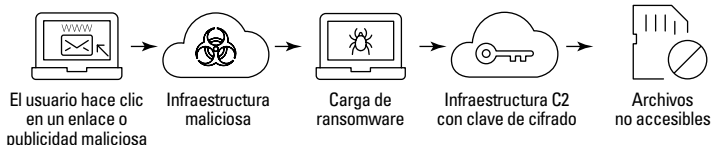


FIGURA 1-3: Cómo funciona el ransomware



ADVERTENCIA

Entre ladrones no existe el honor. Aunque lo normal es que un atacante entregue la clave de descifrado de los archivos cuando se paga el rescate, no hay ninguna garantía de que el atacante no haya instalado también otro malware y exploit kit en el terminal o en otros sistemas de la red, o que no vaya a robar tus datos con otros fines delictivos o para extorsionarte y obtener más pagos en el futuro.

- » Proactividad para defenderse contra el ransomware
- » Automatización de la defensa contra el ransomware para una respuesta rápida
- » Reagrupamiento después de un ataque

Capítulo 2

Prácticas recomendadas para reducir los riesgos de ransomware

En este capítulo, analizo las prácticas recomendadas de seguridad y las estrategias para la reducción de riesgos que, si se aplican de manera correcta, ayudarán a tu organización a defenderse con eficacia contra el ransomware y otras amenazas de seguridad cibernética.

Antes del ataque: descubre, aplica y refuerza

Existen, por supuesto, una serie de prácticas recomendadas que pueden implementar las organizaciones de manera proactiva antes de convertirse en el objetivo de un atacante. Si los atacantes no pueden establecer fácilmente una incursión –poner los pies en la puerta, como si dijéramos– irán a buscar a una víctima más fácil, a menos que tu organización sea el objetivo de un ataque planificado.

Los ataques de ransomware pueden ser oportunistas; el motivo del atacante es a menudo el beneficio, con el menor riesgo y esfuerzo posibles. Por lo tanto, adoptar un enfoque arquitectónico para prevenir que un atacante acceda a tu red es la forma más eficaz de romper la «cadena mortal cibernética» y evitar que un ataque de ransomware tenga éxito.



RECUERDA

El modelo de la cadena mortal cibernética de Lockheed Martin tiene siete fases de ataque: Reconocimiento, fabricación de armamento, entrega, explotación, instalación, comando y control (C2) y acciones sobre el objetivo. Las primeras cinco fases están orientadas a obtener acceso a la red y sistemas que son objetivo.

Los atacantes normalmente logran el acceso inicial al objetivo mediante uno de estos dos métodos:

- » Ingeniería social/phishing para que un usuario desprevenido exponga las credenciales de su red o instale malware.
- » Explotación de una vulnerabilidad en una aplicación o servicio orientada al público (internet).



ADVERTENCIA

En relación con la formación sobre ataques de phishing e información sobre la seguridad, el Informe sobre filtración de datos e investigaciones (DBIR) de Verizon de 2016 lamenta que «aparentemente, la comunicación entre el delincuente y la víctima es mucho más eficaz que la comunicación entre los empleados y el personal de seguridad».



CONSEJO

Deben implementarse las siguientes prácticas recomendadas para evitar que los atacantes consigan acceso a la red y sistemas de tu organización:

- » **Organiza programas de formación e información sobre seguridad de forma regular para los empleados.** Esta formación debe ser participativa e incluir la última información sobre tácticas y amenazas de seguridad. Asegúrate de hacer lo siguiente:
 - Refuerza las políticas de la empresa sobre la no compartición ni revelación de las credenciales de usuario (ni siquiera con los departamentos de TI o seguridad), requisitos de contraseñas seguras, y el papel de la autenticación en la seguridad (incluido el concepto de *falta de reconocimiento* que ofrece a los usuarios defenderse con un «Yo no he sido»).
 - Fomenta el uso de aplicaciones de software como servicio (SaaS) autorizadas por la compañía, como programas para compartir archivos o el intercambio de documentos con terceros en vez de enviar documentos adjuntos por correo electrónico, para reducir (o eliminar por completo) los ataques de phishing a través de los que se envían documentos adjuntos maliciosos.
 - Piensa en la representación de documentos no nativos para archivos PDF y de Microsoft Office en la nube. Las aplicaciones

de escritorio como Adobe Acrobat Reader y Microsoft Word contienen a menudo vulnerabilidades sin parches que pueden utilizar los atacantes.

- Pida a los usuarios que no utilizan macros normalmente que nunca habiliten las macros en los documentos de Microsoft Office. Recientemente, se ha observado un resurgir del malware basado en macros que utiliza técnicas de ofuscación sofisticadas para no ser detectado.
- Explica los procedimientos para informar sobre incidentes y asegúrate de que los usuarios se sienten cómodos a la hora de informar sobre ellos con mensajes como «Tú eres la víctima, no el autor» y «No dar parte de ello (en cuestión de daños) es peor que el acto en sí».
- Recuerda que debes tratar la seguridad física. Aunque es menos común que otras formas de ingeniería social, debe recordarse a los usuarios que los atacantes usan otros métodos y tácticas como buscar en las basuras, espiar por encima del hombro o 'colarse' junto a personas autorizadas, algo que podría amenazar la seguridad personal y de la información.

» **Lleva a cabo evaluaciones de riesgo continuadas para identificar cualquier debilidad y vulnerabilidad de la seguridad en tu organización, y encárgate de las exposiciones a amenazas para reducir el riesgo.** Asegúrate de hacer lo siguiente:

- Realizar exploraciones de vulnerabilidades y puertos de forma periódica.
- Garantizar la gestión de parches de forma continua y puntual.
- Deshabilitar servicios innecesarios y vulnerables y seguir las directrices sobre el endurecimiento de los sistemas de protección.
- Implementar requisitos de contraseñas seguras y autenticación de dos factores (siempre que sea posible).
- Centralizar el registro de seguridad en un recopilador de registros seguro y una plataforma de gestión de eventos (SIEM), y revisar y analizar con frecuencia la información de registros.

Desafortunadamente, a pesar de todo lo que te esfuerces, somos humanos (como Soylen Green) y siempre habrá amenazas de día cero que aprovechen vulnerabilidades desconocidas hasta el momento y, por lo

tanto, sin parches. Si un atacante logra acceder a tu red, su próximo paso será establecer comunicaciones C2 para:

- » Garantizar la persistencia.
- » Aumentar privilegios.
- » Moverse lateralmente por la red, centro de datos y entorno de usuario final.

Para reducir los efectos de una intrusión lograda, debes hacer uso de las siguientes prácticas :

- » Implementa una protección de la capa del sistema de nombres de dominio (DNS) que te permita identificar de forma predictiva los dominios y direcciones IP maliciosos, y una infraestructura de internet que te ayude a reducir el riesgo de un ataque.
- » Habilita automáticamente el firewall, protección avanzada frente a malware, cifrado, y prevención de pérdida de datos en todos los puntos de conexión, incluidos los dispositivos móviles personales (si se permite a los usuarios usar su propio dispositivo en la empres [BYOD]) y medios extraíbles (como unidades USB), de forma que lo sepa el usuario pero sin que necesite hacer nada al respecto. Esto protege a los usuarios remotos y en itinerancia, tanto dentro como fuera de la red, incluso aunque no hagan lo que se supone que tienen que hacer en relación con prácticas recomendadas y políticas establecidas.
- » Habilita la funcionalidad de seguridad en las puertas de enlace del correo electrónico, incluido el bloqueo o eliminación de ejecutables y otros elementos adjuntos que pueden ser maliciosos, la verificación del marco de directivas del remitente (SPF) para reducir la suplantación de identidades de correos electrónicos, y la limitación de correo electrónico (o listas grises) para limitar el volumen de spam potencial a través del correo electrónico.
- » Habilita servicios y productos de seguridad que analicen el tráfico de internet, los correos electrónicos y los archivos para evitar la infección y exfiltración de datos (lo trataremos en mayor profundidad en los capítulos 3 y 4), y haz uso de los servicios de inteligencia de amenazas para obtener un mayor contexto y una investigación rápida.
- » Diseña e implementa una arquitectura de seguridad robusta e inherentemente segura que utilice la segmentación para restringir el movimiento lateral del atacante en tu entorno.

- »» Aplica el principio del privilegio mínimo y elimina la 'adquisición de privilegios' para limitar la habilidad que pueda tener el atacante de ir consiguiendo más privilegios.
- »» Realiza copias de seguridad de datos y sistemas críticos con regularidad, y haz pruebas de las copias de seguridad de vez en cuando para asegurarte de que funcionan y pueden restaurarse. Asimismo, cifra las copias de seguridad y no las guardes en la red, sino en una red para copias de seguridad independiente.
- »» Evalúa y practica las capacidades de respuesta ante incidentes, y controla y mide la eficacia general de tu posición de seguridad de manera habitual y continuada.



