Cisco 2018
Reporte Anual de Ciberseguridad

Tabla de contenido

Resumen ejecutivo

¿Qué pasaría si los defensores pudieran ver el futuro? Si supieran que se aproximaba un ataque, podrían detenerlo, o al menos mitigar su impacto y ayudar a garantizar que lo que necesitan para proteger a la mayoría sea seguro. El hecho es que los defensores pueden ver lo que está en el horizonte.
Muchas pistas están ahí fuera, y son obvias.

Los enemigos y los piratas informáticos ya tienen la experiencia y las herramientas necesarias para derribar las infraestructuras y los sistemas críticos, paralizando así regiones enteras. Pero cuando surgen noticias sobre ciberataques disruptivos y destructivos -como los de Ucrania, por ejemplo, o en cualquier otro lugar del mundo-, algunos profesionales de la seguridad podrían pensar inicialmente: "El entorno de mercado / región / tecnología de nuestra compañía no era un objetivo, entonces, probablemente no estamos en riesgo".

Sin embargo, al restarle valor a lo que parecen ser campañas lejanas o permitir que el caos de las batallas diarias con los atacantes consuma su atención, los defensores fallan al no reconocer la velocidad y la escala a la que los adversarios están reuniendo y mejorando su armamento cibernético.

Durante años, Cisco ha estado advirtiendo a los defensores sobre la creciente actividad de ciberdelincuencia en todo el mundo. En este nuestro más reciente informe anual de ciberseguridad, presentamos datos y análisis de los investigadores de amenazas de Cisco y de varios de nuestros socios tecnológicos sobre el comportamiento observado de los atacantes durante los últimos 12 a 18 meses. Muchos de los temas examinados en este informe están centrados en tres temas generales:

1. **Los adversarios están llevando el malware a niveles de sofisticación e impacto sin precedentes.**

   La evolución del malware (página 6) fue uno de los desarrollos más importantes en el panorama de ataque en 2017. La aparición de los cryptoworms ransomware basados en la red elimina la necesidad del elemento humano en el lanzamiento de campañas de ransomware. Y para algunos adversarios, el premio no es un rescate, sino la eliminación de sistemas y datos, como lo demostró Nyetya -borrado de malware disfrazado de ransomware- (ver página 6). El malware de autopropagación es peligroso y tiene el potencial de acabar con Internet, según los investigadores de amenazas de Cisco.

2. **Los adversarios son cada vez más expertos en la evasión y en usar como armas los servicios de la nube y otras tecnologías utilizadas con fines legítimos.**

   Además de desarrollar amenazas que pueden **evadir los entornos del sandboxing más sofisticados** (página 22), los actores maliciosos están ampliando su **adopción del cifrado para evitar la detección** (página 9). La encriptación está destinada a mejorar la seguridad, pero también proporciona a los actores maliciosos una poderosa herramienta para ocultar la actividad de comando y control (C2), lo que les brinda más tiempo para operar e infligir daños.

   Los ciberdelincuentes también están adoptando **canales C2 que dependen de servicios legítimos de Internet** como Google, Dropbox y GitHub (ver página 24). La práctica hace que el tráfico de malware sea casi imposible de identificar.

   Además, muchos de los atacantes ahora están **lanzando múltiples campañas desde un solo dominio** (página 26) para obtener el mejor retorno de sus inversiones. También están reutilizando los recursos de la infraestructura, como las direcciones de correo electrónico de los subscriptores, los números de sistema autónomo (ASN) y los servidores de nombres.

3. **Los adversarios están explotando grietas en la seguridad, muchas de las cuales surgen de la expansión del Internet de las Cosas (IoT) y del uso de los servicios de la nube.**

   Los defensores están desplegando dispositivos de IoT a un paso rápido, pero a menudo prestan poca atención a la seguridad de estos sistemas. **Los dispositivos IoT sin parche y no monitoreados** brindan a los atacantes

la oportunidad de infiltrarse en las redes (página 34). Una investigación sugiere que las organizaciones con dispositivos IoT susceptibles a ataques también parecen **desmotivadas para acelerar las correcciones** (página 42). Peor aún, estas organizaciones probablemente tengan muchos más dispositivos IoT vulnerables en sus entornos de TI que ni siquiera conocen.

Mientras tanto, **las botnets del IoT se están expandiendo** junto con el IoT y se están volviendo más maduras y automáticas. A medida que crecen, los atacantes las usan para lanzar avanzados ataques distribuidos de la negación del servicio (DDoS) (página 31).

Los atacantes también se están aprovechando del hecho de que los equipos de seguridad están **experimentando dificultades para defender los entornos del IoT y de la nube.** (Ver página 42) Una razón de esto es la falta de claridad sobre quién es exactamente el responsable de proteger esos entornos.

Recomendaciones para los defensores

Cuando los adversarios golpean inevitablemente a sus organizaciones, ¿estarán los defensores preparados y qué tan rápido estos podrán recuperarse? Las conclusiones del **Estudio Comparativo de Capacidades de Seguridad de Cisco 2018**–el cual ofrece información sobre las prácticas de seguridad de más de 3600 encuestados a lo largo de 26 países- muestran que los defensores tienen muchos desafíos que ganar. (ver página 46).

Aun así, los defensores encontrarán que realizar mejoras de seguridad estratégicas y adherirse a las mejores prácticas más comunes puede reducir la exposición a riesgos emergentes, ralentizar el progreso de los atacantes y proporcionar más visibilidad dentro del panorama de las amenazas.

Ellos deben considerar:

- Implementar herramientas en la primera línea de defensa que puedan escalar, como las plataformas de seguridad de la nube.
- Confirmar que se adhieren a las políticas y a las prácticas corporativas para el parcheo de aplicaciones, sistemas y dispositivos.
- Emplear la segmentación de la red para ayudar a reducir las exposiciones a los brotes.
- Adoptar herramientas de monitoreo de procesos Endpoint de próxima generación.
- Acceder a datos y procesos de inteligencia de amenazas de una manera más precisa y oportuna, que permitan que esos datos sean incorporados a la supervisión y al evento de seguridad.
- Realizar análisis más profundos y más avanzados.
- Revisar y practicar los procedimientos de respuesta de seguridad.
- Realizar a menudo una copia de seguridad de datos y realizar pruebas de procedimientos de restauración- procesos que son críticos en un mundo de gusanos ransomware de movimiento rápido, basados en la red y de armas cibernéticas destructivas.
- Revisión de pruebas de eficacia de terceros respecto de tecnologías de seguridad para ayudar a reducir el riesgo de ataques a la cadena de suministro.
- Llevar a cabo un análisis de seguridad del microservicio, del servicio en la nube y de los sistemas de administración de aplicaciones.
- Revisar los sistemas de seguridad y explorar el uso del análisis del SSL- y, en caso de ser posible, el descifrado SSL- tan pronto como sea posible.

Los defensores también deberían considerar la adopción de tecnologías de seguridad avanzadas que incluyen el aprendizaje automático y las capacidades de la inteligencia artificial. Con un malware ocultando su comunicación dentro del tráfico web encriptado, y personas malintencionadas enviando datos confidenciales a través de sistemas corporativos en la nube, los equipos de seguridad necesitan herramientas más efectivas para prevenir o detectar el uso del cifrado para ocultar actividades maliciosas.

Sobre el Reporte

El ***Reporte Anual de Ciberseguridad de Cisco 2018*** presenta nuestros últimos avances en la industria de seguridad diseñados para ayudar a las organizaciones y a los usuarios a defenderse contra los ataques. También observamos las técnicas y estrategias que utilizan los adversarios para romper esas defensas y evadir la detección.

El informe también destaca las principales conclusiones del **Estudio Comparativo de Capacidades de Seguridad de Cisco 2018**, que examina la postura de seguridad de las empresas y sus percepciones acerca de su preparación para defenderse de los ataques.

Parte I:
El panorama de los ataques

Parte I: El panorama de los ataques

Los adversarios están llevando el malware a niveles de sofisticación e impacto sin precedentes. El número y la variedad es cada vez mayor de tipos de malware y familias que perpetúan el caos en el panorama de ataque al socavar los esfuerzos de los defensores para ganar y mantener el terreno ante las amenazas.

LA EVOLUCIÓN DEL MALWARE

Uno de los desarrollos más importantes en el panorama de ataque en 2017 fue la evolución del ransomware. El lle-gada de los ransomware worms basados en la red elimina la necesidad del elemento humano en el lanzamiento de campañas de ransomware. Y para algunos adversarios, el premio no es un rescate, sino la destrucción de sistemas y datos. Esperamos ver más de esta actividad en el año que viene.

Están por ahí: los defensores deben prepararse para enfrentarse a nuevas amenazas basadas en la red que se propagarán por sí mismas en 2018.

En 2017, los adversarios llevaron el ransomware a un nuevo nivel, aunque era de esperarse. Después de la campaña SamSam de marzo de 2016[1], el primer ataque a gran escala que utilizó el vector de red para propagar el ransomware, eliminando así al usuario del proceso de infección: los investigadores de amenazas de Cisco sabían que solo sería una cuestión de tiempo antes de que los actores de la amenaza encontraran la forma de automatizar esta técnica. Los atacantes harán que su malware sea aún más potente al combinarlo con la funcionalidad de "worm" para causar daños generalizados.

Esta evolución del malware no se hizo esperar. En mayo de 2017, apareció WannaCry, un cryptoworm ransomware, que se extendió como un reguero de pólvora a través de Internet.[2] Para propagarse, aprovechó una vulnerabilidad de seguridad de Microsoft Windows llamada EternalBlue, que fue filtrada por el grupo de hackers Shadow Brokers a mediados de abril de 2017.

WannaCry había ganado más de US $143,000 a través de pagos con bitcoins en el momento en que las carteras se cobraron. Dada la línea de tiempo, y calculando la acumulación del valor en el bitcoin originalmente pagado en las carteras a $93,531, los investigadores de amenazas de Cisco estiman que se hicieron aproximadamente 312 pagos de rescate. A modo de comparación, el kit de exploit Angler, cuando estaba activo, ganaba unos 100 millones de dólares anuales como empresa global.

WannaCry no rastreó el daño cifrado y los pagos realizados por los usuarios afectados. También se desconoce la cantidad de usuarios que recibieron claves de descifrado después de realizar un pago. (WannaCry todavía se está propagando, y los usuarios continúan pagando rescates, en vano). Debido al bajo rendimiento de WannaCry como ransomware, el gobierno de EE. UU. y muchos investigadores de seguridad creen que el componente del rescate es efectivamente una cortina de humo para ocultar el verdadero propósito de WannaCry: borrar datos.

Nyetya (también conocido como NotPetya) llegó en junio de 2017.[3] Este malware también se hizo pasar por ransomware y también utilizó la vulnerabilidad de ejecución remota de código denominada "EternalBlue", así como la vulnerabilidad de ejecución remota de código "EternalRomance" (también

1 *SamSam: The Doctor Will See You, After He Pays the Ransom, blog de Cisco Talos, marzo de 2016:* blog.talosintelligence.com/2016/03/samsam-ransomware.html.

2 *2 Player 3 Has Entered the Game: Say Hello to 'WannaCry", blog de Cisco Talos, mayo de 2017:* blog.talosintelligence.com/2017/05/wannacry.html.

3 *New Ransomware Variant 'Nyetya' Compromises Systems Worldwide, blog de Cisco Talos, junio de 2017:* blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.

filtrada por Shadow Brokers) y otros vectores que implicaban la extracción de credenciales no relacionadas con el lanzamiento de Shadow Brokers.[4] Nyetya se implementó a través de sistemas de actualización de software para un paquete de software de impuestos utilizado por más del 80 por ciento de las empresas en Ucrania e instalado en más de 1 millón de computadoras.[5] La policía cibernética de Ucrania confirmó que afectó a más de 2000 empresas ucranianas.[6]

Antes de la aparición del ransomware de propagación automática, el malware se distribuía de tres formas: descarga en disco, correo electrónico o medios físicos como dispositivos de memoria USB maliciosos. Todos los métodos requerían algún tipo de interacción humana para infectar un dispositivo o sistema con ransomware. Con estos nuevos vectores empleados por los atacantes, una estación de trabajo activa y sin parches de seguridad es todo lo que se necesita para lanzar una campaña de ransomware basada en la red.

Los profesionales de la seguridad pueden considerar a los worms como un tipo de amenaza "antigua" porque la cantidad de vulnerabilidades y exposiciones comunes (CVE) se ha reducido a medida que las líneas de base de seguridad del producto han mejorado. Sin embargo, el malware de auto propagación no solo es una amenaza relevante, sino que también tiene el potencial de derribar Internet, de acuerdo con los investigadores de amenazas de Cisco. WannaCry y Nyetya son solo una muestra de lo que está por venir, por lo que los defensores deberían prepararse.

WannaCry y Nyetya podrían haber sido prevenidos, o su impacto reducido, si más organizaciones hubieran aplicado las mejores prácticas básicas de seguridad, como el parcheo de vulnerabilidades, el establecimiento de procesos y políticas apropiadas para la respuesta a incidentes y la segmentación de la red.

Para obtener más consejos sobre cómo enfrentar la amenaza de los ransomware worms automáticos basados en red, lea *Back to Basics: Worm Defense in the Ransomware Age* en el blog de Cisco.

Punto débil de la seguridad: la cadena de suministro

La campaña de Nyetya también fue un ataque de la cadena de suministro, uno de los muchos problemas que los investigadores de amenazas de Cisco observaron en 2017. Una razón por la cual Nyetya logró infectar tantas máquinas tan rápidamente es porque los usuarios no vieron una actualización de software automatizada como un riesgo de seguridad o, en algunos casos, incluso se dieron cuenta de que estaban recibiendo las actualizaciones maliciosas.

Otro ataque a la cadena de suministro, ocurrido en septiembre de 2017, involucró los servidores de descarga utilizados por un proveedor de software para distribuir un paquete de software legítimo conocido como CCleaner.[7] Los binarios de CCleaner, que contenían una puerta trasera troyana, se firmaron utilizando un certificado válido, dando a los usuarios un resultado falso de confianza de que el software que estaban usando era seguro. Los actores detrás de esta campaña estaban apuntando a las principales compañías de tecnología donde el software estaba en uso, ya sea legítimamente o como parte de una TI clandestina.

Los ataques de la cadena de suministro parecen estar aumentando en velocidad y complejidad. Pueden afectar las computadoras en una escala masiva y pueden persistir durante meses o incluso años. Los defensores deben ser conscientes del riesgo potencial de usar software o hardware de organizaciones que no tienen una postura de seguridad responsable. Busque proveedores que emitan CVE, aborden rápidamente las vulnerabilidades y se esfuercen constantemente para garantizar que sus sistemas de compilación no se vean comprometidos. Además, los usuarios deben tomarse un tiempo para analizar el nuevo software antes de descargarlo para verificar que no contenga malware.

La segmentación de la red de software que no está respaldada por una práctica de seguridad integral puede ayudar a contener el daño de los ataques de la cadena de suministro, evitando que se propaguen por toda la organización.

4 Ibid.

5 *Ukraine scrambles to contain new cyber threat after 'NotPetya' attack, por Jack Stubbs y Matthias Williams, Reuters, julio de 2017:* reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.

6 *The MeDoc Connection, blog de Cisco Talos, julio de 2017:* blog.talosintelligence.com/2017/07/the-medoc-connection.html.

7 *CCleaner Command and Control Causes Concern, blog de Cisco Talos, septiembre de 2017:* blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html.

Por qué importa la integridad en los Reportes de inteligencia de amenazas

Todas las organizaciones que comparten información sobre amenazas a los clientes o al público a través de cualquier canal deben emplear pautas que les ayuden a garantizar la precisión en sus reportes. Incluso si todos los hechos no están claros, las organizaciones aún pueden comunicar lo que saben y evitar las suposiciones. Tener la razón es mejor que ser el primero.

Por ejemplo, cuando se desarrolló el ataque WannaCry en mayo de 2017, hubo confusión inicial dentro de la comunidad de seguridad acerca de cómo elransomware worm se estaba infiltrando en los sistemas. Múltiples organizaciones, tanto del sector público como privado, informaron que el ataque se debió a una campaña de phishing y archivos adjuntos de correo electrónico maliciosos. Pero la amenaza basada en la red consistía, de hecho, en buscar e infectar los puertos del servidor de bloques de mensajes de Microsoft Windows Server (SMB) vulnerables y públicos.

Los investigadores de amenazas de Cisco alertaron rápidamente a la comunidad de seguridad de que los correos electrónicos que pensaban que estaban conectados a la campaña WannaCry eran probablemente correos basura del bot de Necurs que propagaban el ransomware “Jaff”. Pasaron varios días antes de que la comunidad de seguridad aceptara que los correos electrónicos sospechosos contenían Jaff, no WannaCry. Y durante ese tiempo, los usuarios estaban actuando con información que no podía ayudarlos a evitar la campaña de rápido crecimiento de WannaCry.

El caos que siguió a la llegada de la campaña WannaCry sirve como un recordatorio de que la comunidad de seguridad debe evitar comunicar hechos inexactos sobre el origen y la naturaleza de los ciberataques. En las primeras horas de una campaña, el sentido de urgencia para detener rápidamente a los adversarios y proteger a los usuarios puede resultar fácilmente en la publicación, sobre todo en las redes sociales, de información que puede crear confusión y evitar que los usuarios defiendan sus sistemas.

Para obtener más información sobre este tema, lea la publicación On Conveying Doubt en el blog de Cisco Talos.

TRÁFICO WEB MALICIOSO CIFRADO

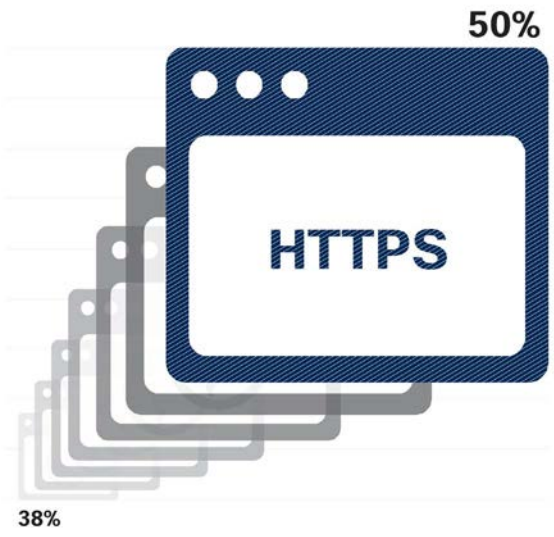
El creciente volumen de tráfico web encriptado, tanto legítimo como malicioso, crea aún más desafíos y confusión para los defensores que intentan identificar y monitorear amenazas potenciales. La encriptación está destinada a mejorar la seguridad, pero también proporciona a los actores malintencionados una poderosa herramienta para ocultar la actividad de comando y control (C2), lo que les brinda más tiempo para operar e infligir daños. Los investigadores de amenazas de Cisco esperan ver que los adversarios aumenten su uso del cifrado en 2018. Para mantener el ritmo, los defensores necesitarán incorporar más automatización y herramientas avanzadas como aprendizaje de máquina e inteligencia artificial para complementar la prevención, detección y reparación de amenazas.

Un punto oscuro para los defensores: tráfico web malicioso encriptado

Los investigadores de amenazas de Cisco informan que el 50 por ciento del tráfico web global se cifró a partir de octubre de 2017. Eso es un aumento de 12 puntos en el volumen a partir de noviembre de 2016 (ver figura 1). Un factor que impulsa ese aumento es la disponibilidad de certificados SSL de bajo costo o gratuitos. Otra es la práctica acelerada de Google Chrome de marcar sitios web no cifrados que manejan información confidencial, como la información de tarjetas de crédito de los clientes, como "no segura". Las empresas están motivadas para cumplir con el requisito de cifrado HTTPS de Google a menos que quieran arriesgarse a una caída potencialmente significativa en su clasificación de la página de búsqueda de Google.

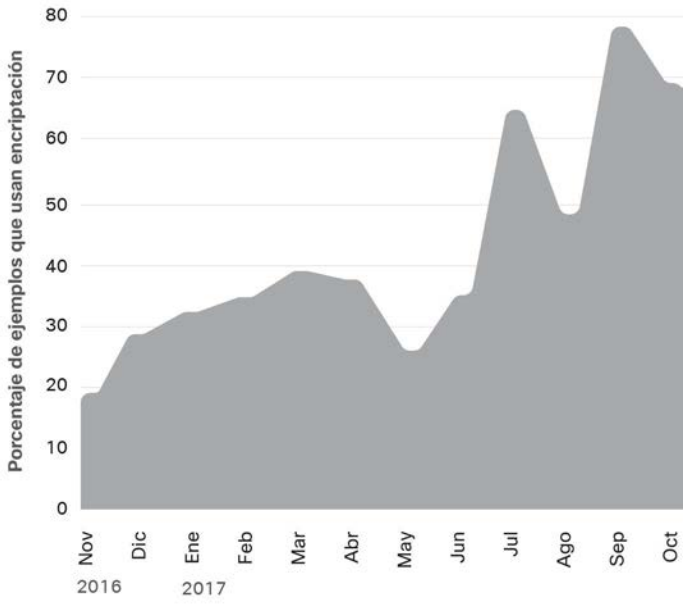
A medida que crece el volumen del tráfico web global cifrado, los adversarios parecen estar ampliando su adopción del cifrado como una herramienta para ocultar su actividad C2. Los investigadores de amenazas de Cisco observaron un aumento de más del triple en la comunicación de red cifrada utilizada por las muestras de malware inspeccionadas durante

Figura 1 Aumento en el volumen de tráfico web global encriptado



Fuente: Cisco Security Research

Figura 2 Aumento en el volumen de binarios maliciosos aprovechando algunas comunicaciones de red encriptadas



Fuente: Cisco Security Research

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

un período de 12 meses (consulte la figura 2). Nuestro análisis de más de 400,000 binarios maliciosos descubrió que alrededor del 70 por ciento había usado al menos algo de encriptación a partir de octubre de 2017.

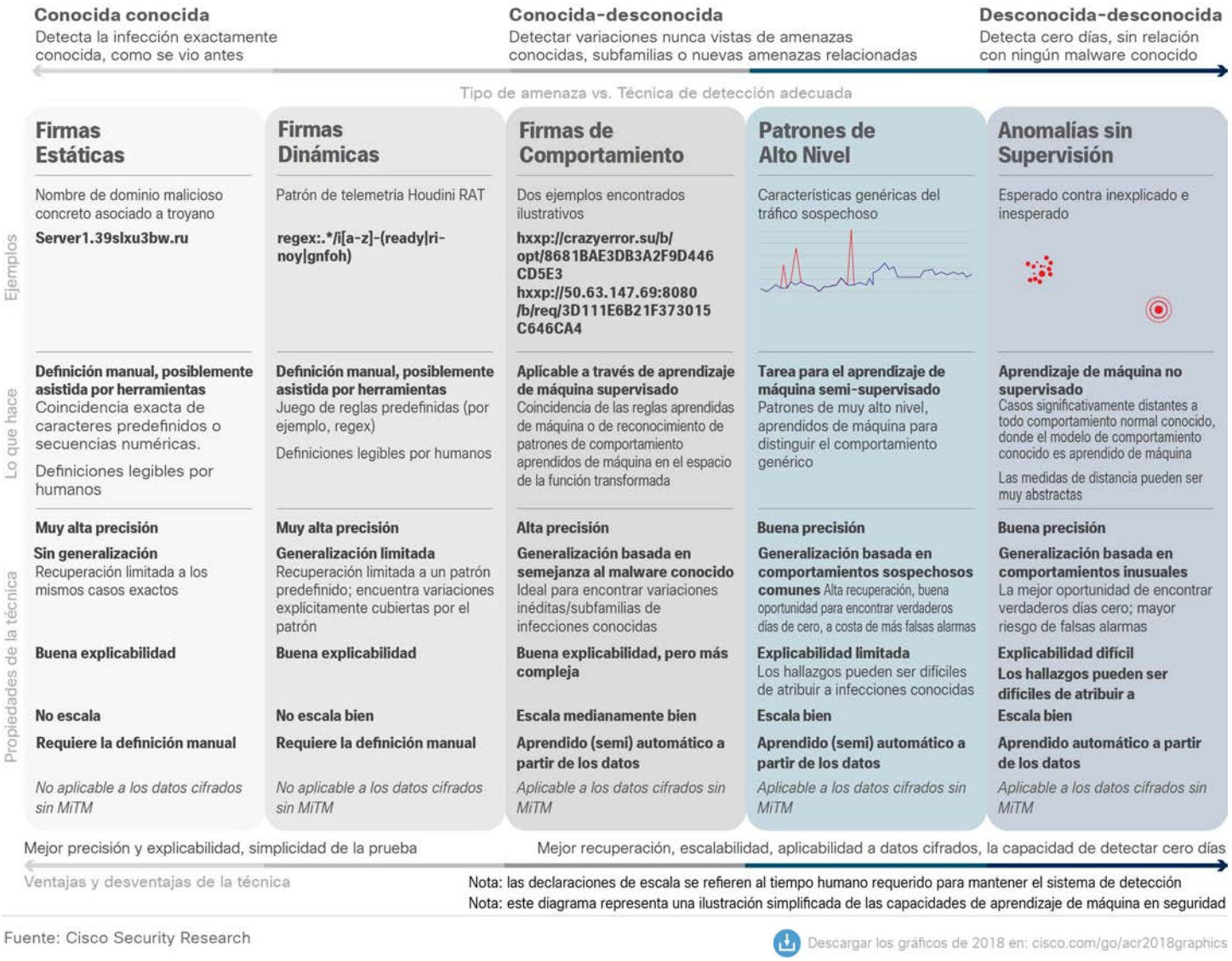
Aplicación de machine learning para el espectro de la amenaza

Para superar la falta de visibilidad que crea el cifrado y reducir el tiempo de los adversarios para operar, vemos que más empresas exploran el uso de machine learning y .artificial Intelligence. Estas capacidades avanzadas pueden mejorar las defensas de seguridad de red y, con el tiempo, "aprender" a detectar automáticamente patrones inusuales de tráfico web que indique actividad maliciosa.

Machine learning es útil para detectar automáticamente las amenazas conocidas-conocidas, los tipos de infecciones que se han visto antes (consulte la figura 3). Pero su valor real, especialmente en la supervisión del tráfico web encriptado, radica en su capacidad para detectar amenazas "conocidas-desconocidas" (variaciones nunca vistas de amenazas conocidas, subfamilias de malware o nuevas amenazas relacionadas) y amenazas "desconocidas-desconocidas" (nuevo malware de red). La tecnología puede aprender a identificar patrones inusuales en grandes volúmenes de tráfico web encriptado y alertar automáticamente a los equipos de seguridad sobre la necesidad de una mayor investigación.

Este último punto es especialmente importante, dado que la falta de personal capacitado es un obstáculo para mejorar las defensas de seguridad en muchas organizaciones, como se ve en los hallazgos del Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 (ver página 35). La automatización y las herramientas inteligentes, como el machine learning y artificial Intelligence y, pueden ayudar a los defensores a superar las habilidades y las brechas de recursos, haciéndolos más efectivos para identificar y responder a amenazas conocidas y emergentes.

Figura 3 Aprendizaje de máquina en seguridad de red: taxonomía



Fuente: Cisco Security Research

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

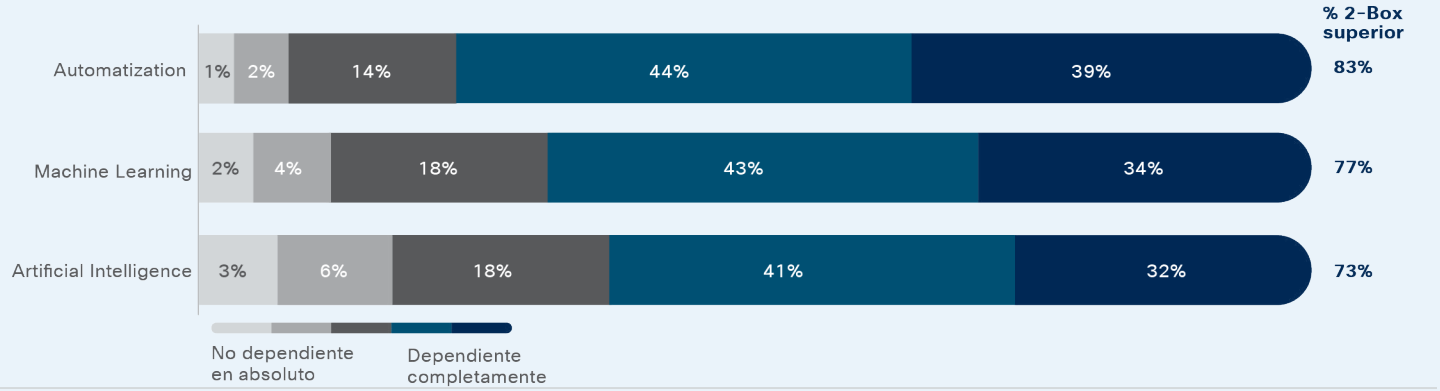
Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018: Los defensores informan una mayor dependencia de la automatización y la inteligencia artificial

Los jefes de seguridad de información (CISO) entrevistados para el Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 informan que están ansiosos por agregar herramientas que usan inteligencia artificial y aprendizaje de máquina, y creen que su infraestructura de seguridad está creciendo en sofisticación e inteligencia. Sin embargo, también se sienten frustrados por la cantidad de falsos positivos que generan dichos sistemas, ya que los falsos positivos aumentan la carga de trabajo del equipo de seguridad. Estas preocupaciones deberían desaparecer con el tiempo a medida que las tecnologías de aprendizaje de máquina e inteligencia artificial maduran y aprenden qué es una actividad "normal" en los entornos de red que están monitoreando.

