Informe anual de seguridad de Cisco 2014

CISCO

Resumen ejecutivo

El problema de la confianza

La explotación de la confianza representa un modus operandi habitual de los atacantes online y de otros sujetos malintencionados. Se aprovechan de la confianza que los usuarios depositan en los sistemas, las aplicaciones, y las personas y empresas con los que interactúan regularmente. Y este planteamiento surte efecto: existen suficientes pruebas que demuestran que los adversarios están concibiendo nuevos métodos para integrar su malware en las redes; así, pasan inadvertidos durante periodos prolongados, y roban datos o interrumpen sistemas esenciales.

Estos sujetos malintencionados continúan explotando la confianza pública para producir unas repercusiones perniciosas; todo ello mediante métodos que abarcan desde el robo de contraseñas y credenciales por medio técnicas de ingeniería social hasta infiltraciones sigilosas en las que el malware pasa desapercibido, las cuales se ejecutan en cuestión de minutos. Sin embargo, el problema de la confianza no se limita a delincuentes que explotan vulnerabilidades o se aprovechan de los particulares mediante la ingeniería social: también mina la tranquilidad que antes reinaba con respecto a las organizaciones públicas y privadas.

En la actualidad, las redes afrontan dos vertientes de erosión de la confianza. Una es un descenso de la credibilidad de los clientes en la integridad de los productos. La otra, por su parte, se resume en los numerosos indicios que apuntan a que los sujetos malintencionados están derrotando los mecanismos de confianza; de esta manera, se pone en duda la eficacia de las arquitecturas de autorización, autenticación y garantía de aplicaciones y redes.

Los sujetos malintencionados continúan innovando maneras de explotar la confianza pública para producir unas repercusiones perniciosas.

En este informe, Cisco ofrece datos e información relevante sobre las principales preocupaciones de seguridad, como los cambios en el malware, las tendencias de las vulnerabilidades y el resurgimiento de los ataques de denegación de servicio distribuida (DDoS). Asimismo, este documento examina las campañas dirigidas contra sectores, grupos u organizaciones específicos, así como la creciente sofisticación de aquellos que tratan de robar información confidencial. Además, el dossier concluye con recomendaciones para analizar los modelos de seguridad de forma holística y obtener visibilidad de todo el proceso del ataque: tanto en el despliegue de este como en los momentos anterior y posterior.

Hallazgos clave

A continuación se exponen tres de los hallazgos principales del *Informe anual de seguridad de Cisco 2014*:

Los ataques contra la infraestructura tienen como objetivo recursos importantes de Internet.

- Las explotaciones malintencionadas están accediendo a servidores de alojamiento web, servidores de nombres y Data Centers. Este dato sugiere que se están formando überbots (bots de gran envergadura) que buscan recursos de elevada reputación y un alto contenido de elementos.
- Los errores de búfer también representan una ofensiva destacada, ya que ascienden al 21% de las categorías de amenazas del estándar de enumeración de vulnerabilidades habituales (CWE, Common Weakness Enumeration).
- Los encuentros con malware se orientan ahora hacia la fabricación de productos electrónicos, y los sectores de la agricultura y de la minería, con una frecuencia de casos unas seis veces superior a la media en sus mercados verticales.

Los sujetos malintencionados están utilizando aplicaciones de confianza para explotar lagunas en la seguridad perimetral.

- El spam prosigue con su tendencia descendente, aunque la proporción de spam malintencionado permanece constante.
- Java protagoniza el 91% de las vulnerabilidades de la Web; de hecho, el 76% de las empresas que utilizan servicios Cisco Web Security ejecutan Java 6, una versión carente de soporte y que ha llegado al fin de su ciclo de vida.
- Los ataques de tipo "watering hole" (abrevadero) tienen como objetivo sitios web relacionados con sectores específicos para distribuir malware.

Las investigaciones de empresas multinacionales revelan indicios de riesgos internos. Desde sus redes, se genera tráfico sospechoso que trata de conectarse a sitios cuestionables (la totalidad de las empresas se comunican con hosts de malware).

- Los indicadores de riesgo sugieren que las penetraciones en redes podrían pasar desapercibidas durante periodos prolongados.
- Las alertas de amenazas crecieron un 14% interanual; el número de nuevas alertas (no las actualizadas) aumenta.
- El 99% de todo el malware para móviles de 2013 estuvo dirigido contra los dispositivos con Android. Los usuarios de este sistema operativo para móviles también presentaron la mayor frecuencia de casos (71%) con todos los formatos de malware distribuido por Web.

Contenido del informe

El *Informe anual de seguridad de Cisco 2014* presenta datos relevantes en materia de seguridad de cuatro áreas clave:

Confianza

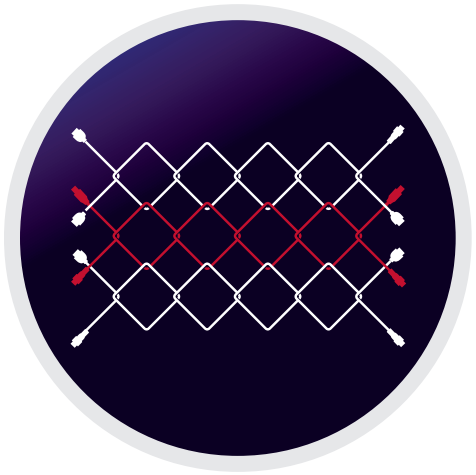
Todas las organizaciones deben tratar de hallar el equilibrio adecuado de confianza, transparencia y privacidad, porque hay mucho en juego. En esta área, abordamos tres factores de presión que dificultan aún más los intentos de los encargados de la seguridad de contribuir a que sus organizaciones logren este equilibrio, los cuales se exponen a continuación:

- Una mayor superficie de ataque
- La proliferación y la sofisticación de los modelos de ataques
- Complejidad de las amenazas y de las soluciones

Inteligencia de amenazas

Mediante el mayor conjunto de telemetría de detección disponible, Cisco y Sourcefire han analizado y recopilado datos de seguridad del último año:

- Los ataques contra la infraestructura tienen como objetivo recursos importantes de Internet.
- Los sujetos malintencionados están utilizando aplicaciones de confianza para explotar lagunas en la seguridad perimetral.
- Los indicadores de riesgo sugieren que las penetraciones de redes podrían pasar desapercibidas durante periodos prolongados.



Sector

En esta sección, los investigadores de Cisco Security Intelligence Operations (SIO) llevan el debate a tendencias del sector que rebasan el ámbito de la telemetría de Cisco, pero que aun así repercuten en las medidas de seguridad; estas van desde intentos de inicio de sesión por fuerza bruta, actividad DDoS a gran escala y métodos de ransomware (pirateo de equipos para, después, solicitar un rescate) hasta la creciente dependencia de la nube, la falta de personas competentes en el tema de la seguridad y otras preocupaciones.

Recomendaciones

Las organizaciones hacen frente a una superficie de ataque mayor, a la creciente proliferación y sofisticación de los modelos de ataques, además de a un aumento de la complejidad dentro de la red. Muchas encuentran dificultades para consolidar una visión de seguridad respaldada por una estrategia eficaz que emplee nuevas tecnologías, simplifique su arquitectura y sus operaciones, y fortalezca sus equipos de seguridad.

Esta sección aborda cómo un modelo de seguridad centrado en las amenazas permite que los defensores hagan frente al proceso del ataque completo, en todos los vectores de ataque, así como que respondan en cualquier momento y de forma continua tanto durante su despliegue como en los momentos anterior y posterior.

Cómo evalúa Cisco el panorama de amenazas

Cisco desempeña un papel crucial a la hora de evaluar amenazas, dada la prevalencia de sus soluciones y la variedad de su inteligencia de seguridad:

- Cada día, se inspeccionan **16 000 millones de solicitudes web** mediante Cisco Cloud Web Security.
- A diario, se analizan **93 000 millones de mensajes de correo electrónico** mediante la solución de correo electrónico alojado de Cisco.
- A diario, se evalúan **200 000 direcciones IP**.
- Diariamente, se analizan **400 000 muestras de malware**.
- Cada día, FireAMP examina **33 millones de archivos de terminales**.
- Diariamente, FireAMP evalúa **28 millones de conexiones de red**.

Esta actividad da como resultado que Cisco detecte las siguientes amenazas:

- Cada día, se bloquean **4500 millones de mensajes de correo electrónico**.
- A diario, se bloquean **80 millones de solicitudes web**.
- Diariamente, se producen **6450 detecciones de archivos de terminales** en FireAMP.
- Cada día, se producen **3186 detecciones terminales de red** en FireAMP.
- A diario, se detectan **50 000 intrusiones de red**.

Índice

Confianza 8

Nuevas formas de hacer negocios, nuevas lagunas de seguridad 9
Una erosión de la confianza 11
Principales retos de seguridad para 2014 12
Sistemas transparentes y de confianza 16

Inteligencia de amenazas 20

Amenazas de seguridad en alza 21
El volumen de spam ha descendido, pero el spam malintencionado sigue representando una amenaza 24
Vulnerabilidades web: Java se encuentra en cabeza 29
BYOD y movilidad: la madurez de los dispositivos beneficia el crimen online 33
Ataques selectivos: el reto de expulsar a "visitantes" ubicuos y persistentes 37
Visión general del malware: tendencias observadas en 2013 39
Objetivos principales: los sectores verticales 42
Fracturas en un ecosistema frágil 44
Se ha detectado tráfico malintencionado, con frecuencia un indicio de ataques selectivos, en todas las redes corporativas 49

Sector 53

Los intentos de inicio de sesión por fuerza bruta suponen una táctica preferida para atacar sitios web 54
Ataques de DDoS: se vuelve a llevar lo antiguo 56
DarkSeoul 58
La laguna de soluciones y la escasez personas competentes en el tema de la seguridad 61
La nube como un nuevo perímetro 62

Recomendaciones 64

Objetivos para 2014: verificar la fiabilidad y mejorar la visibilidad 65

Apéndice 68

Las organizaciones de seguridad precisan científicos de los datos 69

Información sobre Cisco SIO 78

Cisco SIO 79

Información sobre el documento

Este documento presenta contenido que se puede compartir y en el que se pueden efectuar búsquedas.

Busque este icono para abrir la función de búsqueda en Adobe Acrobat.

Busque estos iconos para compartir contenido.

Software recomendado

Adobe Acrobat versión 7.0 y superior

Confianza

Todas las organizaciones deben tratar de hallar el equilibrio adecuado de confianza, transparencia y privacidad, porque hay mucho en juego.

Nuevas formas de hacer negocios, nuevas lagunas de seguridad

Las vulnerabilidades de la cadena de suministro tecnológico suponen una faceta del complejo panorama de riesgos y ciberamenazas de la actualidad.

Como también lo es el auge de la infraestructura de cualquiera a cualquiera, que se apoya en la base de que cualquier dispositivo se podría conectar a cualquier instancia de la red.[1] Asimismo, estamos siendo testigos de una proliferación de dispositivos con acceso a Internet (smartphones, tablets y otros) que tratan de conectarse a aplicaciones que podrían ejecutarse en cualquier lugar, como en una nube pública de software como servicio (SaaS), en una privada o en una híbrida.[2] Incluso los servicios de infraestructura de Internet básica se han convertido en la diana de piratas informáticos que desean aprovecharse de la reputación, el ancho de banda, así como la disponibilidad y la actividad continua de servidores de alojamiento web, servidores de nombres y Data Centers; todo ello con el objetivo de poner en marcha campañas cada vez mayores. (Véase "Fracturas en un ecosistema frágil", página 44).

Aunque las tendencias como el Cloud Computing y la movilidad reducen la visibilidad y aumentan la complejidad de la seguridad, las organizaciones deben adoptarlas a pesar de ello, puesto que constituyen un componente esencial de su ventaja frente a la competencia y de su éxito empresarial. Sin embargo, están surgiendo lagunas de seguridad (y se están ampliando) a la par que los equipos de seguridad tratan de armonizar las soluciones tradicionales con formas nuevas y de rápida evolución de llevar a cabo la actividad comercial. Mientras tanto, los sujetos malintencionados trabajan con mayor celeridad para explotar las lagunas a las que las soluciones puntuales no integradas sencillamente no pueden hacer frente. En este sentido, tienen éxito porque cuentan con los recursos para actuar de forma más ágil.

La infraestructura básica de Internet se ha convertido en un objetivo de los piratas informáticos.

La red de crimen online se amplía, se fortalece y, con mayor frecuencia, funciona como cualquier red empresarial legítima y sofisticada. La jerarquía de los ciberdelincuentes de la actualidad se asemeja a una pirámide (véase la figura 1). En la base se encuentran los oportunistas sin conocimientos técnicos y los usuarios de "crimeware como servicio" que desean lucrarse, enviar un mensaje o lograr ambas

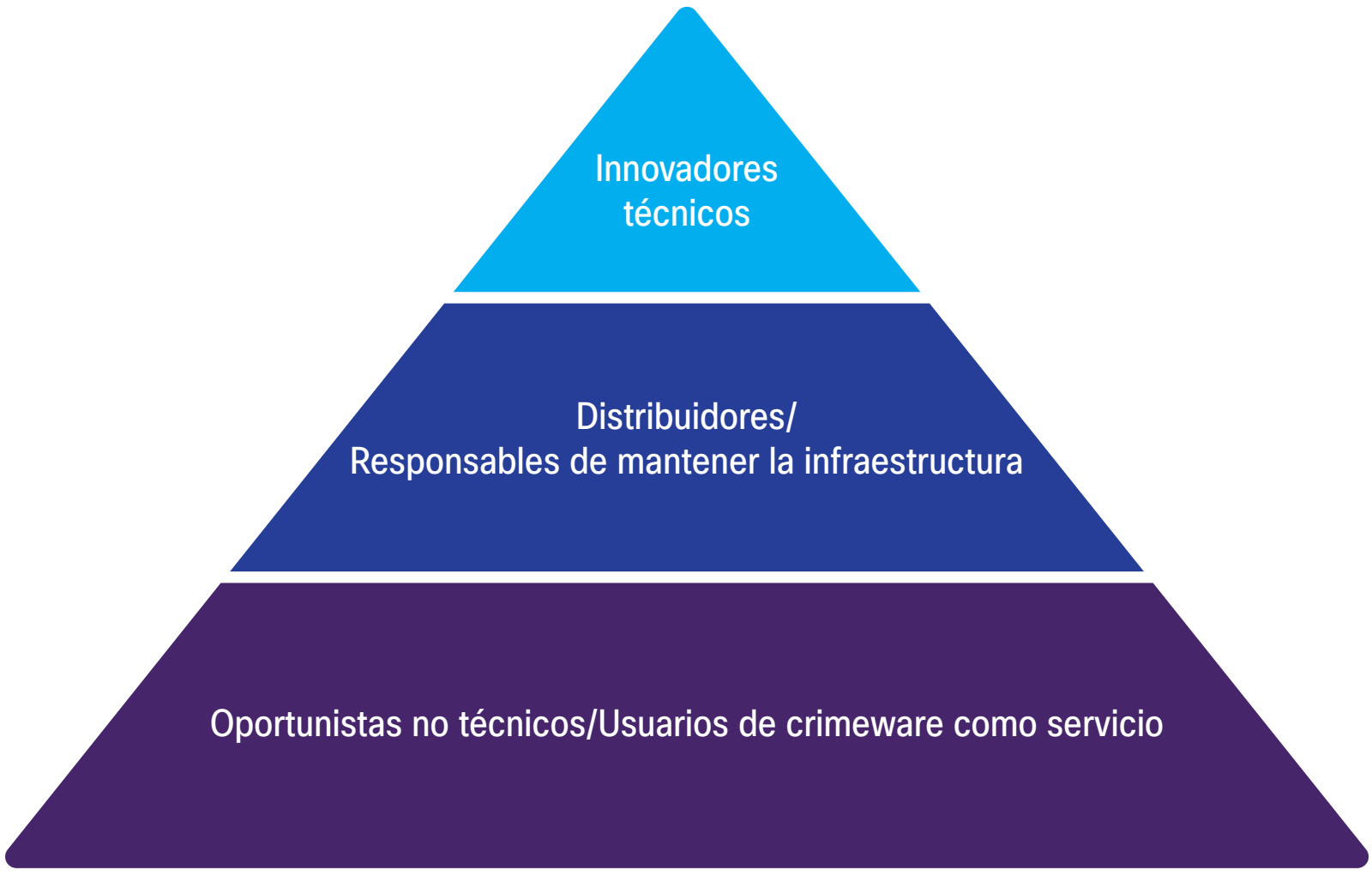
metas con sus campañas. En medio se encuentran los distribuidores y los responsables de mantener la infraestructura: los intermediarios. Por su parte, la cúspide está compuesta por los innovadores técnicos, los actores principales que más buscan las autoridades policiales, pero a los que tienen dificultades para encontrar.

Los ciberdelincuentes modernos cuentan normalmente con objetivos empresariales delimitados a la hora de poner en marcha las explotaciones de vulnerabilidades. Saben qué información buscan o qué resultados desean conseguir, y conocen las medidas que deben adoptar para lograr estos objetivos. Estos adversarios dedicarán un tiempo considerable a investigar sus objetivos, con frecuencia por medio de información disponible públicamente en redes sociales, y a planificar sus objetivos de forma estratégica.