CONSEJO

La mayoría del ransomware depende de una infraestructura de comunicaciones C2 robusta, por ejemplo, para transmitir claves de cifrado y mensajes de pagos. Si se evita que un atacante se conecte con el ransomware que ha infectado la red, una organización puede detener un ataque de ransomware. Si, por ejemplo, el atacante no puede enviar claves de cifrado a un terminal infectado ni dar instrucciones a la víctima sobre cómo enviar un pago por el rescate, el ataque de ransomware fracasará. Como se muestra en la tabla 2-1, las variantes de ransomware más comunes hoy en día dependen en gran medida del DNS para las comunicaciones C2. En algunos casos, se usa también un Tor (enrutamiento cebolla) para las comunicaciones C2.

TABLA 2-1 Comunicaciones C2 en el ransomware.

Nombre*	Clave de cifrado	Mensaje de pago
Locky	DNS	DNS
TeslaCrypt	DNS	DNS
CryptoWall	DNS	DNS
TorrentLocker	DNS	DNS
PadCrypt	DNS	DNS, Tor
CTB-Locker	DNS, Tor	DNS
FAKBEN	DNS	DNS, Tor
PayCrypt	DNS	DNS
KeyRanger	DNS, Tor	DNS

* Principales variantes a fecha de marzo de 2016

Durante el ataque: detecta, bloquea y defiende

Si tu organización ha sufrido un ataque, necesitas una respuesta rápida y eficaz contra el incidente para limitar los posibles daños. Las acciones que emprendas y los esfuerzos para remediar el problema serán distintos en función de la situación. Sin embargo, no es durante el ataque cuando tienes que aprender cuáles son las capacidades de respuesta de tu organización para responder al mismo. Las acciones de respuesta ante el incidente deben comprenderse y coordinarse bien –algo que se consigue antes de un ataque– y deben estar bien documentadas y poder repetirse de forma que puedas reconstruir un incidente después de un ataque y poder identificar las lecciones aprendidas y posibles áreas de mejora.

Un componente clave de una respuesta eficaz ante incidentes que a menudo se descuida es la compartición de información, que incluye lo siguiente:

- » **Comunicación de forma puntual y precisa de la información a todas las partes interesadas:** debe proporcionarse la información pertinente a los ejecutivos para que puedan asignarse los recursos adecuados a la respuesta ante el problema y su solución, para que puedan tomarse decisiones empresariales críticas y bien informadas, y para que la información adecuada pueda a su vez comunicarse a empleados, fuerzas policiales, clientes, accionistas y público en general.
- » **Compartición automática de nueva inteligencia de seguridad a través de la arquitectura:** al reunir datos críticos de sistemas dispares, como la seguridad de la información y gestión de eventos (SIEM), inteligencia de amenazas, y herramientas de espacios seguros, el equipo de respuesta ante incidentes puede sacar a la luz y evaluar rápida y eficazmente los incidentes de seguridad de alto impacto. Por ejemplo, si se detecta una nueva carga de malware en un terminal, deberá enviarse automáticamente a una plataforma de inteligencia de amenazas en la nube para que se analice y puedan encontrarse y extraerse posibles indicadores de compromiso (IoC). Después, deberán implementarse y aplicarse automáticamente nuevas medidas correctivas.

Después del ataque: campo de acción, contención y reparación

Entre las acciones importantes que deben emprenderse una vez que el ataque ha finalizado se incluyen las siguientes:

- » Reanudar las operaciones comerciales normales, incluida la restauración de copias de seguridad y sistemas de restablecimiento de imágenes iniciales, según sea necesario.
- » Recopilar y conservar pruebas para las fuerzas policiales y con fines de auditoría.
- » Analizar datos forenses para predecir y evitar ataques futuros, por ejemplo, mediante la identificación de dominios y malware relacionados con las direcciones IP asociadas, hashes de archivo y dominios.
- » Realizar un análisis de causa, identificar las lecciones aprendidas y volver a implementar activos de seguridad, según sea necesario.



CONSEJO

La inteligencia de amenazas predictiva promueve la adopción de una postura de seguridad proactiva, ya que permite a la organización ver la infraestructura de C2 que están usando los atacantes en ataques actuales y futuros para colocarse siempre por delante de la amenaza.

- » Elegir entre tecnología puntera o una solución integral
- » Lo mejor de ambas cosas con una cartera de seguridad integrada

Capítulo 3

Construcción de una nueva arquitectura puntera de seguridad

En este capítulo, conocerás cuáles son las dificultades a la hora de elegir una arquitectura de seguridad y te informaremos sobre una nueva arquitectura puntera para tratar las amenazas modernas, incluido el ransomware.

Los límites de los diseños de seguridad actuales

Antiguamente, muchas empresas pensaban que debían elegir entre:

- » Utilizar productos punteros que fueran eficaces frente a tipos concretos de amenazas emergentes pero que no se integraran totalmente en una arquitectura que incluyera defensas.
- » Adoptar un enfoque de sistemas que incluyera productos de seguridad independientes (o de punto) que fueran lo 'suficientemente buenos' en una arquitectura de sistemas inteligente.

Hoy en día, muchas organizaciones han implementado una arquitectura de red jerárquica formada por un acceso, distribución y capa central con varios productos de seguridad independientes, instalados en una zona de servicios local o DMZ, como un firewall o servidor proxy.

Desafortunadamente, esto no es lo mismo que una ‘defensa a fondo’ (consulta la figura 3-1).

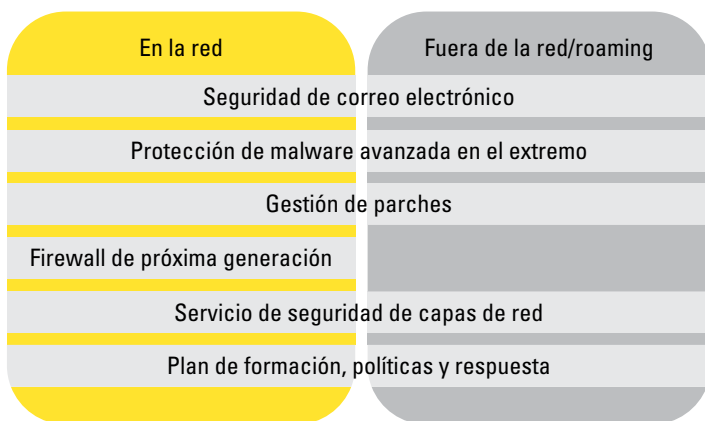


FIGURA 3-1: La seguridad consiste en gestionar el riesgo a través de las capas.

Entre los límites que presentan los métodos actuales se encuentran los siguientes:

- » **No existe integración ni correlación.** Si hay demasiados productos de seguridad independientes, los recursos de seguridad limitados se inundan con demasiados detalles y con información no coordinada que se analiza con dificultad y deja a los equipos de seguridad ‘buscando una aguja en un pajar’.
- » **La seguridad basada en perímetros es solo una parte de una arquitectura efectiva.** Los firewalls, las puertas de enlace a la web seguras y la tecnología de espacios seguros que se han implementado en el perímetro de la red solo ven el tráfico de norte a sur que atraviesa internet. El tráfico de este a oeste del centro de datos –tráfico entre aplicaciones y usuarios finales que nunca cruza el internet– puede ser el responsable del 80 % de todo el tráfico de la red, así que es necesaria una visibilidad completa de toda la red.
- » **Los empleados han salido del edificio.** No solo son los criminales cibernéticos quienes han cambiado su forma de operar (sus tácticas y técnicas), la forma de trabajar y de interactuar digitalmente de nuestros usuarios también ha cambiado. Cada vez hay más usuarios remotos y en itinerancia que trabajan directamente en la nube con varios dispositivos, por lo que las tecnologías que se basan en perímetros y las redes privadas virtuales (VPN) ya no

pueden proteger los dispositivos y los datos de la empresa en su totalidad. Se puede acceder a muchos servicios en la nube (como Salesforce.com y Office 365) a través de una conexión VPN, lo que hace que estas aplicaciones y datos tengan solo una seguridad básica, como una protección frente al malware. Según Gartner, para el año 2018, el 25 % del tráfico de datos de las empresas se desviará de la seguridad del perímetro y fluirá directamente de los dispositivos móviles a la nube. Las soluciones de seguridad modernas deben permitir a tu empresa que trabaje con la nube y desde cualquier dispositivo, en cualquier momento, extendiendo la protección existente mucho más allá del perímetro de la red tradicional.