Cuando se les preguntó de qué tecnologías automatizadas dependen más sus organizaciones, el 39 por ciento de los profesionales de seguridad dijeron que dependen por completo de la automatización, mientras que el 34 por ciento dependen completamente del aprendizaje de máquina; el 32 por ciento dijo que dependen por completo de la inteligencia artificial (figura 4).

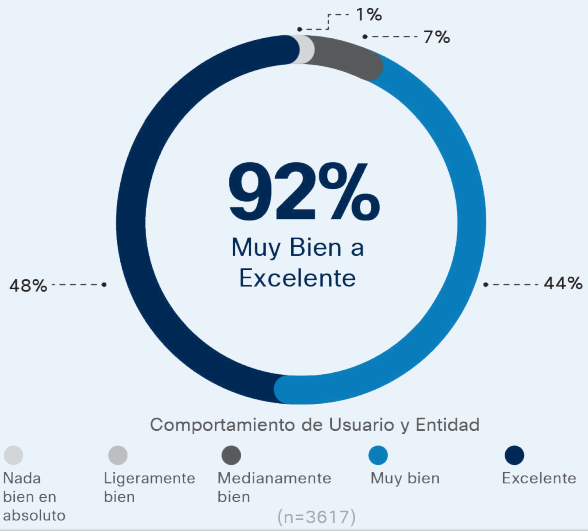
Las herramientas de análisis de comportamiento también se consideran útiles al ubicar actores maliciosos en redes; el 92 por ciento de los profesionales de seguridad dijeron que estas herramientas funcionan muy bien (figura 5).

Figura 4 Las organizaciones dependen en gran medida de la automatización, el aprendizaje de máquina y la inteligencia artificial



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Figura 5 La mayoría de los profesionales de seguridad ven valor en las herramientas de análisis del comportamiento



Excelente
69%

2/3 de las organizaciones de atención médica creen que el análisis del comportamiento / análisis forense ayudan a identificar a los agentes malintencionados

(n=358)

Excelente
38-39%

Menos organizaciones en transporte y gobierno están de acuerdo en que los análisis de comportamiento / análisis forense funcionan de manera excelente

(Transporte: n = 175; Gobierno: n = 639)

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

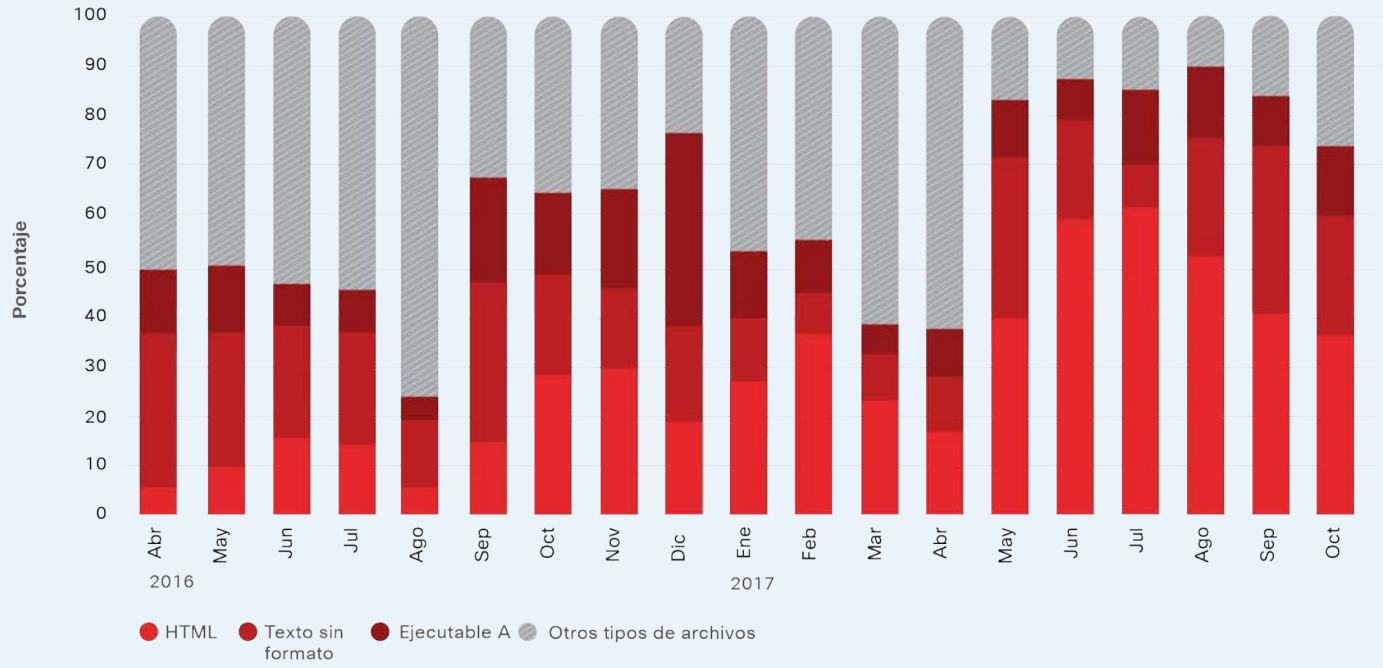
Los métodos de ataque web muestran el intenso enfoque de los adversarios en el compromiso del navegador

Un análisis de los métodos de ataque web durante un período de 18 meses desde abril de 2016 hasta octubre de 2017 muestra un aumento en el uso de contenido web malicioso por parte de los adversarios (figura 6). Esa tendencia se alinea con la orientación agresiva del navegador web Microsoft Internet Explorer por kits de exploits aún activos.

Los investigadores de amenazas de Cisco observaron que el número de detecciones de contenido web de JavaScript malicioso fue significativo y constante durante este período.

Esto subraya la efectividad de esta estrategia para infectar navegadores vulnerables para facilitar otras actividades nefastas como la redirección del navegador o las descargas de troyanos.

Figura 6 Actividad de bloqueo basada en malware según el tipo de contenido, abril de 2016 a octubre de 2017

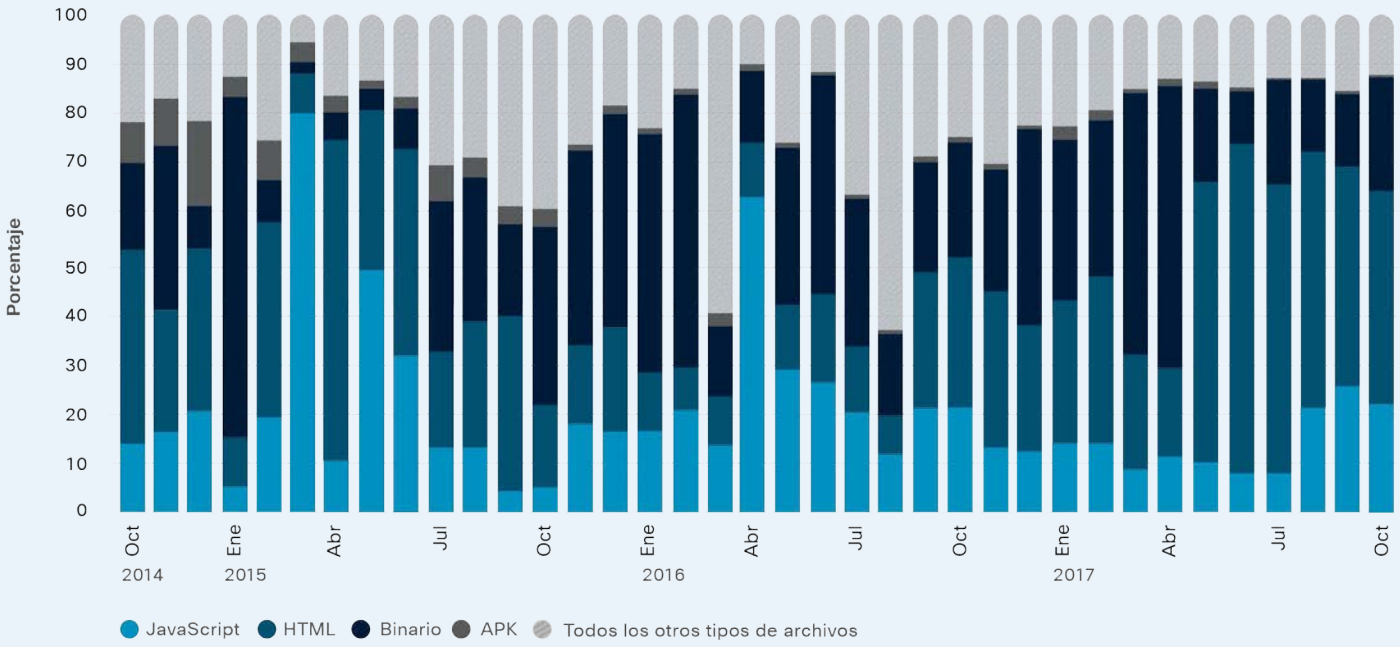


Fuente: Cisco Security Research

La figura 7 es una descripción general de los métodos de ataque web durante el período de tres años, de octubre de 2014 a octubre de 2017. Los adversarios emplearon consistentemente binarios sospechosos durante este período, principalmente para entregar adware y spyware. Como se discutió en el Reporte de seguridad cibernética semestral de Cisco 2017, estos tipos de aplicaciones potencialmente no deseadas (PUA) pueden presentar riesgos de seguridad, como el aumento de infecciones de malware y el robo de información de usuarios o empresas.[8]

La vista de tres años en la figura 7 también muestra que el volumen de contenido web malicioso fluctúa con el tiempo a medida que los atacantes lanzan y finalizan campañas y cambian sus tácticas para evitar la detección.

Figura 7 Actividad de bloqueo basada en malware según el tipo de contenido, octubre de 2014 – octubre de 2017



Fuente: Cisco Security Research

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

8 *Reporte Semestral de Ciberseguridad Cisco 2017:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

AMENAZAS DE CORREO ELECTRÓNICO

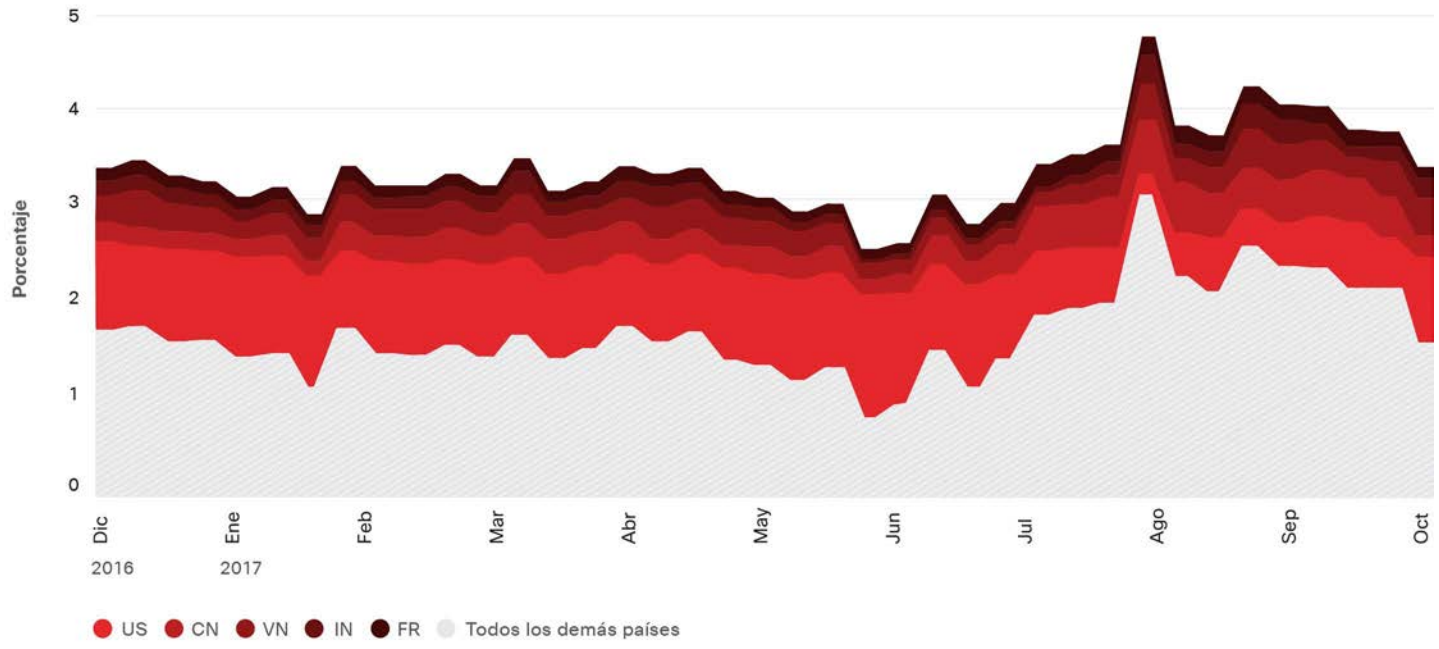
No importa cuánto cambie el panorama de las amenazas, el correo electrónico malicioso y el correo no deseado siguen siendo herramientas vitales para que los adversarios distribuyan malware porque llevan las amenazas directamente al punto final. Al aplicar la combinación correcta de técnicas de ingeniería social, como phishing y enlaces maliciosos y archivos adjuntos, los adversarios solo tienen que sentarse y esperar a que los usuarios desprevenidos activen sus exploits.

Las fluctuaciones en la actividad de botnet de spam afectan el volumen general

A finales de 2016, los investigadores de amenazas de Cisco observaron un aumento notable en la actividad de la campaña de spam que parecía coincidir con una disminución en la actividad del kit de exploits. Cuando los principales kits de exploits como Angler desaparecieron abruptamente del mercado, muchos usuarios de esos kits regresaron al vector de correo electrónico para mantener la rentabilidad.[9]

Sin embargo, después de esa prisa inicial por volver al correo electrónico, el volumen global de spam disminuyó y se niveló durante la mayor parte de la primera mitad de 2017. Luego, a fines de mayo y principios de junio de 2017, el volumen global de spam disminuyó antes de aumentar considerablemente a mediados o fines del verano (ver figura 8).

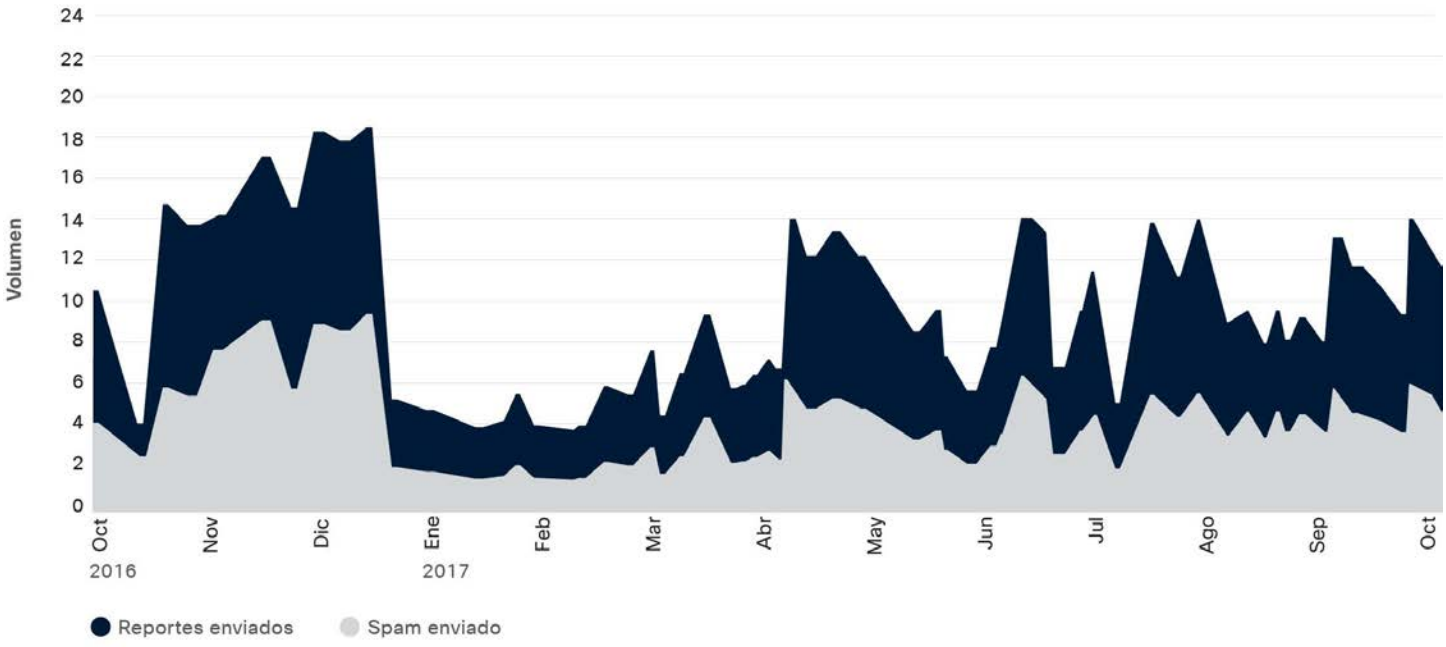
Figura 8 Bloqueo de reputación de IP por país, diciembre de 2016 a octubre de 2017



Fuente: Cisco Security Research

9 Consulte " Disminución en la actividad del kit de explotación que probablemente influya en las tendencias globales de spam " pág. 18, Reporte Semestral de Ciberseguridad de Cisco 2017: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Figura 9 Actividad de botnet de spam, octubre de 2016 – octubre de 2017



Fuente: Cisco SpamCop

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

El reducido volumen de spam de enero a abril de 2017 coincide con una pausa en la actividad de la botnet de spam, como lo muestra un gráfico interno generado por el servicio Cisco® SpamCop (figura 9).

Los investigadores de amenazas de Cisco informan que la botnet Necurs, uno de los principales contribuyentes al volumen general de spam a nivel mundial, estuvo activa, pero distribuyendo menos spam durante el período de enero a abril. En mayo, la botnet estaba difundiendo Jaff ransomware a través de campañas masivas de spam. Las campañas presentaban un archivo PDF con un documento incrustado de Microsoft Office y el descargador inicial del Jaff ransomware.[10] Los investigadores de seguridad descubrieron una vulnerabilidad en Jaff que les permitió crear un descifrador que obligó a los operadores de Necurs a hacer un rápido retorno a la distribución de su amenaza habitual, Locky ransomware.[11] El momento en que los actores detrás de Necurs tuvieron que volver a Locky coincide con la caída significativa en el volumen de spam global observada durante las dos primeras semanas de junio (figura 9).

10 *Jaff Ransomware: Player 2 Has Entered the Game,* by Nick Biasini, Edmund Brumaghin, and Warren Mercer, with contributions from Colin Grady, Cisco Talos blog, May 2017: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

11 *Player 1 Limps Back Into the Ring—Hello Again, Locky!* by Alex Chiu, Warren Mercer, and Jaeson Schultz, with contributions from Sean Baird and Matthew Molyett, Cisco Talos blog, June 2017: blog.talosintelligence.com/2017/06/necurs-locky-campaign.html.

Extensiones de archivo maliciosas en el correo electrónico: las 10 herramientas principales de las familias de malware común

Los investigadores de amenazas de Cisco analizaron la telemetría de correo electrónico de enero a septiembre de 2017 para identificar los tipos de extensiones de archivos maliciosos en los documentos de correo electrónico que las familias de malware comunes emplean con más frecuencia. El análisis produjo una lista de los 10 principales que muestra que el grupo más frecuente de extensiones de archivos maliciosos (38 por ciento) eran los formatos de Microsoft Office como Word, PowerPoint y Excel (consulte la figura 10).

Los archivos de almacenamiento, como .zip y .jar, representaron aproximadamente el 37 por ciento de todas las extensiones de archivos maliciosos observadas en nuestro estudio. El hecho de que los adversarios empleen en gran medida los archivos no es sorprendente, ya que durante mucho tiempo han sido los lugares preferidos para ocultar el malware. Los usuarios deben abrir archivos para ver el contenido, un paso importante en la cadena de infección para muchas amenazas. Los archivos maliciosos también suelen tener éxito al frustrar las herramientas de análisis automatizadas, especialmente cuando contienen amenazas que requieren la interacción del usuario para la activación. Los adversarios también usarán tipos de archivos oscuros, como .7z y .rar, para evadir la detección.

Las extensiones de archivo PDF maliciosas completaron los tres primeros en nuestro análisis, representando casi el 14 por ciento de las extensiones de archivos maliciosos observadas. (Nota: la categoría de "Otras extensiones" se aplica a las extensiones observadas en nuestro estudio que no se pudieron asignar fácilmente a tipos de archivos conocidos. Algunos tipos de malware son conocidos por usar extensiones de archivo aleatorias).

Figura 10 Principales 10 extensiones de archivos maliciosos, enero a septiembre de 2017

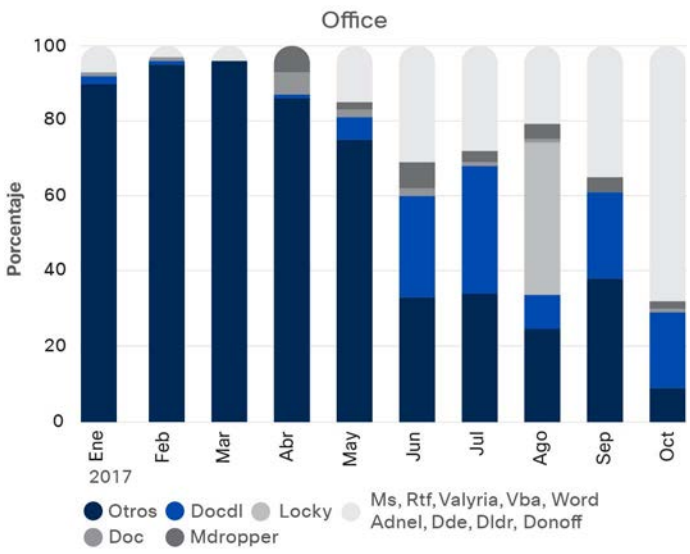
Fuente: Cisco Security Research

Las figuras 11 a-c proporcionan una descripción general de las familias de malware incluidas en nuestra investigación que se asociaron con los tres tipos principales de extensiones de archivos maliciosos: Archivos de MS Office, archivos y documentos PDF. La figura 12 muestra el porcentaje de detecciones, por familia, que incluía una extensión de archivo de carga útil maliciosa.

Los picos de actividad se alinean con las campañas de spam observadas durante esos meses, de acuerdo con los investigadores de amenazas de Cisco.

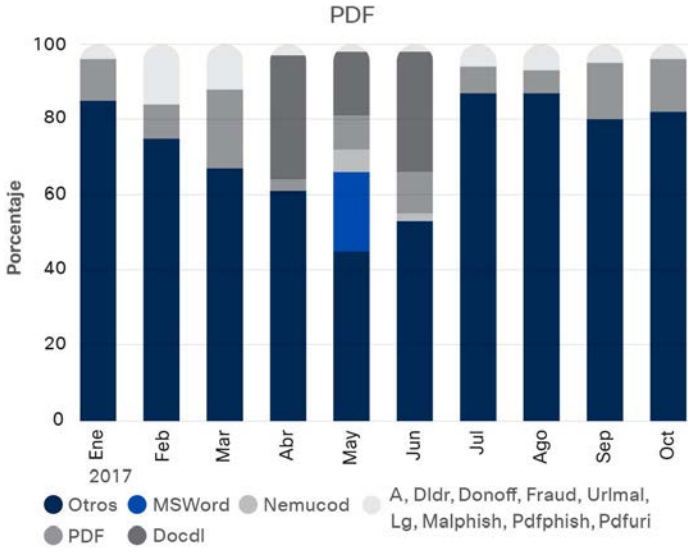
Por ejemplo, a fines del verano, se estaban llevando a cabo importantes campañas de distribución de Nemucod y Locky, dos amenazas que a menudo trabajan juntas. Se sabe que Nemucod envía cargas útiles maliciosas en archivos de almacenamiento como .zip que contienen secuencias de comandos maliciosas, pero se parecen a los archivos .doc normales. ("Dwnldr", también visto en la figura 12, es una variante probable de Nemucod).

Figura 11a Tres tipos principales de extensiones de archivos maliciosos y relaciones familiares de malware



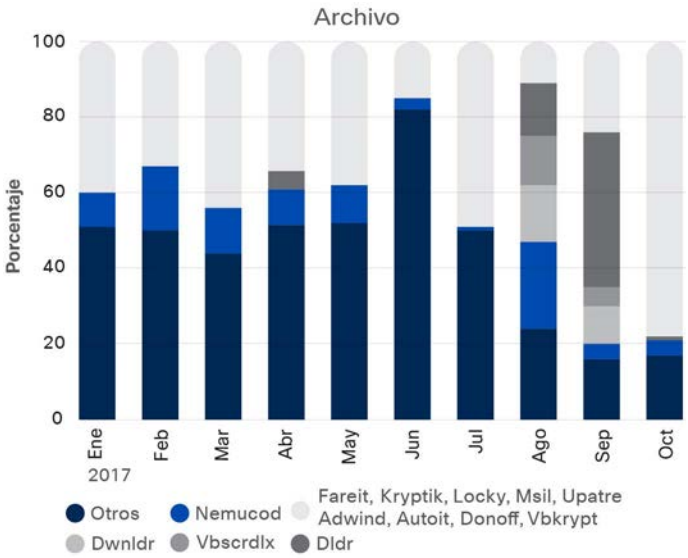
Fuente: Cisco Security Research

Figura 11b Tres tipos principales de extensiones de archivos maliciosos y relaciones de familias de malware



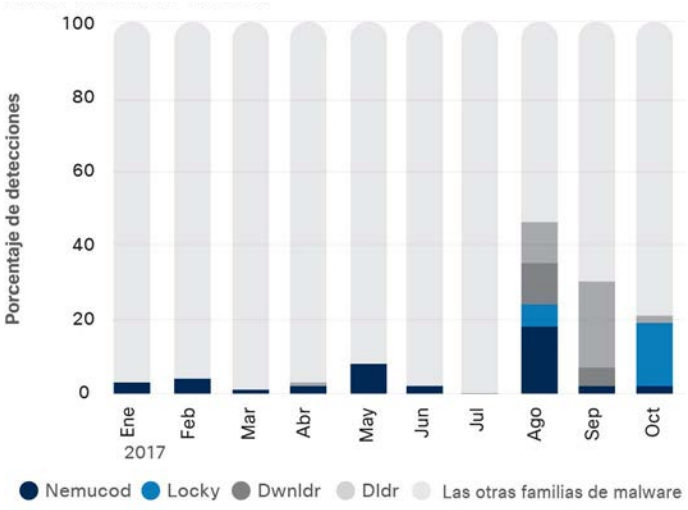
Fuente: Cisco Security Research

Figura 11c Tres tipos principales de extensiones de archivos maliciosos y relaciones de familias de malware



Fuente: Cisco Security Research

Figura 12 Patrones de las principales familias de malware, enero a octubre de 2017



Fuente: Cisco Security Research

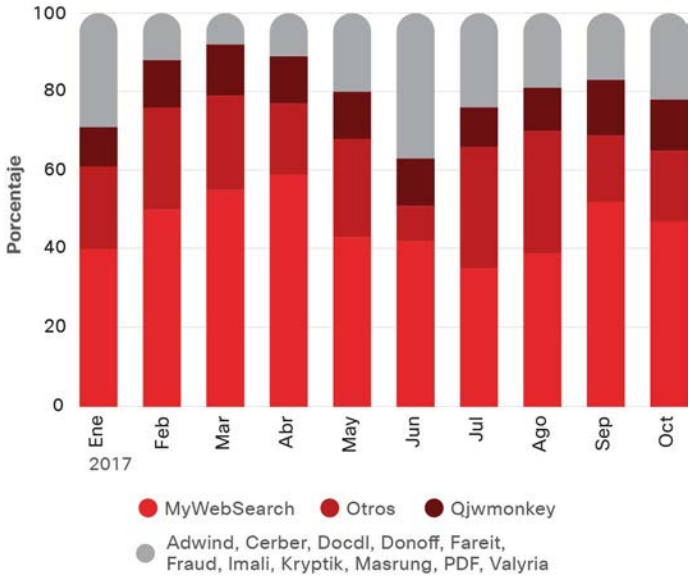
El usuario más activo del spyware MyWebSearch de "otras extensiones"

El grupo de "otras extensiones" en nuestro estudio incluye varios tipos de malware conocido. Pero MyWebSearch, un software malicioso de adware y un secuestrador de navegador que se presenta como una útil barra de herramientas, es el reproductor más activo (consulte la figura 13). Utiliza las extensiones de archivo .exe, a veces sólo un tipo por mes. La aplicación potencialmente no deseada (PUA) ha estado alrededor por años y afecta a diferentes tipos de navegador. A menudo se incluye con programas de software fraudulentos y puede exponer a los usuarios a publicidad maliciosa.