Asimismo, muchos sujetos que trabajan al margen de la legalidad envían ahora malware de vigilancia para recopilar información acerca de un entorno, incluida la tecnología de seguridad que esté implementada; de esta manera, pueden dirigir sus ataques. Este reconocimiento previo a la explotación representa la manera en la que determinados creadores de malware pueden asegurarse de que este funcionará. Una vez integrado en una red, el malware avanzado que diseñan puede comunicarse con servidores de control y mando del exterior y propagarse de forma lateral por la infraestructura con el objetivo de llevar a cabo su misión, con independencia de que se trate del robo de datos vitales o de la interrupción de sistemas esenciales.

FIGURA 1

La jerarquía del ciberdelincuente



Una erosión de la confianza

Las amenazas diseñadas para aprovecharse de la confianza que los usuarios depositan en los sistemas, las aplicaciones, y las personas y las empresas que conocen ya constituyen elementos permanentes del mundo cibernético.

Si se disecciona prácticamente cualquier plan, su aspecto principal es algún abuso de la confianza: malware distribuido a usuarios que navegan de forma correcta por sitios web de uso generalizado. Mensajes de correo electrónico de spam que parecen que han enviado empresas conocidas, pero que contienen enlaces a sitios malintencionados. Aplicaciones para móviles de terceros acompañadas de malware y descargadas de populares mercados online. Infiltrados que utilizan privilegios de información de acceso para robar la propiedad intelectual de sus empleadores.

Quizás, todos los usuarios deberían asumir que no se puede ni se debe confiar en nada en el mundo cibernético. Y los profesionales de la seguridad podrían hacer un favor a sus organizaciones si no confían en ningún tráfico de red[3] o si no se fían completamente en las prácticas de seguridad de los proveedores o de las cadenas de suministros que proporcionan tecnología a la empresa. Sin embargo, aun así las organizaciones de los sectores privado y público, los usuarios individuales e incluso las naciones querrán disfrutar de la garantía de que pueden confiar en las tecnologías de base de las que dependen a diario.

Todos los usuarios deberían asumir que no se puede ni se debe confiar en nada en el mundo cibernético.

Esta necesidad de obtener confianza en la seguridad ha contribuido a proseguir con el avance de los Criterios comunes para la evaluación de la seguridad de la tecnología de la información (Criterios comunes, Common Criteria for Information Technology Security Evaluation), el idioma y el marco que permite que las agencias gubernamentales y otros grupos definan los requisitos que deben cumplir los productos tecnológicos para garantizar su fiabilidad. Hoy, 26 países, incluidos los Estados Unidos, participan en el Acuerdo de reconocimiento de Criterios comunes (Common Criteria Recognition Arrangement), un pacto multilateral que proporciona el reconocimiento mutuo de los productos evaluados por los gobiernos que participen.

Sin embargo, en 2013, la confianza, en términos generales, sufrió un revés. El instigador: Edward Snowden. Este antiguo contratista del gobierno estadounidense filtró información clasificada a *The Guardian*, un periódico británico; unos datos que obtuvo mientras trabajaba en un encargo para la Agencia de Seguridad Nacional (NSA) de Estados Unidos.[4]

Entre las revelaciones de Snowden a los medios de comunicación hasta la fecha, se incluyen detalles acerca del programa de recopilación de datos y vigilancia electrónica de la NSA, PRISM[5], además de sobre un programa de la NSA y el GCHQ[6] independiente conocido como "MUSCULAR", por medio del cual supuestamente se intervinieron las redes de fibra óptica que conducen el tráfico de los Data Centers en el extranjero de destacadas empresas de Internet.[7]

Estas revelaciones de Snowden y otras acerca de las prácticas de vigilancia gubernamentales han hecho mella en la confianza en muchos ámbitos: entre naciones, entre gobiernos y el sector privado, entre los ciudadanos de a pie y los gobiernos, además de entre tales ciudadanos y las organizaciones de los sectores público y privado. Naturalmente, también han suscitado inquietudes acerca de la presencia y los riesgos potenciales de las vulnerabilidades no intencionadas y "puertas traseras" intencionadas en productos tecnológicos, y sobre si los proveedores están tomando las medidas necesarias para evitar estas debilidades y proteger a los usuarios finales.

Principales retos de seguridad para 2014

[Conforme se desvanece la confianza (y resulta más difícil definir qué sistemas y relaciones son fiables y cuáles no), las organizaciones se enfrentan a varios problemas fundamentales que minan su capacidad de abordar la seguridad, como los siguientes:

1 | Una mayor superficie de ataque
2 | La proliferación y la sofisticación de los modelos de ataques
3 | Complejidad de las amenazas y de las soluciones]

Estos problemas combinados generan y agravan las lagunas de seguridad que permiten que los sujetos malintencionados pongan en marcha sus explotaciones antes de que las organizaciones puedan solventar sus debilidades en materia de seguridad.

Estas amenazas y riesgos se analizan en mayor profundidad en las siguientes páginas.

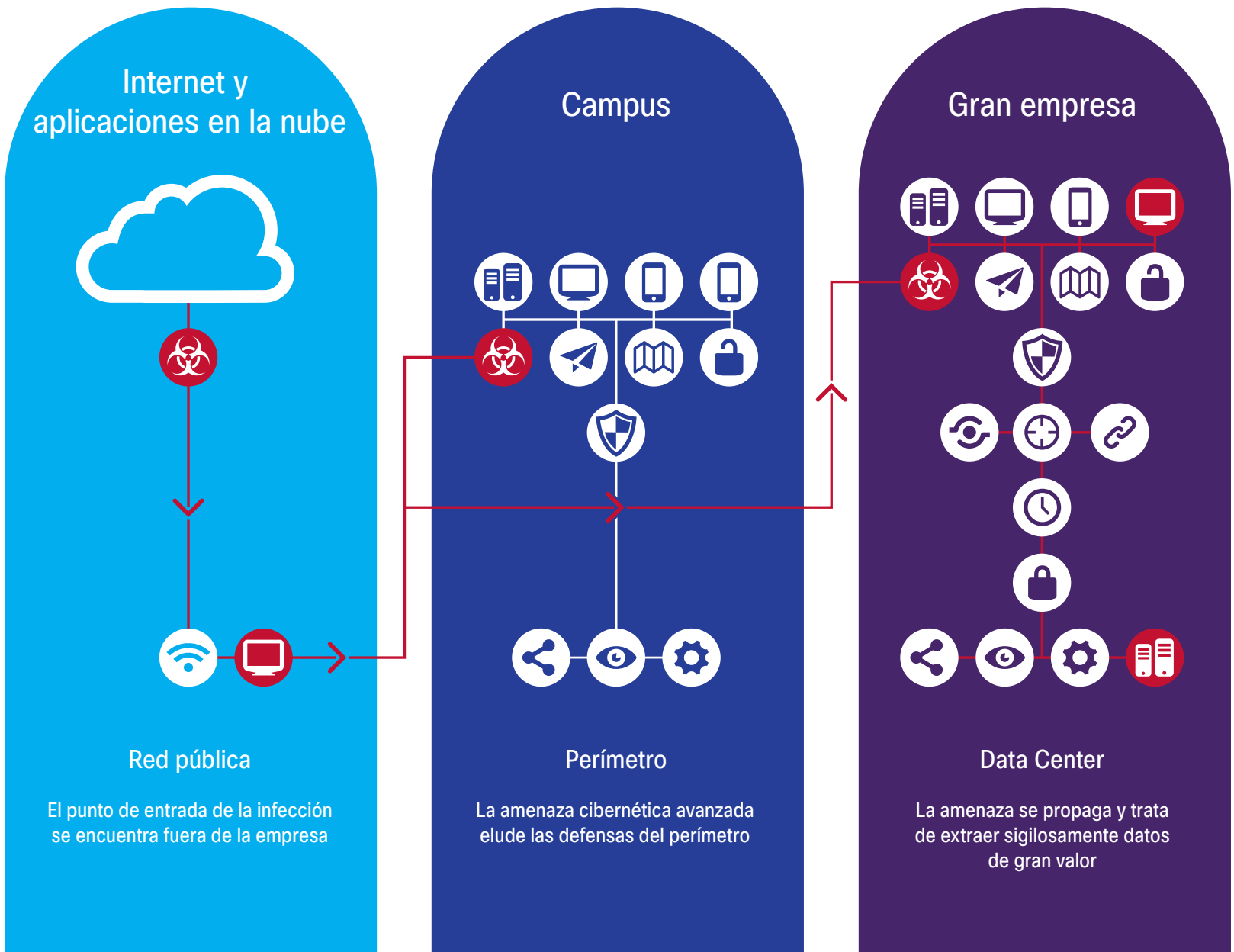
1 | Una mayor superficie de ataque

La superficie de ataque de la actualidad dota a los sujetos malintencionados de un sinfín de posibilidades para minar un ecosistema de seguridad más amplio y frágil. Esta superficie ha aumentado de forma exponencial y continúa ampliándose: tantos terminales, tantas incursiones, tal volumen de datos que no se encuentra bajo el control de las empresas.

Los datos encarnan el premio con el que la mayoría de los adversarios se quieren hacer mediante sus campañas, porque esencialmente constituye una divisa. Si los datos tienen algún valor de venta (con independencia de que se trate de propiedad intelectual de una empresa destacada o los datos sanitarios de una persona), son apetecibles y, por ende, se encuentran en riesgo. Si el valor del objetivo es superior al riesgo de ponerlo en peligro, sufrirá un ataque de piratería. Incluso las pequeñas organizaciones corren el riesgo de sufrirlos. Además, la mayoría de las organizaciones, grandes y pequeñas, ya se han vulnerado y ni siquiera son conscientes de ello: la totalidad de las redes empresariales analizadas por Cisco presentaban tráfico que viajaba a sitios web que alojan malware.

FIGURA 2

La anatomía de una amenaza moderna



La anatomía de la amenaza moderna, descrita en la figura 2, resalta que la meta final de muchas campañas de crimen online consiste en llegar al Data Center y extraer sigilosamente datos de gran valor. En este ejemplo, se produce una acción malintencionada en un dispositivo que se encuentra fuera de la red corporativa. Provoca una infección que se propaga a una red de campus. Dicha red actúa como un trampolín para llegar a la red empresarial y, acto seguido, la amenaza se abre camino hasta el tesoro oculto: el Data Center.

La meta final de muchas campañas de crimen online consiste en llegar al Data Center y extraer sigilosamente datos de gran valor.

A tenor de una superficie de ataque en continua expansión y de los ataques a datos de elevado valor por parte de los piratas informáticos, los expertos de seguridad de Cisco recomiendan que las empresas traten de dar respuesta a dos preguntas importantes en 2014: "¿Dónde se encuentran nuestros datos vitales?" y "¿Cómo podemos crear un entorno de seguridad para protegerlos, en especial cuando los nuevos modelos empresariales, como el Cloud Computing y la movilidad, solo nos permiten controlarlos de forma reducida?".

2 | La proliferación y la sofisticación de los modelos de ataques

El panorama de amenazas de la actualidad no se asemeja para nada al de solo 10 años atrás. Los ataques simples que provocaban daños controlables han dado paso a operaciones de crimen online modernas que presentan una mayor sofisticación, fondos suficientes y la capacidad de ocasionar una interrupción considerable en las organizaciones.

Las empresas se han convertido en el centro de atención de los ataques selectivos. Estas ofensivas resultan muy difíciles de detectar, permanecen en las redes durante periodos prolongados y acumulan recursos de red para asaltar otros lugares.

Para abarcar el proceso del ataque completo, las organizaciones deben hacer frente a un amplio abanico de vectores de ofensivas mediante soluciones que actúen allí donde pueda manifestarse la amenaza: en la red, en los terminales, en los dispositivos móviles y en los entornos virtuales.

"¿Dónde se encuentran nuestros datos vitales?" y "¿Cómo podemos crear un entorno de seguridad para protegerlos, en especial cuando los nuevos modelos empresariales, como el Cloud Computing y la movilidad, solo nos permiten controlarlos de forma reducida?".

Expertos de seguridad de Cisco

3 | Complejidad de las amenazas y de las soluciones

La época en la que los bloqueadores de spam y el software antivirus podían contribuir a proteger un perímetro de red fácilmente definido frente a la mayoría de las amenazas forma parte del pasado. Las redes actuales rebasan las fronteras tradicionales, evolucionan de forma constante y generan nuevos vectores de ataque: dispositivos móviles, aplicaciones para móviles y de Internet, hipervisores, redes sociales, navegadores de web, equipos domésticos e incluso vehículos. Las soluciones que solo actúan en un momento concreto no pueden responder a la infinidad de tecnologías y estrategias que emplean los sujetos malintencionados. De esta manera, la supervisión y la administración de la protección de la información resulta aun más difícil para los equipos de seguridad.

Las vulnerabilidades de las organizaciones se incrementan porque las empresas utilizan soluciones puntuales independientes y múltiples plataformas de gestión. El resultado: un conjunto de tecnologías dispares a lo largo de puntos de control que no se concibieron para funcionar conjuntamente. Así, se aumentan las probabilidades de que se comprometan información de los clientes, propiedad intelectual y otros datos confidenciales; además, esta situación se traduce en un riesgo para la reputación de la empresa.

Las soluciones que solo actúan en un momento concreto no pueden responder a la infinidad de tecnologías y estrategias que emplean los sujetos malintencionados.

En este sentido, se precisa contar con una capacidad continua que confiera la mejor oportunidad para cumplir los retos de los entornos de amenazas complejos. Los ataques implacables no se producen en un momento concreto; son continuos. Una característica que también deben presentar las defensas de una empresa.

Puesto que la complejidad de las amenazas y de las soluciones correspondientes se encuentra en su momento álgido, las organizaciones precisan replantearse su estrategia de seguridad. En lugar de depender de soluciones puntuales, pueden minimizar la complejidad integrando la seguridad de forma continua en el propio fabric de la red, esta podrá reportar las siguientes ventajas:

- Supervisar y analizar los archivos de forma continua, además de identificar comportamiento malintencionado ulterior con independencia de donde se inicie.
- Contribuir a que las organizaciones amplíen la aplicación de políticas; para ello, se expande la superficie en la que se pueden colocar los dispositivos de red.
- Reducir el tiempo necesario para detectar las amenazas, ya que podrá visualizar un mayor volumen de tráfico.
- Conferir a las organizaciones la capacidad de unificar la sensibilidad del contexto exclusiva que no se puede obtener dependiendo únicamente de dispositivos específicos de la seguridad.

La tendencia hacia los servicios de la nube y la movilidad supone una carga de seguridad mayor para los terminales y los dispositivos móviles que, en ciertos casos, es posible que ni siquiera entren en contacto en ningún momento con la red corporativa. Lo cierto es que los dispositivos móviles suponen un riesgo de seguridad cuando se utilizan para acceder a los recursos empresariales; se conectan fácilmente a equipos y servicios en la nube de terceros con condiciones en materia de seguridad que posiblemente se desconocen y se encuentran fuera del control de la empresa. Además, el malware para dispositivos móviles progresa rápidamente, lo que intensifica el riesgo en mayor medida. Dada la carencia de incluso una visibilidad básica, la mayoría de los equipos de seguridad de TI no cuentan con la capacidad de identificar las potenciales amenazas provenientes de estos dispositivos.

Los dispositivos móviles suponen un riesgo de seguridad cuando se utilizan para acceder a los recursos empresariales.

Los enfoques avanzados, como la capacidad continua, desempeñarán un papel más destacado a la hora de hacer frente al malware sofisticado mediante análisis de Big Data que agregan datos y eventos de la red ampliada a fin de proporcionar una visibilidad superior, incluso después de que un archivo se haya trasladado a la red o movido entre terminales. Este planteamiento difiere de la seguridad de terminales puntual que analiza los archivos en un momento concreto inicial para determinar si contienen malware. El malware avanzado puede evitar este análisis para establecerse rápidamente en los terminales y propagarse por todas las redes.

Sistemas transparentes y de confianza

A tenor de una superficie de ataque mayor, de la creciente proliferación y sofisticación de los modelos de ataques, y de la complejidad de las amenazas y las soluciones, precisamos confiar en la información que consumimos, además de en los sistemas que la proporcionan, con independencia de cómo se acceda a los servicios de red.

La creación de un entorno de red verdaderamente seguro se convertirá una tarea aún más compleja a medida que los gobiernos y las empresas inviertan en movilidad, colaboración, Cloud Computing y otros medios de virtualización. Estas capacidades contribuyen a mejorar la

flexibilidad, incrementar la eficacia y reducir los costes, pero también pueden presentar riesgos adicionales. Ahora, la seguridad de los procesos de fabricación que crean los productos de TI también corre un riesgo, puesto que el fenómeno de los productos manipulados y falsificados está suponiendo un problema cada vez mayor. Como consecuencia, los líderes corporativos y gubernamentales identifican, con diferencia, la seguridad cibernética y los problemas de confianza asociados como las preocupaciones principales. La pregunta que los encargados de la seguridad deben formular es la siguiente: ¿Qué haríamos de otra manera si supiéramos que se va a producir una infracción de forma inminente?

Los sujetos malintencionados buscarán y explotarán cualquier debilidad de seguridad en la cadena de suministros tecnológica. Las vulnerabilidades y las puertas traseras intencionales de los productos tecnológicos pueden, en última instancia, conferirles acceso a todo el entramado de red. Las puertas traseras gozan de una dilatada trayectoria como un problema de seguridad y deben figurar entre las preocupaciones de las organizaciones, porque el único propósito de su existencia es facilitar la actividad subrepticia o delictiva.

El concepto de desarrollar sistemas de confianza se traduce en integrar la seguridad desde cero, del principio al final del ciclo de vida de un producto. El ciclo de vida de desarrollo seguro Cisco Secure Development Life cycle (CSDL)[8] dicta una metodología cuantificable y repetible diseñada para integrar la seguridad de los productos en la fase de concepción, minimizar las vulnerabilidades durante el desarrollo e incrementar la flexibilidad de los productos frente a un ataque.