- » **Existe falta de visibilidad.** Los firewalls tradicionales basados en puertos no detectan muchas amenazas que utilizan técnicas evasivas, como puertos no estándar, saltos de puertos, y cifrado.
- » **No hay segmentación suficiente, y la tradicional puede plantear dificultades.** Las redes se segmentan normalmente en zonas 'de confianza' y 'de no confianza' con LAN virtuales (VLAN) estáticas definidas en conmutadores, que pueden ser difíciles de configurar y mantener. Esta estructura arbitraria no trata la nueva cotidianidad de los centros de datos modernos: máquinas virtuales (VM) que se mueven dinámicamente a lo largo y ancho de los centros de datos y en la nube. En lugar de ello, la segmentación granular múltiple (incluida la microsegmentación) debe definirse en dispositivos de red a través del centro de datos con una segmentación dinámica definida por software.
- » **Las actualizaciones estáticas son solo un punto de partida.** La descarga e instalación de archivos de firma contra el malware es solo un punto de partida para luchar eficazmente contra las amenazas de día cero actuales que tan rápidamente evolucionan. Los archivos de firma estáticos deben reforzarse con inteligencia de amenazas en la nube y en tiempo real.

Definición de la nueva arquitectura de seguridad

Para proteger a las empresas contra el ransomware y otras amenazas modernas, la nueva arquitectura de seguridad puntera adopta un enfoque integrado que es simple, abierto y automatizado, al contrario que los productos de punto tradicionales. Esta nueva arquitectura:

- » Comparte automáticamente la inteligencia de amenazas y ofrece un contexto agregado y correlacionado con otros productos y servicios de seguridad, tanto a nivel local como en la nube.
- » Reduce la complejidad y ofrece visibilidad completa en todo el entorno.
- » Facilita la integración con inversiones de seguridad nuevas y existentes al hacer uso de una tecnología y estándares abiertos y ampliables.
- » Utiliza la integración para ofrecer una respuesta de seguridad automática, de forma que la seguridad es más eficaz y reduce la carga de otros equipos de TI.

Esta nueva arquitectura de seguridad está formada por los siguientes componentes (consulta la figura 3-2):

- » Firewalls de próxima generación (NGFW) y sistemas de prevención de intrusiones de próxima generación (NGIPS) con visibilidad de quién está accediendo a la red y qué está haciendo, aplicación de políticas, analítica de flujos, y análisis de la trayectoria de archivos y dispositivos.
- » Inteligencia de amenazas basada en la nube.
- » Seguridad de la capa del sistema de nombres de dominio (DNS) para ampliar la protección más allá del firewall de la organización.
- » Segmentación de red sumamente granular y definida por software con aplicación de políticas con base en roles independientemente de la ubicación, dispositivo o dirección IP.
- » Seguridad web y de correo electrónico.
- » Protección avanzada contra el malware de red y basado en host con capacidades de espacios seguros.

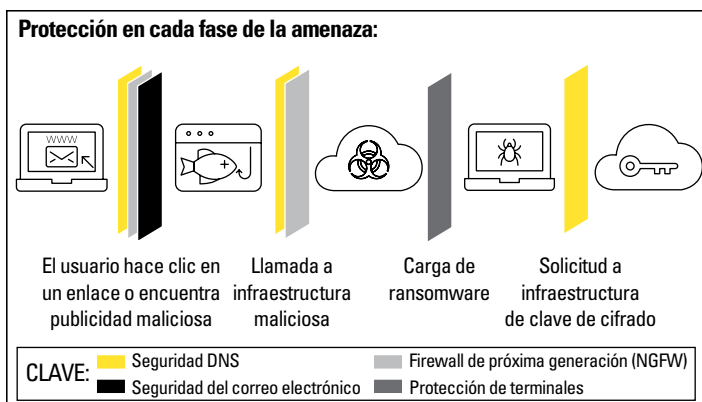


FIGURA 3-2: La nueva arquitectura ofrece la mejor protección de superficie frente a amenazas con defensa de fondo.

CAMUTO GROUP DEFIENDE LA PROPIEDAD INTELECTUAL SIN COMPROMETER LA PRODUCTIVIDAD

El reto: las empresas creativas deben equilibrar la facilidad de acceso con la protección del diseño de activos.

El crecimiento de Camuto Group, una empresa de calzado y moda de marca propia, tiendas en los Estados Unidos y Europa y centros de producción en Brasil, Italia y China, se debe a la virtud de sus diseños exclusivos. La creatividad es el arma competitiva más potente de la empresa, pero para sus profesionales de seguridad de TI, es un arma de doble filo: Camuto debe proteger a sus 500 empleados –100 de los cuales trabajan de manera remota y 250 en itinerancia con sus portátiles– contra el robo de datos. Pero estos profesionales creativos y comerciales deben poder acceder sin restricciones a una gran variedad de sitios web vanguardistas que muchas soluciones de filtración web bloquean de manera incorrecta.

«Proteger los productos de Camuto Group con seguridad es uno de nuestros objetivos principales», comenta Tom Olejniczak, director de Ingeniería de Red de Camuto Group. «Nuestros productos y

diseños son los que impulsan la compañía, así que proteger estos activos es fundamental para respaldar el negocio con éxito».

En misiones anteriores, Olejniczak descubrió que el enfoque tradicional para garantizar la seguridad de la experiencia web –servidores proxy– generaba obstáculos que debían resolverse de forma manual. «Muchos sitios web no maliciosos tienen un cifrado incorrecto o dependen de controles de contenido anticuados, como ActiveX», dice. «Cada vez que alguien necesitaba acceder a un sitio web problemático, necesitaba la ayuda práctica del departamento de TI».

En Camuto, con la gran cantidad de trabajadores móviles que hay, este tipo de intervención manual era simplemente imposible. A medida que aumentó el malware y las redes sociales incidieron en la productividad, Camuto Group necesitaba una solución de seguridad de red que protegiera los dispositivos con conexión y sin conexión a la red sin que añadiera latencia ni obstaculizara la actividad laboral.

La solución: Cisco Umbrella ofrece la línea de defensa más eficaz.

Olejniczak dice que «pensó en Umbrella desde el principio», incluso antes de que Umbrella fuera una opción. Como parte de su investigación para encontrar la solución adecuada para Camuto, TI probó dos opciones: Zscaler y Websense.

Durante el mes que Olejniczak dejó Umbrella para probar Zscaler, «el malware aumentó un 30 %». Estábamos enfrentándonos con tres ataques diarios, pasando un mínimo de una a tres horas cada uno limpiando los sistemas, más que si creáramos nuevas compilaciones». Olejniczak descubrió que los filtros de internet basados en proxy que había usado en el pasado no funcionaban bien en sitios que requerían certificados. «Fue necesaria mucha intervención manual», dice.

«El producto Websense simplemente era lento, era como tener un PC con software extra», añade Olejniczak. «Aumentó la latencia entre un 40-50 %». Al final, Camuto se decidió por Umbrella, e implementó el cliente de itinerancia en los ordenadores portátiles para ampliar la seguridad de Umbrella y sus capacidades de filtrado. «Usamos Umbrella como primera línea de defensa junto a

nuestra protección antivirus y otras protecciones de la red y contra amenazas proactivas», explica Olejniczak.

El impacto: Camuto Group bloquea 400 intentos de malware cada día a la vez que acelera el rendimiento de internet.

«Lo que me gusta de Umbrella es que es una solución en la nube que sustituye el trabajo de filtrado web que hacíamos antes internamente», dice Olejniczak. Para proteger a los empleados en la empresa física, Camuto implementó dispositivos virtuales de Umbrella, con los que pueden identificar redes internas o usuarios de Active Directory que estén infectados o que hayan sufrido un ataque sin la necesidad de tocar los dispositivos ni de volver a autenticar a los usuarios. Los empleados que trabajan fuera de la red de la empresa están protegidos con el cliente itinerante de Umbrella, una instalación que es «tan sencilla como añadir a alguien a un grupo a través de Active Directory de Microsoft».

Camuto Group observó un impacto inmediato y medible en su seguridad. «Cuando llego al panel de control de Umbrella por la mañana», dice Olejniczak, «normalmente veo unos 400 elementos de malware que han sido redireccionados, o sea, miles cada semana». Aun así, el poder de Umbrella no obstaculiza el trabajo de los usuarios. «En realidad, mejoró ligeramente la velocidad de internet», añade Olejniczak. «Hemos observado una mejora de entre el 5-10 %, lo que hace que sea un producto un 30 % mejor que otros».