Nuestro análisis de los tipos de extensiones de archivos maliciosos muestra que incluso en el sofisticado y complejo entorno de amenazas actual, el correo electrónico sigue siendo un canal vital para la distribución de malware. Para las empresas, estrategias de defensa básicas incluyen:

- Implementar defensas de seguridad de correo electrónico potentes y completas.
- Educar a los usuarios sobre la amenaza de archivos adjuntos maliciosos y enlaces en correos electrónicos de phishing y correo no deseado.

Figura 13 MyWebSearch, el usuario más activo de "otras extensiones"



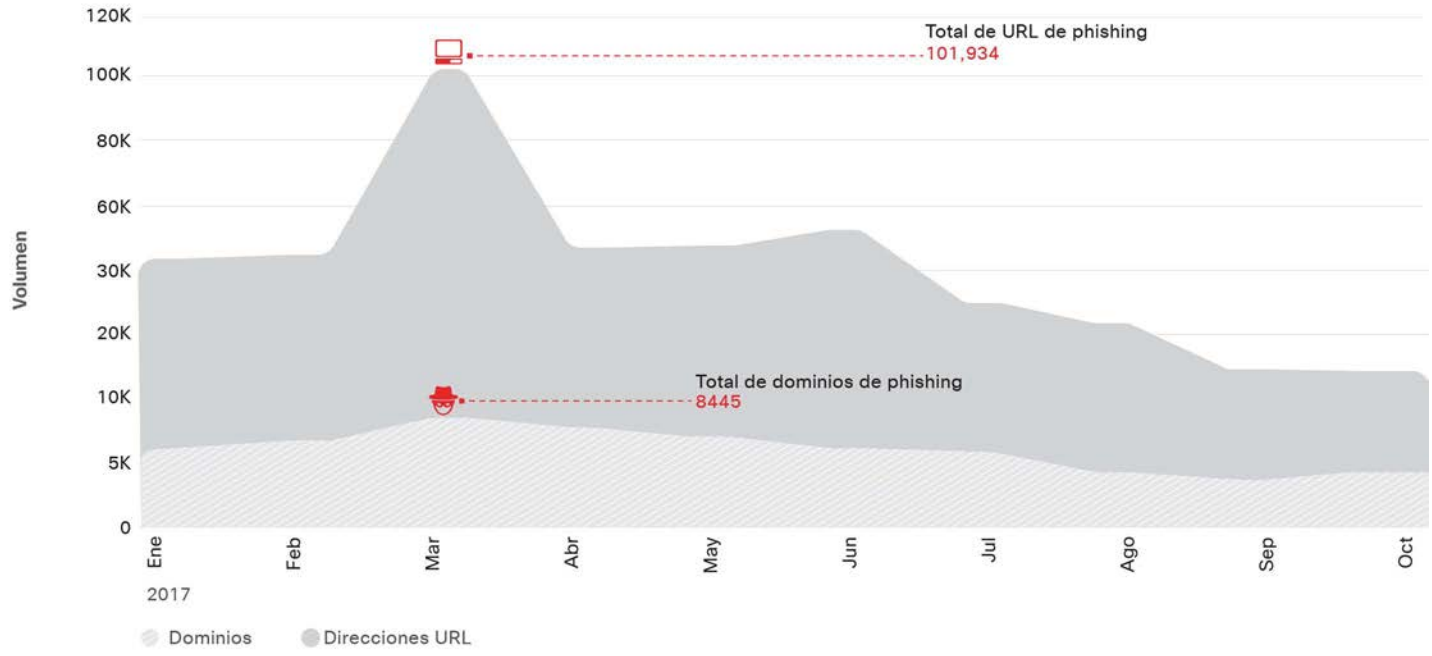
Fuente: Cisco Security Research

La ingeniería social sigue siendo una plataforma critica para el lanzamiento de ataques de correo electrónico

El phishing y el spear phishing son tácticas usadas para robar las credenciales de los usuarios y otra información sensible y eso se debe a que son muy efectivas. De hecho, los correos electrónicos de phishing y spear phishing fueron la raíz de algunas de las brechas más grandes que acaparan los titulares en los últimos años. Dos ejemplos de 2017 incluyen un ataque generalizado dirigido a usuarios de Gmail users[12] Gmail12 y una piratería de sistemas energéticos irlandeses.[13]

Para evaluar cuán prevalentes son las URL y los dominios de phishing en la Internet de hoy, los investigadores de amenazas de Cisco examinaron datos de fuentes que investigan correos electrónicos potencialmente "phishy" enviados por usuarios a través de inteligencia contra amenazas de phishing basada en la comunidad. La figura 14 muestra el número de URL de phishing y dominios de phishing observados durante el período de enero a octubre de 2017.

Figura 14 Número de URL y dominios phishing observados por mes



Fuente: Cisco Security Research

Los picos vistos en marzo y junio se pueden atribuir a dos campañas diferentes. El primero parecía dirigirse a los usuarios de un importante proveedor de servicios de telecomunicaciones. La campaña:

- Involucró 59,651 URL que contenían subdominios bajo aaaainfomation[dot]org.
- Tenía subdominios que contenían secuencias al azar consistentes de 50-62 letras.

Cada longitud de subdominio (50-62) contenía aproximadamente 3500 URL, lo que permitió el uso programático de los subdominios (por ejemplo: Cewekonuxykysowegulukozapojygepuqybyteqe johofopefogu[dot]aaaainfomation[dot]org).

Los adversarios usaron un servicio de privacidad de bajo costo para registrar los dominios observados en esta campaña.

12 *Massive Phishing Attack Targets Gmail Users, por Alex Johnson, NBC News, mayo de 2017:* nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501

13 *Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure, por Lizzie Deardon, The Independent, julio de 2017:* independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

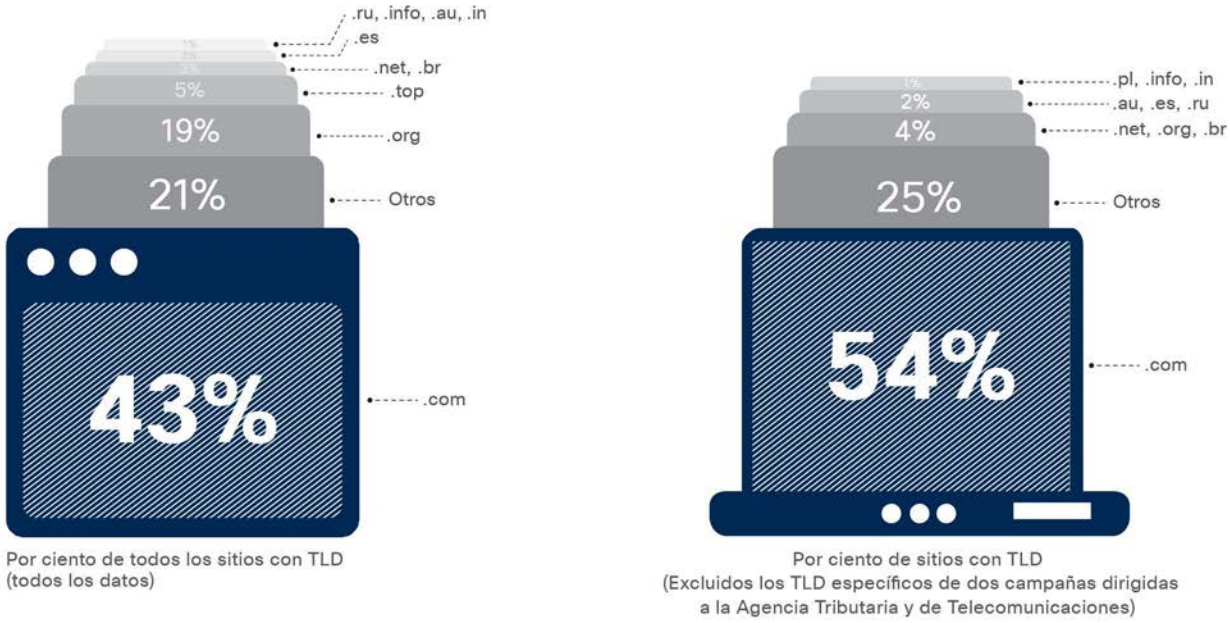
En la segunda campaña, que fue más activa en junio, los actores de la amenaza usaron el nombre de una agencia tributaria legítima en el Reino Unido para disfrazar sus acciones. Emplearon 12 dominios de nivel superior (TLD). Once de los dominios eran URL con seis cadenas aleatorias de seis caracteres (por ejemplo: jyzwyp[dot]top). Y nueve de los dominios estaban asociados con más de 1600 sitios de phishing cada uno.

Al igual que la campaña de marzo, los adversarios registraron los dominios mediante un servicio de privacidad para ocultar la información de registro de dominio. Registraron todos los dominios durante un período de dos días. El segundo día, se observaron casi 19,000 URL conectadas a la campaña, y todas fueron descubiertas en un plazo de cinco horas (para obtener más información sobre la rapidez con la que los agentes de la amenaza ponen en uso dominios recientemente registrados, consulte "Uso malicioso de recursos legítimos para C2 de puerta trasera", en la página 24).

Distribución de TLD en todos los sitios de phishing conocidos

Nuestro análisis de los sitios de phishing durante el período comprendido entre enero y agosto de 2017 descubrió que los actores de amenazas empleaban 326 TLD exclusivos para estas actividades, incluidos .com, .org, .top (en gran parte debido a la campaña de la agencia tributaria del Reino Unido) y TLD específicos de cada país (ver figura 15). Emplear TLD menos conocidos puede ser ventajoso para los adversarios; estos dominios son generalmente económicos y a menudo ofrecen protección de privacidad de bajo costo.

Figura 15 Distribución de los TLD en sitios conocidos de phishing



Fuente: Cisco Security Research

Los defensores deben estar atentos en el monitoreo de esta "vieja" amenaza

En 2017, decenas de miles de intentos de phishing se reportaron mensualmente a los servicios de inteligencia contra amenazas de phishing basados en la comunidad, incluidos en nuestro análisis. Algunas de las tácticas y herramientas más comunes que utilizan los adversarios para ejecutar campañas de phishing incluyen:

- **Domains Squatting:** dominios nombrados para que parezcan dominios válidos (ejemplo: cisco[dot]com).
- **Domain Shadowing:** subdominios agregados bajo un dominio válido sin el conocimiento del propietario (ejemplo: badstuff[dot]cisco[dot]com).
- **Maliciously registed domains:** un dominio creado para fines maliciosos (ejemplo: viqpbe[dot]top).
- **URL Shorteners:** una URL maliciosa disfrazada con un acortador de URL (ejemplo: bitly[dot]com/random-string).
- **URL shorteners:** A malicious URL disguised with a URL shortener (example: bitly[dot]com/random-string). Nota: en los datos que examinamos, Bitly.com era la herramienta de acortamiento de URL que más utilizaban los adversarios. Las URL acortadas maliciosas representaron el 2% de los sitios de phishing en nuestro estudio. Ese número llegó a 3.1 por ciento en agosto.
- **Servicios de subdominio:** un sitio creado en un servidor del subdominio (ejemplo: mybadpage[dot]000webhost[dot]com).

Los agentes de amenazas en el juego phishing y spear phishing están perfeccionando continuamente los métodos de ingeniería social para engañar a los usuarios para que hagan clic en enlaces maliciosos o visiten páginas web fraudulentas y proporcionen credenciales u otro tipo de información de alto valor. La capacitación y la responsabilidad del usuario y la aplicación de las tecnologías de seguridad del correo electrónico, siguen siendo estrategias cruciales para combatir estas amenazas.

TÁCTICAS DE EVASIÓN DE SANDBOX

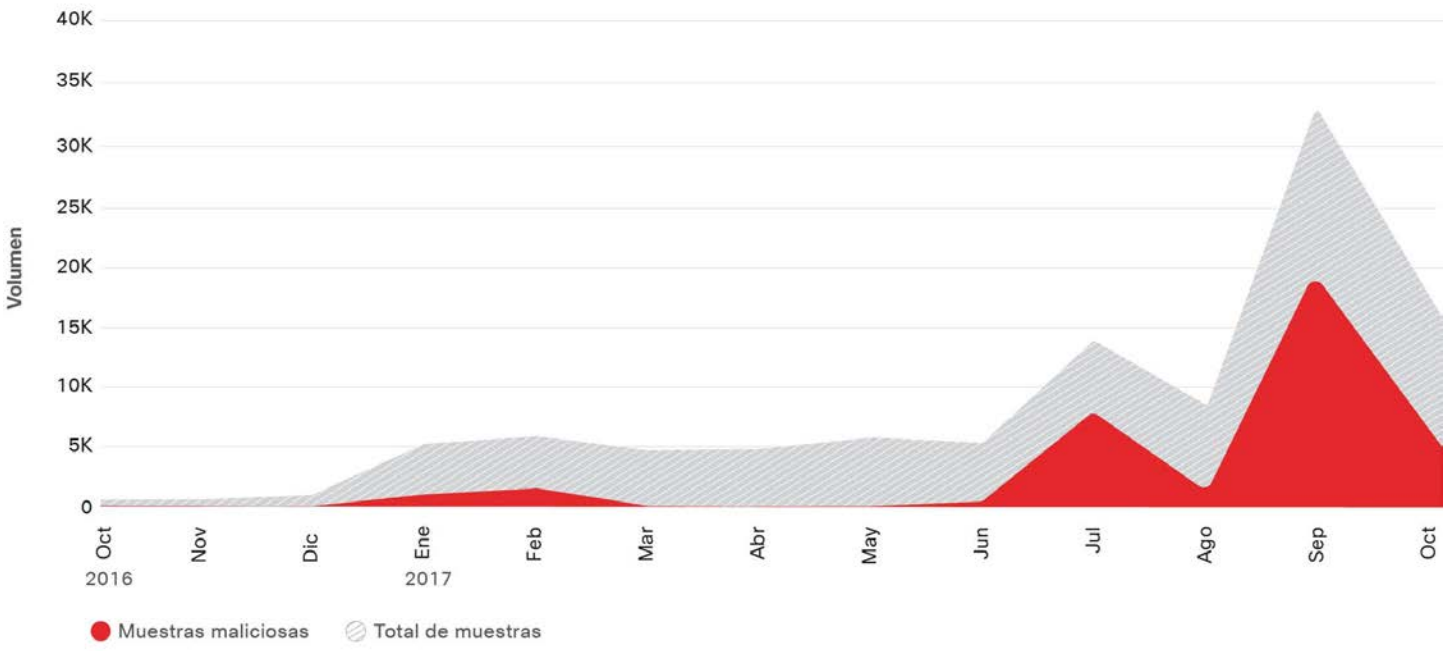
Los adversarios se están convirtiendo en expertos en el desarrollo de amenazas que pueden evadir entornos de sandboxing cada vez más sofisticados. Cuando los investigadores de amenazas de Cisco analizaron archivos adjuntos de correo electrónico malicioso que estaban equipados con varias técnicas de evasión de sandbox, descubrieron que la cantidad de muestras maliciosas que utilizaban una técnica de evasión de sandbox específico mostraba picos agudos y luego disminuía rápidamente. Este es otro ejemplo más de cómo los atacantes son rápidos para aumentar el volumen de intentos de romper las defensas una vez que encuentran una técnica efectiva.

Los autores de malware juegan trucos sucios en las zonas de seguridad (sandbox) de los defensores.

En septiembre de 2017, los investigadores de amenazas de Cisco observaron grandes volúmenes de muestras donde se entrega una carga útil maliciosa después de cerrar un documento (figura 16). En este caso, el malware se activa con el evento "document_close". La técnica funciona porque, en muchos casos, los documentos no se cierran después de que el documento se haya abierto y analizado en la zona protegida (sandbox). Debido a que el sandbox no cierra el documento explícitamente, los archivos adjuntos se consideran seguros por el sandbox y se entregarán a los destinatarios previstos. Cuando un destinatario abre el documento adjunto y luego lo cierra, se entrega la carga útil maliciosa. Los sandboxes que no detectan adecuadamente las acciones en el cierre del documento se pueden eludir con esta técnica.

El uso del evento "document_close" es una opción inteligente para los atacantes. Aprovecha la macro funcionalidad integrada en Microsoft Office, así como la tendencia de los usuarios a abrir archivos adjuntos que creen que son relevantes para ellos. Una vez que los usuarios se dan cuenta de que el archivo adjunto no es relevante para ellos, cierran el documento y desencadenan las macros en las que se oculta el malware.

Figura 16 Alto volumen de documentos maliciosos de Microsoft Word que utilizan "llamadas de función cerradas" observadas en septiembre de 2017

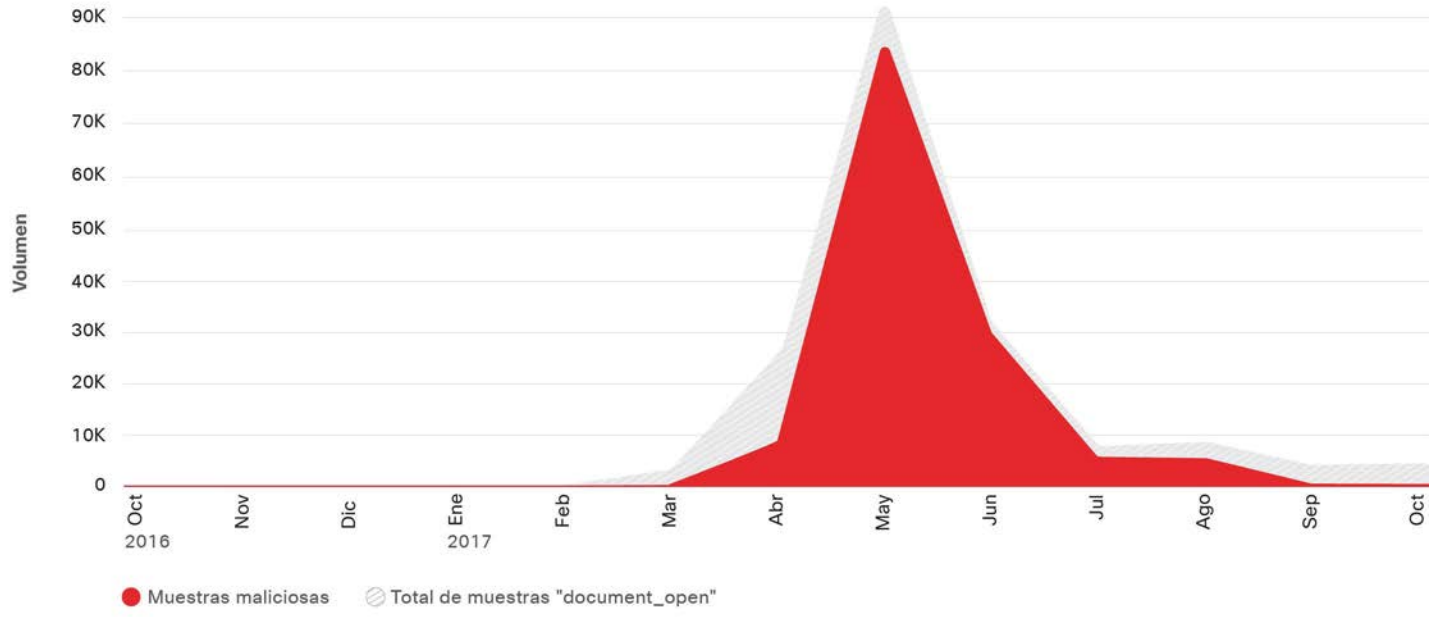


Fuente: Cisco Security Research

Algunos atacantes evaden el sandboxing al disfrazar el tipo de documento en el que existe la carga maliciosa. Como se ve en la figura 17, notamos un ataque significativo en mayo de 2017 que fue construido alrededor de documentos maliciosos de Word incrustados en documentos PDF. Los documentos pueden pasar por alto los sandboxes que simplemente detectan y abren el PDF, en lugar de abrir y analizar el documento incrustado de Word. El documento PDF generalmente contenía una tentación para que el usuario haga clic y abra el documento de Word, lo que desencadenaría el comportamiento malicioso. Los sandboxes que no abren y analizan documentos incrustados en archivos PDF se pueden pasar por alto con esta técnica.

Después de ver el pico en las muestras maliciosas que involucran estos archivos PDF, nuestros investigadores de amenazas refinaron el entorno sandbox para detectar si los archivos PDF contenían acciones o incitaciones a abrir documentos incrustados de Word.

Figura 17 El gran ataque en mayo de 2017 involucró archivos PDF con documentos maliciosos incrustados de Word



Fuente: Cisco Security Research

Los picos en muestras maliciosas que usan diferentes técnicas de evasión de sandbox apuntan al deseo de los actores maliciosos de seguir un método que parece funcionar para ellos, o para otros atacantes. Además, si los adversarios se toman la molestia de crear malware y la infraestructura asociada, quieren un retorno de sus inversiones. Si determinan que el malware puede pasar por las pruebas de sandbox, a su vez, aumentarán el número de intentos de ataque y los usuarios afectados.

Los investigadores de Cisco recomiendan usar sandboxing que incluye funciones de "contenido consciente" para ayudar a garantizar que el malware que utiliza las tácticas descritas anteriormente no evada el análisis de sandbox. Por ejemplo, la tecnología de sandboxing debe mostrar conocimiento de las características de metadatos de las muestras que está analizando, como por ejemplo, determinar si la muestra incluye una acción al cerrar el documento.

ABUSO DE SERVICIOS EN LA NUBE Y OTROS RECURSOS LEGÍTIMOS

A medida que las aplicaciones, los datos y las identidades se trasladan a la nube, los equipos de seguridad deben gestionar el riesgo que implica perder el control del perímetro de la red tradicional. Los atacantes se están aprovechando del hecho de que los equipos de seguridad tienen dificultades para defenderse de la evolución y la expansión de entornos cloud y IoT. Una razón es la falta de claridad sobre quién es exactamente el responsable de proteger esos entornos.

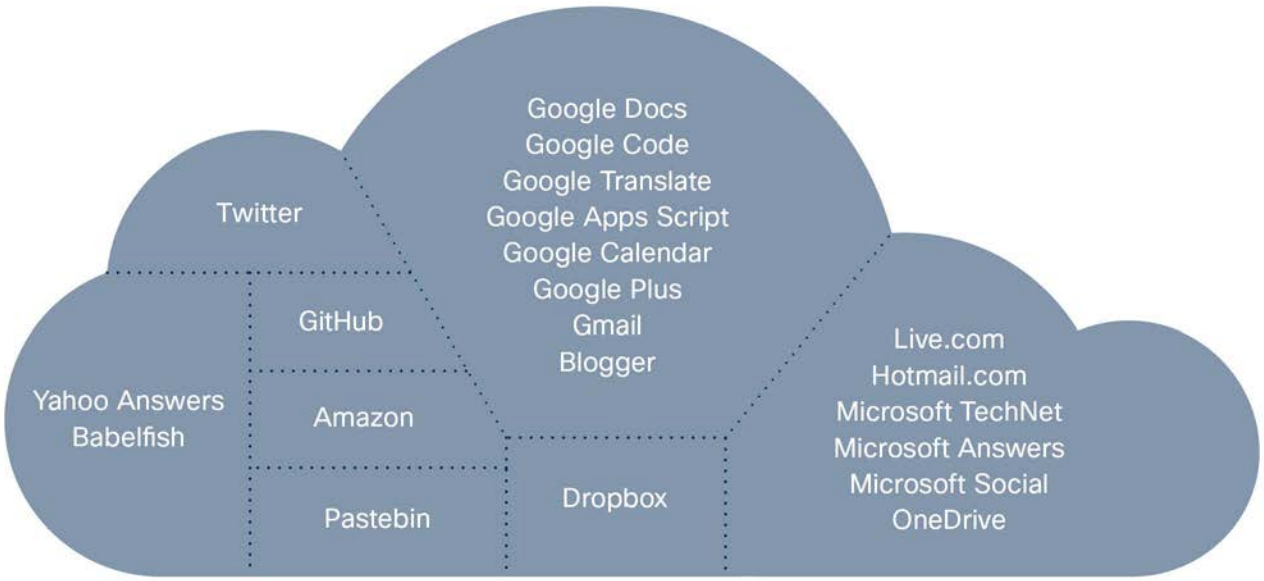
Para enfrentar este desafío, las empresas pueden necesitar aplicar una combinación de mejores prácticas, tecnologías de seguridad avanzadas como machine learning e incluso algunas metodologías experimentales, según los servicios que utilizan para su negocio y cómo evolucionan las amenazas en este espacio.

Uso malicioso de recursos legítimos para puerta trasera C2

Cuando los agentes de amenazas utilizan servicios legítimos de comando y control (C2), el tráfico de la red de malware se vuelve casi imposible de identificar para los equipos de seguridad porque imita el comportamiento del tráfico de red legítimo. Los adversarios tienen mucho "ruido" de Internet para usar como cubierta porque mucha gente hoy en día confía en servicios como Google Docs y Dropbox para hacer su trabajo, independientemente de si estos servicios son ofrecidos o respaldados sistémicamente por sus empleadores.

La figura 18 muestra varios de los servicios legítimos conocidos que los investigadores de Anomali, un socio de Cisco y proveedor de inteligencia de amenazas, han observado que se han utilizado en esquemas C2 de puerta trasera de malware[14] en los últimos años. (Nota: estos tipos de servicios se enfrentan a un dilema para combatir el abuso, ya que dificultar a los usuarios la configuración de cuentas y el uso de sus servicios puede afectar negativamente su capacidad de generar ingresos).

Figura 18 Ejemplos de servicios legítimos abusados por malware para C2



Fuente: Anomali

14 Anomali define un esquema C2 como "la totalidad de direcciones IP, dominios, servicios legítimos y todos los sistemas remotos que forman parte de la ... arquitectura de comunicaciones" de malware.

De acuerdo con la investigación de Anomali, los actores de la amenaza persistente avanzada (APT) y los grupos patrocinados por el gobierno estuvieron entre los primeros adversarios en usar servicios legítimos para C2; sin embargo, la técnica ahora es adoptada por una gama más amplia de adversarios sofisticados en la economía sumergida. El uso de servicios legítimos para C2 atrae a los actores malintencionados porque es fácil:

- El registro de nuevas cuentas en estos servicios.
- Configurar una página web en Internet de acceso público.
- Usurpar el cifrado de protocolos de C2. (En lugar de configurar servidores C2 con encriptación o crear cifrado en malware, los atacantes pueden simplemente adoptar el certificado SSL de un servicio legítimo).
- Adaptar y transformar recursos sobre la marcha. (Los atacantes pueden aprovechar los implantes a través de ataques sin necesidad de reutilizar direcciones IP o DNS, por ejemplo.)
- Reducir la probabilidad de "quemar" la infraestructura. (Los adversarios que usan servicios legítimos para C2 no necesitan codificar el malware con direcciones IP o dominios. Cuando se complete su operación, simplemente pueden eliminar sus páginas de servicios legítimos, y nadie sabrá nunca las direcciones IP).
- Los atacantes se benefician de esta técnica porque les permite reducir gastos indirectos y mejorar su retorno de la inversión.

Para los defensores, el uso por los adversarios de servicios legítimos para C2 presenta algunos desafíos importantes:

Los servicios legítimos son difíciles de bloquear.
¿Pueden las organizaciones, desde una mera perspectiva empresarial, incluso considerar bloquear partes de servicios legítimos de Internet como Twitter o Google?

Los servicios legítimos suelen estar encriptados y son innatamente difíciles de inspeccionar
El descifrado SSL es caro y no siempre es posible a escala empresarial. Por lo tanto, el malware oculta su comunicación dentro del tráfico cifrado, por lo que es difícil, si no imposible, para los equipos de seguridad identificar el tráfico malicioso.