Los sujetos malintencionados buscarán y explotarán cualquier debilidad de seguridad en la cadena de suministros tecnológica.

Los sistemas de confianza suponen la piedra angular de un planteamiento de mejora continua a la seguridad que anticipa y previene nuevas amenazas. Tales infraestructuras no solo protegen la información vital, sino que contribuyen a evitar interrupciones de servicios esenciales, un aspecto que reviste aún más importancia. Los productos fiables respaldados por proveedores de confianza permiten que sus usuarios minimicen los costes y el daño a la reputación que se deriva de la apropiación indebida de la información, de las interrupciones del servicio e infracciones de datos.

No obstante, no se debe creer que los sistemas fiables se traducen en inmunidad frente a un ataque externo. Los usuarios y los clientes de TI tienen que desempeñar un papel destacado a la hora de mantener la eficacia de estos sistemas cuando estos repelan intentos de dañar sus operaciones. Esto se traduce en la instalación oportuna de actualizaciones y parches centrados en la seguridad, una supervisión constante para detectar si el sistema se comporta de manera anormal y la aplicación de contramedidas eficaces frente a un ataque.

Las principales preocupaciones para 2014 de los CISO de la actualidad

Conforme los directores de seguridad de la información (CISO) observan el panorama de amenazas actual, se enfrentan a crecientes factores de presión para proteger terabytes de datos, cumplir estrictas regulaciones de conformidad, todo ello con presupuestos austeros y equipos de TI reducidos. Los CISO desempeñan más tareas que nunca y amenazas complejas y sofisticadas que administrar. Los principales estrategas de seguridad de los servicios de Cisco, que asesoran a los CISO acerca de planteamientos de seguridad para sus organizaciones, ofrecen esta lista de los retos y las preocupaciones más apremiantes de 2014:

Gestión de la conformidad

La inquietud más generalizada entre los CISO podría ser la necesidad de proteger los datos que se encuentran en toda una red cada vez más permeable y, al mismo tiempo, dedicar recursos valiosos a la conformidad con las regulaciones. La conformidad por sí sola se traduce en protección; no es más que una base mínima que se centra en las necesidades de un entorno regulado especial. Mientras tanto, la seguridad representa un planteamiento integral que engloba todas las actividades empresariales.

Confianza en la nube

Los CISO deben tomar decisiones sobre como gestionar la información de forma segura con presupuestos limitados y dentro del plazo definido.

Continúa en la siguiente página

Las tecnologías no permanecen estáticas, ni tampoco los atacantes. La garantía de la fiabilidad del sistema debe abarcar el ciclo de vida completo de una red, desde el diseño inicial hasta la fabricación, la integración del sistema, el funcionamiento diario, el mantenimiento y las actualizaciones, y, en última instancia, hasta la retirada de la solución.

La necesidad de sistemas fiables no se limita a la propia red de una organización e incluye aquellas a las que se conecta tal organización. Los equipos de operaciones y estudio de seguridad de Cisco han observado un mayor uso del "pivoting" durante el año pasado. La técnica del pivoting del crimen online conlleva el uso de una puerta trasera, una vulnerabilidad o una sencilla explotación de la confianza en cierto eslabón del despliegue del ataque como un trampolín para poner en marcha una campaña mucho más sofisticada contra objetivos de mayor envergadura, como la red de una empresa de energía importante o el Data Center de una institución financiera. Algunos piratas informáticos utilizan la confianza que existe entre organizaciones como la base para el pivote; así, se aprovechan de un partner empresarial de confianza para atacar a otro partner comercial o gubernamental fiable desprevenido y explotarlo.

Resulta apropiado prestar atención en el panorama de amenazas moderno. La seguridad debe adaptarse a todos los estados transitorios que forman parte del entorno de TI empresarial mediante la valoración de forma objetiva y tangible de la fiabilidad del sistema, de acuerdo con procesos y datos independientes y que se pueden confirmar. El planteamiento más adecuado consiste en una defensa dinámica personalizada para el entorno único de una organización, en la que se incluyen controles de seguridad que evolucionan constantemente para que sigan siendo relevantes.[9]

Los sistemas de confianza pueden existir en este entorno y la transparencia resulta esencial para crearlos. "Los sistemas de confianza se deben construir sobre una base sólida: prácticas de desarrollo de productos, una cadena de suministros fiable y un enfoque de arquitectura que se componga de políticas, implementación y diseño de red.

Continuación de la página anterior

Por ejemplo, la nube se ha convertido en una manera ágil y rentable de gestionar grandes almacenes de información que crecen de forma constante, pero esto suscita más preocupaciones para los CISO. Los directores ejecutivos y las juntas directivas ven a la nube como una panacea que eliminará el hardware costoso. Desean disfrutar de las ventajas de descargar datos en la nube y esperan que el CISO convierta esta visión en realidad, con seguridad y celeridad.

Confianza en los proveedores

Al igual que ocurre con la nube, las organizaciones recurren a proveedores para obtener soluciones especializadas. El modelo de costes de acudir a terceros supone una opción lógica. Sin embargo, estos proveedores constituyen objetivos de gran valor para los delincuentes, que saben que las defensas de los terceros podrían no presentar la misma solidez.

Recuperación tras las violaciones de la seguridad

Todas las organizaciones deben asumir que han sufrido un ataque de piratería o, al menos, aceptar que es cuestión de si constituirán el objetivo de una ofensiva, sino de cuándo. Los recientes ataques de piratas, como la operación Night Dragon, la ofensiva contra RSA, y el asalto de Shamoon contra una gran empresa petrolera y del gas en 2012, rondan la mente de muchos CISO. (Consulte la investigación de Cisco sobre la prevalencia de la actividad malintencionada en las redes corporativas en la página 49).

Stewart, vicepresidente sénior y director de seguridad de Cisco. "Pero el atributo más importante es la transparencia de los proveedores".

El sacrificio a cambio de más transparencia es menos privacidad, pero es posible hallar el equilibrio adecuado mediante la cooperación, que conduce a mayores oportunidades para armonizar las prácticas recomendadas de seguridad e inteligencia de seguridad. Todas las organizaciones deben tratar de hallar el equilibrio adecuado de confianza, transparencia y privacidad, porque hay mucho en juego.

A largo plazo, es posible lograr una mejor seguridad cibernética para todos los usuarios; así, se podrán aprovechar todas las posibilidades del Internet of Everything[10] emergente. A pesar de todo, la consecución de estas metas dependerá de defensas de red resistentes y políticas de privacidad eficaces que distribuyan la carga de la seguridad de forma inteligente por los terminales y la red. A corto plazo, y quizás una noción más cercana, se encuentra la necesidad de cualquier empresa moderna de utilizar los mejores métodos e información disponibles para ayudar a proteger sus recursos más valiosos, así como a garantizar que no constituye un contribuidor directo de retos de seguridad cibernética más amplios.

Las organizaciones de la actualidad deben considerar qué repercusión podrían conllevar sus prácticas de seguridad para un ecosistema de seguridad cibernética de mayor envergadura y cada vez más complejo e interconectado. Si una organización no adopta este punto de vista amplio, podría conllevar que obtuviera un índice de reputación inadecuado, lo que significa que ningún proveedor de seguridad importante permitirá que los usuarios accedan a su sitio. Una empresa no puede reponerse fácilmente de que la incluyan en la lista negra y algunas podrían no recuperarse completamente jamás.

Para obtener más información acerca de las prácticas de sistemas de confianza de Cisco, visite www.cisco.com/go/trustworthy.

Inteligencia de amenazas

Mediante el mayor conjunto de telemetría de detección con la que trabajar, Cisco y Sourcefire han analizado y recopilado informaciones de seguridad del último año:

Amenazas de seguridad en alza

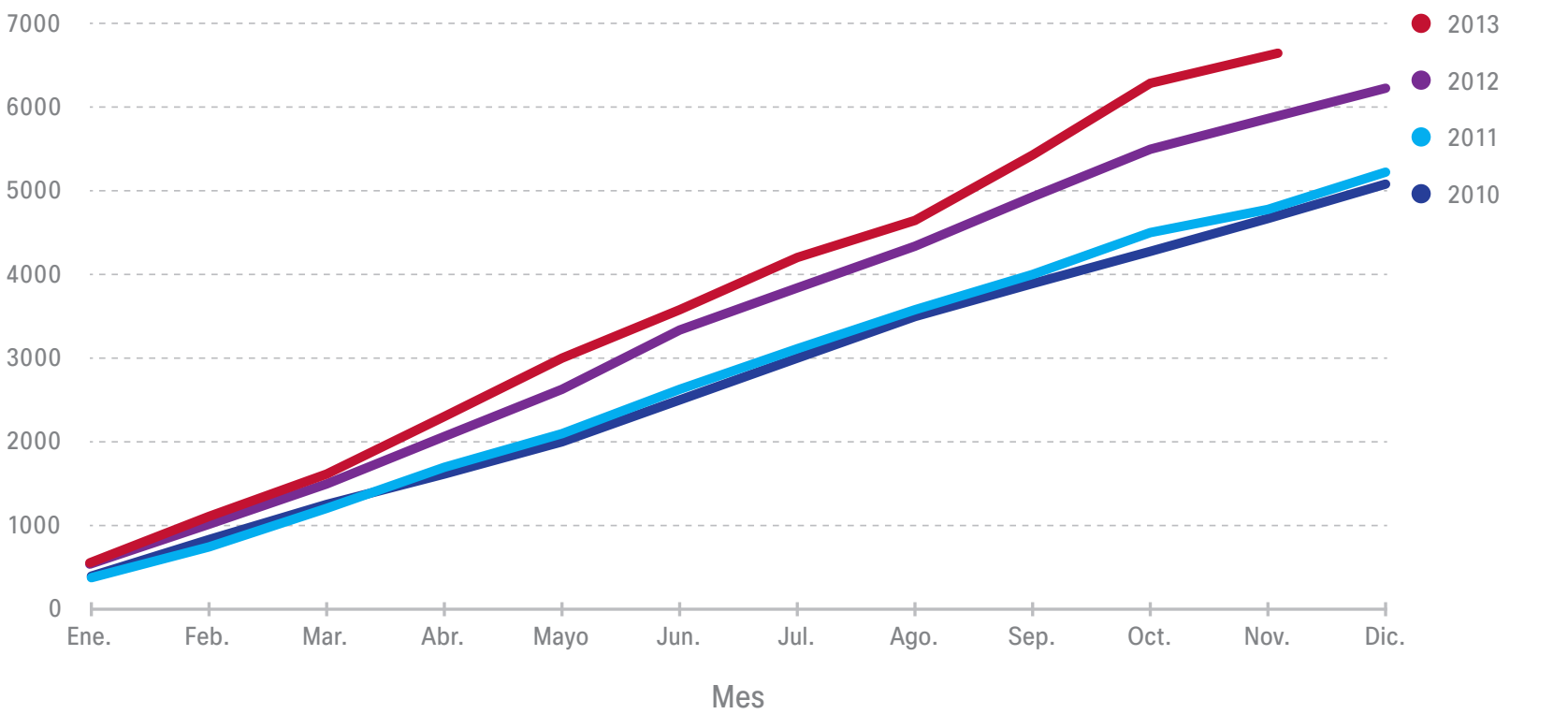
Las vulnerabilidades y las amenazas que indica Cisco IntelliShield® revelaron un crecimiento constante en 2013: a fecha de octubre de 2013, los volúmenes totales de alertas anuales acumulados aumentaron un 14% interanual desde el año 2012 (Figura 3).

En octubre de 2013, las alertas se encontraban en su nivel más elevado desde que IntelliShield comenzó a registrarlas en mayo de 2000.

También cabe destacar el aumento considerable de nuevas alertas, en contraposición a las actualizadas, según el seguimiento que efectúa IntelliShield (Figura 4). Los proveedores de tecnología están hallando una cantidad cada vez mayor de nuevas vulnerabilidades (Figura 5); estos descubrimientos se deben a un mayor hincapié en el uso de un ciclo de vida de desarrollo muy seguro, así como a mejoras en la seguridad de sus propios productos. Este mayor número de nuevas vulnerabilidades también podría representar la señal de que los proveedores están examinando el código de sus productos y reparándolas antes de que se comercialicen los productos y alguien se aproveche de ellas.

FIGURA 3

Volúmenes totales de alertas anuales acumulados (2010-2013)



Prestar más atención al desarrollo de software seguro puede contribuir a incrementar la confianza en las soluciones de los proveedores. Un ciclo de vida de desarrollo seguro no solo mitiga el riesgo de que surjan vulnerabilidades y permite que los proveedores detecten los posibles defectos en fases tempranas del proceso, sino que también transmite a los compradores que pueden depositar su confianza en estas soluciones.

FIGURA 4:

Alertas nuevas y actualizadas (2013)

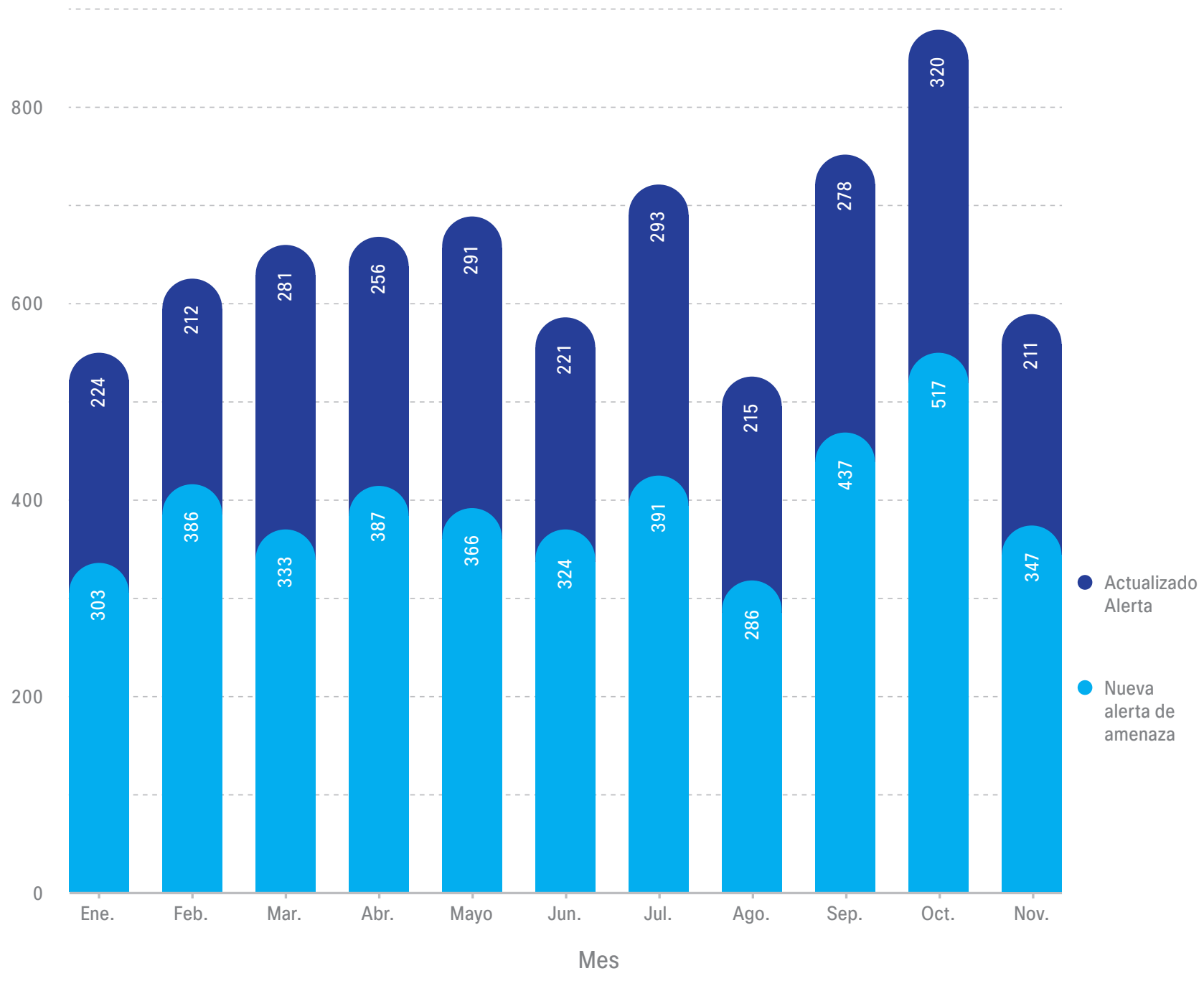


FIGURA 5

Categorías de amenazas habituales a las que Cisco IntelliShield ha realizado un seguimiento

NOTA: Estas categorías de amenazas de CWE (Common Weakness Enumeration), como las define la base de datos nacional de vulnerabilidades (National Vulnerability Database, https://nvd.nist.gov/cwe.cfm), encajan con los métodos que los sujetos malintencionados utilizan para atacar redes.