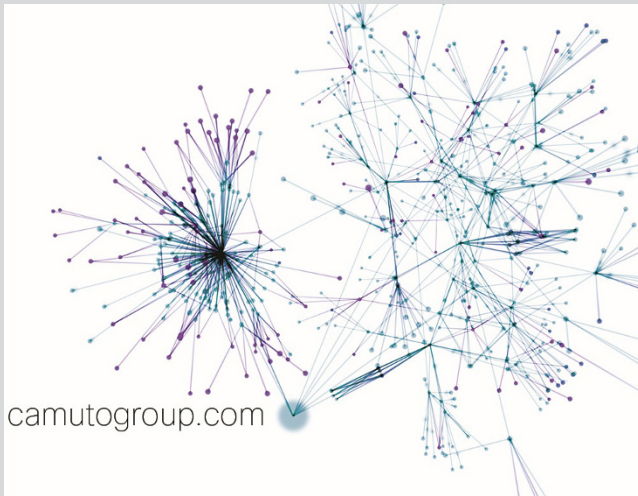
En un negocio que depende de que personas creativas tengan acceso a sitios de moda punteros, la capacidad de poder gestionar listas blancas y negras con rapidez es un factor crítico. «Podemos elegir categorías seguras y aceptables de RR. HH. para filtrar el contenido con rapidez», dice Olejniczak. Cuando los informes señalan sitios desconocidos previamente que son inadecuados o arriesgados, o cuando los empleados solicitan acceso a sitios legítimos que se han bloqueado, actualizar las listas es sencillo. «Es sumamente eficiente: Puedo iniciar sesión, hacer los cambios y cerrar sesión en menos de tres minutos».

Olejniczak ha observado también que el valor de Umbrella ha aumentado con el tiempo. Como él dice: «Cuanto más usas el producto, más ventajas obtienes. Hay muy pocos productos que haya usado a lo largo de mi carrera y que realmente hagan lo que pro-

(continuación)

(continuación)

meten, y Umbrella es uno de ellos. Esta visualización de datos (consulta la figura más abajo) es un resumen de alto nivel de cómo Cisco Umbrella ve la infraestructura del dominio de un cliente y de cómo una parte de los usuarios de Umbrella (más de 65 millones) interactúa con dicho dominio y su infraestructura relacionada.



CONSEJO

En el capítulo 4, puedes ver el acercamiento de Cisco a su nueva y mejorada arquitectura de Seguridad con Cisco Ransomware Defense. La figura 3-3 explica los productos de Seguridad de Cisco que previenen, detectan y responden a los ataques de ransomware.

	Rápida prevención <i>Prevención en la nube</i>	Avanzado <i>Prevención y Contención</i>
<i>Detén el ataque antes de que ocurra</i>	<ul style="list-style-type: none">• Cisco Umbrella/Umbrella Roaming• AMP para puntos de acceso• Seguridad para Email en la Nube con AMP• Servicios de Desarrollo de AMP	<ul style="list-style-type: none">• Rápida prevención +<ul style="list-style-type: none">• NGFW• Seguridad Web con AMP• AnyConnect• Servicio de Respuesta a Incidentes• Servicios de Prueba de Penetración y Aplicación de la Red
<i>Detén y contiene cuando el ataque esté presente</i>		<ul style="list-style-type: none">• La red como responsable del cumplimiento de las normas de seguridad<ul style="list-style-type: none">• Stealthwatch• ISE• Switches con TrustSec• AMP ThreatGrid• NGIPS• Servicios de Desarrollo y Diseño de ISE and Stealthwatch

FIGURA 3-3: Bundles disponibles de la solución Cisco Ransomware Defense

- » **Trasladar la defensa contra el ransomware a la nube**
- » **Cerrar los vectores de ataque de ransomware en terminales y correo electrónico**
- » **Aplicar las políticas de seguridad con firewalls y segmentación de próxima generación**
- » **Utilizar los servicios de consultoría de seguridad de Cisco**

Capítulo **4**

Implementación de Cisco Ransomware Defense

Cisco Ransomware Defense utiliza la arquitectura de seguridad de Cisco para proteger a las empresas. Esta solución ofrece un enfoque arquitectónico para combatir el ransomware en todos los lugares a través de los que intenta atacar a una red. Esto significa una protección por capas complementaria que va desde la capa DNS hasta el correo electrónico, la red y el terminal. En este capítulo, conocerás la solución Cisco Ransomware Defense.

Uso del DNS como primera línea de defensa en la nube

Un ataque de ransomware tiene muchas fases. Antes del lanzamiento del ataque, el atacante necesita organizar la infraestructura de internet para poder ejecutar, dar órdenes y controlar (C2) las diferentes fases. Cisco Umbrella ofrece la primera línea de defensa, deteniendo los ataques de ransomware (y otros ataques cibernéticos) antes en la cadena mortal mediante el bloqueo de las conexiones a internet de sitios maliciosos a través de los que llega el malware. Umbrella, construido en las bases de internet, implementa la seguridad en las capas del sistema de nombre de dominio (DNS) y de protocolo de internet (IP) (consulta la figura 4-1).

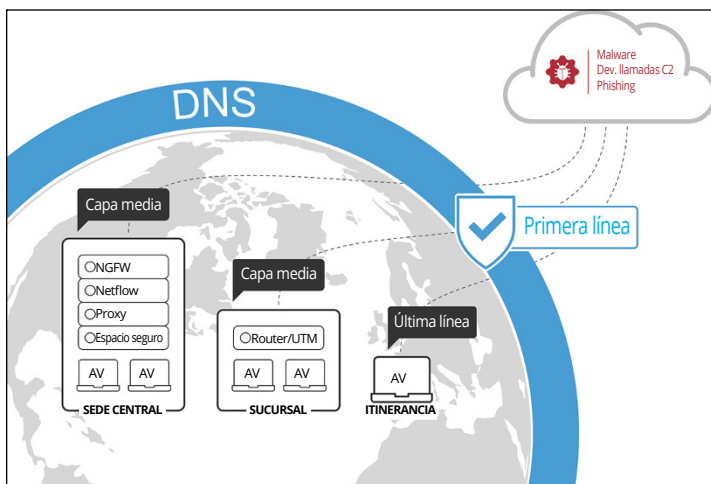


FIGURA 4-1: El DNS es la primera línea de defensa contra los ataques de ransomware.

Umbrella ofrece visibilidad completa de la actividad de internet a través de todas las ubicaciones, dispositivos y usuarios, y bloquea las amenazas sobre cualquier puerto o protocolo incluso antes de que lleguen a la red o terminales. Al analizar y aprender con los patrones de actividad de internet, Umbrella descubre automáticamente la infraestructura que ha organizado el atacante para las amenazas actuales y emergentes, y bloquea de manera proactiva las solicitudes a destinos maliciosos incluso antes de que se establezca una conexión o se descargue un archivo malicioso. Umbrella puede también bloquear las devoluciones de llamadas C2 a los servidores de los atacantes y detener la exfiltración de datos de los sistemas comprometidos. Con Umbrella puedes detener antes las infecciones de malware y phishing, identificar dispositivos ya infectados con mayor rapidez, y evitar la exfiltración de datos.



Al contrario que con las aplicaciones, el servicio en la nube protege los terminales tanto dentro como fuera de la red de la empresa. Al contrario que los agentes, la protección de las capas DNS llega a cada dispositivo conectado a la red, incluso el internet de las cosas. Es la forma más rápida y sencilla de proteger a todos los usuarios, y puede implementarse en tan solo 30 minutos. Descarga el documento informativo: “Why a DNS Layer Matters: 30 Minutes to a More Secure Enterprise» (La importancia de la capa DNS: 30 minutos para conseguir una empresa más segura) en <http://cs.co/30-mins-to-a-more-secure-enterprise> para obtener más información.

CISCO TI IMPLEMENTA UMBRELLA PARA DEFENDERSE DEL RANSOMWARE Y DE OTROS MALES RESIDENTES

En abril de 2016, Cisco adoptó Umbrella en su departamento de TI interno con dos objetivos principales:

- **Aumentar la protección contra el malware, redes de robots (botnets) y filtraciones:** como red proveedora de DNS a nivel global, Umbrella recibe un 2 % de las solicitudes de internet de todo el mundo. Aprende con rapidez y bloquea las amenazas emergentes antes de que tengan oportunidad de causar daños.
- **Obtener información sobre los comportamientos arriesgados de los usuarios:** Umbrella genera un registro que muestra toda la actividad de internet, independientemente del puerto y protocolo. El registro ofrece a los equipos de TI y de seguridad de Cisco una mayor visibilidad y capacidades de auditoría.

El cambio a Umbrella fue increíblemente simple. «Añadimos controles nuevos y potentes sin la necesidad de implementar nuevo hardware, reconfigurar la red, realizar grandes pruebas de interoperabilidad ni cambiar ningún otro sistema», dice Rich West, arquitecto de información de seguridad (InfoSec) de Cisco.

Cisco formó un equipo de ocho miembros de TI e InfoSec para planificar e implementar Umbrella. Los aspectos técnicos de la transición llevaron muy poco tiempo. Los miembros del equipo pasaron la mayor parte del tiempo reuniéndose con propietarios de aplicaciones y equipos de operaciones de redes para explicar las ventajas de la transición y para responder a cualquier pregunta relacionada con los posibles efectos sobre el rendimiento de las aplicaciones o la red.