El uso de servicios legítimos subvierte la inteligencia de dominio y certificado, y complica la atribución.
Los adversarios no necesitan registrar dominios porque la cuenta de servicio legítima se considera la dirección inicial de C2. Además, no es probable que sigan registrando certificados SSL o que utilicen certificados SSL auto firmados para los esquemas C2. Ambas tendencias obviamente tendrán un impacto negativo en las transmisiones de indicadores para el filtrado de reputación y la lista negra de indicadores, que se basan en dominios recién generados y recientemente registrados, y los certificados y direcciones IP conectadas a ellos.

Detectar el uso de servicios legítimos para C2 es difícil. Sin embargo, los investigadores de amenazas de Anomali recomiendan que los defensores consideren la aplicación de algunas metodologías experimentales. Por ejemplo, los defensores pueden identificar malware utilizando servicios legítimos para C2 buscando:

- Conexiones que no son de navegador ni de aplicación a servicios legítimos
- Tamaños de respuesta de página única o baja de servicios legítimos
- Alta frecuencia de intercambio de certificados para servicios legítimos
- Ejemplos de sandboxing masivo para llamadas DNS sospechosas a servicios legítimos

Todos estos comportamientos únicos merecen una mayor investigación de los programas de origen y los procesos.[15]

15 Para obtener detalles sobre estas metodologías experimentales y más información sobre cómo los adversarios usan servicios legítimos para C2, descargue el documento de investigación de Anomali: Rise of Legitimate Services for Backdoor Command and Control, disponible en: anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf.

Extrayendo valor óptimo de los recursos

Los investigadores de seguridad de Cisco analizaron nombres de consulta únicos (dominios) recientemente vistos asociados con consultas DNS realizadas en un período de siete días en agosto de 2017. Tenga en cuenta que "recién visto" en esta discusión no tiene relación con la creación de un dominio; se relaciona con cuando un dominio fue "visto" por primera vez por la tecnología de seguridad en la nube de Cisco durante el período de observación.

El objetivo de esta investigación fue obtener más información sobre la frecuencia con que los adversarios usan y reutilizan los dominios de nivel registrado (RLD) en sus ataques. Comprender el comportamiento de los actores amenazados a nivel de dominio puede ayudar a los defensores a identificar dominios maliciosos y subdominios relacionados que deberían bloquearse con herramientas de primera línea como las plataformas de seguridad en la nube.

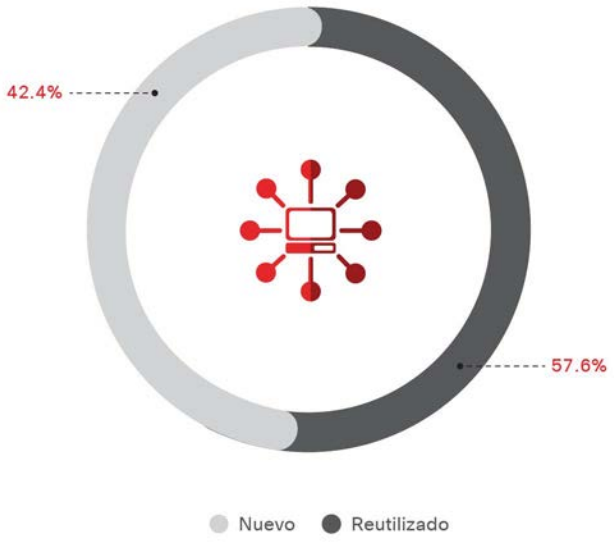
Para que nuestros investigadores pudieran centrarse únicamente en el grupo básico de RLD únicos, unos 4 millones en total, los subdominios se eliminaron de la muestra de dominios recién vistos. Solo un pequeño porcentaje de los RLD en esa muestra fue categorizado como malicioso. De los RLD que eran maliciosos, más de la mitad (alrededor del 58 por ciento) se reutilizaron, como muestra la figura 19.

Ese hallazgo sugiere que, si bien la mayoría de los atacantes crean nuevos dominios para sus campañas, muchos se concentran en tratar de obtener el mejor rendimiento de sus inversiones lanzando múltiples campañas desde un único dominio. El registro de dominios puede ser costoso, especialmente en la escala que la mayoría de los atacantes requieren para ejecutar sus campañas y evadir la detección.

Una quinta parte de los dominios maliciosos puestos en uso rápidamente

Los adversarios pueden sentarse en dominios durante días, meses o incluso años después de registrarlos, esperando el momento adecuado para usarlos. Sin embargo, los investigadores de amenazas de Cisco observaron que un porcentaje significativo de dominios maliciosos, alrededor del 20 por ciento, se usaban en campañas menos de una semana después de su registro (consulte la figura 20).

Figura 19 Porcentaje de dominios nuevos vs. reutilizados



Fuente: Cisco Security Research

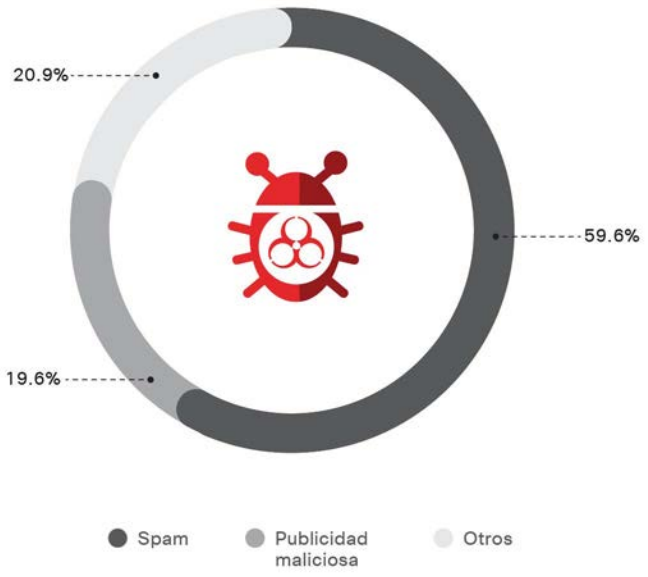
Figura 20 Tiempos de registro RLD

Fuente: Cisco Security Research

Muchos dominios nuevos vinculados a campañas de publicidad maliciosa

La mayoría de los dominios maliciosos que analizamos se asociaron con campañas de spam, alrededor del 60 por ciento. Casi una quinta parte de los dominios se conectaron a campañas publicitarias (ver figura 21). La publicidad maliciosa se ha convertido en una herramienta esencial para dirigir a los usuarios a los kits de exploits, incluidos aquellos que distribuyen ransomware.

Figura 21 Categorizaciones maliciosas



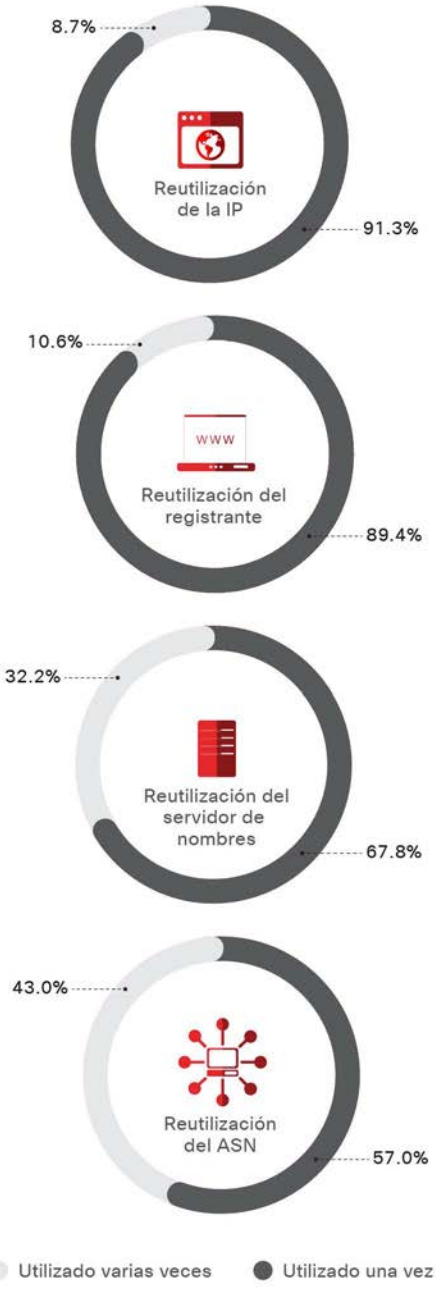
Fuente: Cisco Security Research

Las técnicas bien usadas y relacionadas con el dominio para crear campañas maliciosas incluyen domain shadowing. En esta técnica, los atacantes roban las credenciales legítimas de la cuenta de dominio para crear subdominios dirigidos a servidores maliciosos. Otra táctica es el abuso de servicios de DNS gratuitos y dinámicos para generar dominios y subdominios maliciosos. Eso les permite a los agentes de las amenazas entregar cargas maliciosas que cambian constantemente las IP de alojamiento, ya sea las computadoras de los usuarios infectados o los sitios web públicos comprometidos.

Los dominios reutilizan los recursos de infraestructura

Los RLD maliciosos en nuestra muestra también parecían reutilizar los recursos de infraestructura, como las direcciones de correo electrónico del registrante, las direcciones IP, los números de sistema autónomo (ASN) y los servidores de nombres (consulte la figura 22). Esto es una prueba más de que los adversarios intentan obtener el máximo valor de sus inversiones en nuevos dominios y preservar los recursos, de acuerdo con nuestros investigadores. Por ejemplo, una dirección IP puede ser utilizada por más de un dominio. Por lo tanto, un atacante que siente las bases para una campaña podría decidir invertir en unas pocas direcciones IP y una serie de nombres de dominio en lugar de servidores, que cuestan más.

Figura 22 Reutilización de la infraestructura por RLD maliciosos



Fuente: Cisco Security Research

Los recursos que los RLD reutilizan dan pistas sobre si el dominio es probablemente malicioso. Por ejemplo, la reutilización de correos electrónicos de registrantes o direcciones IP ocurre con poca frecuencia, por lo que un patrón de reutilización en cualquiera de los frentes sugiere un comportamiento sospechoso. Los defensores pueden tener un alto grado de confianza en el bloqueo de esos dominios, sabiendo que hacerlo probablemente no tendrá un impacto negativo en la actividad comercial.

El bloqueo estático de ASN y los servidores de nombres no es factible en la mayoría de los casos. Sin embargo, los patrones de reutilización por RLD son dignos de una mayor investigación para determinar si ciertos dominios deben ser bloqueados.

El uso de herramientas inteligentes de seguridad en la nube de primera línea para identificar y analizar dominios y subdominios potencialmente maliciosos puede ayudar a los equipos de seguridad a seguir el rastro de un atacante y responder preguntas tales como:

- ¿Qué dirección IP resuelve el dominio?
- ¿Qué ASN está asociado con esa dirección IP?
- ¿Quién registró el dominio?
- ¿Qué otros dominios están asociados con ese dominio?

Las respuestas pueden ayudar a los defensores no solo a refinar las políticas de seguridad y bloquear ataques, sino también a evitar que los usuarios se conecten a destinos maliciosos en Internet mientras están en la red de la empresa.

Las tecnologías DevOps en riesgo de ataques de ransomware

En 2017 surgieron los ataques de ransomware de DevOps, comenzando con una campaña en enero dirigida a la plataforma de base de datos de código abierto, MongoDB.[16] Los atacantes encriptaron las instancias públicas de MongoDB y exigieron pagos de rescate por claves y software de descifrado. Poco después, pusieron la mira en bases de datos comprometedoras, como CouchDB y Elasticsearch, con ransomware orientado al servidor.

Rapid7 es un socio de Cisco y proveedor de datos de seguridad y soluciones de análisis. Tal como explicaron los investigadores de Rapid7 en nuestro Reporte Semestral de Ciberseguridad de Cisco 2017, los servicios de DevOps a menudo se implementan incorrectamente o se dejan abiertos intencionalmente para un acceso conveniente por parte de usuarios legítimos, dejando estos servicios abiertos para ataques.

Rapid7 realiza barridos regulares de Internet para tecnologías DevOps y cataloga instancias abiertas e instancias rescatadas. Algunos de los servicios de DevOps que encuentran durante sus barridos pueden contener información de identificación personal (PII), basada en los nombres de las tablas expuestas a Internet.

Para reducir el riesgo de exposición a los ataques de ransomware de DevOps, las organizaciones que utilizan instancias públicas de Internet de las tecnologías DevOps deben:

- Desarrollar estándares sólidos para el despliegue seguro de tecnologías DevOps
- Mantener un conocimiento activo de la infraestructura pública utilizada por la empresa
- Mantener las tecnologías de DevOps actualizadas y parcheadas
- Realizar análisis de vulnerabilidad

Para obtener más detalles sobre la investigación de Rapid7, consulte "No permita que las tecnologías DevOps dejen el negocio expuesto" en el Reporte Semestral de Ciberseguridad de Cisco 2017.

16 *After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters, por Lucian Constantin, IDG News Service, 13 de enero de 2017:* **pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.**

Amenazas internas: Tomando ventaja de la nube

En Reportes de seguridad anteriores, hemos discutido el valor de los permisos de OAuth y los privilegios de super usuario para imponer quién puede ingresar a las redes y cómo pueden acceder a los datos.[17] Para examinar más a fondo el impacto de la actividad del usuario sobre la seguridad, los investigadores de amenazas de Cisco examinaron recientemente las tendencias de exfiltración de datos. Emplearon un algoritmo de machine learning para perfilar 150,000 usuarios en 34 países, todos usando proveedores de servicios en la nube, de enero a junio de 2017. El algoritmo explica no solo el volumen de documentos que se descargan, sino también variables como la hora del día de las descargas, las direcciones IP y las ubicaciones.

Después de perfilar a los usuarios durante seis meses, nuestros investigadores pasaron 1.5 meses estudiando anormalidades, marcando el 0.5 por ciento de los usuarios por descargas sospechosas. Es una cantidad pequeña, pero estos usuarios descargaron, en total, más de 3.9 millones de documentos de sistemas corporativos en la nube, o un promedio de 5200 documentos por usuario durante el período de 1.5 meses. De las descargas sospechosas, 62 por ciento se produjo fuera del horario normal de trabajo; 40 por ciento se llevó a cabo los fines de semana.

Los investigadores de Cisco también realizaron un análisis de text-mining sobre los títulos de los 3.9 millones de documentos descargados sospechosamente.

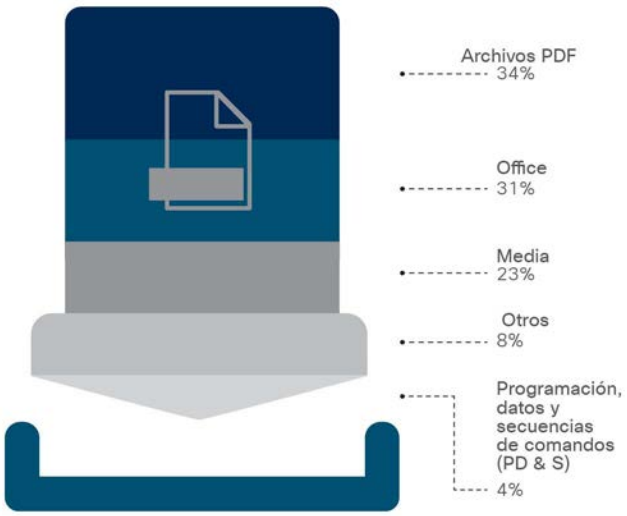
Una de las palabras clave más populares en los títulos de los documentos fue "datos". Las palabras clave que aparecen más comúnmente con la palabra "datos" fueron "empleado" y "cliente." De los tipos de documentos descargados, el 34 por ciento eran PDF y el 31 por ciento eran documentos de Microsoft Office (consulte la figura 23).

La aplicación de algoritmos de machine learning ofrece una visión más matizada de la actividad del usuario en la nube más allá del número de descargas. En nuestro análisis, el 23 por ciento de los usuarios que estudiamos fueron marcados más de tres veces para descargas sospechosas, generalmente comenzando con un número pequeño de documentos. El volumen aumentó lentamente cada vez y finalmente, estos usuarios mostraron picos repentinos y significativos en las descargas (figura 24).

Los algoritmos de machinge learning mantienen la promesa de proporcionar una mayor visibilidad de la nube y el comportamiento del usuario. Si los defensores pueden comenzar a predecir el comportamiento del usuario en términos de descargas, pueden ahorrar el tiempo que lleva investigar el comportamiento legítimo. También pueden intervenir para detener un posible ataque o incidente de exfiltración de datos antes de que ocurra.

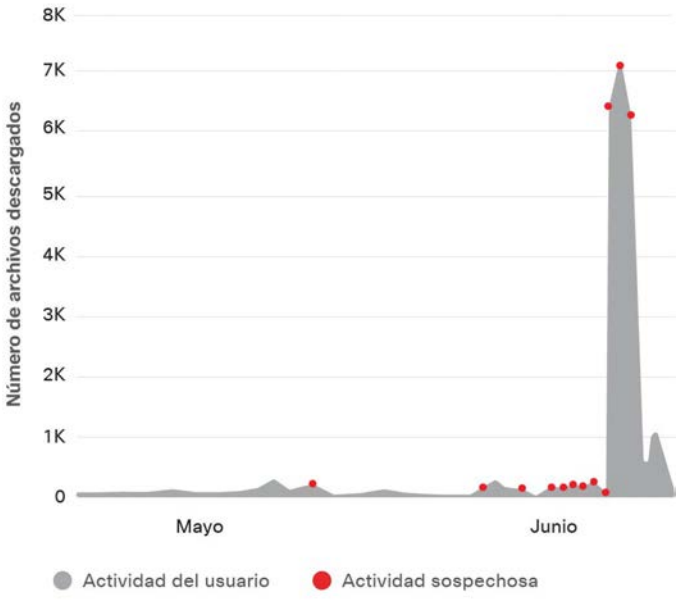
17 *Reporte Semestral de Ciberseguridad de Cisco 2017:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Figura 23 Documentos más comúnmente descargados



Fuente: Cisco Security Research

Figura 24 Algoritmos de mchine learning capturan el comportamiento sospechoso de descarga del usuario

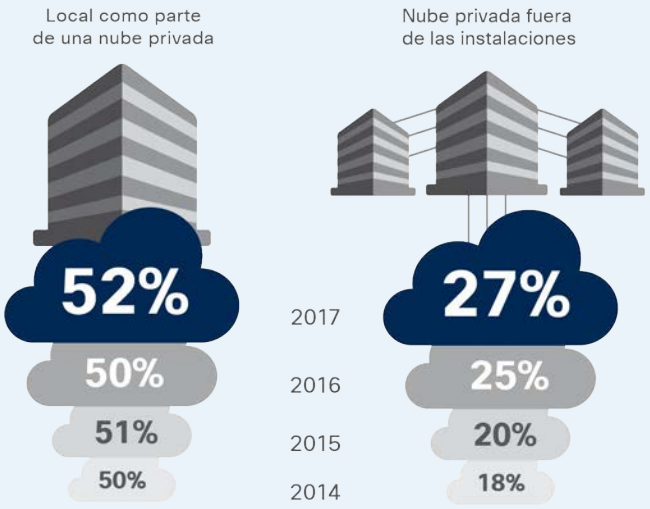


Fuente: Cisco Security Research

Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018: La seguridad se ve como un beneficio clave de las redes de hosting en la nube

El uso de la infraestructura en la nube pública y en las instalaciones está creciendo, de acuerdo con el Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018, aunque muchas organizaciones todavía alojan redes locales. En el estudio de 2017, el 27 por ciento de los profesionales de seguridad dijeron que están utilizando nubes privadas fuera del establecimiento, en comparación con el 25 por ciento en 2016 y el 20 por ciento en 2015 (figura 25). El cincuenta y dos por ciento (52%) dijo que sus redes están alojadas en las instalaciones como parte de una nube privada.

Figura 25 Más organizaciones están usando nubes privadas



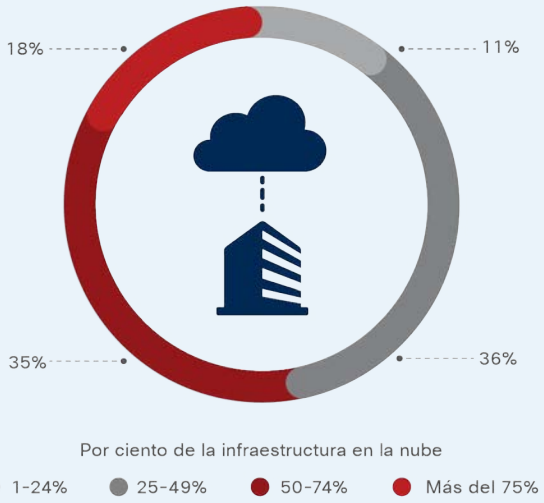
Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

De las organizaciones que usan la nube, el 36 por ciento aloja del 25 al 49 por ciento de su infraestructura en la nube, mientras que el 35 por ciento aloja del 50 al 74 por ciento de su infraestructura en la nube (figura 26).

La seguridad es el beneficio más común de las redes de hosting en la nube, según los encuestados del personal de seguridad. Entre ellos, el 57 por ciento dijo que aloja redes en la nube debido a una mejor seguridad de los datos; 48 por ciento, debido a la escalabilidad; y 46 por ciento, debido a la facilidad de uso (ver figura 27).

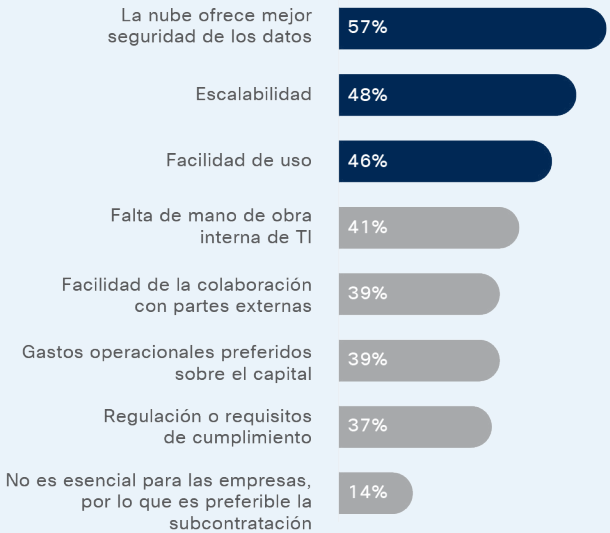
Los encuestados también dijeron que, a medida que se transfiera más infraestructura a la nube, es posible que busquen invertir en el Agente de seguridad para el acceso a la nube (CASB) para agregar seguridad adicional a los entornos de la nube.

Figura 26 El cincuenta y tres por ciento de las organizaciones alojan al menos la mitad de la infraestructura en la nube



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Figura 27 El cincuenta y siete por ciento cree que la nube ofrece una mejor seguridad de los datos



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

ATAQUES IoT y DDoS

La IoT aún está evolucionando, pero los adversarios ya están explotando las debilidades de seguridad en los dispositivos IoT para obtener acceso a los sistemas, incluidos los sistemas de control industrial que admiten infraestructura crítica. Las botnets también están creciendo en tamaño y pode, y son cada vez más capaces de desencadenar ataques poderosos que podrían afectar gravemente a Internet. El cambio de los atacantes hacia una mayor explotación de la capa de aplicación indica que este es su objetivo. Pero muchos profesionales de la seguridad no son conscientes de, o descartan la amenaza que representan las botnets de la IoT. Las organizaciones siguen agregando dispositivos IoT a sus entornos de TI con poca o ninguna atención a la seguridad o, lo que es peor, no se toman tiempo para evaluar cuántos dispositivos IoT están tocando sus redes. De esta manera, facilitan que los adversarios tomen el mando de la IoT.

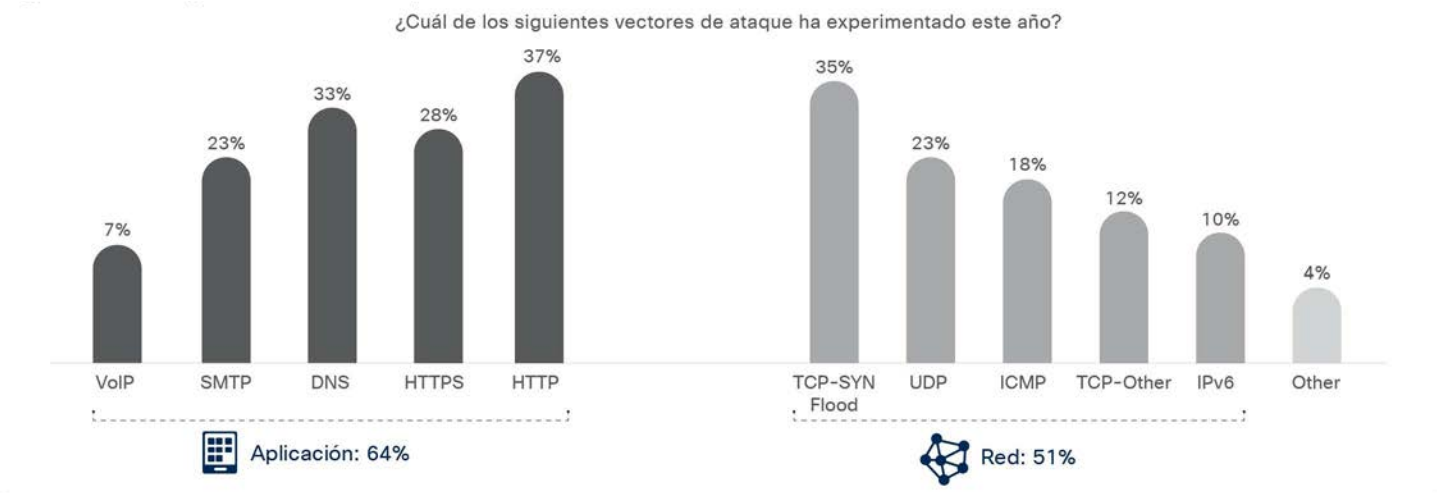
Pocas organizaciones ven las botnets de la IoT como una inminente amenaza, aunque deberían.

A medida que la IoT se expande y evoluciona, también lo hacen las botnets. Y a medida que estas botnets crecen y maduran, los atacantes las usan para lanzar ataques DDoS de mayor alcance e intensidad. Radware, un socio de Cisco, ofreció un análisis de tres de las redes de bots más grandes: Mirai, Brickerbot y Hajime en el Reporte Semestral de Ciberseguridad de Cisco 2017 y retoma el tema de las botnet de la IoT en nuestro último Reporte para subrayar la gravedad de esta amenaza.[18] Su investigación muestra que solo el 13 por ciento de las organizaciones creen que las botnets de la IoT serán una gran amenaza para sus negocios en 2018.

Las botnets de la IoT están prosperando porque las organizaciones y los usuarios están implementando dispositivos IoT de bajo costo rápidamente y con poca o ninguna consideración por la seguridad. Los dispositivos IoT son sistemas basados en Linux y Unix, por lo que a menudo son objetivos de binarios de formato ejecutable y vinculable (ELF). También son menos difíciles de controlar que una PC, lo que significa que es fácil para los adversarios formar rápidamente un gran ejército.

Los dispositivos IoT funcionan las 24 horas y pueden ponerse en marcha en cualquier momento. Y a medida que los adversarios aumentan el tamaño de sus botnets de IoT,

Figura 28 La aplicación de ataques DDoS aumentó en 2017



Fuente: Radware

18 Para obtener más detalles sobre la investigación de botnet IoT de Radware, consulte "La IoT recién está surgiendo, pero las botnets IoT ya están aquí", pág. 39, Reporte Semestral de Ciberseguridad de Cisco 2017: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

están invirtiendo en códigos y malware más sofisticados y cambiando a ataques DDoS más avanzados.

La aplicación DDoS supera a la red DDoS

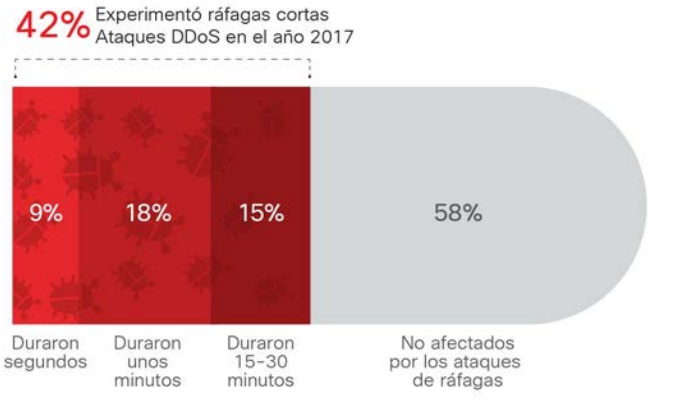
Los ataques de la capa de aplicación van en aumento mientras que los ataques de la capa de red están disminuyendo (consulte la figura 28). Los investigadores de Radware sospechan que este cambio se puede atribuir al crecimiento en las botnets de la IoT. La tendencia es preocupante porque la capa de aplicación es tan diversa y tiene tantos dispositivos dentro, lo que significa que los ataques dirigidos a esta capa podrían tirar grandes porciones de Internet.