1
CWE-119: Errores de búfer

2
Otras alertas de IntelliShield (actividad, problemas, CRR, AMB)

3
CWE-399: Errores de administración de recursos

4
CWE-20: Validación de entradas

5
CWE-264: Permisos, privilegios y control de acceso

6
CWE-200: Divulgación/filtro de información

7
CWE-79: Scripting entre sitios (XSS)

8
CWE-94: Inserción de código

9
CWE: Error de diseño

CWE-310: Problemas criptográficos

CWE-287: Problemas de autenticación

CWE-352: Falsificación de solicitudes entre sitios (CSRF)

CWE-22: Traspaso de rutas

CWE-78: Inserciones de comandos de SO

CWE-89: Inserción de SQL

CWE-362: Ejecución de código malintencionado concurrente

CWE-255: Administración de credenciales

CWE-59: Enlaces falsos

CWE-16: Configuración

CWE: Información insuficiente

CWE: Otros

CWE-189: Errores numéricos

El volumen de spam ha descendido, pero el spam malintencionado sigue representando una amenaza

El volumen de spam siguió una tendencia descendente en todo el mundo durante 2013. Sin embargo, a pesar de que el volumen global ha descendido, la proporción de spam malintencionado permaneció constante.

Los spammers emplean la velocidad como una herramienta para abusar de la confianza de los usuarios de correo electrónico y envían un gran volumen de spam cuando tendencias o acontecimientos de actualidad hacen mella en la resistencia de los receptores a los fraudes de spam.

Tras los atentados del maratón de Boston el 15 de abril de 2013, comenzaron dos campañas de spam a gran escala (una el 16 de abril y otra al día siguiente, el 17) concebidas para atraer a los usuarios de correo electrónico ávidos de noticias sobre las repercusiones del suceso. Los investigadores de Cisco detectaron en un principio el registro de cientos de nombres de dominio relacionados con bombas solo horas después de que se produjeran los atentados del maratón de Boston.[11]

Ambas campañas de spam presentaban asuntos acerca de supuestos boletines de noticias relacionados con los atentados, mientras que los mensajes contenían enlaces que afirmaban llevar a los vídeos de las explosiones de las bombas o a noticias de fuentes periodísticas respetadas. Los enlaces llevaban a los remitentes a páginas web que incluían enlaces a vídeos o noticias reales, pero también a marcos iFrame malintencionados diseñados para infectar los equipos de los visitantes. En su punto álgido, el spam relacionado con los atentados del maratón de Boston suponía el 40% de todos los mensajes de spam enviados en todo el mundo el 17 de abril de 2013.

Los spammers se aprovechan del deseo de las personas de más información tras un acontecimiento significativo.

La figura 6 muestra una de las campañas de spam de Botnet de spam haciéndose pasar por un mensaje de la CNN.[12] La figura 7 muestra el código fuente HTML de un mensaje de spam de los atentados del maratón de Boston. El marco iFrame final (oculto) lleva a un sitio web malintencionado.[13]

Como el spam de las últimas noticias exhibe un carácter tan inmediato, es más posible que los usuarios de correo electrónico crean que los mensajes de spam son legítimos. Los spammers se aprovechan del deseo de las personas de más información tras un acontecimiento significativo. Cuando los spammers ofrecen a los usuarios online lo que desean, resulta mucho más sencillo engañarlos para que realicen la acción que los primeros quieren, como que hagan clic en un enlace infectado. También resulta muchísimo más sencillo evitar que sospechen de que se trata de un mensaje falso.

FIGURA 6

Spam sobre el maratón de Boston

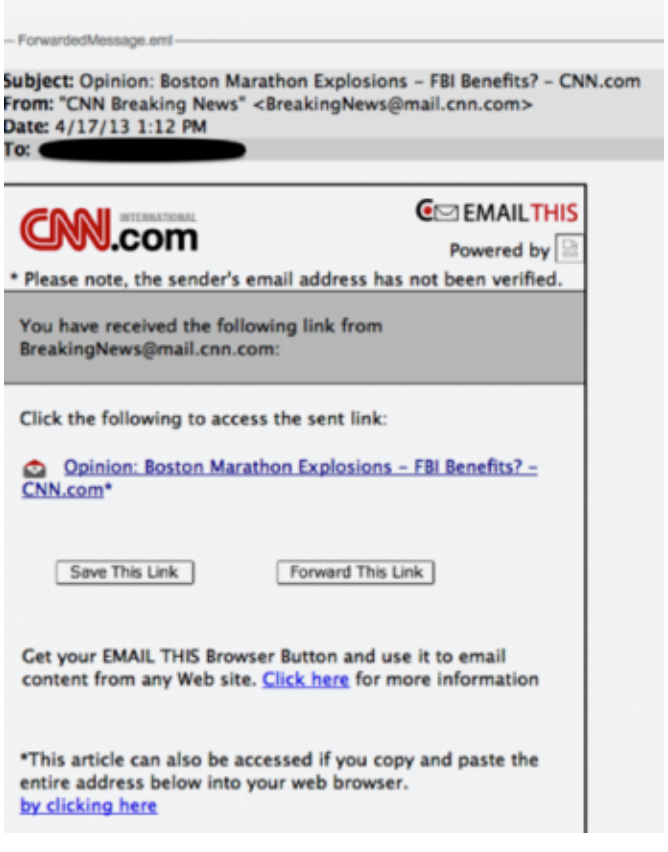


FIGURA 7

Código fuente HTML de un mensaje de spam sobre los atentados del maratón de Boston

Spam en cifras

El volumen de spam global está disminuyendo, según los datos recopilados por el equipo de comunicaciones y análisis de investigaciones de amenazas de Cisco (TRAC)/SIO (Figura 8), aunque las tendencias varían según el país (Figura 9).

FIGURA 8

Volumen de spam global (2013)

Fuente: Cisco TRAC/SIO

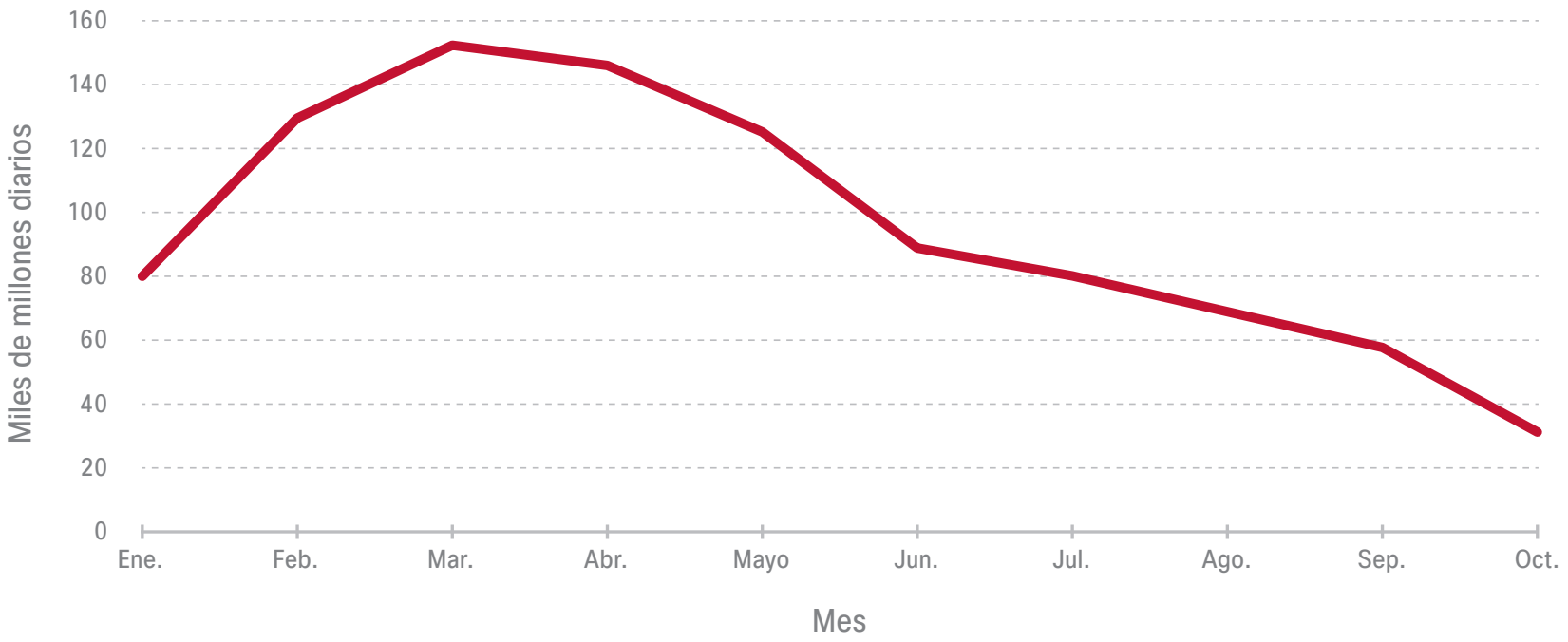


FIGURA 9

Tendencias de volumen (2013)

Fuente: Cisco TRAC/SIO

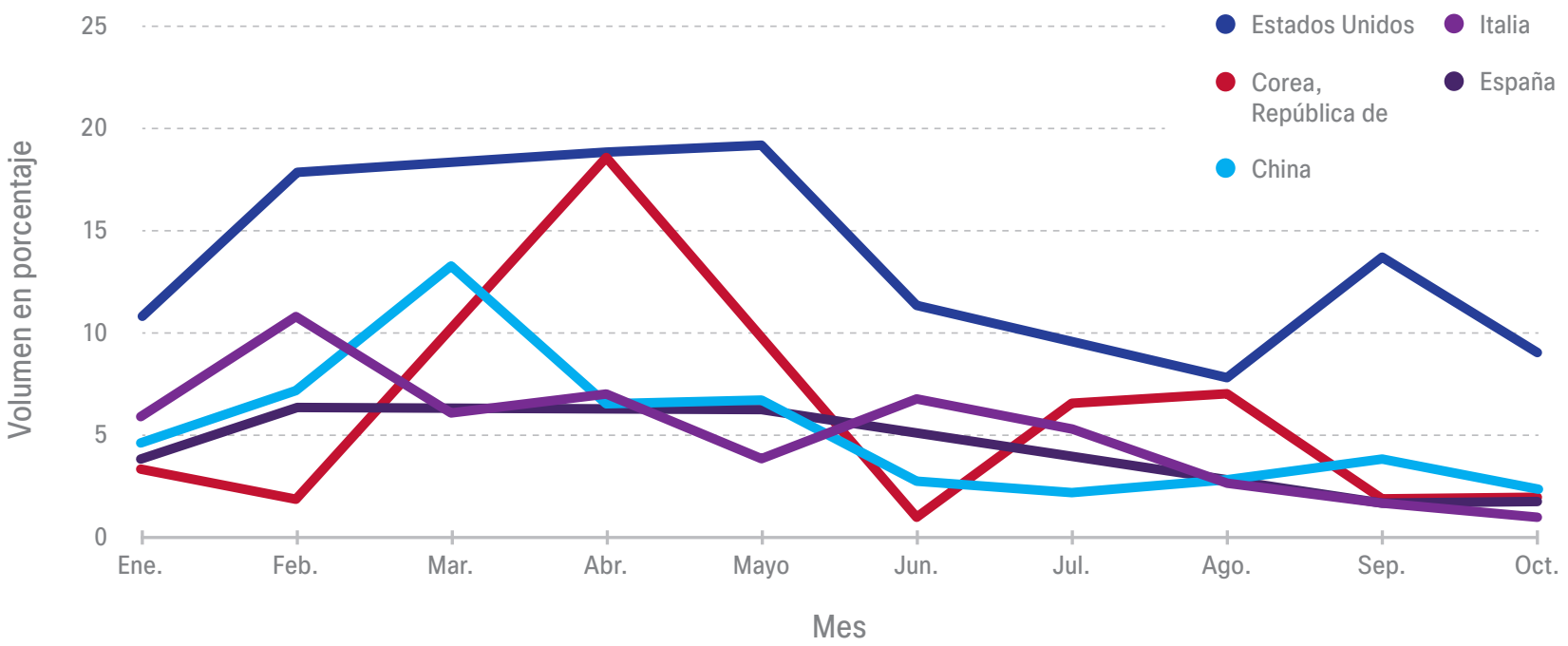


FIGURA 10

Principales temas de los mensajes de spam en todo el mundo

1. Depósito bancario/Notificaciones de pago

Notificaciones de depósitos, transferencias, pagos, cheques devueltos y alertas contra fraudes.

2. Compra de productos online

Confirmación de pedido del producto, solicitud de pedido, presupuesto y prueba.

3. Foto adjunta

Fotos adjuntas malintencionadas.

4. Avisos de envío

Facturas, entrega o recogida y seguimiento.

5. Citas online

Sitios de citas online.

6. Impuestos

Documentos fiscales, devoluciones, informes, información sobre la deuda y declaraciones tributarias online.

7. Facebook

Estado de la cuenta, actualizaciones, notificaciones y software de seguridad.

8. Cupón o tarjeta regalo

Alertas de una gran variedad de tiendas (Apple fue la más popular).

9. PayPal

Actualización de la cuenta, confirmación, notificación de pago y disputa de pago.

Vulnerabilidades web: Java se encuentra en cabeza

De todas las amenazas basadas en la Web que minan la seguridad, las vulnerabilidades del lenguaje de programación Java siguen constituyendo el objetivo más explotado por los criminales online, de acuerdo con los datos de Cisco.

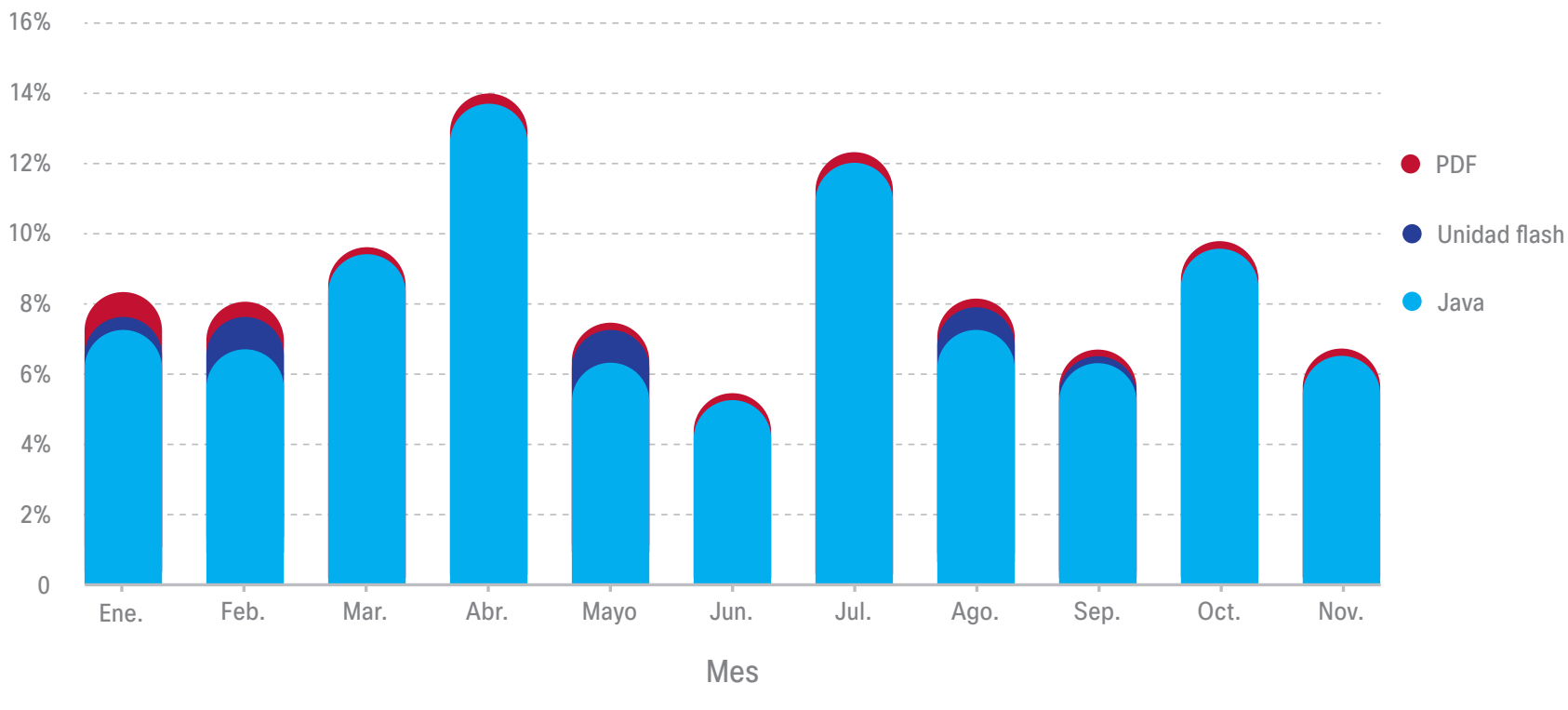
Las vulnerabilidades de Java superan con creces a aquellas detectadas en Flash o en los documentos en formato Adobe PDF, que también representan vectores populares de actividad criminal (Figura 11).

Los datos de Sourcefire, que ahora forma parte de Cisco, también muestran que las vulnerabilidades de Java conforman la amplia mayoría (91%) de los indicadores de riesgo (IoC) que supervisa la solución FireAMP de Sourcefire, que está destinada a la protección frente al malware avanzado y a su análisis (Figura 12). FireAMP detecta situaciones en las que los terminales se han visto comprometidos en tiempo real y, a continuación, registra el tipo de software que ha provocado cada una.