La conversión fue tan sencilla como añadir cuatro líneas de código al archivo de configuración del DNS en los servidores de DNS internos de Cisco para dirigir las consultas a Umbrella. Ahora los servidores del DNS de TI de Cisco recurren a Umbrella para las consultas al DNS en lugar de acudir a sus vecinos de arriba. La conversión fue tan fluida que los usuarios internos ni siquiera se dieron cuenta del cambio.

ASÍ ACABÓ CON EL RANSOMWARE UN FABRICANTE DE PROTEÍNAS

El reto: luchar contra dificultades de seguridad ilimitadas con recursos limitados

En los años que han pasado desde su fundación en 1983, Octapharma se ha convertido en uno de los mayores fabricantes de proteínas humanas del mundo. Con una iniciativa empresarial en curso diseñada para duplicar la capacidad de producción y aumentar las eficiencias generales para el 2019, la compañía está experimentando una expansión sin precedentes.

El impacto de este crecimiento acelerado es evidente en toda la organización, incluso a nivel de red. «A medida que contamos con más empleados en más ubicaciones que usan dispositivos móviles y servicios en la nube, añadimos también nuevas vulnerabilidades de seguridad en la red», dice Jason Hancock, el ingeniero de redes senior global de Octapharma. «Hemos observado un aumento en una variedad de actividades maliciosas, incluido el ransomware».

«En lugar de intentar cubrir cualquier exposición contratando al tipo de personal de seguridad con formación que ya escasea, nuestra prioridad ha sido identificar nuevas soluciones para tratar estas vulnerabilidades y trabajar en línea con los objetivos de eficiencia de la organización», añade.

«Para centrarnos en esto», comenta Hancock, «primero teníamos que evitar que la red cayera cada 15 minutos y mejorar las eficiencias para nuestros equipos y usuarios. Cuando me incorporé a la compañía en 2014, mi objetivo inicial fue estabilizar las cosas para poder centrarme en evitar los ataques de un malware cada vez más agresivo, como la filtración de CryptoLocker que habíamos sufrido».

La solución: funcionalidad que encaja

«Antes de mi llegada a Octapharma, el equipo había estado trabajando durante algún tiempo para migrar las aplicaciones de seguridad web a nivel local al servicio en la nube del mismo proveedor, que había seleccionado un antecesor. Mi tarea inicial fue finalizar esa implementación», recuerda Hancock. «En el momento que vi con lo que tenía que

trabajar, me di cuenta de que no iba a satisfacer nuestras necesidades».

«Nos encontramos con problemas significativos que nos hicieron dudar sobre la viabilidad del producto en nuestro entorno, comenzando con la funcionalidad de internet». Hancock continúa: «Nuestro equipo recibió muchos comentarios de usuarios que estaban descontentos con el servicio de internet, lo que se atribuyó al servicio en la nube y al cliente de terminales en los equipos de los usuarios».

«Además de todo eso», continúa, «el conjunto de funciones era incoherente con nuestras necesidades y el equipo tenía cada vez más dificultades en torno a la administración. Esto significaba que teníamos que ofrecer mucha formación para dar soporte a una gestión muy detallada y no intuitiva de las políticas y de los diversos componentes».

«Después de una implementación en Norte América cargada de problemas, nuestra red estaba inactiva de forma habitual. La inestabilidad de no tener internet durante varias horas tuvo un efecto negativo en nuestro equipo, y no pudo resolverse a través de los canales de soporte del producto», explica Hancock. «Finalmente, [el proveedor] sugirió que dejáramos nuestra migración a la nube para usar aplicaciones virtuales, lo que requería un redireccionamiento del tráfico desde más de 50 ubicaciones en todo el mundo, algo que no queríamos y que, en algunos casos, era imposible».

«En ese momento fue cuando levanté la mano y dije que la única forma de resolver el problema sería con Cisco Umbrella, que se podría implementar para proteger la red global en un plazo de seis semanas». Después de invertir tanto en una solución que no funcionó, estábamos listos para pasar a una solución que, gracias a mi experiencia anterior, yo sabía que funcionaría: Umbrella».

Los resultados: una reducción drástica del ransomware

Después de una sencilla implementación, Octapharma vio resultados de inmediato. «Desde que implementamos Umbrella, no hemos tenido problemas de seguridad web», dice Hancock.

«Hemos reducido drásticamente nuestra exposición al ransomware, y desde la implementación, no hemos sido víctimas del ransomware por hacer clic en un enlace malicioso. En realidad vemos miles de bloqueos cada semana debidos a la política de seguridad, y eso sin contar los bloqueos que se basan en las políticas de categorías», añade. «Hemos

(continuación)

(continuación)

cubierto un gran riesgo en el vector del ransomware de ataques web, y mejorado en gran medida la experiencia del usuario en relación con la conectividad a internet».

«Incluso hemos identificado algunos correos electrónicos de phishing y los hemos probado intentando hacer clic en los enlaces; gracias a Umbrella, no pudimos acceder a los sitios».

¿Otra ventaja inesperada? El ingeniero de redes dice: «Al correlacionar la cantidad de datos que sale del panel de control de Umbrella con nuestros sistemas internos, hemos descubierto equipos infectados que antes no habíamos detectado».

Con su solución de seguridad que ahora puede bloquear amenazas en la capa DNS, la compañía continúa buscando maneras de seguir reforzando la red con una gestión proactiva de la seguridad. «Aunque Umbrella es muy capaz de bloquear sitios en base a políticas de categorías, es mucho más efectiva como herramienta de seguridad y, con esto en mente para nuestra implementación, es un componente crítico de nuestra estrategia de defensa de fondo. Actualmente, estoy investigando herramientas adicionales que son parte de la cartera de seguridad de Cisco para continuar reforzando esta estrategia», comenta el ingeniero de redes. «Estoy pensando en mejorar el firewall, la protección contra malware para terminales, y una mayor coordinación de los productos de nuestro conjunto de herramientas de seguridad».

Para Jason Hancock, ver siempre ha sido creer. «He estado utilizando Umbrella en mi casa durante años», dice. «Y ahora he visto lo bien que funciona también en dos organizaciones diferentes. Mis colegas me hablan también maravillas del enfoque único y sumamente eficaz que adopta Cisco ante la seguridad».

La seguridad en los terminales y las amenazas por correo electrónico

Las amenazas de malware actuales son las más sofisticadas que se han conocido. El malware avanzado, incluido el ransomware, evoluciona con rapidez y puede evadir la detección después de haber puesto ya en peligro a un sistema a través de distintos métodos, incluidos los siguientes:

» Técnicas de suspensión

- » Polimorfismo y metamorfismo
- » Cifrado y ofuscación
- » Uso de protocolos desconocidos

Al mismo tiempo, el malware avanzado proporciona una plataforma de lanzamiento a un atacante persistente para que se pueda mover lateralmente por la red de una organización comprometida.

Para los criminales cibernéticos, las campañas de phishing por correo electrónico son las favoritas –e increíblemente efectivas– del vector de ataque de malware. Las variaciones de ransomware recientes, como Locky y Chimera, usan todas ellas técnicas de phishing para infectar a las víctimas.

Entre las soluciones de Cisco Ransomware Defense que aseguran los terminales y evitan las amenazas por correo electrónico se incluyen Cisco Advanced Malware Protection (AMP) para terminales y Cisco Cloud Email Security con AMP.

Cisco Advanced Malware Protection (AMP) para terminales

El software antimalware tradicional que solo usa técnicas de detección en un momento dado no será nunca 100% efectivo. Y la verdad es que solo es necesaria una amenaza que evada la detección para poner en peligro todo tu entorno. Mediante el malware dirigido y conocedor del contexto, los atacantes sofisticados tienen los recursos, conocimientos y persistencia para engañar a las defensas que solo se usan en un momento dado. La detección en un momento dado está también totalmente ciega, al alcance y profundidad de una filtración una vez que haya ocurrido, dejando a las organizaciones incapaces de evitar que la irrupción se extienda o de evitar que se produzca de nuevo un ataque similar.



CONSEJO

Aunque ninguna solución de antimalware puede eliminar el ransomware ni descifrar los archivos una vez que un terminal está infectado, Cisco ayuda a las organizaciones a detectar el ransomware de manera proactiva y bloquearlo antes de que llegue a la red.

Basándose en esta concepción del malware, Cisco creó AMP para terminales, con el fin de brindar un marco completo de capacidades de detección y análisis de macrodatos para analizar de manera continuada los archivos y el tráfico y poder, así, identificar y bloquear las amenazas de malware avanzado. Las sofisticadas técnicas de aprendizaje automático evalúan más de 400 características asociadas a cada archivo. La seguridad retrospectiva –la capacidad para retroceder en el tiempo y trazar procesos, actividades de archivos y comunicaciones para comprender el

alcance total de una infección, establecer la causa y aplicar una solución— puede detectar los archivos que se hayan infectado y avisarte de ello. Esta combinación de análisis continuo y seguridad retrospectiva proporciona una protección contra el malware avanzado que va más allá de la detección tradicional en un momento dado (consulta la figura 4-2).