Cada vez más atacantes recurren a la capa de aplicaciones porque queda muy poco por explotar en la capa de red, según investigadores de Radware. Las botnets de la IoT también requieren menos recursos que las botnets de PC para compilar. Eso significa que los adversarios pueden invertir más recursos en el desarrollo de código avanzado y malware. Los operadores de la botnet multivector Mirai, conocida por los ataques de aplicaciones avanzadas, se encuentran entre los que realizan ese tipo de inversión.

Los “ataques de ráfaga” aumentan en complejidad, frecuencia y duración

Una de las tendencias de ataques DDoS más importantes que Radware observó en 2017 fue un aumento en los ataques de ráfaga corta, que se están volviendo más complejos, frecuentes y persistentes. Cuarenta y dos por ciento de las organizaciones en la investigación de Radware experimentaron este tipo de ataque DDoS en 2017 (figura 29). En la mayoría de los ataques, las ráfagas recurrentes duraron sólo unos minutos.

Figura 29 Experiencia con ataques DDoS en ráfagas recurrentes



Fuente: Radware

Las tácticas de ráfaga generalmente están dirigidas a sitios web de juegos y proveedores de servicios debido a la sensibilidad de sus objetivos a la disponibilidad del servicio y su incapacidad para sostener tales maniobras de ataque. Las ráfagas oportunas o aleatorias de altas tasas de tráfico durante un período de días o incluso semanas pueden dejar a estas organizaciones sin tiempo para responder, lo que causa interrupciones graves en el servicio.

Los investigadores de Radware dicen que los ataques de ráfagas:

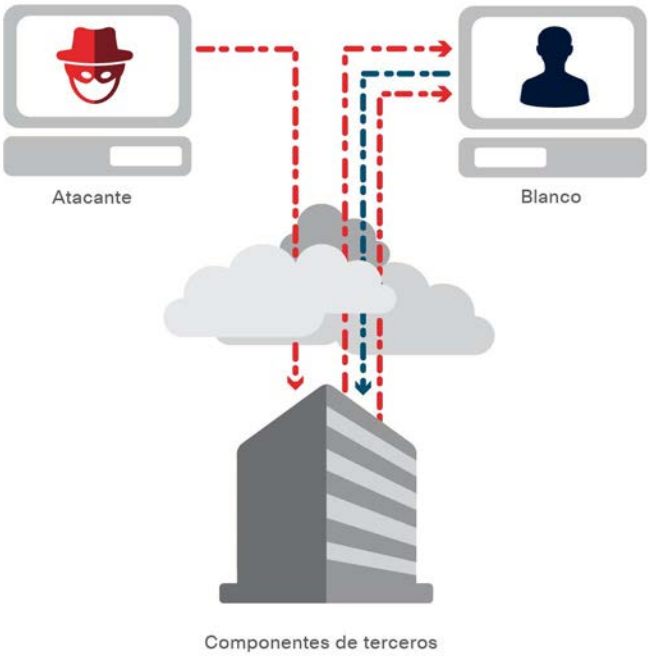
- Se componen de múltiples vectores de cambio. Los ataques se distribuyen geográficamente y se manifiestan como una serie sostenida de inundaciones SYN de alta precisión y alto volumen, inundaciones de ACK e inundaciones del Protocolo de Datagrama de Usuario (UDP) en múltiples puertos.
- Combinan ataques de gran volumen con diferentes duraciones, de dos a 50 segundos de alto tráfico de ráfaga con intervalos de aproximadamente cinco a 15 minutos.
- A menudo se combinan con otros ataques DDoS de larga duración.

Crecimiento en los ataques de amplificación de reflejo

Otra tendencia DDoS Radware observada durante 2017 es el crecimiento en la amplificación por reflejo de los ataques DDoS como un vector principal contra un amplio espectro de servicios. Según Radware, dos de cada cinco empresas experimentaron un ataque de amplificación de reflejo en el 2017. Un tercio de las organizaciones informó que fueron incapaces de mitigar estos ataques.

Un ataque de amplificación de reflejo utiliza un componente de terceros potencialmente legítimo para enviar tráfico de ataque a un objetivo, ocultando la identidad del atacante. Los atacantes envían paquetes a los servidores de reflector con una dirección IP a la IP del usuario destino. Eso hace que sea posible abrumar indirectamente al objetivo con paquetes de respuesta y agotar la utilización de los recursos del objetivo (ver figura 30).

Figura 30 Ataque de amplificación de reflejo



Fuente: Radware

Para ejecutar con éxito un ataque de amplificación de reflejo, los adversarios deben tener una capacidad de ancho de banda mayor que sus objetivos. Los servidores reflector lo hacen posible: el atacante simplemente refleja el tráfico de una o más máquinas de terceros. Dado que estos son servidores comunes, este tipo de ataque es particularmente difícil de mitigar. Ejemplos comunes incluyen:

Ataques reflectivos de amplificación de DNS
Este sofisticado ataque de denegación de servicio aprovecha el comportamiento de un servidor DNS para 10amplificación DNS, el atacante selecciona cuidadosamente una consulta DNS que da como resultado una respuesta larga que es hasta 80 veces más larga que la solicitud (por ejemplo, "ANY"). El atacante envía esta consulta utilizando una botnet a servidores DNS de terceros y suplantación de dirección IP de origen con la dirección IP del usuario destino. Los servidores DNS de terceros envían sus respuestas a la dirección IP del objetivo. Con esta técnica de ataque, una botnet relativamente pequeña puede canalizar una inundación volumétrica de grandes respuestas hacia el objetivo.

Reflejo de NTP
Este tipo de ataque de amplificación explota los servidores de protocolo de tiempo de red (NTP) a los que se accede públicamente para abrumar y agotar a los defensores con tráfico UDP. NTP es un antiguo protocolo de red para sincronización de reloj entre sistemas informáticos a través de redes conmutadas por paquetes. Todavía se usa ampliamente en Internet mediante computadoras de escritorio, servidores e incluso teléfonos para mantener sus relojes sincronizados. Varias versiones antiguas de servidores NTP contienen un comando llamado monlist, que envía al solicitante una lista de hasta los últimos 600 hosts que se conectaron al servidor consultado.

En un escenario básico, el atacante envía repetidamente la solicitud "get monlist" a un servidor NTP aleatorio y falsifica la dirección IP de origen para el servidor solicitante como servidor de destino. Respuestas del servidor NTP se dirigen entonces al servidor de destino para causar un aumento significativo en tráfico UDP del puerto fuente 123.

Reflejo de SSDP
Este ataque explota el Simple Service Discovery Protocol (SSDP), que se utiliza para permitir que los dispositivos Universal-Plug-and-Play (UPnP) transmitan su existencia. También ayuda a permitir el descubrimiento y control de dispositivos y servicios en red, como cámaras, impresoras conectadas a la red y muchos otros tipos de equipos electrónicos.

Una vez que un dispositivo UPnP está conectado a una red y después de recibir una dirección IP, el dispositivo puede anunciar sus servicios a otras computadoras en la red mediante el envío de un mensaje en una IP de multidifusión. Cuando una computadora recibe el mensaje de descubrimiento sobre el dispositivo, solicita una descripción completa de los servicios del dispositivo. El dispositivo UPnP luego responde directamente a esa computadora con una lista completa de los servicios que tiene para ofrecer.

Al igual que con los ataques DDoS amplificados por NTP y DNS, el atacante puede usar una botnet pequeña para consultar esa solicitud final de los servicios. El atacante luego suplanta la IP de origen a la dirección IP del usuario objetivo y apunta las respuestas directamente al objetivo.

Los defensores deben remediar las "rutas de fuga"

Una "ruta de fuga", definida por el socio de Cisco Lumeta, es una política o violación de segmentación o conexión no autorizada o mal configurada creada en Internet en una red empresarial o incluso desde la nube, que permite reenviar el tráfico a una ubicación en Internet, por ejemplo a un sitio web malicioso. Estas conexiones inesperadas también pueden ocurrir internamente entre dos segmentos de red diferentes que no deberían comunicarse entre sí. Por ejemplo, en entornos de infraestructura crítica, una ruta de fuga inesperada entre la planta de fabricación y los sistemas de TI comerciales podría indicar actividad maliciosa. Las rutas de fuga también pueden derivarse de enrutadores e interruptores configurados incorrectamente.

Una "ruta de fuga", definida por el socio de Cisco Lumeta, es una política o violación de segmentación o conexión no autorizada o mal configurada creada en Internet en una red empresarial o incluso desde la nube, que permite reenviar el tráfico a una ubicación en Internet, por ejemplo a un sitio web malicioso. Estas conexiones inesperadas también pueden ocurrir internamente entre dos segmentos de red diferentes que no deberían comunicarse entre sí. Por ejemplo, en entornos de infraestructura crítica, una ruta de fuga inesperada entre la planta de fabricación y los sistemas de TI comerciales podría indicar actividad maliciosa. Las rutas de fuga también pueden derivarse de enrutadores e interruptores configurados incorrectamente.

La detección de rutas de fuga existentes es crítica, ya que pueden explotarse en cualquier momento. Sin embargo, las rutas de fuga recientemente creadas son importantes para detectar en tiempo real, ya que son indicadores inmediatos de compromiso y están asociadas con la mayoría de los ataques avanzados, incluido el ransomware.

El análisis reciente de Lumeta de la infraestructura de TI en más de 200 organizaciones en varias industrias subraya la brecha de visibilidad del punto final. También muestra que muchas empresas subestiman significativamente el número de puntos finales en sus entornos de TI (consulte la figura 31). La falta de conocimiento sobre la cantidad de dispositivos IoT habilitados para IP conectados a la red suele ser una razón clave para subestimar los puntos finales.

Figura 31 Descripción de los puntos ciegos de la infraestructura en varias industrias

Lumeta Actual Customers	Government	Healthcare	Tech	Finance
Presumed endpoints	150,000	60,000	8000	600,000
Discovered endpoints	170,000	89,860	14,000	1,200,000
Endpoint visibility gap	12%	33%	43%	50%
Unmanaged networks	3278	24	5	771
Unauthorized or unsecured forwarding devices	520	75	2026	420
Known but unreachable networks	33,256	4	16,828	45
Leak paths to Internet identified on deployment	3000	120	9400	220

Source: Lumeta

Los investigadores de Lumeta sugieren que las vías de escape van en aumento, especialmente en entornos de nube, donde hay menos visibilidad de red y menos controles de seguridad.

Los actores malintencionados no siempre usan de inmediato las rutas de fuga que crean o encuentran. Cuando regresan a estos canales, los utilizan para instalar malware o ransomware, robar información y más. Los investigadores de Lumeta dicen que una razón por la cual las vías de escape a menudo no se detectan es porque los actores de la amenaza son expertos en encriptar y ocultar su actividad, por ejemplo, usando TOR. También tienen cuidado de usar las rutas de fuga juiciosamente, para no alertar a los equipos de seguridad sobre su actividad.

Los investigadores de Lumeta dicen que las brechas en las habilidades del equipo de seguridad, es decir, la falta de conocimiento fundamental sobre las redes, pueden interferir con la capacidad de las organizaciones para investigar y remediar los problemas de las fugas de manera oportuna. Una mejor colaboración entre los equipos de seguridad y de red puede ayudar a agilizar las investigaciones y la reparación de las vías de fuga.

Las herramientas para la automatización que brindan contexto de red también pueden brindar a los analistas de seguridad una idea de los posibles problemas de fuga. Además, la implementación de políticas de segmentación apropiadas puede ayudar a los equipos de seguridad a determinar rápidamente si la comunicación inesperada entre redes o dispositivos es maliciosa.

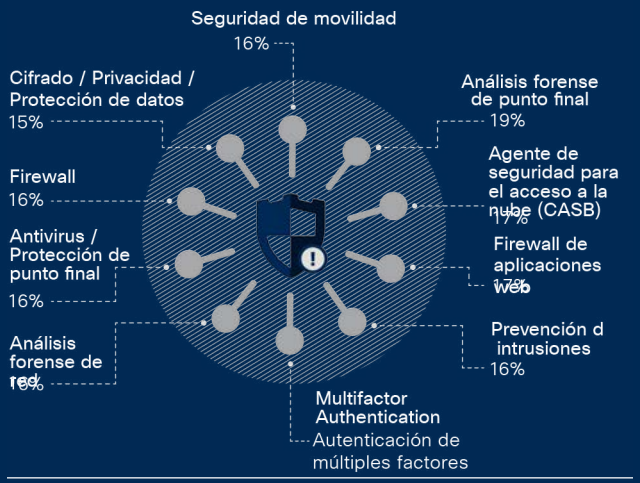
Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018: La falta de personal de seguridad impide que muchas organizaciones implementen nuevas capacidades cibernéticas

La grave escasez de personal sigue siendo un problema importante para los defensores. Como se señaló anteriormente, las brechas de habilidades pueden interferir con la capacidad de una organización para investigar y remediar ciertos tipos de amenazas.

Además, sin el talento adecuado, los defensores no pueden implementar nuevas tecnologías y procesos que podrían ayudar a fortalecer sus posturas de seguridad (figura 32).

Muchos profesionales de seguridad entrevistados para el Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 dijeron que, idealmente, automatizarían o subcontratarían más actividades rutinarias para redirigir al personal a actividades de mayor valor.

Figura 32 Las capacidades clave que los defensores agregarían, si los niveles de personal mejoran



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Las vulnerabilidades de los sistemas de control industrial ponen en riesgo la infraestructura crítica

Los sistemas de control industrial (ICS) están en el corazón de todos los sistemas de control de procesos y fabricación. ICS se conecta a otros sistemas electrónicos que son parte del proceso de control, creando un ecosistema altamente conectado de dispositivos vulnerables que muchos de los atacantes están ansiosos por comprometer.

Los actores de amenazas que quieren apuntar a los ICS para paralizar la infraestructura crítica participan activamente en la investigación y crean puntos pivotantes de puerta trasera para facilitar ataques futuros, según TrapX Security, un socio de Cisco que desarrolla defensas de ciberseguridad basadas en engaños. Entre los atacantes cibernéticos potenciales se encuentran expertos con conocimiento avanzado de sistemas de TI, arquitecturas ICS y los procesos que respaldan. Algunos también saben cómo programar los controladores y subsistemas de administración del ciclo de vida del producto (PLM).

Investigadores de amenazas con TrapX realizaron recientemente investigaciones sobre varios ataques cibernéticos dirigidos a ICS de clientes para ayudar a resaltar problemas inesperados con la ciberdefensa de ICS. Dos de los incidentes, que se describen a continuación, tuvieron lugar en 2017 y continúan bajo investigación.

Target : Gran empresa internacional de tratamiento de agua y procesamiento de residuos

Los atacantes utilizaron el servidor de la zona desmilitarizada (DMZ) de la compañía como un punto de pivote para comprometer la red interna. El equipo de operaciones de seguridad recibió alertas de la tecnología de seguridad engañosa integrada en la red DMZ. Esta subred física o lógica une las redes internas de las redes que no son de confianza, como Internet y protege otras infraestructuras internas. La investigación encontró que:

- El servidor DMZ fue violado debido a una mala configuración que permite las conexiones RDP.
- El servidor fue violado y controlado desde varias IP, que fueron conectadas a hacktivistas políticos hostiles a la planta.
- Los atacantes pudieron lanzar múltiples ataques importantes contra varias de las otras plantas de la red interna comprometida.

Target: Planta de energía

Los activos críticos de esta central eléctrica incluyen una gran infraestructura de ICS y los componentes necesarios de control de supervisión y adquisición de datos (SCADA) que administran y ejecutan sus procesos. La planta se considera infraestructura nacional crítica y está sujeta a escrutinio y supervisión por parte de la agencia de seguridad nacional responsable. Por lo tanto se considera una instalación de alta seguridad.

El CISO involucrado decidió implementar la tecnología de engaño para proteger los recursos de TI estándar de la planta de los ataques de ransomware. La tecnología también fue distribuida dentro de la infraestructura ICS. Poco después, el equipo de operaciones de seguridad recibió varias alertas que indicaban una infracción a los sistemas dentro de las operaciones críticas de la planta de infraestructura. Su inmediata investigación concluyó:

- Un dispositivo en la red de control de procesos intentaba interactuar con las trampas de engaño, que estaban camufladas como controladores PLM. Este fue un intento activo de mapear y comprender la naturaleza exacta de cada controlador PLM dentro de la red.
- El dispositivo comprometido normalmente se habría cerrado, pero un proveedor que realizó el mantenimiento no cerró la conexión cuando terminó. Esa supervisión dejó la red de control del proceso vulnerable a los atacantes.
- La información que los adversarios estaban recolectando es exactamente del tipo necesario para interrumpir la actividad de la planta y potencialmente causar un gran daño a las operaciones en curso de la planta.

Recomendaciones

Muchas infracciones de ICS comienzan con el compromiso de servidores y recursos informáticos vulnerables dentro de la red informática corporativa. Los grandes investigadores de TrapX recomiendan que las organizaciones tomen las siguientes medidas para reducir los riesgos y ayudar a garantizar la integridad de las operaciones dentro de sus instalaciones:

- Revisar proveedores, sistemas y asegurarse de que todos los parches y actualizaciones se apliquen con prontitud. (Si los parches no están disponibles, considere migrar a la nueva tecnología).
- Reducir el uso de sticks de memoria USB y unidades de DVD.
- Aislar los sistemas ICS de las redes informáticas. No permitir ninguna conexión directa entre los dos. Eso incluye conexiones de red, computadoras portátiles y tarjetas de memoria.
- Implementar políticas que limiten severamente el uso de las redes ICS para cualquier cosa que no sean operaciones esenciales. Reducir el acceso a estaciones de trabajo y monitores ICS con acceso externo al navegador de Internet. Asumir que estas políticas fallarán y planificar en consecuencia.
- Investigar y eliminar todas las contraseñas incorporadas o las contraseñas predeterminadas en su red de producción. Y siempre que sea posible, implementar la autenticación de dos factores.
- Revisar los planes de recuperación de desastres luego de un ciberataque importante.

Para estudios de casos adicionales, consulte el documento de investigación de TrapX Security, *Anatomy of an Attack: Industrial Control Systems Under Siege.*

Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018: Más ataques de OT y de IoT en el horizonte

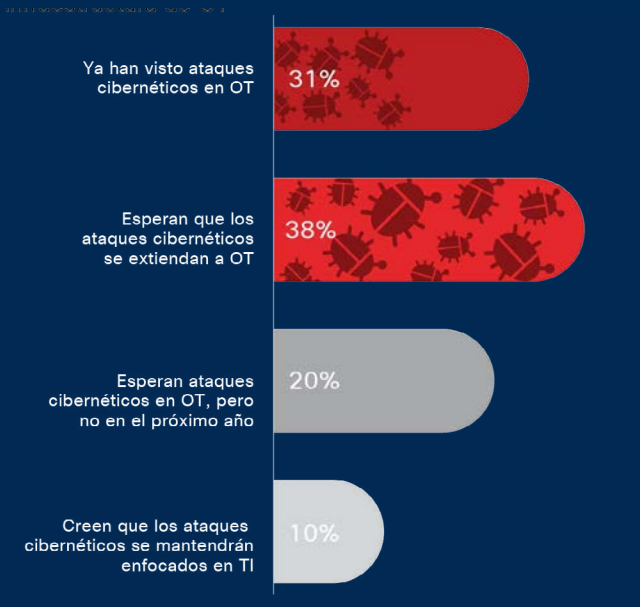
Los ataques dirigidos a la tecnología operativa (OT), como los dispositivos ICS e IoT, todavía son poco comunes y muchos profesionales de la seguridad no los han experimentado de primera mano. Pero de acuerdo con las investigaciones para el **Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018**, los profesionales de la seguridad esperan que ocurran dichos ataques, y están tratando de determinar cómo responderán a ellos.

Los profesionales de seguridad reconocen que estos sistemas a menudo tienen pocas protecciones y software sin parchear y desactualizado, haciéndolos vulnerables a los ataques.

"Todavía tenemos dispositivos de OT que tienen 25 años y compresores y máquinas que tienen 40 años", dijo uno de los encuestados. "Los profesionales de TI están acostumbrados al horario. [Ellos dicen] 'Dime cuando Windows X ya no es compatible' o 'Mira, esta versión de Oracle está en su EOL [fin de vida útil]'. No existe tal cosa en el entorno de OT."

Pocos profesionales de seguridad pueden hablar con confianza sobre cuestiones relacionadas con la protección de OT en sus organizaciones. Eso es porque no tienen o anticipan agregar mucho OT, o porque las implementaciones de IoT son nuevas. De estos profesionales, el 31 por ciento dijo que sus organizaciones ya habían experimentado ciberataques en la infraestructura de OT, mientras que el 38 por ciento dijo que esperaba que los ataques se extendieran desde TI a OT el próximo año (figura 33).

Figura 33 El treinta y uno por ciento de las organizaciones han experimentado ataques cibernéticos en la infraestructura de OT



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

VULNERABILIDADES Y PARCHEO

En medio del caos de las preocupaciones de seguridad, los defensores pueden perder de vista las vulnerabilidades que afectan su tecnología. Pero puede estar seguro de que los atacantes están prestando atención y calculando cómo explotar estas debilidades potenciales para lanzar ataques.

Hubo un momento en que reparar las vulnerabilidades conocidas dentro de los 30 días se consideró la mejor práctica. Ahora, esperar todo ese tiempo para remediarlo podría aumentar el riesgo de una organización de ser atacada porque los actores de amenazas se están moviendo más rápido para lanzar y explotar vulnerabilidades activas. Las organizaciones también deben evitar descuidar brechas de seguridad pequeñas, pero significativas que podrían beneficiar a los adversarios, especialmente durante la fase de reconocimiento de los ataques cuando buscan vías hacia los sistemas.

Las vulnerabilidades prevalentes en 2017 incluyen errores de desbordamiento de búfer, Apache Struts

Los errores de desbordamiento de búfer encabezaron la lista de vulnerabilidades de Enumeración de debilidad común (Common Weakness Enumeration, CWE) rastreadas por Cisco en 2017, aunque otras categorías mostraron un movimiento hacia arriba y hacia abajo.

Las vulnerabilidades de validación de entrada aumentaron, mientras que los errores de búfer disminuyeron (figura 34).

Figura 34 Actividad de la categoría de amenaza CWE

Categoría de amenaza	Ene-Sep 2016	Ene-Sep 2017	Cambio
CWE-11 9: Errores del búfer	493	403	(-22%)
CWE-20: Validación de entrada	227	268	+15%
CWE-264: Permisos y privilegios de acceso	137	163	+18%
CWE-200: Fuga / divulgación de información	125	250	+100%
CWE-310: Temas criptográficos	27	17	(-37%)
CWE-78: Inyecciones de comando del OS	7	15	+114%
CWE-59: Siguiente enlace	5	0	

Fuente: Cisco Security Research

Al examinar los avisos críticos (figura 35), las vulnerabilidades de Apache Struts seguían siendo prominentes en 2017. Apache Struts es un marco de código abierto para crear aplicaciones de Java que es ampliamente utilizado. Las vulnerabilidades de Apache Struts estuvieron implicadas en fallas de seguridad en 2017 que involucraron a los principales corredores de datos.

Si bien Apache tiende a identificar vulnerabilidades y ofrecer parches rápidamente, las soluciones de infraestructura como Apache Struts pueden ser difíciles de parchar sin interrumpir el rendimiento de la red. Como se discutió en los Reportes de seguridad anteriores de Cisco,[19] vulnerabilidades de software de código abierto o de terceros pueden requerir el parcheo manual, lo que puede no hacerse tan frecuentemente como el parcheo automatizado de los proveedores de software estándar. Eso les da a los actores maliciosos un mayor margen de tiempo para lanzar ataques.

La exploración profunda de los sistemas operativos hasta la biblioteca o el nivel de archivo individual puede proporcionar a las organizaciones inventarios de los componentes de las soluciones de código abierto.

Figura 35 Asesoramiento crítico y actividades de ataque

Fuente: Cisco Security Research

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

19 *Reporte Semestral de Ciberseguridad de Cisco 2017:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Las vulnerabilidades del IoT y de las bibliotecas se hicieron más grandes en 2017

Entre el 1 de octubre de 2016 y el 30 de septiembre de 2017, los investigadores de amenazas de Cisco descubrieron 224 nuevas vulnerabilidades en productos que no son de Cisco, de las cuales, 40 vulnerabilidades estaban relacionadas con bibliotecas de software de terceros incluidas en estos productos y 74 estaban relacionadas con dispositivos IoT (figura 36).

El número relativamente grande de vulnerabilidades en las bibliotecas apunta a la necesidad de profundizar en soluciones de terceros que proporcionan el marco para muchas redes empresariales. Los defensores deben suponer que las bibliotecas de software de terceros pueden ser objetivos para los atacantes; no es suficiente simplemente asegurarse de que se está ejecutando la última versión del software, o que no se han informado CVE abiertas (vulnerabilidades comunes). Los equipos de seguridad deben consultar con frecuencia los parches y revisar las prácticas de seguridad de los proveedores externos. Los equipos podrían, por ejemplo, solicitar que los proveedores brinden declaraciones de ciclo de vida de desarrollo seguro.

Otra práctica recomendada para examinar el software de terceros es ayudar a garantizar que las funciones de actualización automática o comprobación de actualización se ejecuten de forma segura. Por ejemplo, cuando se inicia una actualización, los profesionales de la seguridad deben estar seguros de que la comunicación de ese software se realiza a través de un canal seguro (como SSL) y de que el software está firmado digitalmente. Ambas cosas son necesarias: Si solo se utilizan firmas digitales, pero no un canal seguro, un atacante podría interceptar el tráfico y posiblemente reemplazar una actualización con una versión anterior del software que está firmado digitalmente, pero puede contener vulnerabilidades. Si solo se usa un canal seguro, un atacante podría poner en peligro el servidor de actualización del proveedor y reemplazar la actualización con malware.

Figura 36 Biblioteca de terceros y vulnerabilidades del IoT

Fuente: Cisco Security Research

Vulnerabilidades de Spectre y Meltdown: la preparación proactiva puede acelerar la remediación

El anuncio en enero de 2018 de las vulnerabilidades de Spectre y Meltdown, que podría permitir a los atacantes poner en peligro los datos de las plataformas con procesadores informáticos de última generación, generó inquietud sobre la capacidad de los profesionales de seguridad para proteger los datos de los ataques. Las vulnerabilidades podrían permitir a los atacantes ver los datos de las aplicaciones en la memoria del chipset, con el potencial de daños generalizados, ya que los microprocesadores afectados se encuentran en todo, desde teléfonos móviles hasta hardware del servidor.

Las amenazas planteadas por las vulnerabilidades Spectre y Meltdown resaltan la importancia de comunicarse con las organizaciones de seguridad sobre soluciones tales como parches y también aseguran que terceros proveedores, como proveedores de la nube y de la cadena de suministro, se adhieran a las mejores prácticas para remediar las lagunas de seguridad planteadas por tales vulnerabilidades. Los equipos de respuesta a incidentes de seguridad del producto, o PSIRT (como el PSIRT de Cisco), están diseñados para responder rápidamente a los anuncios de vulnerabilidad, proporcionar parches y asesorar a los clientes sobre cómo evitar los riesgos.

Las organizaciones necesitan planear para que ocurran vulnerabilidades como Spectre y Meltdown, en lugar de esperar que no ocurran. La clave es prepararse para tales anuncios y contar con sistemas para mitigar el daño potencial. Por ejemplo, los equipos de seguridad deben realizar un inventario proactivo de los dispositivos bajo su control y documentar las configuraciones en las características en uso, ya que algunas vulnerabilidades dependen de la configuración e impactan en la seguridad solo cuando ciertas características están activadas.

Los equipos de seguridad también deberían consultar a terceros proveedores, como proveedores de la nube, sobre sus procesos de actualización y parcheo. Las organizaciones deben pedir transparencia a sus proveedores de servicios de nube en términos de cómo remediar dichas vulnerabilidades y qué tan rápido responden a las alertas. Pero al final, la responsabilidad de la preparación recae en las propias organizaciones; deben comunicarse con las organizaciones PSIRT y establecer procesos para responder rápidamente a las vulnerabilidades.

Para obtener más información, lea la publicación del blog de Talos sobre Spectre y Meltdown.