FIGURA 11

Ataques malintencionados generados mediante PDF, Flash y Java (2013)

Fuente: informes de Cisco Cloud Web Security



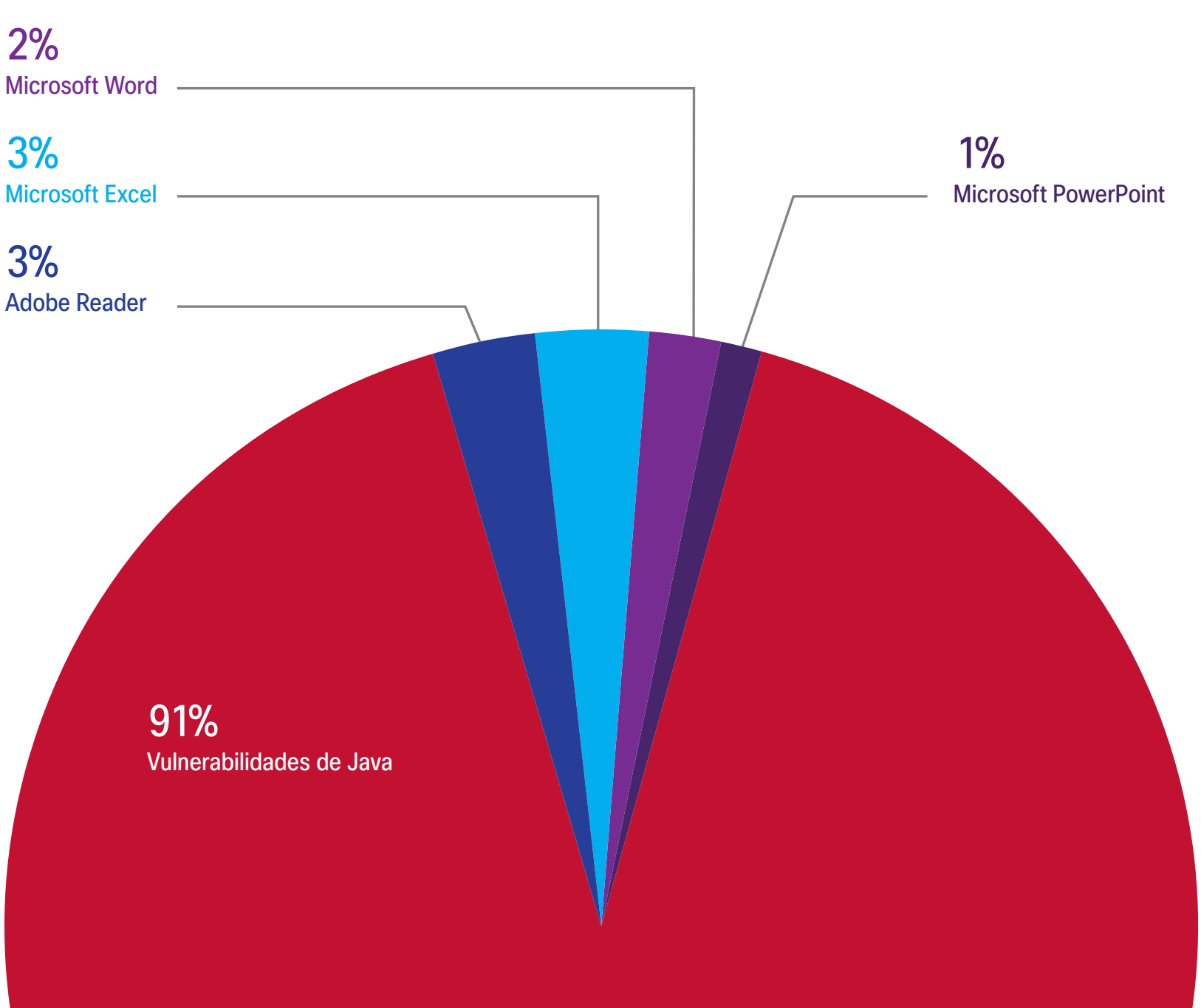
En el caso de las amenazas como las vulnerabilidades de Java, entre los problemas más significativos que afrontan los responsables de la seguridad figuran el modo en el que el malware accede a su entorno de red y el lugar en el que deben centrar sus esfuerzos para minimizar la infección. Es posible que las acciones individuales no parezcan malintencionadas, pero el seguimiento de la cadena de eventos podría arrojar luz sobre la historia del malware. El encadenado de eventos consiste en la capacidad de llevar a cabo un análisis retrospectivo de datos que conectan la ruta que han seguido los sujetos malintencionados para evitar la seguridad del perímetro e infiltrarse en la red.

Por sí solos, los indicadores de riesgo pueden demostrar que resulta seguro visitar determinado sitio web. En cambio, el inicio de Java podría constituir una acción segura, al igual que el arranque de un archivo ejecutable. Sin embargo, una organización corre riesgos si un usuario visita un sitio web con un marco iFrame incrustado, que se, a su vez, inicia Java; a continuación, este último software descarga un archivo ejecutable y ese archivo ejecuta acciones malintencionadas.

FIGURA 12

Indicadores de riesgo por tipo

Fuente: Sourcefire (solución FireAMP)



La ubicuidad de Java se traduce en que mantenga un lugar destacado en la lista de herramientas preferidas de los criminales, lo que conlleva que las explotaciones de vulnerabilidades de Java sean la actividad de "cadena de eventos" más malintencionada con mucha diferencia en 2013. Como expone la página web de "Acerca de" de Java, el 97% de los equipos de escritorio empresariales ejecutan Java, al igual que el 89% de los equipos de sobremesa globales en Estados Unidos.[14]

Java ofrece una superficie de ataque de tal envergadura que los delincuentes no pueden ignorarla. Tienden a compilar soluciones que se aprovechan de las vulnerabilidades en orden; por ejemplo, primero tratan de infiltrarse en una red o robar datos mediante la más sencilla o la más conocida antes de pasar a otros métodos. En la mayoría de los casos, Java constituye la vulnerabilidad por la que primero optan los criminales, ya que ofrece el mejor retorno de la inversión.

Mitigación del problema de Java

Aunque el aprovechamiento de vulnerabilidades basado en Java es habitual y estas resultan difíciles de eliminar, existen métodos para reducir su impacto, como los siguientes:

- Cuando suponga una solución práctica, es posible evitar que se inicien este software de aprovechamiento de vulnerabilidades deshabilitando Java en los navegadores de toda la red.
- Las herramientas de telemetría, como Cisco NetFlow, integradas en muchas soluciones de seguridad, pueden supervisar el tráfico asociado con Java, lo que permite que los profesionales de la seguridad comprendan mejor las fuentes de las amenazas.
- En este sentido, una completa administración de parches puede solventar muchos fallos de seguridad.
- Herramientas de análisis y supervisión de terminales que sigan efectuando un seguimiento de los archivos y analizándolos después de que accedan a la red puede detectar y detener de forma retrospectiva las amenazas que parecen seguras, pero que después exhiben un comportamiento malintencionado.
- Es posible elaborar una lista de dispositivos potencialmente vulnerables por orden de prioridad mediante los indicadores de riesgo con el fin de establecer una correlación con la inteligencia de malware (incluso eventos aparentemente benignos), además de para identificar una infección de día cero sin firmas de antivirus existentes.

Actualizar a la versión más reciente de Java también contribuirá a eludir las vulnerabilidades. Según un estudio de Cisco TRAC/SIO, el 90% de los clientes de Cisco una versión de Java Runtime Environment 7, la más reciente del programa. Se trata de una buena noticia desde el punto de vista de la seguridad, puesto que esta versión probablemente ofrecerá una mayor protección frente a las vulnerabilidades.

Sin embargo, este estudio de Cisco TRAC/SIO revela asimismo que el 76% de las empresas que utilizan soluciones de Cisco también usan Java Runtime Environment 6, además de Java 7. Java 6 es una versión anterior que ha llegado al final de su ciclo de vida y ya no recibe soporte. Las empresas utilizan con frecuencia ambas versiones de Java Runtime Environment porque varias aplicaciones pueden necesitar las diferentes versiones para ejecutar códigos de Java. Sin embargo, teniendo en cuenta que más de tres cuartos de las empresas encuestadas por Cisco utilizan una solución que ha llegado al final de su ciclo de vida con vulnerabilidades que podrían no solucionarse públicamente nunca, los criminales disfrutan de una gran oportunidad para explotar las debilidades.

En 2013, los encuentros con malware web en Java alcanzaron su punto álgido en abril, con un 14% la totalidad del malware web hallado. Estos disminuyeron hasta su nivel más bajo en mayo y junio de 2013, con aproximadamente el 6 y el 5% de todos los encuentros con malware web, respectivamente (Figura 13).

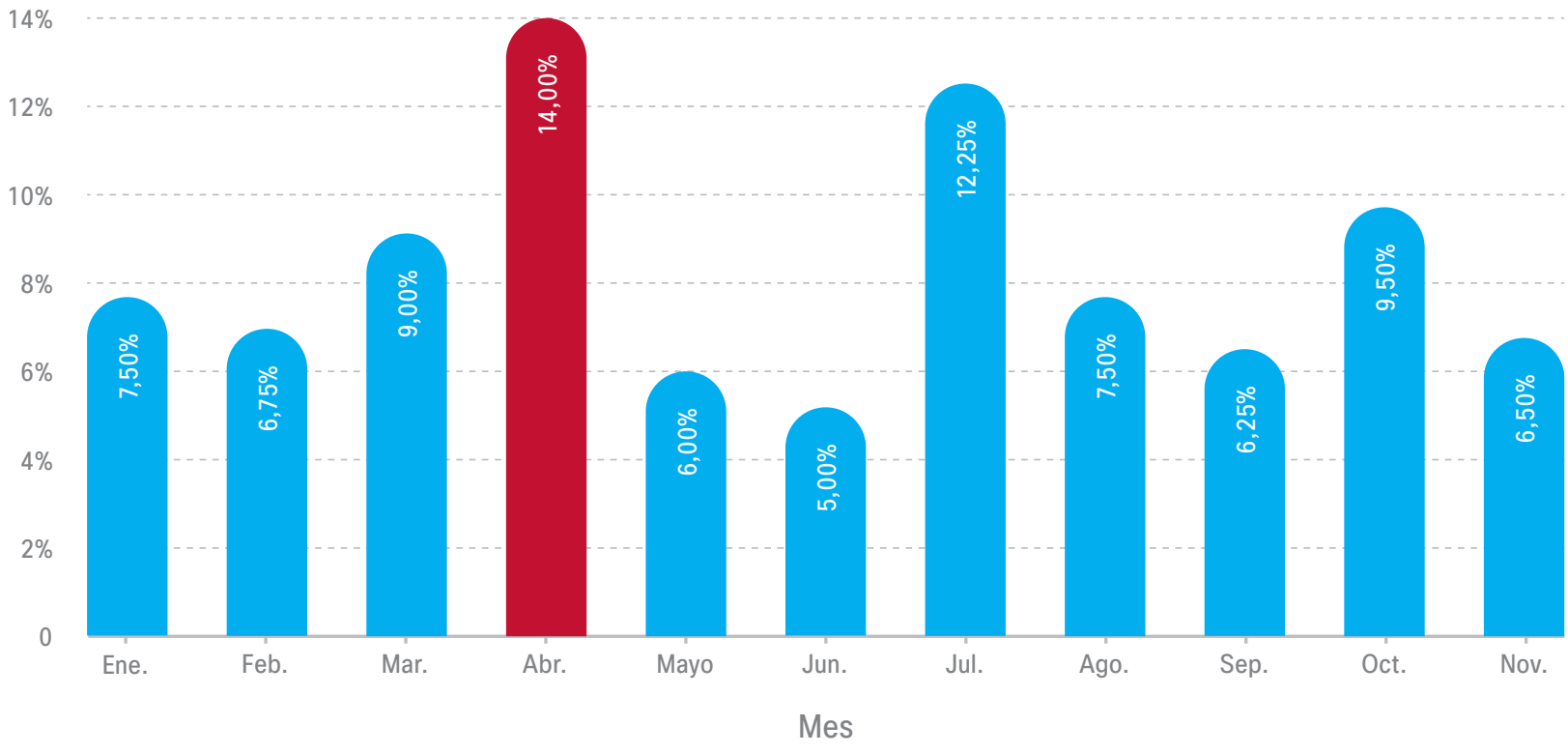
(A principios de este año, Oracle anunció que dejaría de publicar actualizaciones de Java SE 6 en su sitio de descarga público, aunque las actualizaciones existentes para Java SE 6 se encontrarán disponibles en Java Archive en la Oracle Technology Network).

Si los profesionales de la seguridad que cuentan con un tiempo limitado para luchar contra las vulnerabilidades web deciden centrar su atención en Java, estarán utilizando sus recursos de forma adecuada.

FIGURA 13

Encuentros con malware web en Java (2013)

Fuente: Cisco TRAC/SIO



BYOD y movilidad: la madurez de los dispositivos beneficia el crimen online

Los ciberdelincuentes y sus objetivos comparten un reto común: ambos tratan de descubrir cómo utilizar las tendencias de traiga su propio dispositivo (BYOD) y de movilidad para obtener de una ventaja empresarial.

Dos aspectos parecen contribuir a que los delincuentes partan con ventaja. El primero es la madurez de las plataformas móviles. Los expertos de seguridad de Cisco señalan que, cuanto más similares resulten los smartphones, las tablets y otros dispositivos a los equipos portátiles y de sobremesa tradicionales en lo relativo a su funcionamiento, más sencillo será diseñar malware para ellos.

El segundo es el aumento del uso de las aplicaciones para móviles. Cuando los usuarios descargan aplicaciones para móviles, esencialmente están colocando un cliente ligero en el terminal y descargando código. Otro reto: muchos usuarios descargan aplicaciones para móviles de forma regular sin considerar los aspectos de seguridad.

Mientras tanto, los equipos de seguridad de la actualidad tratan de resolver el "problema de cualquiera a cualquiera": cómo proteger a cualquier usuario, en cualquier dispositivo, ubicado en cualquier lugar y que accede a cualquier aplicación o recurso.[15] La tendencia BYOD solo consigue complicar aún más estos esfuerzos. Resulta difícil administrar todos estos tipos de equipos, especialmente si solo se dispone de un presupuesto de TI limitado. En un entorno BYOD, el director de seguridad de la información debe cerciorarse especialmente de que la sala de datos está estrictamente controlada.

Muchos usuarios descargan aplicaciones para móviles de forma regular sin considerar los aspectos de seguridad.

La movilidad presenta nuevos riesgos para los usuarios y los datos. Los investigadores de Cisco han observado a sujetos que utilizan canales inalámbricos para interceptar los datos que se intercambian a través de tales canales y obtener acceso a ellos. La movilidad presenta asimismo un abanico de problemas de seguridad para las organizaciones, entre los que se incluyen la pérdida de propiedad intelectual y de otros datos confidenciales si un empleado extravía un dispositivo o es víctima de un robo, y no contaba con la seguridad pertinente.

Según los expertos de Cisco, una solución para mejorar la seguridad de la empresa consistiría en establecer un programa formal destinado a la administración de los dispositivos móviles con el objetivo de garantizar que todos los dispositivos son seguros antes de que puedan acceder a la red. Como mínimo, se debe exigir el bloqueo por número de identificación personal (PIN) para autenticar al usuario y el equipo de seguridad debe poder apagar o borrar el dispositivo de forma remota si se pierde o lo roban.

Tendencias de malware para dispositivos móviles: 2013

Cisco TRAC/SIO y Sourcefire, que ahora forma parte de Cisco, llevaron a cabo las siguientes investigaciones sobre las tendencias de malware para dispositivos móviles durante 2013.

El malware para dispositivos móviles que tiene como objetivo dispositivos específicos solo constituyó el 1,2% de todos los encuentros con malware web de 2013. Aunque no se trata de un porcentaje significativo, merece la pena señalarlo porque el malware para dispositivos móviles representa sin lugar a dudas un área de exploración emergente –y lógica– para los desarrolladores de malware.

Según los investigadores de Cisco TRAC/SIO, cuando el malware para dispositivos móviles tiene como objetivo poner en peligro un dispositivo, el 99% de todos los encuentros están dirigidos a dispositivos con Android. Los troyanos dirigidos a dispositivos habilitados para Java Micro Edition (J2ME) ostentaron el segundo puesto en 2013, con un 0,84% de todos los encuentros con malware para móviles.

No obstante, no todo el malware para móviles está diseñado para atacar dispositivos específicos. Muchos encuentros involucran suplantación de identidad, usos obligados del botón "Me gusta" (likejacking) y otras estratagemas de ingeniería social, o bien redireccionamientos forzosos a sitios web diferentes a los esperados. Un análisis de los agentes de usuario de Cisco TRAC/SIO revela que los de Android, con un 71%, presentan la mayor frecuencia de casos con todos los formatos de malware distribuido por Web, seguidos por los de Apple iPhone, con un 14% de todos los encuentros con malware web (Figura 14).

Además, los investigadores de Cisco TRAC/SIO indicaron que existían indicios de que intentaron monetizar las vulnerabilidades de Android durante 2013, incluida la puesta en marcha de publicidad no deseada (adware) y de spyware relacionado con las pequeñas y medianas empresas (PYMES).

Con un 43,8%, Andr/Qdplugin-A representó el malware para móviles encontrado con más frecuencia, según el estudio de Cisco TRAC/SIO. Los encuentros habituales se producían mediante copias reempaquetadas de aplicaciones legítimas que se distribuían por medio de mercados oficiosos (Figura 15).