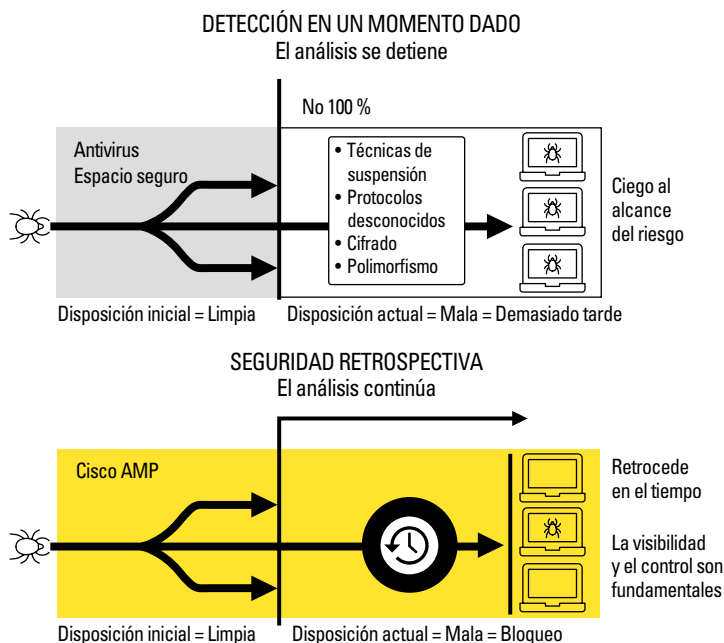


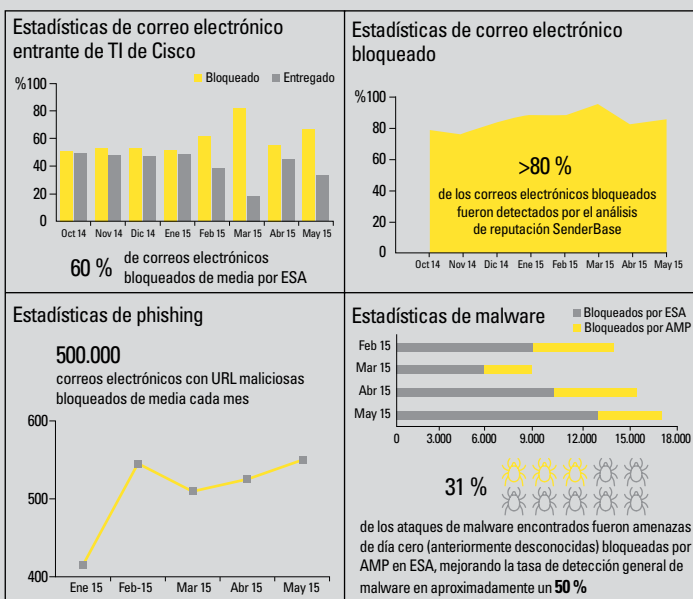
FIGURA 4-2: Detección en un momento dado comparada con el análisis continuo y la seguridad retrospectiva.

Cisco Email Security con protección contra malware avanzado (AMP)

El correo electrónico es una herramienta de comunicación fundamental en la empresa, pero puede exponer a las organizaciones a una gran variedad de amenazas sofisticadas. Cisco Email Security con protección contra malware avanzado (AMP) bloquea los correos electrónicos de spam y phishing y las URL y elementos adjuntos maliciosos, que son un vector de ataque importante del ransomware. La tecnología AMP es la misma que se aplica al terminal, pero se implementa en la puerta de enlace del correo electrónico.

CISCO BEBE SU PROPIO CHAMPÁN

Cisco TI depende de Cisco Email Security con AMP a la hora de implantar su estrategia de seguridad de correo electrónico contra las amenazas. Como muestra la gráfica siguiente, los resultados hablan por sí mismos.



Cisco Email Security con AMP protege el correo electrónico crítico para la empresa con una protección por capas que incluye:

- » Inteligencia de amenazas global
- » Bloqueo de spam
- » Detección de correo no deseado y cancelación segura de la suscripción
- » Protección contra malware avanzado
- » Filtros contra infiltración
- » Seguimiento de interacción web
- » Control de mensajes salientes

- » Detección de correo electrónico falsificado
- » Prevención de pérdida de datos

Protección de la red con firewalls y segmentación de próxima generación

Cisco Firepower, los firewalls de próxima generación (NGFW) contra las amenazas, ofrecen una defensa integrada contra amenazas en toda la secuencia de un ataque –antes, durante y después– con una visibilidad sin igual que no es posible en los firewalls existentes basados en puertos. La tecnología Cisco TrustSec ofrece una segmentación de la red dinámica y definida por software. Utiliza la red existente para que las políticas de seguridad granulares basadas en funciones se implementen en segmentos de red discretos, independientemente de la ubicación o dispositivo del usuario. El resultado es una segmentación más simple que ayuda a evitar que el malware se mueva lateralmente por la red de la organización; esto puede limitar el daño del malware una vez que se ha producido una violación.

Firewall de próxima generación (NGFW) Cisco Firepower

El firewall de próxima generación (NGFW) Cisco Firepower con protección contra el malware avanzado (AMP) y tecnología de espacios seguros Threat Grid bloquea las amenazas conocidas y la devolución de llamadas de comando y control (C2) mientras proporciona a la vez un análisis dinámico para malware y amenazas desconocidos. Cisco Firepower ofrece:

- » Visibilidad y control de la aplicación (AVC) precisos: identifica y controla el acceso de los usuarios a más de 4.000 aplicaciones comerciales, además de ser compatible con aplicaciones personalizadas.
- » IPS de próxima generación de Cisco: prevención de amenazas sumamente efectiva y conocimiento contextual completo de los usuarios, infraestructuras, aplicaciones y contenido para ayudarte a detectar amenazas multivector y automatizar la respuesta de la defensa.
- » Filtrado de URL basado en reputación y categorías: este filtrado ofrece un sistema de alerta y control exhaustivo sobre el tráfico web sospechoso. Implementa las políticas de cientos de millones de URL en más de 80 categorías.

- » Protección contra malware avanzado: detección de filtraciones efectiva con un coste total de propiedad reducido que ofrece valor a la protección. Descubre, comprende y detiene el malware y las amenazas emergentes que no detectan otras capas de seguridad, y se activa con una simple licencia de software.

Usa la red como un sensor y ejecutor

Cisco utiliza la red para hacer cumplir dinámicamente la política de seguridad con una segmentación definida por software que se ha diseñado para reducir la superficie del ataque general, contener los ataques evitando el movimiento lateral de las amenazas por la red, y reducir el tiempo necesario para aislar las amenazas una vez que se han detectado.

Las soluciones de Cisco permiten a la propia red actuar como un sensor y ejecutor. El motor de servicios de identidad (ISE) con TrustSec y Stealthwatch simplifica el aprovisionamiento y gestión del acceso a la red seguro, ofrece mayor visibilidad de actividades anómalas en la red, acelera las operaciones de seguridad y aplica las políticas de manera coherente en cualquier lugar de la red. Al contrario que los mecanismos de control de acceso, que se basan en la topología de la red, los controles de Cisco TrustSec están definidos por medio de agrupamientos lógicos, por lo que la segmentación de recursos y el acceso seguro se mantienen continuamente, incluso cuando los recursos se mueven a través de redes móviles y virtualizadas. ¿Qué significa todo esto? La aplicación de políticas de TrustSec puede evitar que un ataque de ransomware se extienda por la red.



RECUERDA

La funcionalidad Cisco TrustSec está incluida en los productos de conmutación, enrutamiento, LAN inalámbrica (WLAN) y firewall de Cisco para proteger los activos y aplicaciones en las redes de los centros de datos y de las empresas.

Los métodos de control de acceso tradicionales segmentan y protegen los activos usando LAN virtuales (VLAN) y listas de control de acceso (ACL). En lugar de esto, Cisco TrustSec utiliza políticas de grupos de seguridad que están escritas con una matriz de lenguaje simple y desacopladas de direcciones IP y VLAN. Los usuarios y activos con la misma clasificación de funciones se asignan a un grupo de seguridad.

Las políticas de Cisco TrustSec se crean centralmente y se distribuyen automáticamente a redes VPN cableadas e inalámbricas para que los usuarios y activos reciban acceso y protección de manera constante cuando se mueven en redes virtuales y móviles. La segmentación definida por software ayuda a reducir el tiempo que se dedica a las tareas de ingeniería de red y a la validación del cumplimiento normativo.