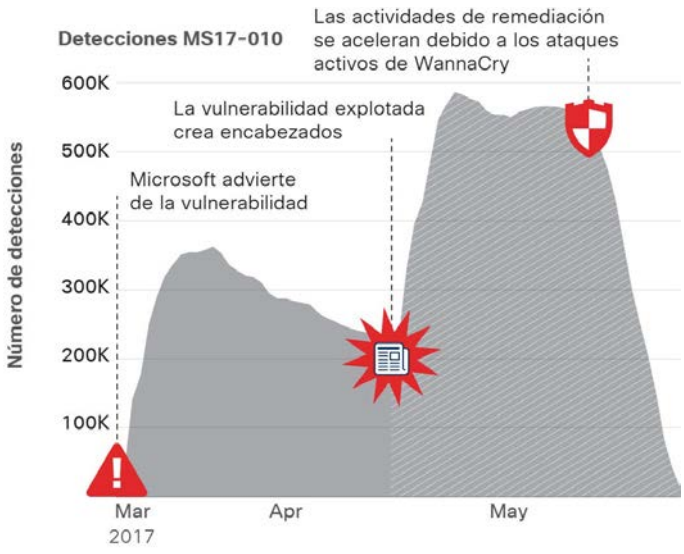
Los exploits activos alimentan la carrera para remediar, a excepción de los dispositivos IoT

Qualys, Inc., socio y proveedor de Cisco de soluciones de cumplimiento y seguridad basadas en la nube, analizó retrospectivamente el comportamiento de administración de parches de las empresas antes y después de la campaña WannaCry que afectó a muchas organizaciones en todo el mundo en mayo de 2017.

Para propagarse, aprovechó una vulnerabilidad de seguridad de Microsoft Windows llamada EternalBlue, que fue filtrada por el grupo de hackers Shadow Brokers a mediados de abril de 2017. (Para más información sobre este tema, vea "Están por ahí: los defensores deben prepararse para enfrentarse a nuevas amenazas basadas en la red que se propagarán por sí mismas en 2018", en la página 6.)

El 14 de marzo de 2017, Microsoft emitió una actualización de seguridad (MS17-010) alertando a los usuarios sobre una vulnerabilidad crítica en su servidor SMB de Microsoft Windows. La figura 37 muestra cómo el número de dispositivos detectados con los picos de vulnerabilidad y luego disminuye gradualmente entre mediados de marzo y mediados de abril a medida que las organizaciones escanean sus sistemas y aplican el parche.

Figura 37 Comportamiento de parcheado antes y después de la campaña WannaCry



Fuente: Qualys

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Sin embargo, un número importante de dispositivos seguía sin parches a mediados de abril. Luego, el 14 de abril, Shadow Brokers lanzó el exploit activo para atacar esa vulnerabilidad conocida en varias versiones de Microsoft Windows. La figura 37 muestra que la cantidad de dispositivos detectados con la vulnerabilidad casi se duplicó poco después. Eso sucedió cuando las organizaciones se enteraron del exploit y su potencial para impactar las versiones compatibles y no compatibles de Windows a través de un control remoto de Qualys que utilizó una parte del código de explotación.

Pero incluso después de que se lanzó el exploit, el parche general no se produjo hasta mediados de mayo, después de que el ataque WannaCry apareciera en los titulares de todo el mundo. La figura 37 muestra la curva de remediación pronunciada después de esa campaña. Hacia finales de mayo, quedaban algunos dispositivos sin parchear.

La investigación de Qualys sobre el comportamiento de parchado de sus clientes indica que se necesita un evento importante para motivar a muchas organizaciones a parchear vulnerabilidades críticas; incluso el conocimiento de un exploit activo no es suficiente para acelerar la corrección. Y en el caso de la campaña de WannaCry, las empresas tuvieron acceso al parche para la vulnerabilidad de Microsoft durante dos meses antes de los ataques de ransomware.

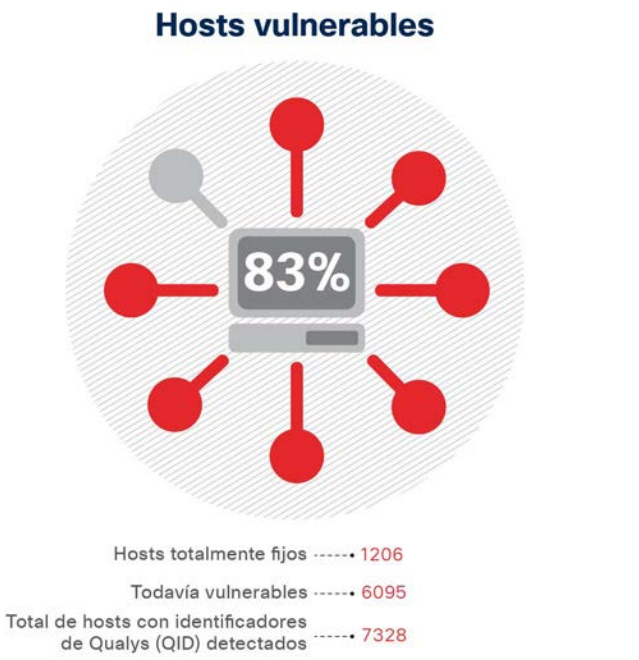
Otro factor, según lo descrito por los investigadores con Lumeta, socio de Qualys y Cisco, fue que los puntos finales de TI desconocidos, no administrados, impostores y en la sombra, quedaron sin parchear. Los atacantes fueron capaces de aprovechar estos puntos ciegos. Sin el conocimiento de estos sistemas, los escáneres de vulnerabilidad no pudieron evaluar y recomendar el parcheo de estos sistemas, dejándolos vulnerables a WannaCry.

La aplicación de parches es aún más lenta, o no ocurre en absoluto, para los dispositivos IoT

Qualys también examinó las tendencias de parcheo para dispositivos del IoT. Los dispositivos en la muestra incluían sistemas HVAC habilitados para IP, cerraduras de puertas, paneles de alarmas contra incendios y lectores de tarjetas.

Los investigadores buscaron específicamente dispositivos IoT vulnerables a varias amenazas conocidas, incluido el malware Devil´s Ivy que explota una vulnerabilidad en un código llamado gSOAP que se usa ampliamente en productos de seguridad física, y Mirai, una botnet IoT que se conecta a máquinas específicas a través de ataques de fuerza bruta contra servidores Telnet.

Figura 38 Tendencias de parcheo para dispositivos IoT



Fuente: Qualys

Qualys había detectado 7328 dispositivos en total, pero solo 1206 habían sido fijados (ver figura 38). Eso significa que el 83 por ciento de los dispositivos IoT en la muestra todavía tienen vulnerabilidades críticas. Mientras que Qualys no halló pruebas de agentes de amenaza dirigidos activamente a esas vulnerabilidades, las organizaciones todavía eran susceptibles al ataque. Sin embargo, no parecen motivadas a acelerar la corrección.

Hay varias explicaciones posibles para la inercia del parcheo, según Qualys. Algunos dispositivos pueden no ser actualizables, por ejemplo. Otros pueden requerir apoyo directo del vendedor. Además, no siempre está claro quién dentro de la organización es responsable del mantenimiento de los dispositivos IoT. Por ejemplo, un equipo de ingeniería que se hace cargo del sistema HVAC de la empresa puede no estar al tanto de los riesgos de TI que podrían afectar a ese sistema, o incluso de que el sistema esté habilitado para IP.

Sin embargo, más preocupante es la baja cantidad de dispositivos IoT que detectó Qualys. Es probable que el número real sea mucho mayor porque las organizaciones simplemente no saben cuántos dispositivos IoT están conectados a su red. Esa falta de visibilidad los pone en serio riesgo de compromiso (vea la página 34 para más información sobre este tema).

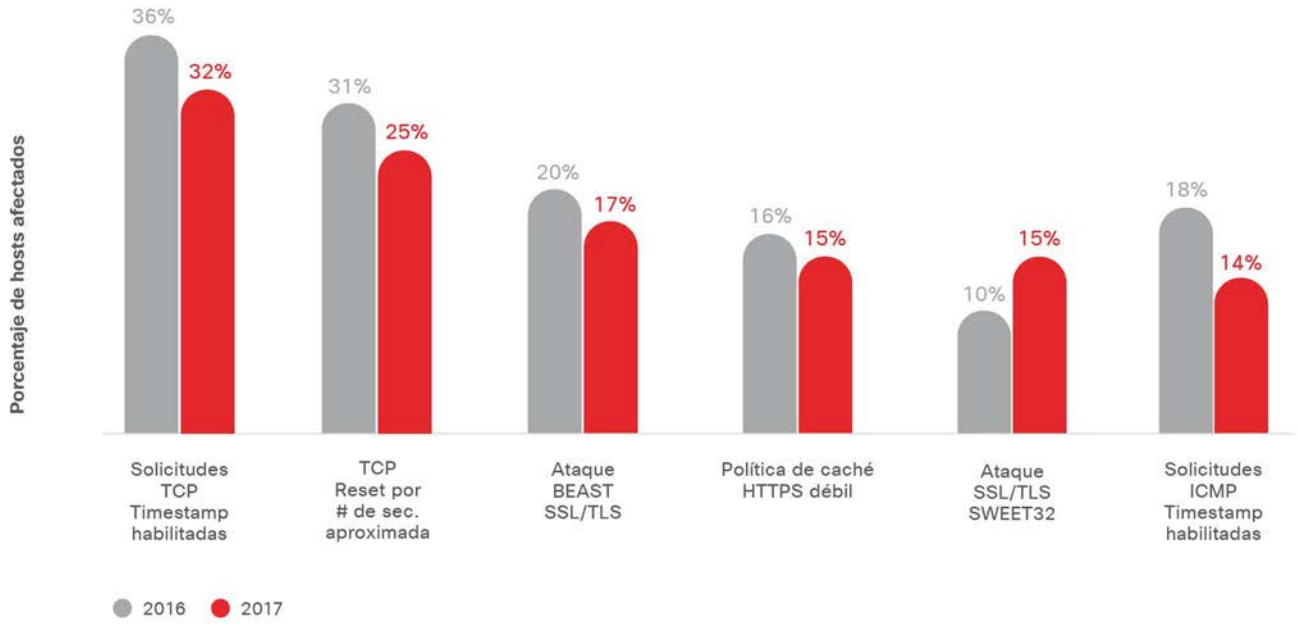
Un primer paso para abordar este problema es inventariar todos los dispositivos IoT en la red. Las organizaciones pueden determinar si los dispositivos son escaneados y si siguen siendo compatibles con los proveedores, y qué empleados de la empresa los poseen y los utilizan. Las organizaciones también pueden mejorar la seguridad de IoT al tratar todos los dispositivos IoT como otros dispositivos informáticos, lo que ayuda a garantizar que reciban actualizaciones de firmware y que se actualicen periódicamente.

Las vulnerabilidades más comunes son de baja gravedad, pero de alto riesgo

Las vulnerabilidades de baja gravedad a menudo no se remedian durante años porque las empresas o no saben que existen o no las consideran riesgos importantes, según los expertos en seguridad de SAINT Corporation, una compañía de soluciones de seguridad y socio de Cisco. Sin embargo, estas brechas de seguridad pequeñas, pero significativas, podrían proporcionar a los adversarios caminos hacia los sistemas.

Los investigadores de SAINT examinaron los datos de exposición a la vulnerabilidad recopilados de más de 10,000 hosts en 2016 y 2017. La compañía desarrolló una lista de las principales vulnerabilidades detectadas con mayor frecuencia en todas las organizaciones del estudio, lo que indica que las vulnerabilidades de baja gravedad ocurren con mayor frecuencia (consulte la figura 39). (Nota: algunas organizaciones incluidas en la investigación tenían más de un host).

Figura 39 Vulnerabilidades de baja gravedad más a menudo detectadas, 2016-2017



Fuente: SAINT Corporation

Aquí le damos una mirada más cercana a las tres principales vulnerabilidades de baja gravedad en la figura 39 y por qué podrían ser valiosas para los actores amenazantes:

Solicitudes TCP Timestamp habilitadas
Los TCP timestamps ofrecen información sobre cuánto tiempo ha estado en funcionamiento una máquina o cuándo se reinició por última vez, lo que podría ayudar a los adversarios a conocer qué tipos de vulnerabilidades de parches podría tener que explotar la máquina. Además, los programas de software pueden usar los timestamp del sistema para generar un generador de números aleatorios para crear claves de cifrado.

Restablecimiento de TCP por número de secuencia aproximado
Los atacantes remotos pueden adivinar los números de secuencia y provocar una denegación de servicio a las conexiones TCP persistentes al inyectar repetidamente un paquete TCP RST, especialmente en los protocolos que usan conexiones de larga duración, como el Border Gateway Protocol.

“Ataque “BEAST”
Un atacante puede usar la vulnerabilidad Exploit Contra SSL / TLS (BEAST) para lanzar un ataque de “hombre en el medio” (MiTM) para esencialmente "leer" el contenido protegido que se intercambia entre las partes. (Nota: se trata de un complicado ataque a ejecutar, a medida que el actor de la amenaza también debe tener el control del navegador del lado del cliente para leer e inyectar paquetes de datos muy rápidamente).

Los investigadores de seguridad con SAINT no detectaron adversarios que exploten activamente estas vulnerabilidades de baja gravedad durante su análisis.

Las vulnerabilidades que se muestran en la figura 39 son conocidas por la comunidad de seguridad, pero algunas de ellas normalmente no se señalarán ni provocarán fallas automáticas durante una verificación rutinaria de cumplimiento, como una auditoría del estándar de seguridad de datos de la industria (PCI DSS). No son vulnerabilidades críticas definidas por las normas pertinentes para esa industria. Cada industria evalúa la criticidad de las vulnerabilidades de forma diferente.

Además, la mayoría de las vulnerabilidades comunes que son de baja gravedad mostradas en la figura 39 no se pueden remediar fácilmente, o en absoluto, a través de la administración de parches porque surgen de problemas de configuración o de certificados de seguridad (por ejemplo, cifrados SSL débiles o un certificado SSL autofirmado).

Las organizaciones deben actuar con prontitud para abordar las vulnerabilidades de baja gravedad que pueden presentar riesgos. Deben evaluar e identificar las prioridades de remediación en función de cómo perciben el riesgo, en lugar de confiar en las calificaciones de terceros o el uso parcial de un sistema de puntuación, como un puntaje básico de CVSS o una determinada calificación de cumplimiento. Solo las organizaciones conocen sus entornos únicos y sus estrategias de gestión de riesgos.

Parte II:
El panorama de los defensores

Parte II: El panorama de los defensores

Sabemos que los atacantes están evolucionando y adaptando sus técnicas a un ritmo más rápido que los defensores. También están armando y probando en el campo sus hazañas, estrategias de evasión y habilidades para que puedan lanzar ataques de magnitud creciente. Cuando los adversarios golpeen inevitablemente a sus organizaciones, ¿estarán los defensores preparados y qué tan rápido podrán recuperarse? Depende en gran medida de los pasos que están tomando hoy en día para fortalecer su postura de seguridad.

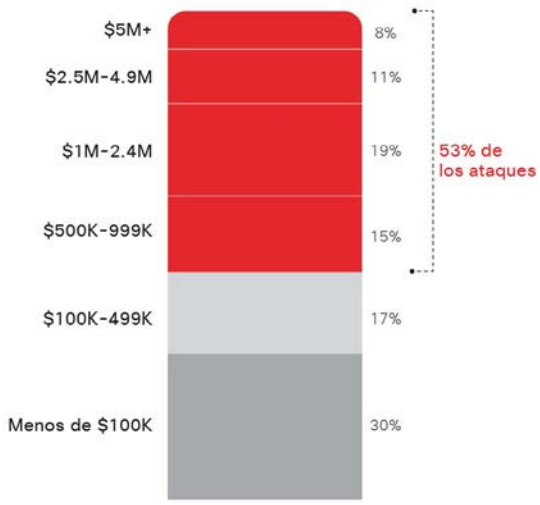
Lo que hemos aprendido a través de nuestra investigación para el Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 es que los defensores tienen mucho trabajo por hacer y desafíos por superar. Para evaluar las percepciones de los defensores sobre el estado de la seguridad en sus organizaciones, preguntamos a los gerentes de seguridad de la información (CISO) y de operaciones de seguridad (SecOps) en varios países y organizaciones de diversos tamaños sobre sus recursos y procedimientos de seguridad.

El Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018 ofrece información sobre prácticas de seguridad actualmente en uso y compara estos resultados con los de los estudios de 2017, 2016 y 2015. La investigación implicó a más de 3600 personas en 26 países.

El costo de los ataques

El miedo a las violaciones se basa en el costo financiero de los ataques, que ya no es un número hipotético. Las infracciones causan un daño económico real a las organizaciones, daños que pueden tardar meses o años en resolverse. Según los encuestados del estudio, más de la mitad (53 por ciento) de todos los ataques resultaron en daños financieros de más de USD $500,000, que incluyen, entre otros, pérdida de ingresos, clientes, oportunidades y costos de bolsillo (figura 40).

Figura 40 El cincuenta y tres por ciento de los ataques resultan en daños de $500,000 o más



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

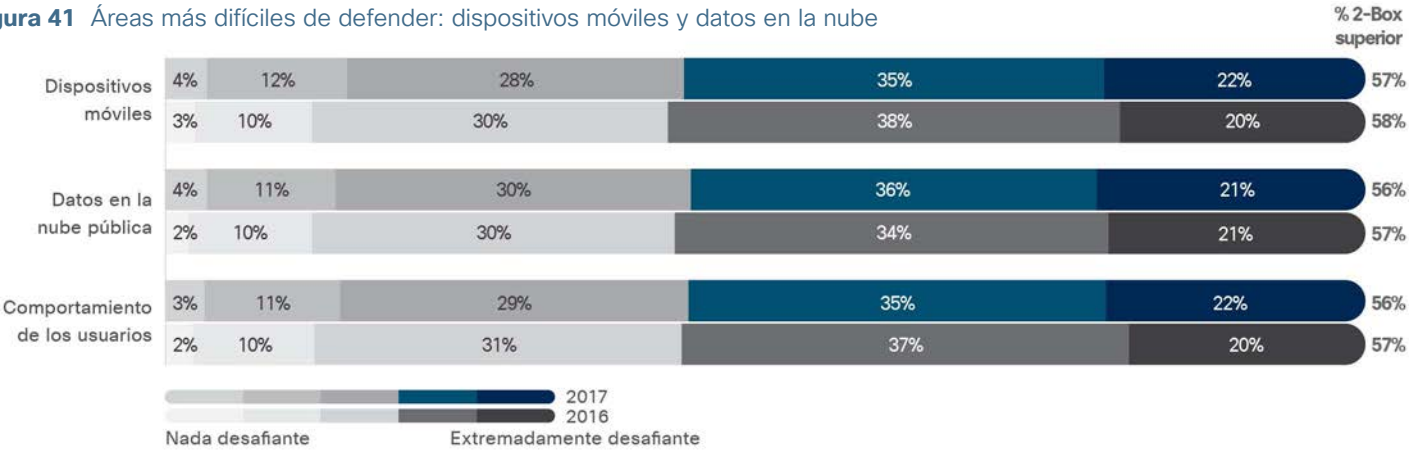
Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Retos y obstáculos

En sus esfuerzos por proteger sus organizaciones, los equipos de seguridad se enfrentan a muchos obstáculos. Las organizaciones deben defender varias áreas y funciones, lo que aumenta los desafíos de seguridad.

Las áreas y funciones más desafiantes para defender son los dispositivos móviles, los datos en la nube pública y el comportamiento del usuario (figura 41).

Figura 41 Áreas más difíciles de defender: dispositivos móviles y datos en la nube



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Los profesionales de la seguridad citan el presupuesto, la interoperabilidad y el personal como sus principales limitaciones a la hora de administrar la seguridad (figura 42). La falta de personal capacitado también se menciona como un desafío para la adopción de tecnología y procesos de seguridad avanzados. En 2017, el 27 por ciento citó la falta de talento como un obstáculo, en comparación con el 25 por ciento en 2016 y el 22 por ciento en 2015.

Figura 42 El mayor obstáculo para las restricciones presupuestarias de seguridad

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

La falta de talento calificado encabeza la lista de obstáculos en todas las industrias y en todas las regiones. "Si pudiera mover una varita mágica y obtener un 10 por ciento más de personas para quitarle algo de la carga a las personas que realmente sienten la presión debido a la gran demanda de sus áreas de servicio particulares, sería un tipo muy, muy feliz", dijo un CISO para una gran firma de servicios profesionales.

Si bien la brecha de talento experto es un desafío continuo, las organizaciones informan que están buscando y contratando más recursos para sus equipos de seguridad. En 2017, la mediana del número de profesionales de seguridad en las organizaciones fue de 40, un aumento significativo con respecto a la mediana de 2016 de 33 (figura 43).

Figura 43 Las organizaciones contratan a más profesionales de seguridad

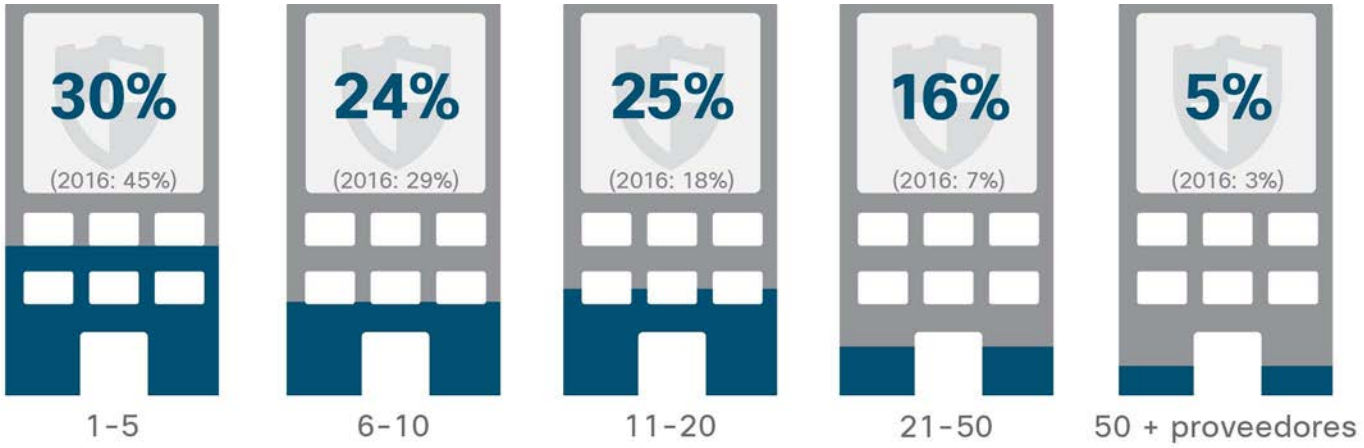
Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Complejidad creada por los proveedores en coordinación

Los defensores están implementando una combinación compleja de productos de una muestra representativa de proveedores: un arsenal de herramientas que pueden nublar en lugar de aclarar el panorama de la seguridad. Esta complejidad tiene muchos efectos posteriores sobre la capacidad de una organización para defenderse de los ataques, como mayor riesgo de pérdidas.

En 2017, el 25 por ciento de los profesionales de seguridad dijeron que usaron productos de 11 a 20 proveedores, en comparación con el 18 por ciento de los profesionales de seguridad en 2016. También en 2017, el 16 por ciento dijo que usan entre 21 y 50 proveedores, en comparación con el 7 por ciento de los encuestados en 2016 (figura 44) .

Figura 44 Las organizaciones utilizaron más proveedores de seguridad en 2017

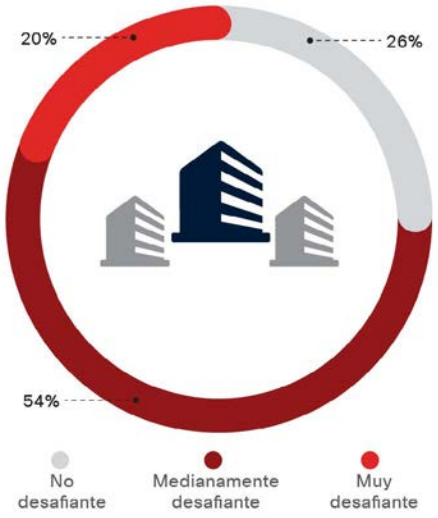


Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

A medida que aumenta el número de proveedores, también aumenta el desafío de orquestar alertas de estas soluciones de muchos proveedores. Como se ve en la figura 45, 54 por ciento de los profesionales de seguridad dijeron que la administración de alertas de múltiples proveedores es un tanto desafiante, mientras que el 20 por ciento dijo que es muy desafiante.

Figura 45 El desafío de organizar alertas



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

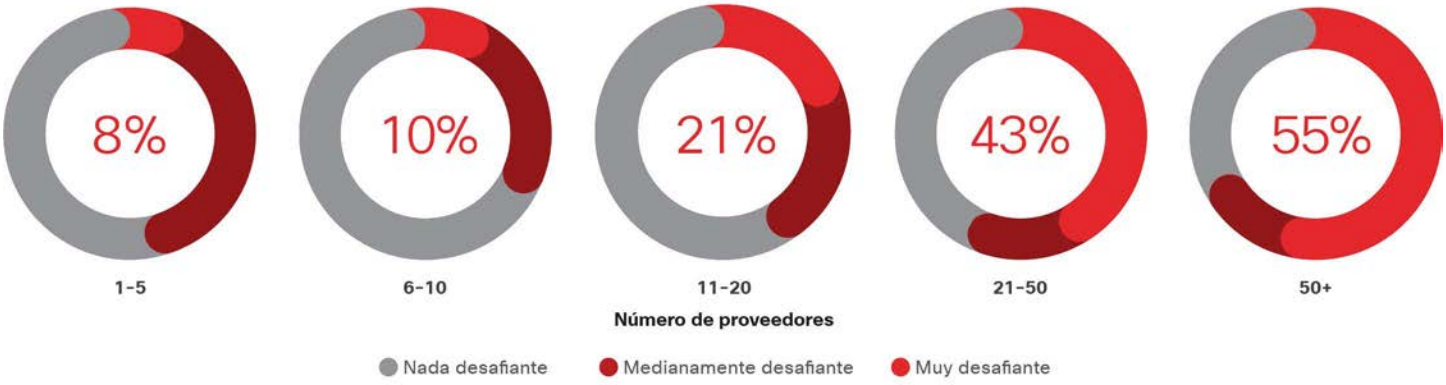
Los equipos de seguridad enfrentan desafíos para orquestar alertas de múltiples proveedores

Como se ve en la figura 46, entre organizaciones con solo 1 a 5 proveedores, el 8 por ciento dijo que orquestar alertas es muy desafiante.

Entre las organizaciones que utilizan más de 50 proveedores, el 55 por ciento dijo que dicha orquestación es muy desafiante.

Cuando las organizaciones no pueden organizar y comprender las alertas que reciben, las amenazas legítimas pueden pasar desapercibidas.

Figura 46 A medida que aumentan los proveedores, también aumenta el desafío de orquestar alertas de seguridad



	Educación	Servicios financieros	Gobierno	Atención médica	Fabricación	Farma	Venta por menor	Telecomunicaciones	Transporte	Utilidad/ energía
Muy desafiante	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

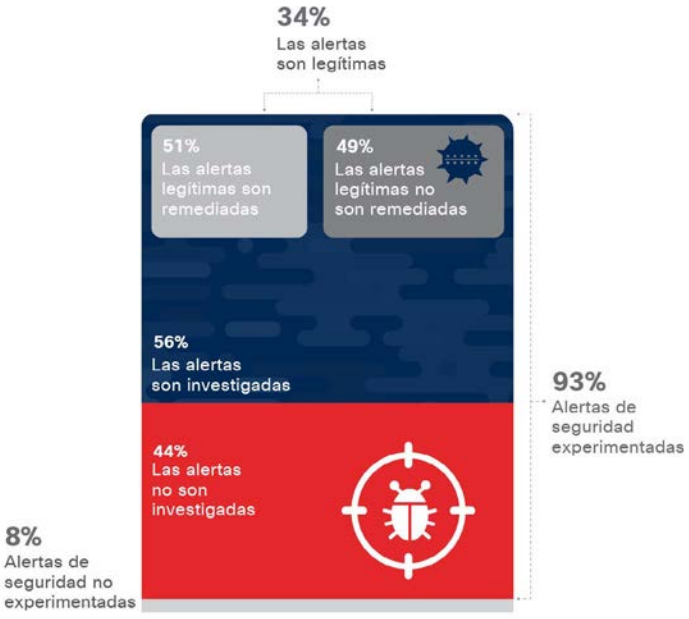
Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Los datos de los encuestados indican que continúan existiendo lagunas entre las alertas generadas, las que se han investigado y las que finalmente se remedian. Como se muestra en la figura 47:

- Entre las organizaciones que reciben alertas de seguridad, un promedio de 44 por ciento de las alertas no son investigadas.
- Aquellas alertas investigadas, 34 por ciento se consideran legítimas.
- De las consideradas legítimas, 51 por ciento de las alertas son remediadas.
- Casi la mitad (49%) de las alertas legítimas no son remediadas.