FIGURA 14

Encuentros con malware web por dispositivo móvil

Fuente: informes de Cisco Cloud Web Security

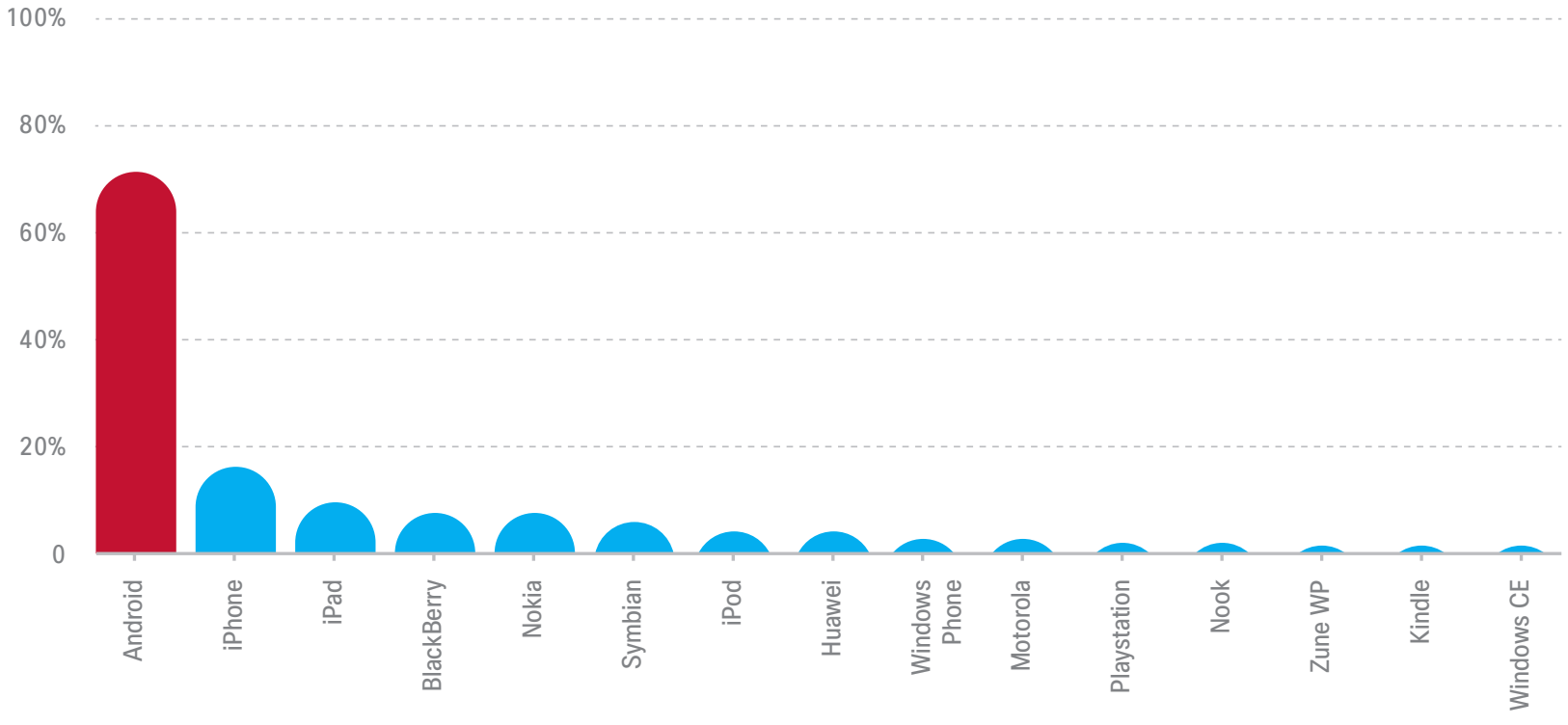


FIGURA 15

Los 10 principales encuentros con malware para móviles (2013)

Fuente: informes de Cisco Cloud Web Security

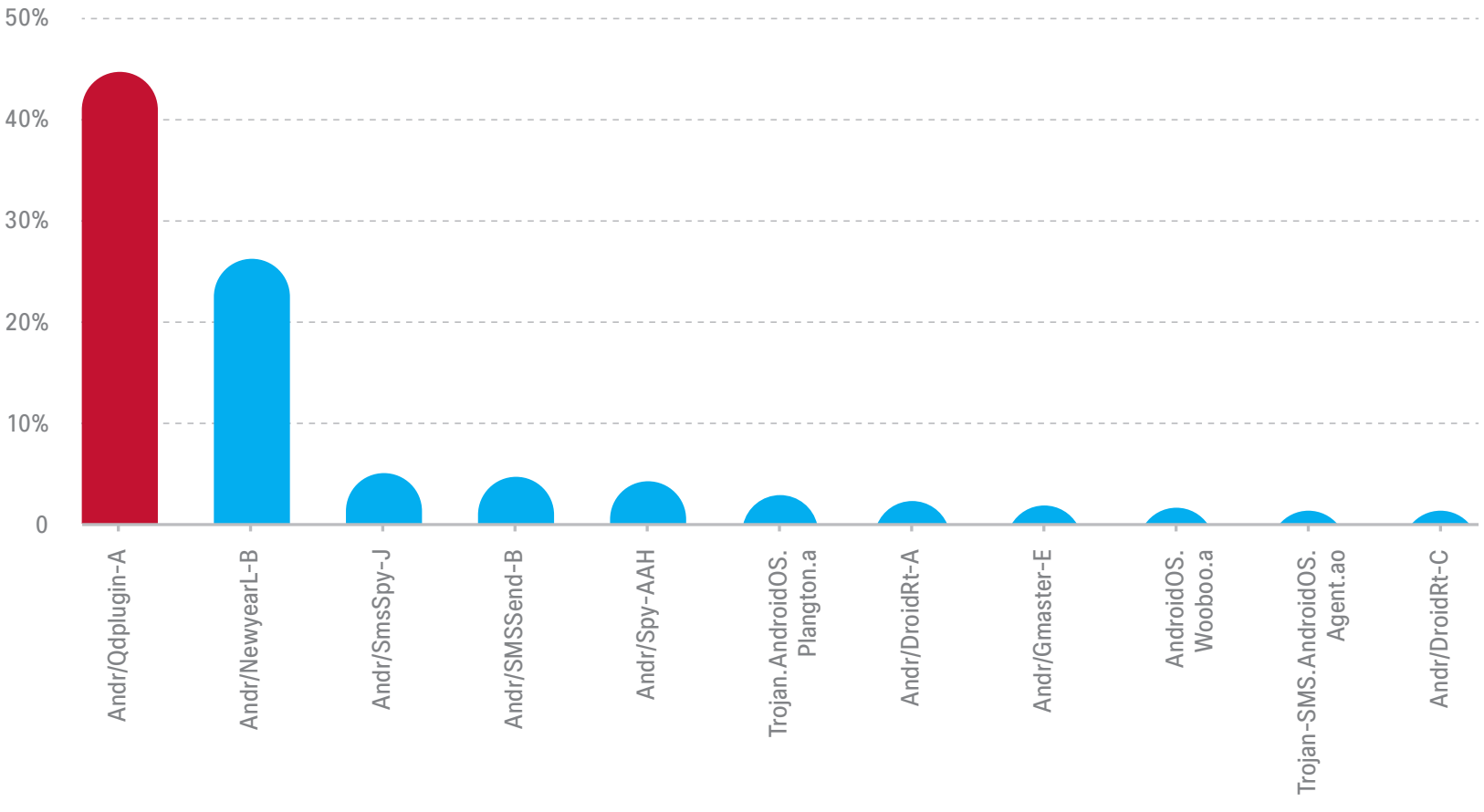
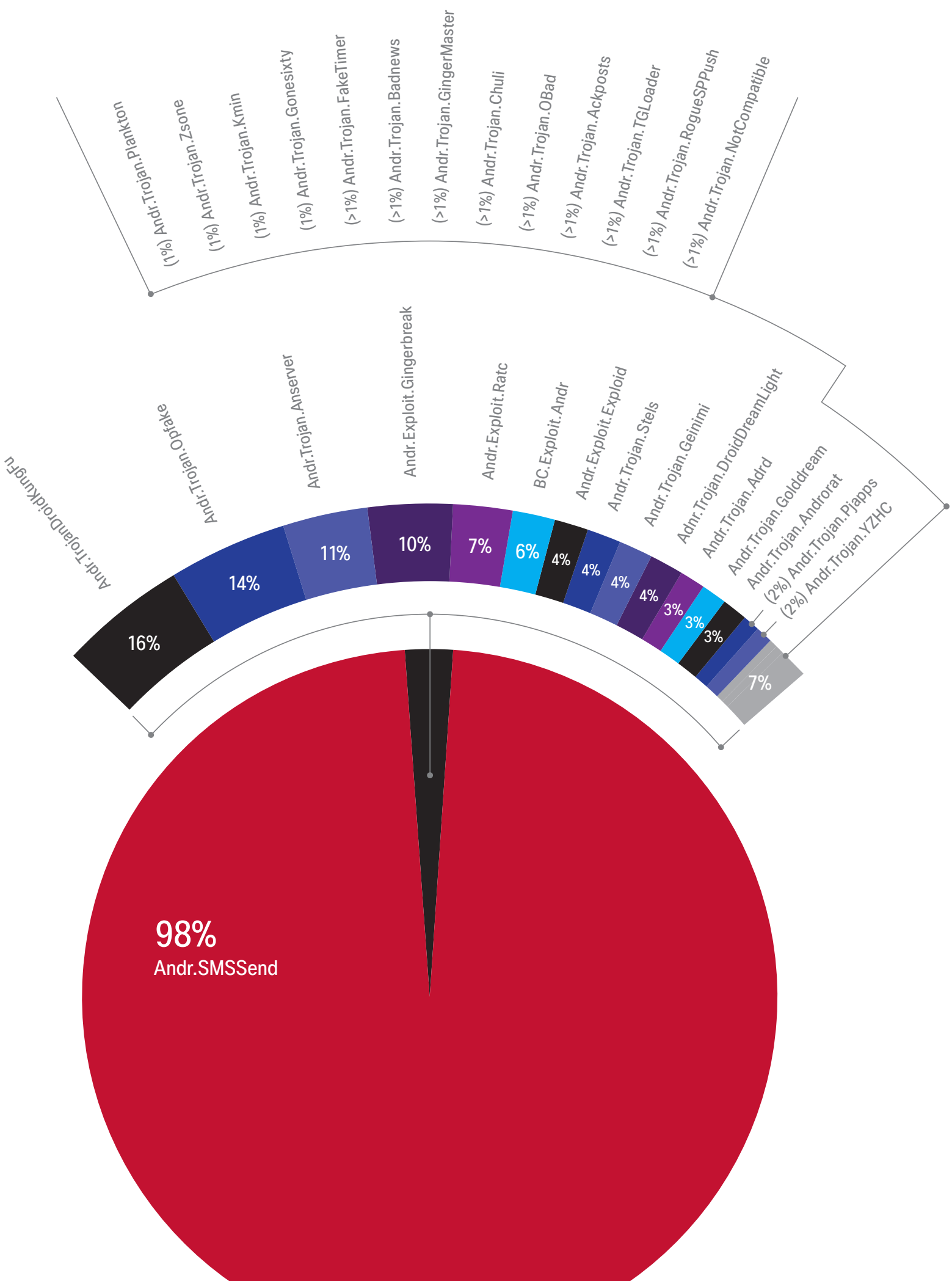


FIGURA 16

Principales familias de malware de Android observadas en 2013

NOTA: SMSSend representa el 98% de todo el malware de Android, el 2% restante se muestra de forma proporcional. Fuente: Sourcefire



Ataques selectivos: el reto de expulsar a "visitantes" ubicuos y persistentes

Existen muchas probabilidades de que los ataques selectivos ya se hayan infiltrado en sus redes.

En este sentido, cuando se alojan dentro de una red, tienden a quedarse, y roban datos o utilizan los recursos de la red de forma sigilosa como trampolín a fin de atacar otras entidades (para obtener más información acerca de la técnica del "pivoting", consulte la página 18). El daño no se limita al robo de datos o a la interrupción en el trabajo: la confianza entre los partners y los clientes puede desvanecerse si no se los expulsa a tiempo.

Los ataques selectivos amenazan la propiedad intelectual, los datos de clientes y la información confidencial del gobierno. Sus creadores emplean herramientas sofisticadas que eluden la infraestructura de seguridad de las organizaciones. Los criminales no escatiman esfuerzos para garantizar que estas infiltraciones pasan desapercibidas; así, utilizan métodos que desembocan en unos "indicadores de riesgo" (IoC) prácticamente imperceptibles. Su planteamiento metódico para obtener acceso a las redes y llevar a cabo su misión involucra un "despliegue del ataque": la cadena de acontecimientos que, dispuestos en fases, desembocan en una ofensiva.

Una vez que estos ataques selectivos hallan un lugar donde ocultarse dentro de la red, llevan a cabo sus tareas de forma eficaz y, normalmente, lo hacen pasando desapercibidos.

Los delincuentes no escatiman esfuerzos para garantizar que estas infiltraciones pasan desapercibidas.

FIGURA 17

El despliegue del ataque

Para comprender el espectro de amenazas de la actualidad y defender la red de forma eficaz, los profesionales de la seguridad de TI deben pensar como los atacantes. Las organizaciones pueden identificar maneras de fortalecer sus defensas si comprenden mejor el planteamiento metódico que usan los sujetos malintencionados para llevar a cabo su misión. El despliegue del ataque (la expresión abreviada del "despliegue del ciberataque") describe los acontecimientos que, dispuestos en fases, desembocan en una ofensiva.

1. Reconocimiento

Obtener una perspectiva completa de un entorno: redes, terminales, móviles y virtuales, incluidas las tecnologías implementadas para proteger la infraestructura.

2. Escritura

Crear un malware selectivo y con identificación del contexto.

3. Prueba

Garantizar que el malware funciona adecuadamente, específicamente si puede evitar las herramientas de seguridad establecidas.

4. Ejecutar

Navegar por la red más amplia; identificar el contexto, pasar desapercibido y desplazarse lateralmente hasta llegar al objetivo.

5. Cumplir la misión

Recopilar datos, crear interrupciones o provocar una destrucción.

Visión general del malware: tendencias observadas en 2013

Los expertos de seguridad de Cisco efectúan investigaciones y análisis continuos del tráfico de malware y de otras amenazas descubiertas, lo que puede ofrecer una serie de indicadores sobre un posible comportamiento delictivo futuro, así como ayuda a la hora de detectar las amenazas.

FIGURA 18

Categorías principales de malware

Esta figura muestra las principales categorías de malware. Los troyanos constituyen el malware más habitual, seguidos de la publicidad no deseada (adware). Fuente: Sourcefire (soluciones ClamAV y FireAMP)

FIGURA 19

Las principales familias de malware para Windows

Esta figura muestra las principales gamas de malware para Windows. La más grande, Trojan.Onlinegames, se compone esencialmente de ladrones de contraseñas. La solución antivirus ClamAV de Sourcefire lo detecta. Fuente: Sourcefire (solución ClamAV)

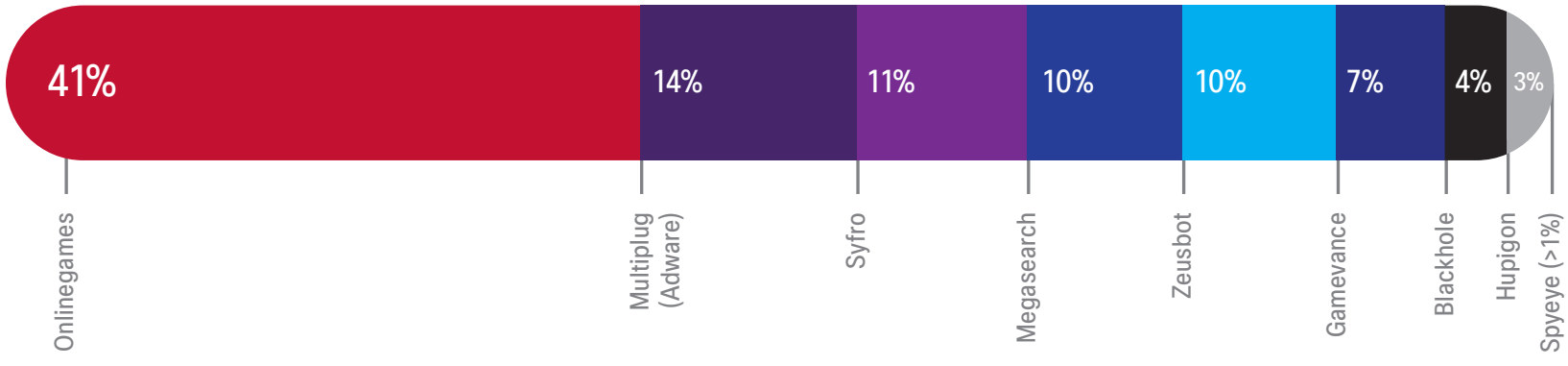


FIGURA 20

Las 10 principales categorías de hosts de malware web (2013)

Esta figura muestra los hosts de malware más frecuentes, de acuerdo con el estudio de Cisco TRAC/SIO.
Fuente: informes de Cisco Cloud Web Security