Agilización de las implementaciones y refuerzo de la respuesta ante incidentes

Los servicios de consultoría de seguridad de Cisco incluyen la implementación de servicios para las soluciones de Cisco Ransomware Defense, incluidos Firepower y AMP, además de respuesta ante incidentes.

El equipo de respuesta ante incidentes de los servicios de seguridad de Cisco puede proporcionar:

- » Servicios proactivos de preparación de respuesta ante incidentes para ayudar a tu organización a desarrollar o evaluar sus capacidades de respuesta ante incidentes.
- » Respuesta reactiva ante incidentes en caso de producirse un ataque de ransomware u otros incidentes de seguridad.

Asimismo, los servicios de integración de seguridad de Cisco tratan las dificultades arquitectónicas a nivel de soluciones. Agilizan la implementación de las tecnologías de soluciones como la protección contra malware avanzado (AMP) para terminales y los firewalls de próxima generación (NGFW) de Cisco.

CÓMO AUMENTA LA SEGURIDAD Y EL RENDIMIENTO CON CISCO UN LÍDER DEL SECTOR INMOBILIARIO LOGÍSTICO

El reto: desarrollar una protección de defensa de fondo

Prologis, Inc., líder mundial del sector inmobiliario logístico, alquila instalaciones de distribución modernas a una variedad de aproximadamente 5.200 clientes que entran dentro de dos categorías principales: los negocios de empresa a empresa y la venta minorista/en línea. Cuenta con más de 60 oficinas en 20 países en cuatro continentes. Prologis, que cotiza en la Bolsa de Nueva York con el símbolo PLD, está en la lista de las compañías más admiradas del mundo y en la de las 100 empresas más sostenibles del mundo.

«Ser global significa trabajar en cualquier lugar, y poder hacerlo con éxito significa depender mucho de la informática en la nube», comenta el arquitecto de soluciones de seguridad de Prologis, Tyler Warren.

«Como la mayor parte de la infraestructura de TI de Prologis está en la nube, no tenemos una infraestructura ni perímetro típicos, lo que dificulta la implementación de soluciones».

Como organización global que cotiza en bolsa y con muchas operaciones en la nube, Prologis necesita proteger sus sistemas para no dejarlos en peligro, y asegurarse de que esto no ocurra al ampliar la pila de seguridad es la misión de Warren.

«A medida que vimos el aumento de la actividad de amenazas, tuvimos claro que Prologis necesitaba fortalecer las medidas de seguridad existentes para proteger la red y a los usuarios, dentro y fuera de la red, contra actividades maliciosas, como la devolución de llamadas de comando y control, malware y phishing», continúa. «Para nosotros, un modelo de seguridad por capas tenía sentido, ya que ningún elemento de seguridad por sí solo es lo suficientemente fuerte para detener los ataques».

La solución: seguridad reforzada que se adapta a la pila y a los usuarios

«Para ampliar nuestra pila de seguridad tuvimos que probar varias cosas. Queríamos que todos los elementos fueran compatibles y capaces de integrarse de manera eficiente sin que ello afectara a los usuarios. También debían protegernos allí donde trabajáramos: en cualquier lugar del mundo y en la nube», señala Warren.

La breve lista de bloqueo de Prologis de tipos de contenido ofensivo muy específicos necesitaba el filtrado web, de lo que se ocupó inicialmente otro proveedor. Según Warren: «Nos resultaba difícil gestionarlo. Pero lo más importantes es que no encajaba en nuestro objetivo empresarial de trasladar todo a la nube».

«Necesitábamos una capa de seguridad que nos ayudara a combatir ciertos problemas de seguridad derivados del uso de internet por los empleados, y también necesitábamos intensificar el filtrado web», recuerda Warren. «Nos dimos cuenta de que Umbrella es la primera capa que bloquea la actividad maliciosa».

En su búsqueda para encontrar la mejor manera de satisfacer sus necesidades, Prologis realizó ensayos de prueba de concepto con otros tres proveedores y con Cisco. Después de descartar a los demás con base en una variedad de factores, incluidos los requisitos del hardware, complejidad, configuración que consumía mucho tiempo, y precio, Prologis eligió Cisco Umbrella.

(continuación)

(continuación)

«Umbrella satisface todas nuestras necesidades», dice Warren. «Aborda nuestras preocupaciones de seguridad específicas, se encarga del filtrado web, y protege a nuestros usuarios remotos, todo ello en una sola solución en la nube fácil de implementar».

Los resultados: aplicación de políticas con sustanciales mejoras de rendimiento

«No tuvimos que esperar mucho para ver los resultados», afirma Warren. «Para Prologis, poder aplicar las políticas en cualquier sitio – incluidos los dispositivos fuera de la red– de manera coherente es sumamente importante», añade. «La implementación de cliente itinerante de Umbrella fue tan eficiente que nadie se ha dado cuenta de que se llevó a cabo».

En cuanto al bloqueo de actividades y sitios web maliciosos, «en los últimos seis meses, solo hemos tenido unos cuatro o cinco falsos positivos, y eran de sitios que no estaban en los EE. UU. Esta cifra es extraordinaria; menos de uno al mes es verdaderamente asombroso».

Warren señala también el aumento significativo del rendimiento como otro resultado positivo. «Después de instalar Umbrella, vimos un gran aumento del rendimiento. Por ejemplo, en China y Japón, los tiempos de respuesta de la aplicación mejoraron hasta el 50 %. En nuestra oficina de Denver, el tiempo de descarga de 10 MB de la nube pasó de los 11,4 segundos antes de la implementación a 4,4 segundos después de ella. Debido a que la mayoría de las aplicaciones que usa Prologis están en la nube, para nosotros el rendimiento es sumamente importante. El 100 % de las aplicaciones que usamos han conseguido un aumento del rendimiento».

Otras características de Umbrella también han resultado útiles. «La generación de informes automática también es práctica –sobre todo el informe de servicios en la nube– ya que me permite compartir datos claros y asimilables sobre lo bien que está protegida la red y sobre el trabajo informático en paralelo que tiene lugar en la nube, lo que nos ha abierto realmente los ojos», señala Warren. «Los informes me permiten identificar problemas con facilidad, y facilitan la vida a muchas personas al hacer hincapié en la necesidad de una infraestructura de seguridad de defensa de fondo».

«Añadir Umbrella a nuestra solución de seguridad ha sido una excelente decisión. Todo el mundo está muy satisfecho con la mejora de la seguridad y el rendimiento que hemos obtenido gracias a su implementación».

- » Retos de la defensa contra el ransomware
- » Creación e implementación de un entorno inherentemente seguro
- » Cómo evitar la complejidad
- » Automatización de tareas para anticipar amenazas de rápida evolución

Capítulo 5

Diez recomendaciones clave para la defensa contra el ransomware

En este capítulo trato algunos puntos sobre la defensa contra el ransomware que es importante recordar.

El ransomware está evolucionando

El ransomware es la amenaza de malware que más rápido está creciendo hoy en día, y evoluciona con rapidez. Por ejemplo, CryptoWall –una de las campañas de ransomware más lucrativas y de mayor alcance de Internet actualmente– surgió inicialmente en 2014 e infectó a miles de millones de archivos de todo el mundo. Desde entonces, se han desarrollado tres variantes adicionales de CryptoWall, cada una de ellas más sofisticada que la anterior.

El ritmo de la evolución también está aumentando. En los últimos tres años, el número de campañas y variantes de ransomware ha eclipsado muchas veces el total de campañas y variantes de ransomware de los 25 años anteriores, desde que tuviera lugar la primera campaña de

ransomware –PC Cyborg– en 1989. Durante el primer trimestre de 2016, las variantes descubiertas fueron la mitad de las que se descubrieron en todo el 2015, y casi el doble que las que se descubrieron en todo el 2014.

Son varios los factores que han contribuido al rápido crecimiento y evolución del ransomware, incluida la omnipresencia de los teléfonos Android (que se han convertido en un vector de ataque popular), el aumento de los bitcoins (que permite realizar pagos prácticamente indetectables a los criminales cibernéticos) y el surgimiento del ransomware como servicio (RaaS; consulta el apartado siguiente), que hace que casi cualquier persona pueda usar fácilmente el ransomware.

El ransomware como servicio es una amenaza emergente

El RaaS es una nueva amenaza que hace que, prácticamente para cualquier persona, sea tan fácil como contar hasta tres convertirse en un criminal cibernético, incluso si sus habilidades técnicas son limitadas. Por ejemplo, Tox –una de las primeras ofertas de RaaS conocidas– descubierto en mayo de 2015, puede descargarse de la web oscura usando un navegador Tor y configurarse después así:

1. Introduce la cantidad del rescate.
2. Crea una nota de rescate.
3. Escribe un *captcha* para que los creadores de Tox sepan que no eres un robot.