Este proceso deja muchas alertas legítimas sin remediar. Una razón parece ser la falta de personal y recursos humanos capacitados que puedan facilitar la demanda para investigar todas las alertas.

Figura 47 Muchas alertas de amenaza no son investigadas o remediadas



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Impacto: Escrutinio público de las violaciones, mayor riesgo de pérdidas

"Hay dos tipos de empresas: aquellas que han sido violadas y aquellas que no saben que han sido violadas", dijo un encuestado del estudio de referencia. (La respuesta se hace eco de una cita conocida del ex CEO de Cisco, John Chambers: "Hay dos tipos de empresas: las que han sido hacked y las que aún no saben que han sido hacked".) Aunque las organizaciones intentan enfrentar los futuros desafíos de seguridad con una preparación adecuada, los profesionales esperan ser víctimas de una brecha y pasar al escrutinio público. El cincuenta y cinco por ciento de los encuestados dijeron que sus organizaciones tuvieron que manejar el escrutinio público de una violación en el último año (figura 48).

Figura 48 El cincuenta y cinco por ciento de las organizaciones han tenido que gestionar el escrutinio público de una violación

2016 (n=2824), 2017 (n=3548)

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

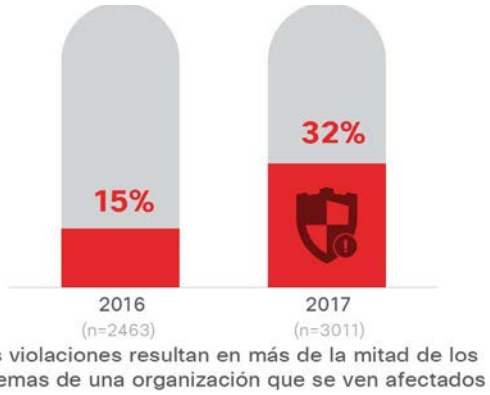
Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

> *"La norma será que casi todas las compañías de Fortune 500 hayan sido violadas en los últimos 24 meses. Tienes que estar preparado para eso, especialmente desde una perspectiva de marketing o de relaciones públicas".*
>
> *—Encuesta del estudio de referencia*

Las organizaciones informaron significativamente más infracciones de seguridad que afectan a más del 50 por ciento de los sistemas (figura 49), que las organizaciones que respondieron el año pasado. En 2017, el 32 por ciento de los profesionales de seguridad dijeron que las infracciones afectaban a más de la mitad de sus sistemas, en comparación con el 15 por ciento en 2016. Las funciones comerciales más comúnmente afectadas por las violaciones son operaciones, finanzas, propiedad intelectual y reputación de marca (figura 50).

En entornos de seguridad complejos, las organizaciones son más propensas a lidiar con infracciones. De las organizaciones que usan de 1 a 5 proveedores, el 28 por ciento dijo que tenía que manejar el escrutinio público después de una violación; ese número aumentó a 80 por ciento para las organizaciones que usan más de 50 proveedores (figura 51). Eso puede deberse a una mayor visibilidad de las amenazas, que más productos pueden permitir.

Figura 49 Fuerte aumento en las brechas de seguridad que afectan a más del 50 por ciento de los sistemas

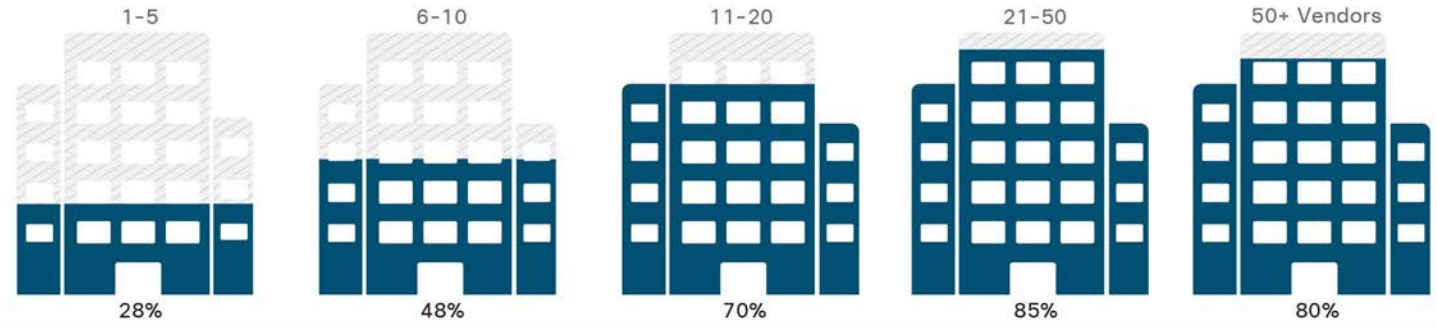


Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Figura 50 Es muy probable que las operaciones y las finanzas se vean afectadas por las brechas de seguridad

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Figura 51 El ochenta por ciento de las organizaciones que usan más de 50 proveedores tuvieron que manejar el escrutinio de las infracciones públicas



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

El valor de un marco integrado

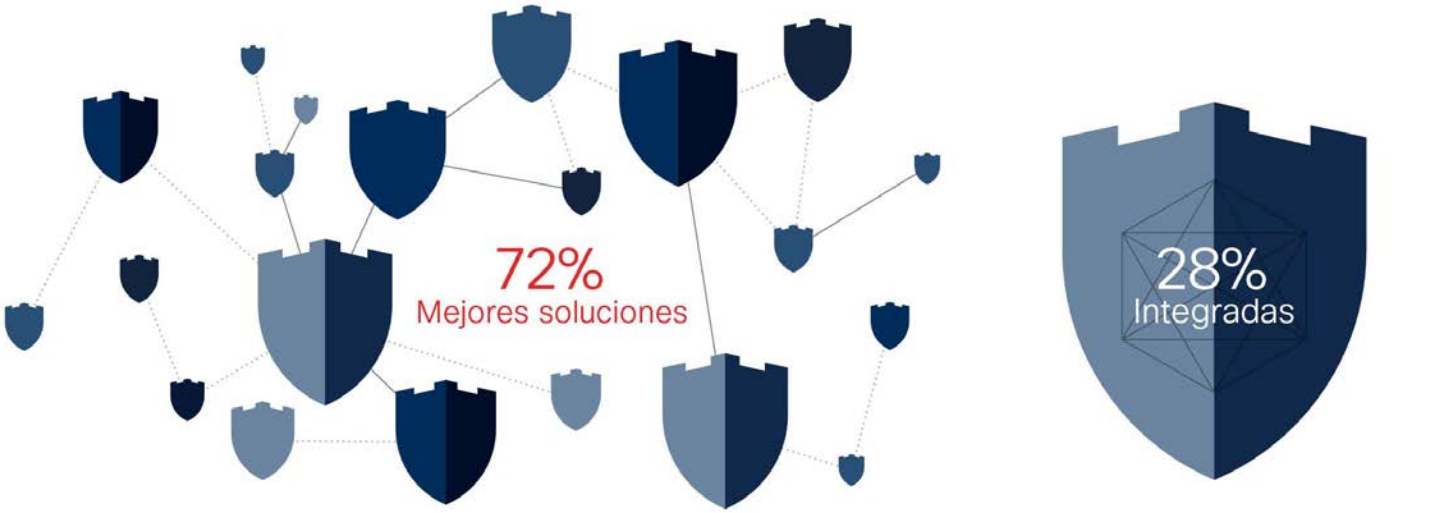
¿Por qué utilizar una multitud de productos de muchos proveedores si el entorno resultante es difícil de manejar? El mejor escenario , en el cual los equipos de seguridad eligen la mejor solución para cada necesidad de seguridad, es la clave. Los profesionales de la seguridad que practican el mejor enfoque de su clase también creen que es más rentable, según una investigación del estudio de referencia.

Al comparar lo mejor de su clase para soluciones integradas, el 72 por ciento de los profesionales de seguridad dijeron que compraron las mejores soluciones de puntos para satisfacer necesidades específicas, en comparación con el 28 por ciento que compraron productos destinados a trabajar juntos como una solución integrada (consulte la figura 52). De las organizaciones que adoptan el mejor enfoque, el 57 por ciento menciona la relación costo-efectividad, mientras que el 39 por ciento dijo que el mejor enfoque es más fácil de implementar.

Curiosamente, las organizaciones que adoptan un enfoque integrado de seguridad citan razones similares para su elección. Cincuenta y seis por ciento dijo que un enfoque integrado es más rentable. Cuarenta y siete por ciento dijo que es más fácil de implementar.

La facilidad de implementación se cita cada vez más como un factor para utilizar un enfoque de arquitectura integrada: Solo el 33 por ciento de las organizaciones dijo que la facilidad de implementación fue una razón para elegir un enfoque integrado en 2016, en comparación con el 47 por ciento en 2017. Si bien las soluciones de un único proveedor pueden no ser prácticas para todas las organizaciones, los compradores de soluciones de seguridad deben ayudar a garantizar que las soluciones trabajen en conjunto para reducir el riesgo y aumentar la eficacia.

Figura 52 El 72% compra las mejores soluciones porque satisfacen necesidades específicas



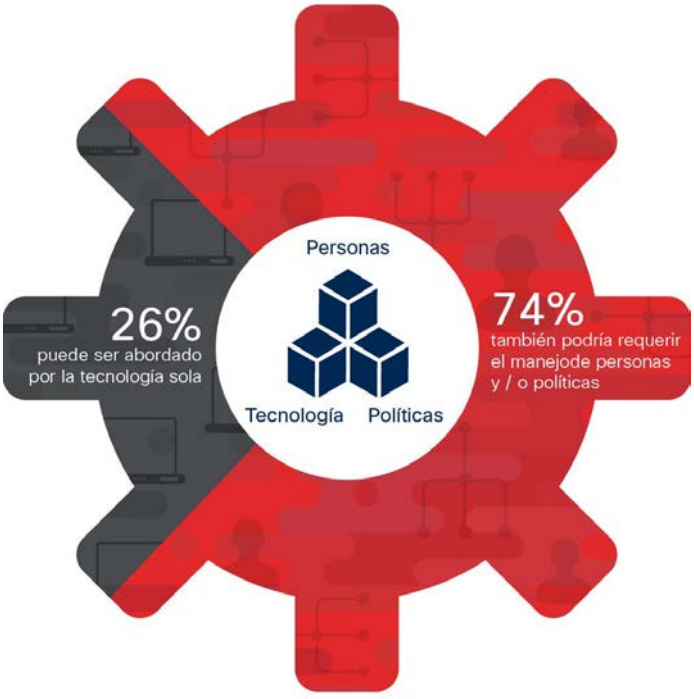
Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Servicios: gestión de personas y políticas, así como de la tecnología

Ante las posibles pérdidas y el impacto adverso en los sistemas, las organizaciones deben ir más allá de depender exclusivamente de la tecnología para la defensa. Eso significa examinar otras oportunidades para mejorar la seguridad, como aplicar políticas o capacitar a los usuarios. Este enfoque holístico de la seguridad se puede ver en los problemas identificados durante Intellegence Lead Security Assurance (conocida como evaluación del "Red Team") proporcionada por el equipo de asesoramiento de seguridad de servicios avanzados de Cisco.

Al examinar los datos de recomendación de varias evaluaciones del Red Team realizadas en 2017, los miembros del equipo de servicios identificaron tres capacidades defensivas clave: personas, políticas y tecnología. Si una organización utilizara solo la tecnología para remediar las vulnerabilidades de seguridad, solo resolvería el 26 por ciento de los problemas que se identificaron durante las simulaciones de ataque del Red Team . Eso dejaría a 74 por ciento de los problemas sin resolver (ver figura 53). Del mismo modo, si las organizaciones usan solo políticas para abordar problemas de seguridad, resolverían solo el 10 por ciento de los problemas; con capacitación del usuario para las personas, solo el 4 por ciento de los problemas. Las tres áreas de defensa deben abordarse en concierto.

Figura 53 Solo el 26% de los problemas de seguridad pueden abordarse con la tecnología sola



Fuente: Cisco Security Research

La figura 54 ofrece ejemplos de problemas identificados por categoría durante las simulaciones. Algunos problemas, como las contraseñas débiles, cruzan las tres categorías. El fortalecimiento de las contraseñas puede requerir mejoras en las personas (capacitación del usuario), productos (configuración de servidores para contraseñas más complejas) y políticas (establecimiento de requisitos de contraseña más estrictos).

Figura 54 Tipos de problemas descubiertos durante simulaciones de ataques categorizados por requisitos de remediación

Fuente: Cisco Security Research

Las organizaciones pueden aumentar sus posibilidades de gestionar con éxito los tres factores si ayudan a garantizar que la seguridad esté integrada en todas las capas de la organización, no de forma generalizada aquí y allá. También deben evitar confiar únicamente en productos o mejoras técnicas para reparar la seguridad. Para que los productos sean exitosos, las organizaciones necesitan comprender e implementar políticas y procesos sensatos para la tecnología.

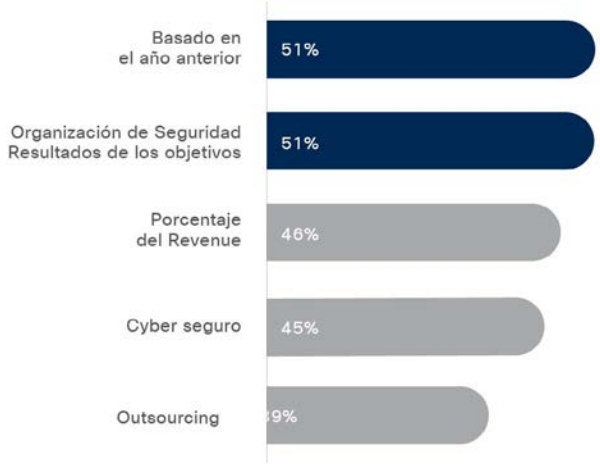
Expectativas: Invertir en tecnología y capacitación

Los profesionales de la seguridad anticipan por completo que las amenazas que enfrentan sus organizaciones seguirán siendo complejas y desafiantes.

Esperan que los actores maliciosos desarrollen formas más sofisticadas y dañinas de violar las redes. También saben que el lugar de trabajo moderno crea condiciones que favorecen a los atacantes: La movilidad de los empleados y la adopción de dispositivos IoT brindan a los atacantes nuevas oportunidades. Junto con el aumento de las amenazas, muchos profesionales de la seguridad esperan que estén bajo escrutinio adicional: de reguladores, ejecutivos, partes interesadas, socios y clientes.

Para reducir la probabilidad de riesgo y pérdidas, los defensores deben determinar dónde invertir los recursos limitados. En su mayor parte, los profesionales de la seguridad dijeron que los presupuestos de seguridad permanecen relativamente estables, a menos que una brecha pública importante provoque un replanteamiento y nuevos gastos para la tecnología y los procesos. El cincuenta y uno por ciento dijo que el gasto en seguridad se basa en los presupuestos de años anteriores, mientras que un porcentaje igual de encuestados dijo que los objetivos de resultados impulsan el presupuesto (figura 55). La mayoría de los líderes de seguridad dijeron que creen que sus compañías están gastando apropiadamente en seguridad.

Figura 55 El cincuenta y uno por ciento dijo que el gasto en seguridad es impulsado por los presupuestos de años anteriores



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Al planificar los presupuestos, muchas empresas trabajan sistemáticamente a través de listas de deseos desarrolladas como parte de planes de seguridad integrales, priorizando las inversiones a medida que los recursos se vuelven disponibles. Las inversiones pueden restablecerse si se exponen nuevas vulnerabilidades, ya sea por un incidente interno, una infracción pública muy publicitada o una evaluación de riesgos de terceros de rutina.

Los factores más importantes que impulsan las inversiones futuras y, por lo tanto, las mejoras en la tecnología y los procesos, parecen ser infracciones. En 2017, el 41 por ciento de los profesionales de seguridad dijeron que las brechas de seguridad están impulsando una mayor inversión en tecnologías y soluciones de seguridad, un aumento del 37 por ciento en 2016 (figura 56). El cuarenta por ciento dijo que las infracciones están impulsando una mayor inversión en la capacitación del personal de seguridad, en comparación con el 37 por ciento en 2016.

Figura 56 Las infracciones de seguridad están impulsando la inversión en tecnología y capacitación

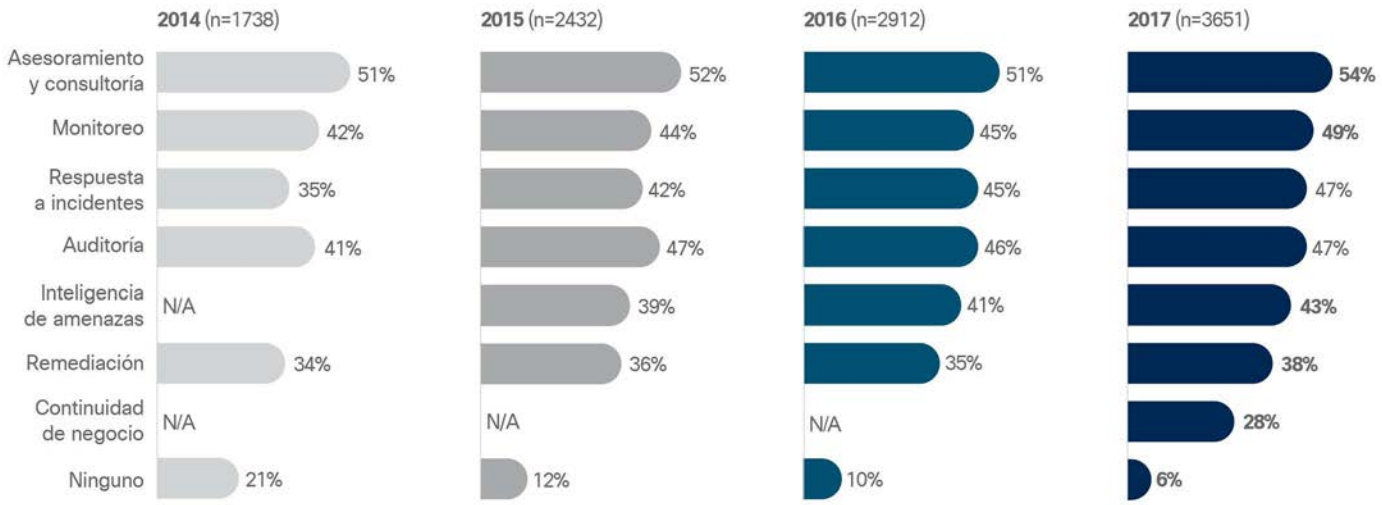
Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Los profesionales de la seguridad esperan gastar más en herramientas que usan artificial Intelligence y learning machine en un intento por mejorar las defensas y ayudar a soportar la carga de trabajo. Además, planean invertir en herramientas que brinden salvaguardas para sistemas críticos, como servicios de infraestructura crítica.

Para estirar los recursos y fortalecer las defensas, las organizaciones están aumentando su dependencia de la contratación externa. Entre los profesionales de seguridad, el 49 por ciento dijo que subcontrató servicios de monitoreo en 2017, en comparación con el 44 por ciento en 2015; 47 por ciento de respuesta a incidentes tercerizados en 2017, en comparación con 42 por ciento en 2015 (figura 57).

Figura 57 El uso de la subcontratación para el monitoreo y la respuesta a incidentes crece año tras año



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Para obtener más resultados del Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018, consulte el Apéndice en la **página 64**.

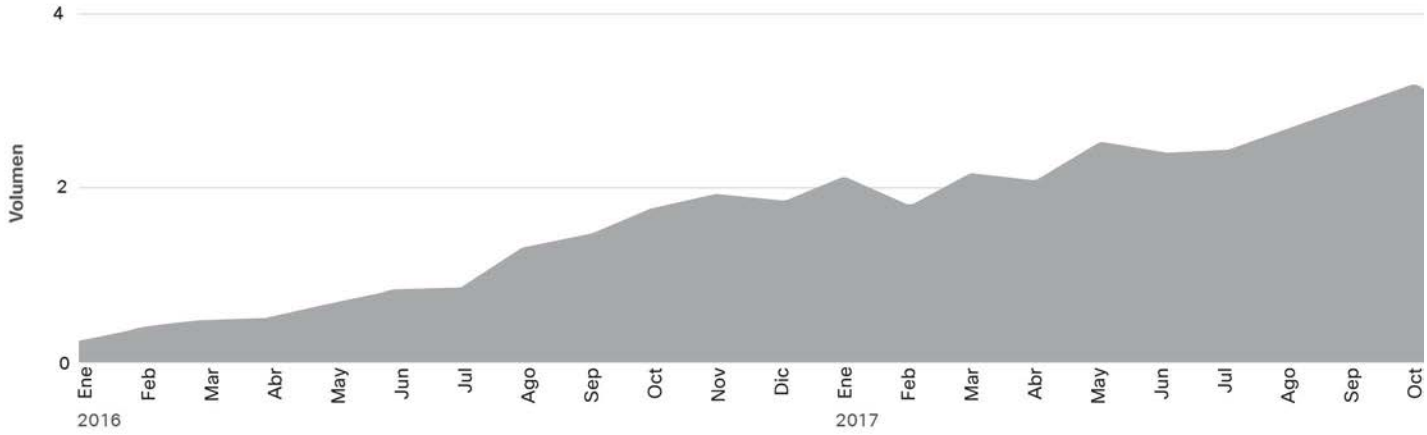
Conclusión

Conclusión

En el moderno panorama de las amenazas, los adversarios son expertos en evadir la detección. Tienen herramientas más efectivas, como encriptación, y tácticas más avanzadas e inteligentes, como el abuso de servicios legítimos de Internet, para ocultar su actividad y socavar las tecnologías de seguridad tradicionales. Y están desarrollando constantemente sus tácticas para mantener su malware fresco y efectivo. Incluso las amenazas conocidas por la comunidad de seguridad pueden tardar mucho tiempo en identificarse.

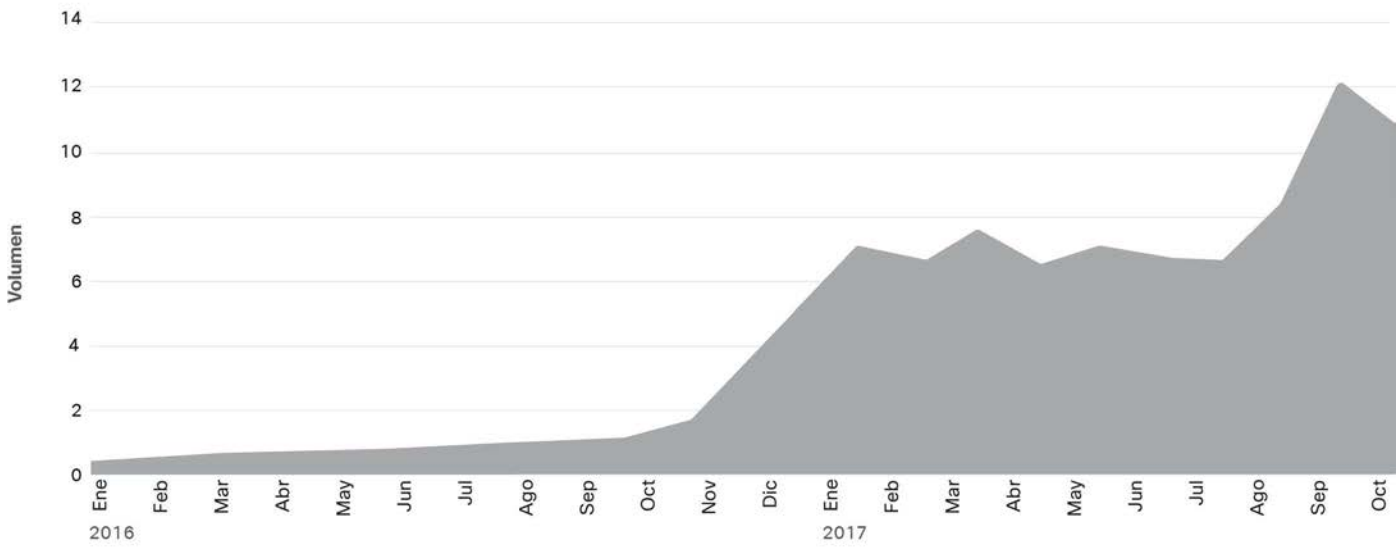
Una razón por la que los defensores luchan para superar el caos de la guerra con los atacantes y realmente ven y entienden lo que está sucediendo en el panorama de las amenazas, es el gran volumen de tráfico potencialmente malicioso que enfrentan. Nuestra investigación muestra que el volumen de eventos totales vistos por productos de seguridad de punto final basados en la nube de Cisco se multiplicó por cuatro desde enero de 2016 hasta octubre de 2017 (consulte la figura 58). "Total de eventos" es el recuento de todos los eventos, benignos o maliciosos, vistos por nuestros productos de seguridad de punto final basados en la nube durante el período observado.

Figura 58 Volumen Total de eventos



Fuente: Cisco Security Research

Figura 59 Volumen total de malware



Fuente: Cisco Security Research

Nuestros productos de seguridad también vieron un aumento de once veces en el volumen general de malware durante ese mismo período, como muestra la figura 59.

Las tendencias en el volumen de malware tienen un impacto en el tiempo de detección de los defensores (TTD), que es una medida importante para que cualquier organización comprenda qué tan bien se desempeñan sus defensas de seguridad bajo la presión del aluvión constante de malware desplegado por los adversarios.

La mediana de Cisco TTD de 4.6 horas para el período de noviembre de 2016 a octubre de 2017 ayuda a ilustrar el desafío permanente de identificar amenazas rápidamente en el paisaje caótico de la amenaza. Aun así, esa cifra está muy por debajo del TTD medio de 39 horas que reportamos en noviembre de 2015, después de que comenzamos a rastrear TTD, y la mediana de 14 horas reportada en el Reporte Anual de Ciberseguridad de Cisco 2017 para el período de noviembre de 2015 a octubre de 2016.[20]

El uso de la tecnología de seguridad basada en la nube ha sido un factor clave para ayudar a Cisco a conducir y mantener su TTD medio en un nivel bajo. La nube ayuda a escalar y mantener el rendimiento ya que tanto el volumen de eventos totales como los puntos finales de orientación de malware continúan aumentando. Las soluciones de seguridad local tendrían dificultades para ofrecer la misma flexibilidad. Diseñar uno a escala que pueda manejar más de 10 veces la capacidad de volumen de eventos maliciosos durante un período de dos años y mantener o aumentar los tiempos de respuesta sería una tarea muy difícil y costosa para cualquier organización.

20 *Reporte Anual de Ciberseguridad de Cisco 2017:* cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.

Cisco define "el tiempo de detección" o TTD, como la ventana de tiempo entre un compromiso y la identificación de una amenaza. Determinamos esta ventana de tiempo utilizando telemetría de seguridad opt-in recopilada a partir de los productos de seguridad de Cisco implementados en todo el mundo. Utilizando nuestra visibilidad global y un modelo de análisis continuo, podemos medir desde el momento en que se descarga un archivo malicioso en un punto final hasta el momento en que se determina que es una amenaza que no se clasificó en el momento del encuentro.

El "TTD mediano" es el promedio de las medianas mensuales para el período observado.

Acerca de Cisco

Acerca de Cisco

Cisco ofrece seguridad cibernética inteligente para el mundo real, brindando el portafolio de soluciones de protección contra amenazas más completo de la industria,en el conjunto con el mas amplio set de vectores de ataque. Nuestro enfoque centrado en las amenazas reduce la complejidad y la fragmentación, al mismo tiempo que proporcionamos mayor visibilidad, control consistente y una protección avanzada durante y después de un ataque.

Los investigadores de amenazas del ecosistema de Inteligencia Colectiva de Seguridad de Cisco (CSI) reúnen, bajo un solo paraguas, la inteligencia de amenazas líder de la industria usando telemetría obtenida de la vasta huella de dispositivos y sensores, fuentes públicas, privadas y la comunidad de código abierto. Esto equivale a una entrada diaria de miles de millones de solicitudes web y millones de correos electrónicos, muestras de malware e intrusiones en la red.

Nuestra sofisticada infraestructura y sistemas consumen esta telemetría, ayudando a los sistemas machine learning e investigadores a rastrear amenazas en redes, centros de datos, puntos finales, dispositivos móviles, sistemas virtuales, web y correo electrónico. Y desde la nube, para identificar las causas de raíz y el alcance de los brotes. La inteligencia resultante se traduce en protecciones en tiempo real para nuestras ofertas de productos y servicios que se entregan de forma inmediata a clientes de Cisco.