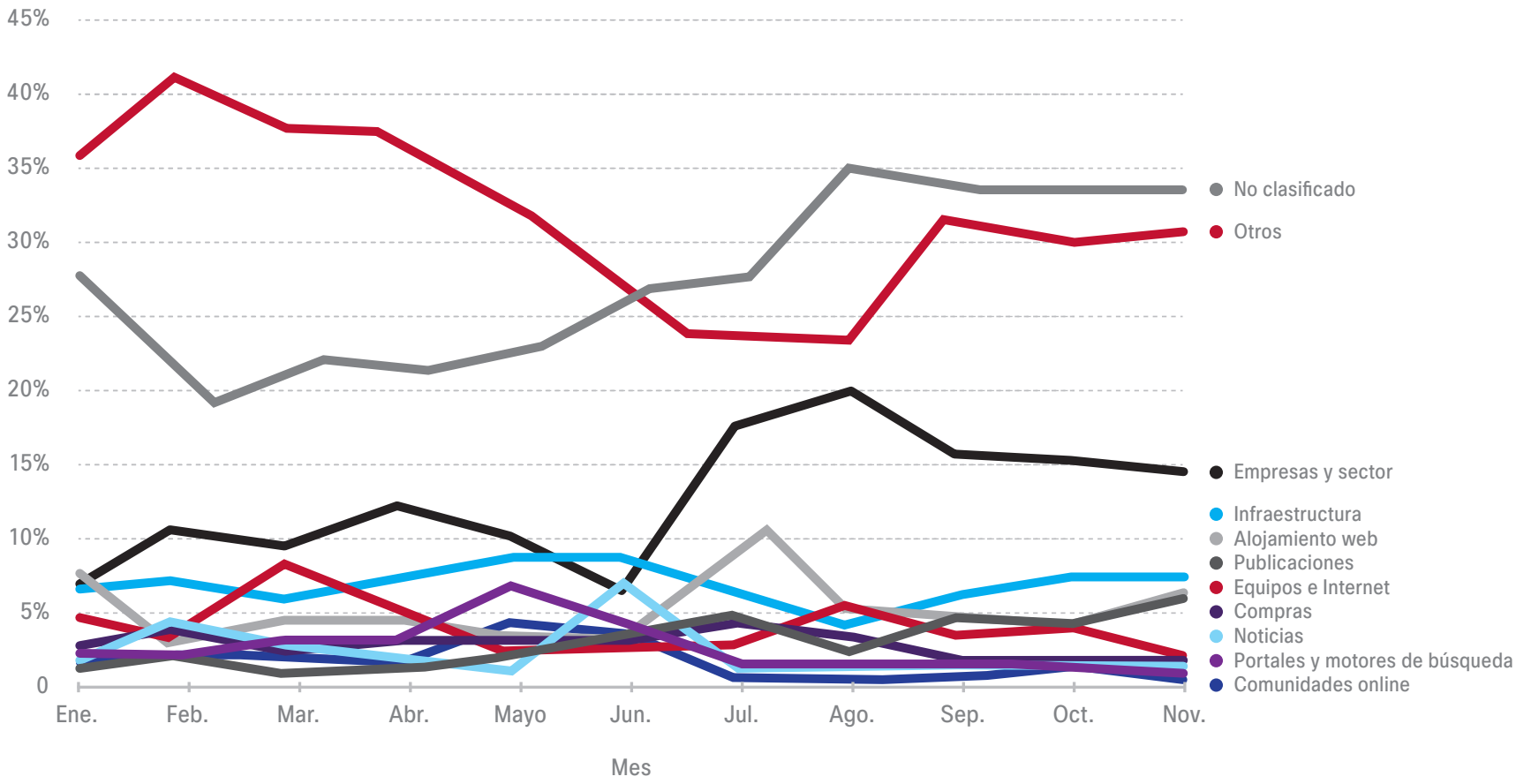
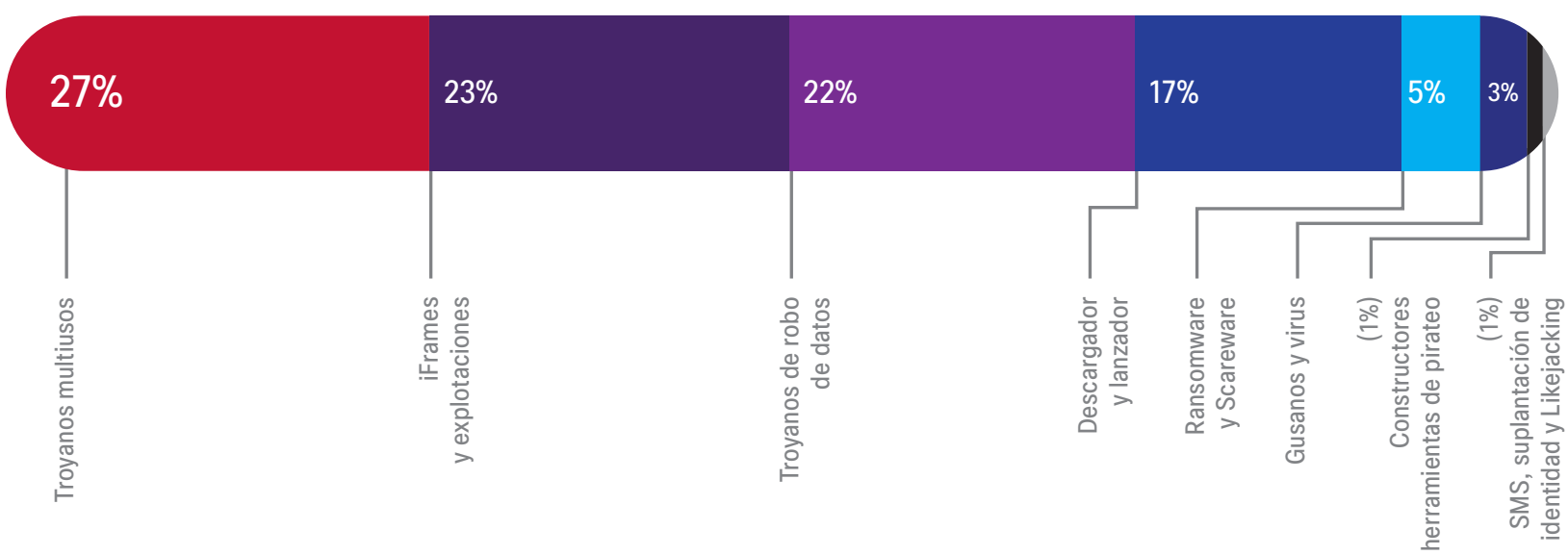


FIGURA 21

Categorías de malware por porcentaje de encuentros totales (2013)

Fuente: Cisco TRAC/SIO



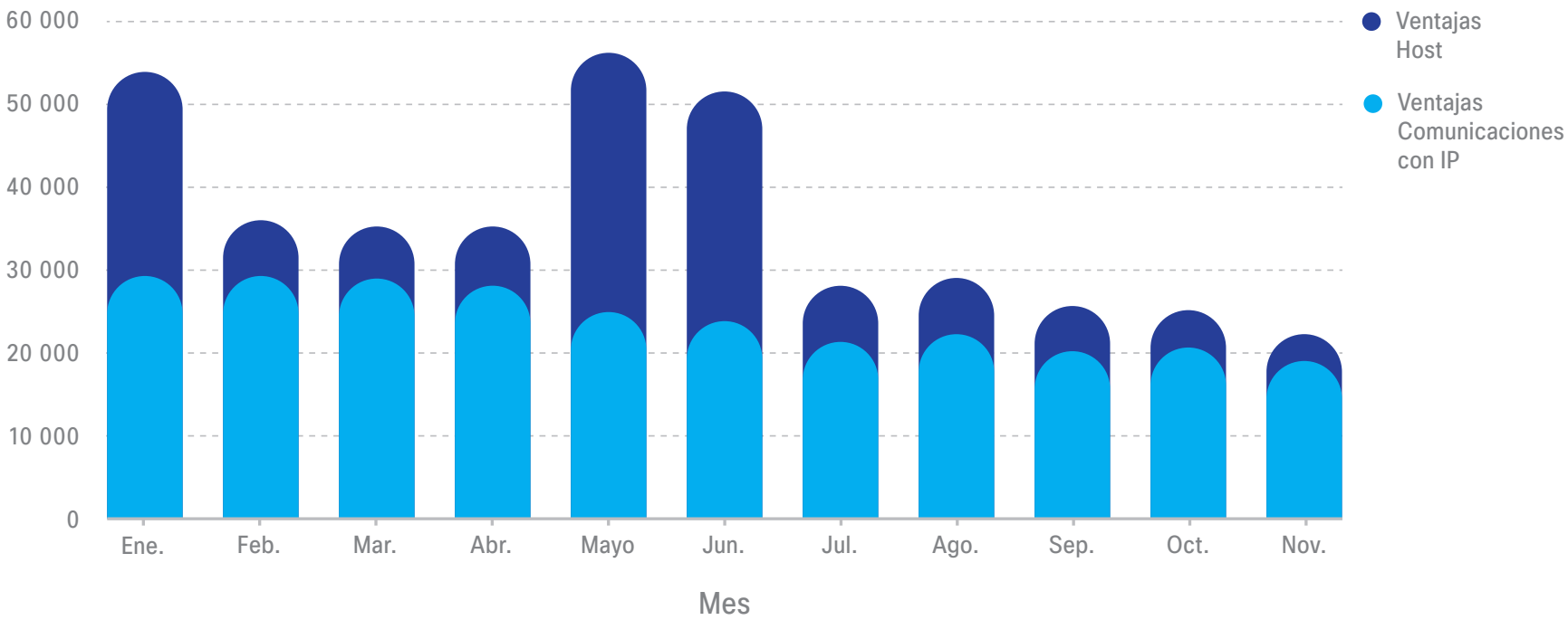
Las investigaciones de Cisco TRAC/SIO durante 2013 muestran que los troyanos multiusos representaron el malware distribuido por Web que se encontraba con más frecuencia, con un 27% de los casos totales. Los scripts malintencionados, como marcos iFrame y aprovechamientos de vulnerabilidades, constituyeron la segunda categoría hallada con mayor frecuencia, con un 23%. Los troyanos de robo de datos, como los ladrones de contraseñas y las puertas traseras, formaron el 22% de los casos totales de malware web, mientras que los troyanos descargadores y lanzadores descendieron al cuarto puesto, con un 17% de los encuentros totales (véase la figura 21).

La disminución constante de direcciones IP y hosts de malware únicos —una reducción del 30% entre enero y septiembre de 2013— indica que el malware se está concentrando en menos direcciones IP y menos hosts (Figura 22). (Nota: Una dirección IP puede publicar sitios web a varios dominios). Conforme el número de hosts disminuya, aunque el volumen de malware permanezca estable, el valor y la reputación de estos hosts revestirá una mayor importancia, dado que los buenos hosts contribuyen a que los criminales logren sus objetivos.

FIGURA 22

Direcciones IP y hosts de malware únicos (2013)

Fuente: informes de Cisco Cloud Web Security



Los abrevaderos no representan un oasis para las empresas objetivo

El uso de ataques de tipo "watering hole" (abrevadero) representa una forma en la que los sujetos malintencionados tratan de distribuir malware a las organizaciones de sectores verticales específicos. Al igual que los depredadores observan a sus presas, los ciberdelincuentes que desean dirigir sus esfuerzos a un grupo particular (por ejemplo, las personas que trabajan en el sector de la aviación) supervisarán qué sitios web frecuenta tal grupo, infectarán uno o varios de estos sitios con malware y, a continuación, se relajarán y esperarán que al menos un usuario del grupo objetivo visite tal sitio y quede comprometido.

Este tipo de ataques representan esencialmente un aprovechamiento de la confianza porque se emplean sitios web legítimos. Asimismo, constituye una forma de ataque de suplantación de identidad dirigido. Sin embargo, mientras que la suplantación de identidad dirigida está orientada a individuos concretos, el método de "watering hole" está diseñado para comprometer a grupos de personas con intereses comunes. Estos ataques no distinguen entre objetivos: cualquiera que visite un sitio web infectado corre un riesgo.

A finales de abril, se puso en marcha un ataque "watering hole" desde páginas específicas que alojaban contenidos relacionados con la energía nuclear en el sitio web del Departamento de trabajo estadounidense.[16] A continuación,

Continúa en la siguiente página

Objetivos principales: los sectores verticales

Según los datos de Cisco TRAC/SIO, las empresas pertenecientes a mercados verticales de elevados beneficios, como los sectores farmacéutico, de productos químicos y de fabricación de dispositivos electrónicos, presentan el mayor índice de casos de malware web.

Este índice aumenta y desciende según el valor de los productos y los servicios de ese mercado vertical concreto se incremente o disminuya.

Los investigadores de Cisco TRAC/SIO han observado un crecimiento notable de casos de malware en los sectores de la agricultura y de la minería, que antiguamente constituían unos mercados con un riesgo relativamente reducido. Atribuyen este aumento de los casos de malware en estos sectores a que los ciberdelincuentes están aprovechando las tendencias como recursos de metales preciosos reducidos e interrupciones en el suministro alimentario relacionadas con las condiciones atmosféricas.

Además, los encuentros con malware del sector de la electrónica prosiguen con su tendencia al alza. Los expertos de seguridad de Cisco señalan que el malware dirigido a este mercado vertical está diseñado habitualmente para contribuir a que los sujetos accedan a la propiedad intelectual, que, a su vez, utilizan para disfrutar de una ventaja frente a la competencia o con el objetivo de venderla al mejor postor.

Para determinar los índices de casos de malware, los investigadores de Cisco TRAC/SIO comparan el índice medio de todas las organizaciones que utilizan Cisco Cloud Web Security como proxy con el de todas las empresas de un sector específico que utilizan este servicio como proxy.

Continuación de la página anterior

desde principios de mayo de 2013, los investigadores de Cisco TRAC/SIO observaron otro ataque de este tipo que se originaba en diversos otros sitios centrados en los sectores energético y petrolífero. Determinadas similitudes, como la creación específica de una vulnerabilidad utilizada en ambos ataques, confirieron credibilidad a la posibilidad de que ambas ofensivas guardaran una relación. El estudio de Cisco TRAC/SIO también indicó que muchos de los sitios utilizaban el mismo diseñador web y proveedor de alojamiento. Este dato podría significar que la vulnerabilidad inicial se debía a unas credenciales robadas o suplantadas a ese proveedor.[17]

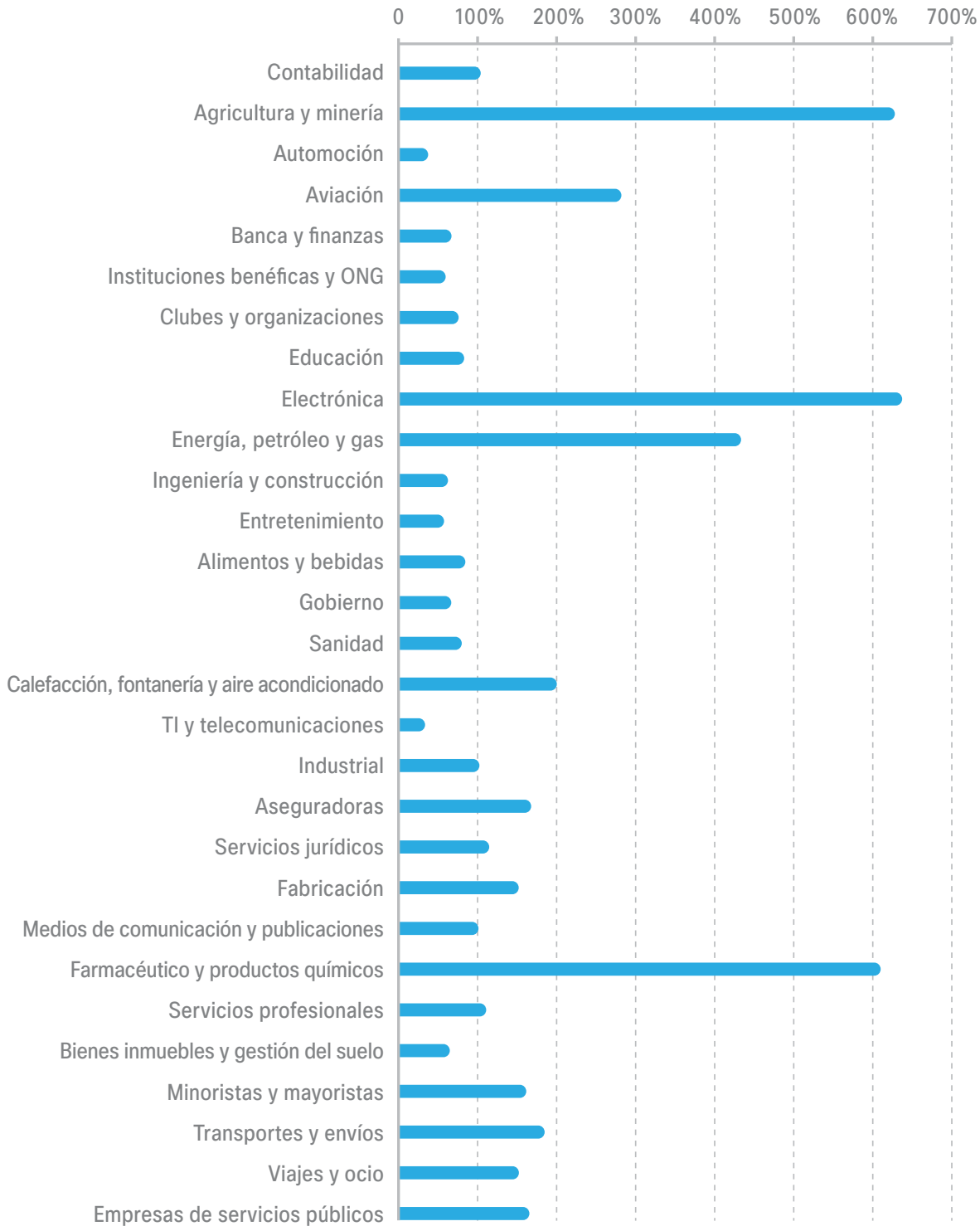
Para proteger a los usuarios frente a estos ataques, se deben aplicar todas las revisiones pertinentes a los equipos y los navegadores de web a fin de minimizar el número de debilidades que puede explotar un atacante. Además, resulta esencial garantizar que el tráfico web se filtre y analice con el propósito de hallar malware antes de distribuirlo al navegador del usuario.