El software RaaS puede normalmente descargarse de forma gratuita o por una pequeña tarifa. El verdadero beneficio para los creadores de software RaaS se encuentra en el porcentaje de los pagos del rescate que reciben, normalmente entre el 5–30 %.

El pago de un rescate no soluciona tus problemas de seguridad

Para la mayoría de las víctimas de ransomware, la forma más rápida y sencilla de solucionar el problema es simplemente pagar el rescate. Sin embargo, pagar el rescate –aunque puedas acceder a tus archivos– no solucionará tus problemas.

En la mayoría de los casos, los archivos estarán descifrados si pagas el rescate, pero no tienes ninguna garantía. Aunque al criminal cibernético le interesa restaurar tus archivos si pagas el rescate (si se empieza a extender la información de que el creador de una campaña de ransomware no descifra los archivos después de haber recibido el rescate, las futuras víctimas no tendrán ningún motivo para pagarlo), no existe el honor entre los ladrones. Esto es especialmente cierto con la aparición de RaaS porque un criminal cibernético «novato» puede no ver la situación en conjunto. También, si la clave de cifrado no funciona por algún motivo, no puedes llamar al servicio de atención al cliente.

Tampoco hay garantías de que el delincuente no haya instalado otro malware o exploit kit para facilitar nuevos ataques cibernéticos contra tu organización. Además es posible que se haya exfiltrado una copia de tus archivos con otros fines, como vender la información confidencial de tu organización en la web oscura.

El pago de un rescate financia directamente el delito cibernético y lo mantiene. Es exactamente lo mismo que pagar un rescate a un terrorista o a un estado a cambio de rehenes y al margen de la ley. Fomenta y financia actos semejantes en el futuro.

Finalmente, pagar un rescate no niega el hecho de que se haya producido una violación de seguridad grave en la organización. En función de la naturaleza, alcance y circunstancias de la violación, y de las regulaciones de la industria y jurisdicciones legales a las que esté sometida la organización, es posible que tengas que revelar esta violación públicamente y pagar grandes multas y sanciones.



CONSEJO

Para reducir los posibles daños de un ataque de ransomware, las organizaciones deben asegurarse de realizar de manera periódica copias de seguridad de todos los archivos importantes, así como de las imágenes de todos los sistemas críticos.

Construcción de una arquitectura de seguridad por capas basada en estándares abiertos

Los estándares abiertos facilitan la creación de una arquitectura puntera que permite a las tecnologías de seguridad nuevas y existentes integrarse fácilmente en una solución de seguridad.

Implementa soluciones integradas y punteras

La defensa de fondo es desde hace tiempo una práctica recomendada de la industria de seguridad. Desafortunadamente, hasta la fecha, la defensa de fondo ha obligado a las organizaciones a implementar productos de seguridad independientes (o de punto) que no se integran fácilmente con otras soluciones de seguridad en el entorno.

Con la nueva arquitectura, las organizaciones pueden implementar soluciones integradas basadas en carteras de productos que reducen la complejidad en el entorno de seguridad y que mejoran su posición de seguridad en general.

Integra la seguridad en el entorno de red

La seguridad debe ser inherente y generalizada en todo el entorno informático de la organización, que debe incluir la red, el centro de datos, los terminales y dispositivos móviles y la nube.

Reduce la complejidad de tu entorno de seguridad

Las tecnologías de seguridad deben ser fáciles de implementar y usar. La complejidad presenta riesgos a causa de la posibilidad de configuraciones erróneas y errores, y puede ocultar indicadores de compromiso (IoC) y otros puntos de datos importantes en registros engorrosos y con demasiados detalles. No dudes a la hora de hacer uso de los servicios de seguridad de terceros y aprovecha su amplia experiencia. Esto te permitirá complementar tus profundos conocimientos y comprender el entorno y la postura ante las amenazas de tu organización con el fin de crear un plan de seguridad integrado y eliminar una complejidad innecesaria.

Haz uso de la inteligencia de amenazas en la nube y en tiempo real

El ransomware y otras amenazas de seguridad cibernética están evolucionando con rapidez. Los ataques de día cero son la mayor amenaza para la mayoría de las organizaciones. La inteligencia de amenazas en la nube y en tiempo real permite a los equipos de TI implementar las

medidas correctivas más actuales lo más rápido posible cuando aparecen nuevas amenazas, y aprovechar los conocimientos de seguridad que llegan mucho más allá de su organización.

Automatiza las acciones de seguridad para reducir el tiempo de respuesta

Siempre que sea posible, las acciones de seguridad deben automatizarse para que sigan el ritmo de amenazas que pueden extenderse por toda la red de la empresa en cuestión de minutos o segundos.

Estos son algunos ejemplos de acciones de seguridad que pueden automatizarse:

- » Distribución e instalación de archivos de firma de sistemas de prevención de intrusiones (IPS) y antimalware.
- » Recopilación, correlación y análisis centralizados de registros de seguridad y datos de amenazas.
- » Protección contra amenazas que bloquee solicitudes a destinos maliciosos incluso antes de que se establezca una conexión y que detenga las amenazas a través de cualquier puerto antes de que lleguen a la red y a los terminales.
- » Listas de control de acceso (ACL) dinámicas, listas blancas y listas negras de dominios y sitios web, y creación de reglas de firewalls.
- » Aprovisionamiento/desaprovisionamiento de cuentas y gestión de derechos de acceso.

Si ves algo, informa de ello

La Oficina Federal de Investigación (FBI) de los Estados Unidos insta a las víctimas de ransomware a que informen sobre los detalles de la infección, lo que dará al FBI una visión más generalizada de la extensión e impacto del ransomware. El FBI dice que ha sido difícil «determinar el verdadero número de víctimas de ransomware, ya que muchas infecciones no se denuncian».

Al FBI le preocupa que las víctimas no denuncien las infecciones por diversas razones, siendo la principal que no vean motivo para hacerlo, sobre todo si solucionan el problema internamente, bien sea pagando el rescate o eliminando la infección de malware.



RECUERDA

El FBI no defiende el pago del rescate. Según el FBI, «el pago del rescate no garantiza que la víctima recobre el acceso a sus datos. De hecho, algunas personas u organizaciones nunca reciben claves de descifrado después de pagar el rescate. Pagar el rescate envalentona al adversario para atacar a otras víctimas y obtener beneficios, y puede ser un incentivo para que otros delincuentes participen en actividades ilícitas similares con el fin de obtener beneficios económicos».



CONSEJO

Para informar sobre una infección, acude a www.ic3.gov y proporciona los datos siguientes:

- » Fecha de la infección e información sobre la empresa que ha sido víctima (como tipo de industria y tamaño).
- » Variante de ransomware (identificada en la página del rescate o por la extensión del archivo cifrado).
- » Cómo se produjo la infección (por ejemplo, mediante un enlace en un correo electrónico o navegando por internet).
- » Rescate solicitado y cantidad pagada (si la hay).
- » Dirección del monedero bitcoin del atacante (puede aparecer en la página del rescate).
- » Pérdidas generales asociadas a la infección de ransomware (incluida la cantidad del rescate y la declaración del impacto de la víctima).

NUNCA HA HABIDO UN MOMENTO MEJOR

Nunca ha habido un momento mejor para preocuparse menos e innovar más.

¿Estamos seguros? ¿Estamos innovando? Buena pregunta. En Cisco sabemos que cuanto más sencillas y efectivas sean tus soluciones de seguridad, más sencillo te será traspasar las fronteras de lo que es posible. Aquí puedes ver porqué nunca ha habido un momento mejor para generar tu próxima gran idea: www.cisco.com/neverbetter



©2016 Cisco and/or its affiliates. All rights reserved.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

¡No dejes que el ransomware secuestre tus archivos!

Ransomware es un amenaza de malware de rápida evolución que en 2016 ha ocasionado unas pérdidas de 1 billón de dólares americanos y se prevé que esa cifra siga creciendo. Peor todavía, las víctimas que pagan los rescates exigidos –que van de cientos a miles de dólares– están financiando directamente la próxima generación de ransomware.

Descubre en este libro cómo defender a tu organización del ransomware y de otros ataques.

En el interior...

- Detén el ransomware antes de que llegue a tu red
- Utiliza la protección contra el malware avanzado en puertas de enlace de correo electrónico y terminales
- Bloquea la devolución de llamadas de comando y control (C2) del ransomware
- Simplifica las operaciones de seguridad

Lawrence Miller, CISSP ha trabajado en seguridad de la información en diversas industrias durante más de 25 años. Es coautor de *CISSP For Dummies* y ha escrito más de 90 libros *For Dummies* sobre numerosos temas de tecnología y seguridad.

Visita **Dummies.com**[®]
para ver vídeos, ejemplos paso a paso, artículos con instrucciones, o para comprar.

for
dummies[®]
A Wiley Brand

ISBN: 978-1-119-37845-7
Queda prohibida la
reventa de este libro.

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.