Para obtener más información sobre nuestro enfoque de seguridad centrado en las amenazas, visite cisco.com/go/security.

CONTRIBUYENTES DEL REPORTE ANUAL DE CIBERSEGURIDAD DE CISCO 2018

Queremos agradecer a nuestro equipo de investigadores de amenazas y otros expertos en la materia dentro de Cisco, así como a nuestros socios tecnológicos, que contribuyeron al **Reporte Anual de Ciberseguridad de Cisco 2018**. *Su investigación y perspectivas son esenciales para ayudar a Cisco a brindar a las empresas de seguridad de la comunidad y a los usuarios información relevante sobre la complejidad y la vastedad del panorama global y moderno de ciberamenazas, y las mejores prácticas actuales y el conocimiento para mejorar sus defensas.*

Nuestros socios tecnológicos también desempeñan un papel vital para ayudar a nuestra empresa a desarrollar seguridad simple, abierta y automatizada que permita a las organizaciones integrar las soluciones que necesitan para proteger sus entornos.

Cisco Advanced Malware Protection (AMP) para Cisco AMP for Endpoints

Cisco AMP for Endpoints proporciona capacidades automatizadas de prevención, detección y respuesta en una única solución. Continuamente monitorea y analiza en busca de signos de actividad maliciosa para descubrir amenazas que eluden la seguridad de primera línea y representan el mayor riesgo para las organizaciones. Utiliza una variedad de técnicas de detección que incluyen sandboxing avanzado, prevención de vulnerabilidades, así como aprendizaje de máquina para detectar y mitigar rápidamente las amenazas. Cisco AMP for Endpoints es la única solución que ofrece seguridad retrospectiva para responder rápidamente a las amenazas e identificar el alcance, el punto de origen y cómo contener la amenaza para que las organizaciones permanezcan protegidas.

Cisco Cloudlock

Cisco Cloudlock proporciona soluciones al Agente de seguridad para el acceso a la nube (CASB) que ayudan a las organizaciones a usar la nube de forma segura. Ofrece visibilidad y control para entornos de software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS) en usuarios, datos y aplicaciones. También proporciona inteligencia de ciberseguridad procesable a través de su CyberLab dirigido por científicos de datos y análisis de seguridad de fuentes múltiples.

Cisco Cognitive Threat Analytics

Cisco Cognitive Threat Analytics es un servicio basado en la nube que detecta infracciones, malware que opera dentro de redes protegidas y otras amenazas de seguridad por medio de análisis estadísticos de datos de tráfico de red. Aborda las lagunas en las defensas basadas en el perímetro mediante la identificación de los síntomas de una infección de malware o violación de datos mediante el análisis del comportamiento y la detección de anomalías. Cognitive Threat Analytics se basa en el modelado estadístico avanzado y el aprendizaje de máquina para identificar de forma independiente las nuevas amenazas, aprender de lo que ve y adaptarse con el tiempo.

Cisco Product Security Incident Response Team (PSIRT)

El Cisco Product Security Incident Response Team (PSIRT) es una organización mundial dedicada que gestiona la recepción, investigación y divulgación pública de información sobre vulnerabilidades de seguridad y cuestiones relacionadas con productos y redes de Cisco. El PSIRT recibe Reportes de investigadores independientes, organizaciones de la industria, proveedores, clientes y otras fuentes relacionadas con la seguridad de los productos o redes.

Cisco Security Incident Response Services (CSIRS)

El equipo de Cisco Security Incident Response Services (CSIRS) está formado por respondedores de incidentes de clase mundial que tienen la tarea de ayudar a los clientes de Cisco antes, durante y después de que experimenten un incidente. El CSIRS aprovecha el mejor personal de su clase, soluciones de seguridad de nivel empresarial, técnicas de respuesta de vanguardia y las mejores prácticas aprendidas durante años para combatir a los adversarios y asegurar que nuestros clientes puedan defenderse de forma más dinámica, así como responder y recuperarse rápidamente de cualquier ataque.

Grupo de inteligencia de Cisco Talos

El grupo de inteligencia de Cisco Talos es uno de los equipos de inteligencia de amenazas comerciales más grandes del mundo, compuesto por investigadores, analistas e ingenieros de primer nivel. Estos equipos cuentan con el respaldo de sistemas sofisticados de telemetría sin igual para crear inteligencia de amenazas precisa, rápida y procesable para clientes, productos y servicios de Cisco. El grupo Talos

defiende a los clientes de Cisco contra amenazas conocidas y emergentes, descubre nuevas vulnerabilidades en un software común y bloquea amenazas en la naturaleza antes de que puedan dañar aún más a Internet en general. La inteligencia de Talos es el núcleo de los productos de Cisco que detectan, analizan y protegen contra amenazas conocidas y emergentes. Talos mantiene los conjuntos de reglas oficiales de Snort.org, ClamAV y SpamCop, además de lanzar muchas herramientas de investigación y análisis de código abierto.

Cisco Threat Grid

Cisco Threat Grid es una plataforma de inteligencia de amenazas y análisis de malware. Threat Grid realiza análisis estáticos y dinámicos en muestras sospechosas de malware que provienen de clientes e integraciones de productos ubicados en todo el mundo. Cientos de miles de muestras, en una variedad de tipos de archivos, se envían a la nube de Threat Grid todos los días a través de la interfaz de usuario del portal Threat Grid Cloud o mediante la API Threat Grid. Threat Grid también se puede implementar como un dispositivo en el sitio.

Cisco Umbrella

Cisco Umbrella es una puerta de enlace de Internet segura que proporciona la primera línea de defensa contra amenazas en Internet dondequiera que vayan los usuarios. Debido a que está integrado en la base de Internet, Umbrella ofrece visibilidad completa de la actividad en todas las ubicaciones, dispositivos y usuarios. Al analizar y aprender de esta actividad, Umbrella descubre automáticamente la infraestructura del atacante preparada para las amenazas actuales y emergentes, y bloquea de forma proactiva las solicitudes antes de establecer una conexión.

Investigación en seguridad y operaciones (SR & O)

Investigación en seguridad y operaciones (SR & O) es responsable de la gestión de amenaza y vulnerabilidad de todos los productos y servicios de Cisco, incluyendo el líder de la industria Cisco PSIRT . SR & O ayuda a los clientes a comprender el cambiante panorama de amenazas en eventos como Cisco Live y Black Hat, así como a través de la colaboración con sus colegas de Cisco y la industria. Además, SR & O ofrece nuevos servicios tales como Cisco Custom Threat Intelligence (CTI), que puede identificar indicadores de compromiso que no han sido detectados o mitigados por las infraestructuras de seguridad existentes.

Organización de Seguridad y Confianza

La Organización de Seguridad y Confianza de Cisco subraya nuestro compromiso de abordar dos de los problemas más críticos que son prioritarios para las juntas directivas y los líderes mundiales por igual. Las misiones principales de la organización incluyen proteger a los clientes públicos y privados de Cisco, ayudar a habilitar y garantizar el ciclo de vida de desarrollo seguro y los esfuerzos confiables de los sistemas en la cartera de productos y servicios de Cisco, y proteger a la empresa de las amenazas en constante evolución. Cisco adopta un enfoque holístico para la seguridad y la confianza generalizadas, que incluye personas, políticas, procesos y tecnología. La Organización de Seguridad y Confianza impulsa la excelencia operacional, centrándose en InfoSec, Ingeniería de Confianza, Protección de Datos y Privacidad, Seguridad en la Nube, Transparencia y Validación, e Investigación de Seguridad Avanzada y Gobierno. Para obtener más información, visite trust.cisco.com.

Socios tecnológicos del Reporte Anual de Ciberseguridad de Cisco 2018

ANOMALI®

El conjunto de soluciones de inteligencia de amenazas de Anomali faculta a las organizaciones para detectar, investigar y responder a las amenazas activas de ciberseguridad. La galardonada plataforma de inteligencia de amenazas ThreatStream agrega y optimiza millones de indicadores de amenazas, creando una “cyber no-fly list.” Anomali se integra con la infraestructura interna para identificar nuevos ataques, realiza búsquedas forenses durante el año anterior para descubrir infracciones existentes y permite a los equipos de seguridad a comprender y contener amenazas rápidamente. Anomali también ofrece STAXX, una herramienta gratuita para recopilar y compartir inteligencia sobre amenazas, y proporciona un feed de inteligencia gratuito y listo para usar, Anomali Limo. Para más información, visite anomali.com y síganos en Twitter: @anomali.

Lumeta proporciona una conciencia cibernética crítica que ayuda a los equipos de seguridad y de red a prevenir las infracciones. Lumeta ofrece un descubrimiento incomparable de infraestructura de red conocida, desconocida y oculta sobre cualquier otra solución en el mercado hoy en día, así como supervisión en tiempo real de redes y puntos terminales para detectar cambios no autorizados, evitar rutas de fuga, asegurar una segmentación de red adecuada y detectar comportamientos de red sospechosos en elementos de red dinámicos, puntos finales, máquinas virtuales e infraestructura basada en la nube. Para obtener más información, visite lumeta.com.

Qualys, Inc. (NASDAQ: QLYS) es un proveedor pionero y líder de soluciones de cumplimiento y seguridad basadas en la nube con más de 9300 clientes en más de 100 países, incluida la mayoría de cada uno de los Forbes Global 100 y Fortune 100. Qualys Cloud Platform y su conjunto integrado de soluciones ayudan a las organizaciones a simplificar las operaciones de seguridad y a reducir el costo de cumplimiento proporcionando inteligencia de seguridad crítica bajo demanda y automatizando todo el espectro de auditoría, cumplimiento y protección para sistemas de TI y aplicaciones web. Fundada en 1999, Qualys estableció alianzas estratégicas con proveedores líderes de servicios administrados y organizaciones de consultoría de todo el mundo. Para obtener más información, visite qualys.com.

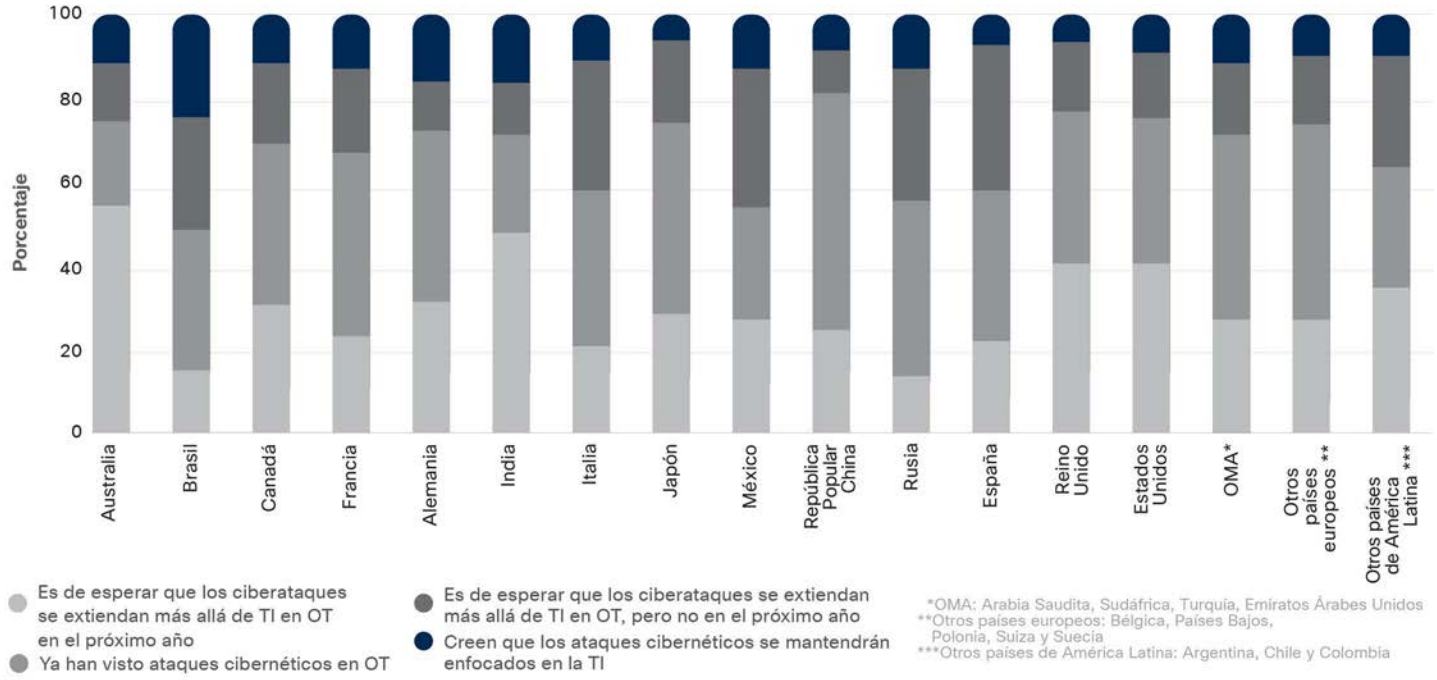
Radware (NASDAQ: RDWR) es un líder global de soluciones de ciberseguridad y entrega de aplicaciones para centros de datos virtuales, en la nube y definidos por software. Su galardonada cartera de soluciones ofrece garantía de nivel de servicio para más de 10,000 empresas y operadores en todo el mundo. Para obtener información y recursos de seguridad expertos adicionales, visite el centro de seguridad en línea de Radware, que ofrece un análisis exhaustivo de las herramientas, tendencias y amenazas de ataque DDoS: security.radware.com.

SAINT Corporation, líder en soluciones integradas de gestión de vulnerabilidades de próxima generación, ayuda a las corporaciones y las instituciones del sector público a identificar exposiciones de riesgo en todos los niveles de la organización. SAINT lo hace bien para que el acceso, la seguridad y la privacidad puedan coexistir en beneficio de todos. Y SAINT permite a los clientes fortalecer las defensas de InfoSec y reducir el costo total de propiedad. Para obtener más información, visite saintcorporation.com.

TrapX Security proporciona una rejilla de seguridad automatizada para la defensa y el engaño adaptativo que intercepta las amenazas en tiempo real a la vez que proporciona la inteligencia procesable para bloquear a los atacantes. TrapX Deception Grid ™ permite a las empresas detectar, capturar y analizar malware de día cero en uso por las organizaciones de amenazas persistentes avanzadas (APT) más efectivas del mundo. Las industrias confían en TrapX para fortalecer sus ecosistemas de TI y reducir el riesgo de compromisos costosos y perjudiciales, violaciones de datos y violaciones de cumplimiento. Las defensas de TrapX están integradas en el corazón de la red y la infraestructura de misión crítica, sin la necesidad de agentes o configuración. La detección de malware de última generación, la inteligencia de amenazas, el análisis forense y la corrección en una única plataforma ayudan a eliminar la complejidad y el costo. Para obtener más información, visite trapx.com.

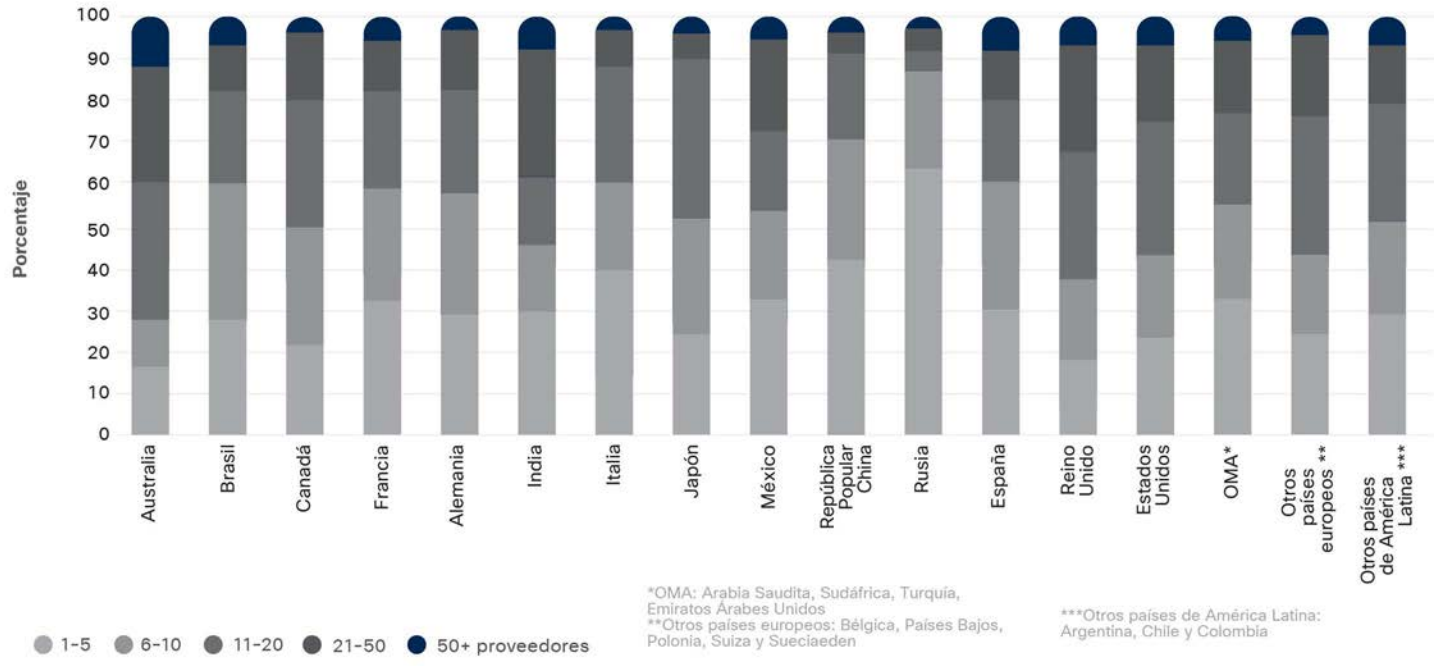
Apéndice

Figura 60 Expectativas para ciberataques en OT e IT, por país o región



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

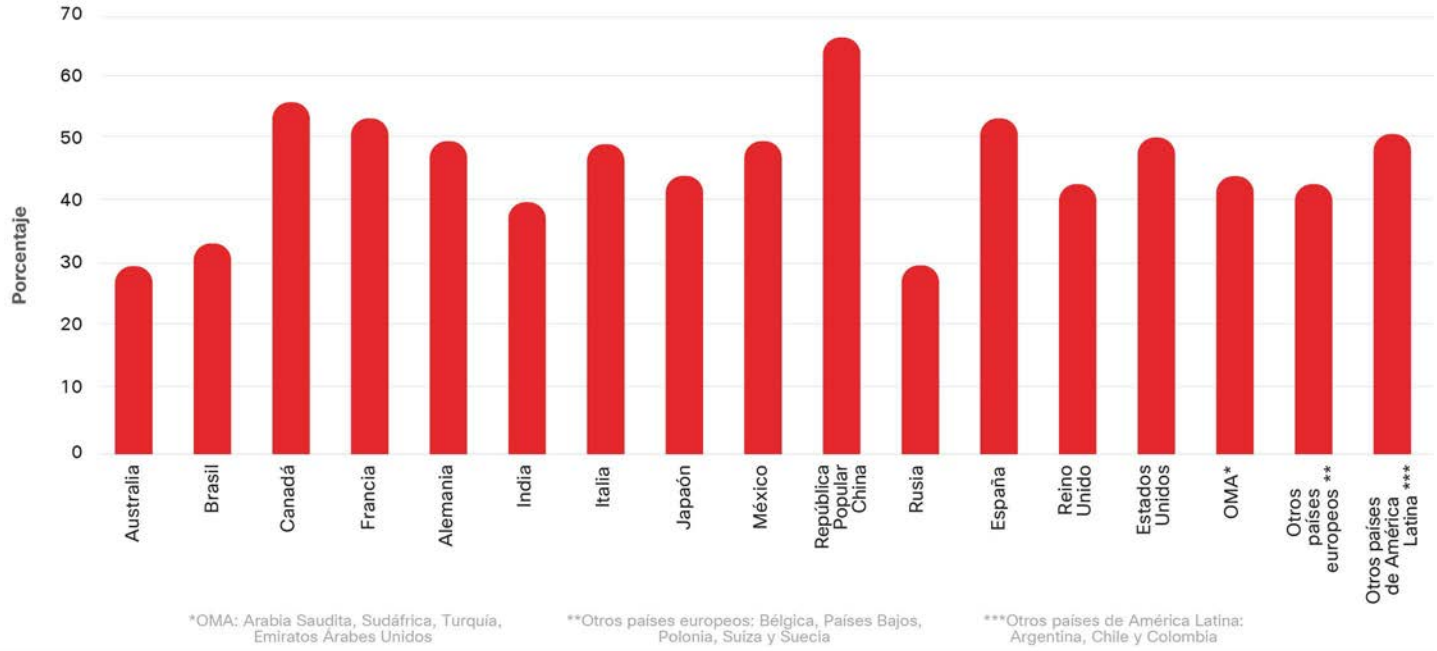
Figura 61 Cantidad de proveedores de seguridad en el entorno, por país o región



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Figura 62 Por ciento de alertas no investigadas, por país



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Figura 63 Obstáculos para adoptar tecnología y procesos de seguridad avanzados, por país o región

¿Cuál de los siguientes considera que son los mayores obstáculos para adoptar procesos y tecnologías de seguridad avanzados?

	Australia	Brasil	Canadá	Francia	Alemania	India	Italia	Japón	México	República Popular China	Rusia	España	Reino Unido	Estados Unidos	OMA*	Otros países europeos **	Otros países de América Latina ***
Restricciones presupuestarias	23%	35%	29%	33%	25%	36%	38%	31%	31%	38%	60%	33%	27%	34%	36%	37%	35%
Prioridades competitivas	28%	11%	29%	27%	28%	26%	24%	27%	16%	27%	20%	18%	32%	32%	25%	18%	24%
Falta de personal capacitado	25%	28%	19%	22%	24%	31%	24%	28%	30%	25%	35%	33%	31%	26%	25%	23%	26%
Falta de conocimiento sobre losprocesos de seguridad avanzada y la tecnología	26%	26%	24%	21%	22%	24%	21%	26%	23%	29%	18%	21%	27%	22%	22%	17%	21%
Problemas de compatibilidad con sistemas heredados	27%	19%	30%	27%	30%	30%	22%	23%	32%	40%	25%	25%	24%	28%	30%	25%	28%
Requisitos de certificación	33%	27%	29%	29%	24%	27%	27%	22%	27%	23%	22%	27%	27%	30%	24%	33%	21%
Cultura organizacional/actitud acerca de la seguridad	30%	23%	25%	20%	16%	26%	17%	21%	26%	17%	19%	24%	28%	25%	20%	20%	27%
Reacios a comprar hasta que se prueben en el mercado	19%	20%	23%	26%	25%	29%	20%	28%	15%	16%	17%	20%	21%	22%	22%	21%	25%
La carga de trabajo actual es demasiado pesada para asumir nuevas responsabilidades	22%	16%	28%	18%	28%	28%	26%	27%	23%	21%	15%	28%	22%	22%	20%	17%	19%
La organización no es un objetivo de alto valor para los ataques	25%	18%	21%	22%	24%	17%	14%	20%	12%	16%	11%	13%	21%	21%	21%	20%	16%
La seguridad no es una prioridad de nivel ejecutivo	22%	10%	17%	17%	20%	13%	13%	23%	15%	18%	11%	11%	19%	19%	17%	19%	21%

*OMA: Arabia Saudita, Sudáfrica, Turquía, Emiratos Árabes Unidos
**Otros países europeos: Bélgica, Países Bajos, Polonia, Suiza y Suecia
***Otros países de América Latina: Argentina, Chile y Colombia

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Figura 64 Compra de soluciones de amenazas de seguridad, por país o región

¿Qué describe mejor cómo su organización adquiere soluciones de defensa contra amenazas de seguridad?

País	N=	Típicamente, compro los mejores productos para satisfacer necesidades específicas	Por lo general, compro productos diseñados para trabajar en conjunto
Australia	203	86	14
Brasil	197	72	28
Canadá	185	67	33
Francia	191	59	41
Alemania	195	69	31
India	199	78	22
Italia	201	71	29
Japón	223	72	28
México	198	77	23
República Popular China	205	63	37
Rusia	196	58	42
España	148	70	30
Reino Unido	194	76	24
Estados Unidos	393	81	19
OMA*	249	69	31
Otros países europeos **	199	73	27
Otros países de América Latina ***	196	71	29

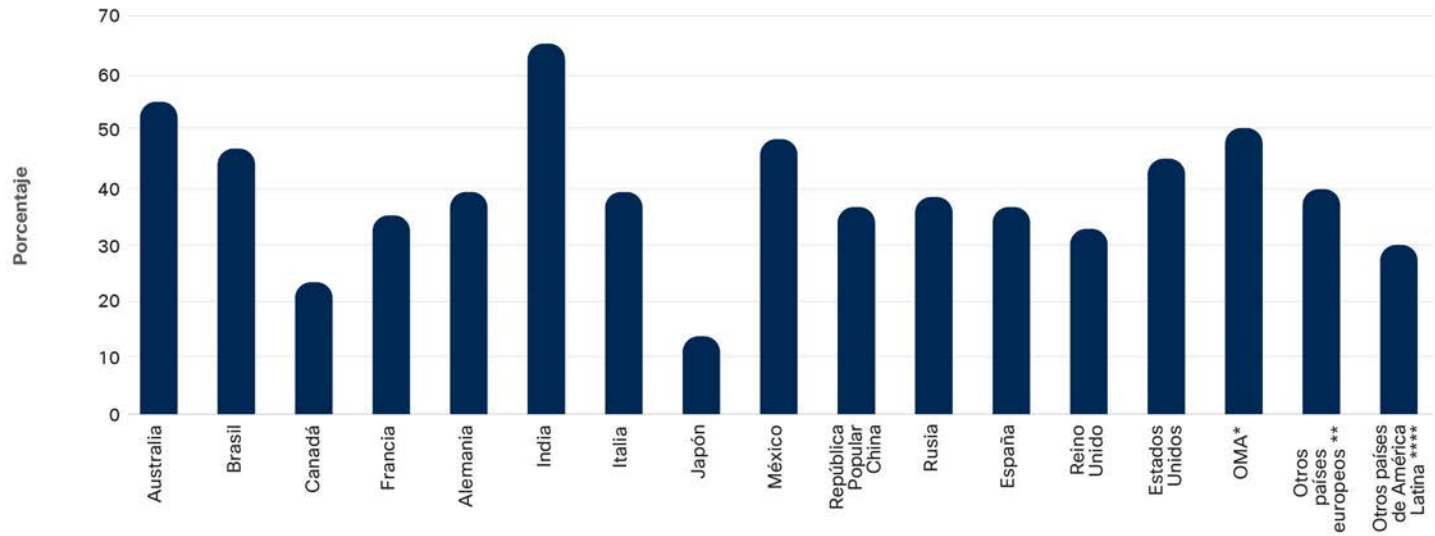
*OMA: Arabia Saudita, Sudáfrica, Turquía, Emiratos Árabes Unidos

**Otros países europeos: Bélgica, Países Bajos, Polonia, Suiza y Suecia

***Otros países de América Latina: Argentina, Chile y Colombia

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Figura 65 Porcentaje de organizaciones que perciben que siguen muy bien el marco infosec estandarizado, por país o región



*OMA: Arabia Saudita, Sudáfrica, Turquía, Emiratos Árabes Unidos

**Otros países europeos: Bélgica, Países Bajos, Polonia, Suiza y Suecia

***Otros países de América Latina: Argentina, Chile y Colombia

Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

Descargar los gráficos de 2018 en: cisco.com/go/acr2018graphics

Descargar los gráficos

Todos los gráficos de este Reporte pueden descargarse en: **cisco.com/go/mcr2018graphics**.

Actualizaciones y correcciones

Para ver las actualizaciones y correcciones a la información en este proyecto, visite cisco.com/go/errata.

Oficinas Centrales en América
Cisco Systems, Inc.
San Jose, CA

Oficinas Centrales en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapore

Oficinas Centrales en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Direcciones, números de teléfono y números de fax aparecen en el sitio web de Cisco en www.cisco.com/go/offices.

Publicado en febrero de 2018

© 2018 Cisco y/o sus filiales. Todos los derechos reservados.

Cisco y el logotipo de Cisco son marcas comerciales o marcas registradas de Cisco y/o sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas comerciales Cisco, ir a esta URL: www.cisco.com/go/trademarks. Las marcas comerciales de terceros mencionadas son propiedad de sus respectivos propietarios. El uso de la palabra socio no implica una relación de asociación entre Cisco y cualquier otra compañía. (1110R)

Adobe, Acrobat y Flash son marcas registradas o marcas comerciales de Adobe Systems Incorporated en los Estados Unidos y / o en otros países.