Un índice de casos del sector superior al 100% refleja un riesgo superior al normal de sufrir encuentros con malware web, mientras que un índice por debajo de tal cifra manifiesta un peligro menor. Por ejemplo, una empresa con un índice de casos de un 170% corre un 70% de más riesgo que la media. En cambio, una empresa con un índice de casos de un 70% se encuentra un 30% por debajo de la media (Figura 23).

FIGURA 23

Riesgos de los sectores y encuentros con malware web (2013)

Fuente: informes de Cisco Cloud Web Security



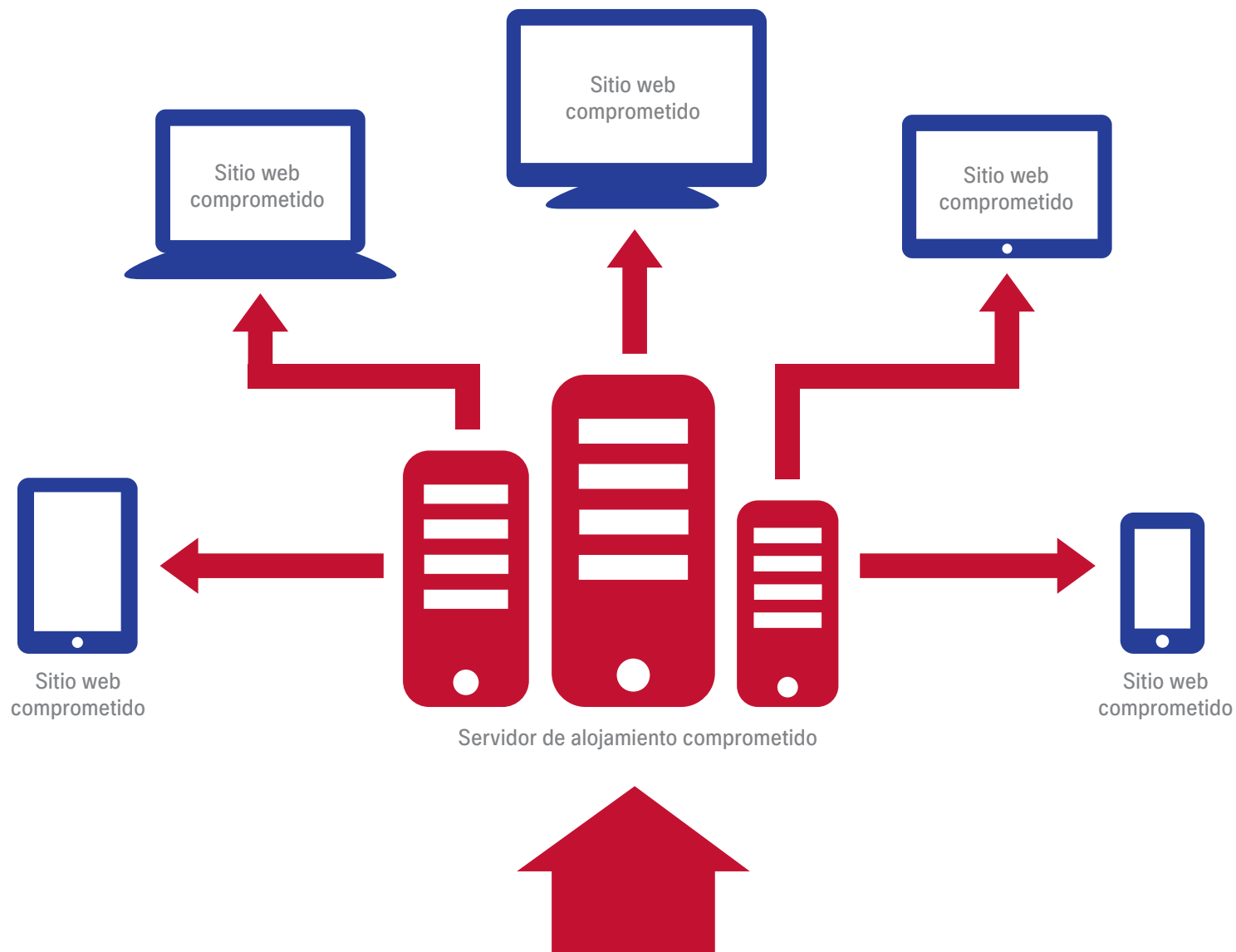
Fracturas en un ecosistema frágil

Los ciberdelincuentes están aprendiendo que el aprovechamiento de las posibilidades de la infraestructura de Internet aporta muchas más ventajas que sencillamente obtener acceso a equipos individuales.

La novedad de las vulnerabilidades malintencionadas es obtener acceso a servidores de alojamiento web, a servidores de nombres y a Data Centers, con el objetivo de sacar partido de la enorme capacidad de procesamiento y ancho de banda que proporcionan. Mediante este planteamiento, las vulnerabilidades pueden llegar a un número mucho mayor de usuarios de equipos desprevenidos y conllevar unas repercusiones muy superiores en la organización objetivo, con independencia de que la meta sea realizar una declaración política, minar un adversario o generar ingresos.

FIGURA 24

Estrategia de infección de gran eficacia



Básicamente, esta tendencia de atacar la infraestructura de Internet implica que no se puede confiar en la propia base de la Web. Los métodos utilizados para obtener, en última instancia, acceso a la raíz de los servidores de alojamiento son diversos y entre ellos se incluyen tácticas como troyanos en estaciones de trabajo de administración que roban credenciales de inicio de sesión en el servidor, vulnerabilidades en herramientas de administración de terceros empleadas en los servidores e intentos de inicio de sesión por fuerza bruta (véase la página 54). Las vulnerabilidades desconocidas del propio software del servidor también podrían ofrecer incursiones.

Un servidor de alojamiento comprometido puede infectar miles de sitios web y propietarios de sitios de todo el mundo (Figura 24).

Los sitios web alojados en servidores comprometidos actúan como un redirector (el intermediario de la cadena de infección) y un repositorio de malware. En lugar de que muchos sitios comprometidos carguen malware de solo unos pocos dominios malintencionados (una relación de "muchos a pocos"), ahora la relación se ha convertido en una de "muchos a muchos", lo que obstaculiza las medidas de desmantelamiento.

Los servidores de nombres de dominio representan los principales objetivos en esta nueva clase de ataques; los métodos exactos de estos continúan siendo objetos de estudio. Los indicadores apuntan a que, además de servidores de alojamiento y sitios web individuales, los servidores de nombres de determinados proveedores de nombres se están viendo comprometidos. Los investigadores de seguridad de Cisco afirman que esta tendencia orientada a atacar la infraestructura de Internet da un vuelco al panorama de amenazas, ya que está proporcionando a los ciberdelincuentes el control sobre una parte considerable de la propia base de la Web.

["El crimen online se ha convertido en una actividad tan lucrativa y altamente esencial que precisa una infraestructura potente para mantenerlo a flote", declara Gavin Reid, director de inteligencia de amenazas de Cisco. "Al comprometer los servidores de alojamiento y Data Centers, los atacantes no solo obtienen acceso a grandes cantidades de ancho de banda, sino también la ventaja de un rendimiento continuo de esos recursos".]

"El crimen online se ha convertido en una actividad tan lucrativa y altamente esencial que precisa una infraestructura potente para mantenerlo a flote".

Gavin Reid, director de inteligencia de amenazas de Cisco

Conexión de los puntos: DarkLeech y Linux/CDorked

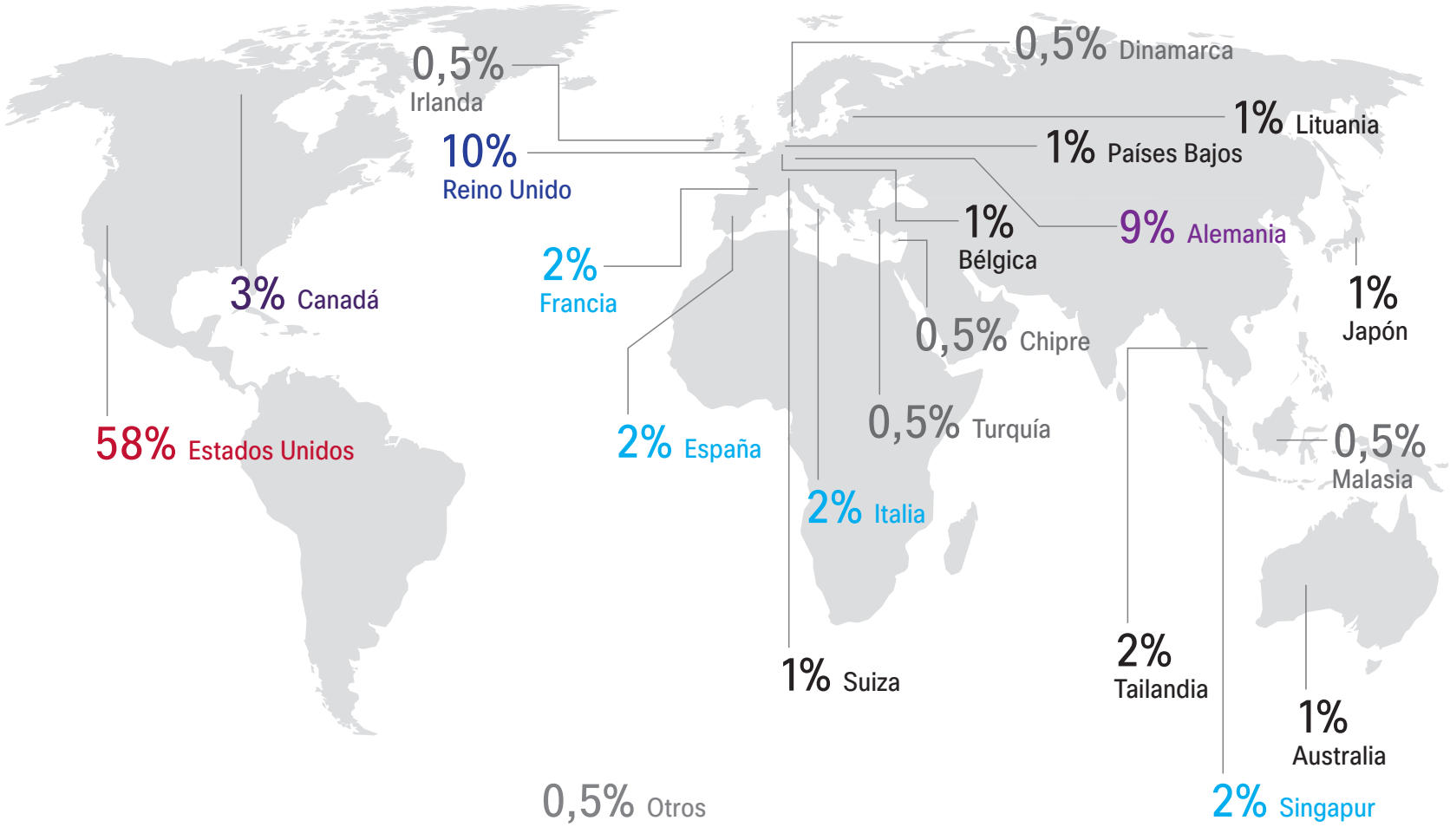
La campaña de ataques DarkLeech sobre la que Cisco informó en 2013[18] pone de manifiesto cómo unos servidores de alojamiento comprometidos pueden servir de trampolín para ejecutar una ofensiva más amplia. Se calcula que los ataques de DarkLeech comprometieron, en un breve lapso de tiempo, al menos 20 000[19] sitios web legítimos de todo el mundo que utilizan el software del servidor Apache HTTP. Los sitios se infectaron con una puerta trasera Secure Shell Daemon (SSHD) que permitía que los atacantes remotos cargaran y configuraran módulos de Apache malintencionados. Esta situación permitió que los atacantes insertaran de forma dinámica marcos iFrame (elementos HTML) en tiempo real en sitios webs alojados, que distribuían código para aprovechar vulnerabilidades y otros contenidos malintencionados mediante el kit de explotación Blackhole.

Como la introducción de un marco iFrame de DarkLeech solo se producen en el momento de la visita del sitio, es posible que los indicios de la infección no sean evidentes. Además, para eludir que se detecte el riesgo, los criminales utilizan una sofisticada gama de criterios

FIGURA 25

Servidores atacados por DarkLeech por país (2013)

Fuente: Cisco TRAC/SIO



condicionales; por ejemplo, solo insertar el marco iFrame si el visitante llega desde la página de resultados de un motor de búsqueda, no insertarlo si la dirección IP del visitante coincide con la del propietario del sitio o la del proveedor de alojamiento, e insertarlo solo una vez cada 24 horas en el caso de los visitantes individuales.

La investigación de Cisco TRAC/SIO desveló que los riesgos derivados de DarkLeech se extendían por todo el mundo; en este sentido, los países con el mayor número de proveedores de alojamiento experimentaron, como es natural, la mayor tasa de infección.

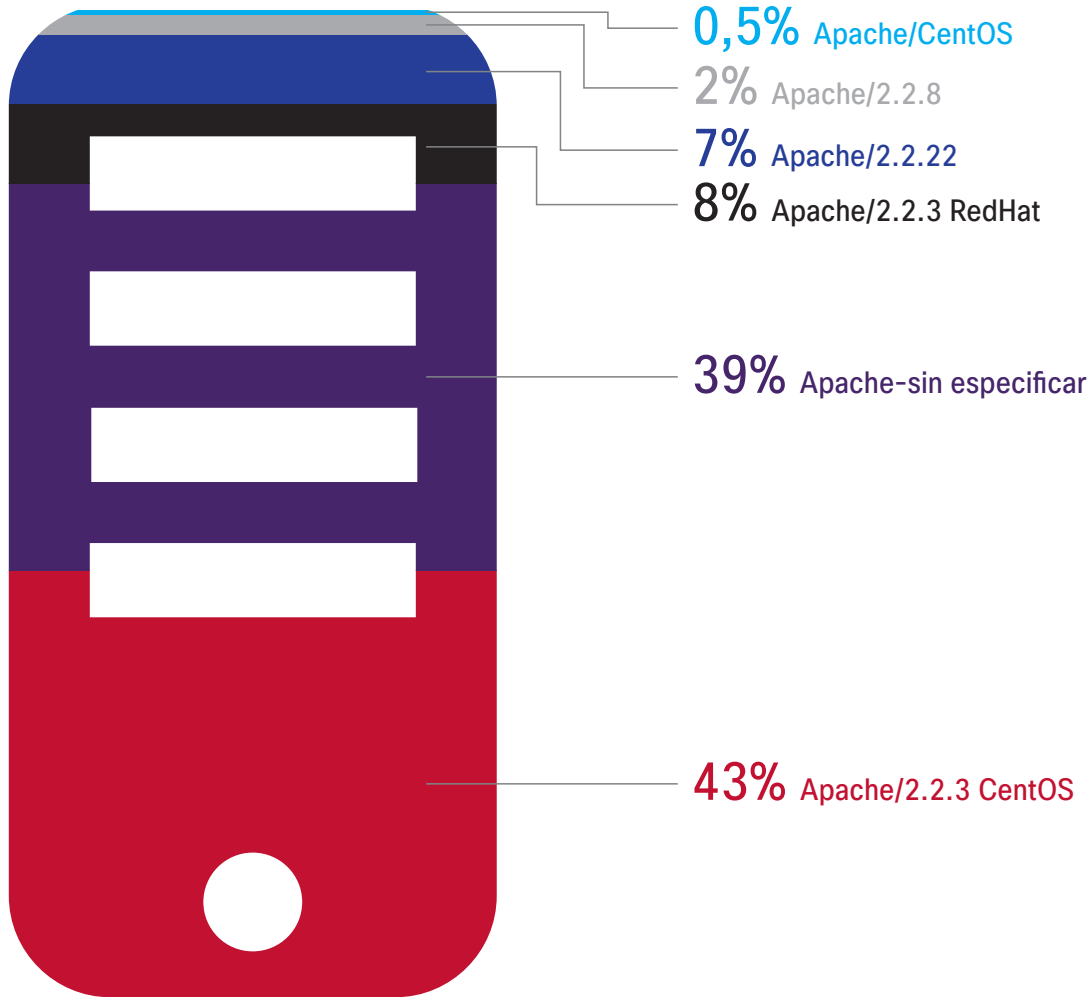
Los investigadores de Cisco SIO/TRAC consultaron miles de servidores comprometidos para conocer en profundidad la distribución de las versiones de software del servidor afectadas.

En abril de 2013, se detectó otra puerta trasera malintencionada que había infectado cientos de servidores que ejecutaban el software del servidor Apache HTTP. Linux/CDorked[20] sustituyó el archivo binario de HTTPD en las versiones de Apache que tenían cPanel instalado. Asimismo, se descubrieron puertas traseras similares dirigidas a Nginx y Lighttpd. CDorked,

FIGURA 26

Respuestas de los servidores atacados por DarkLeech

Fuente: Cisco TRAC/SIO



que presenta unos métodos de ataque tan selectivos como los de DarkLeech, también utiliza criterios condicionales para insertar marcos iFrame de forma dinámica en sitios web alojados en el servidor afectado. A continuación, cualquier visitante que explore el sitio web afectado recibe contenido de malware de otro sitio web malintencionado, donde un kit de herramientas de crimeware trata de comprometer aún más el PC del usuario.[21]

Una característica exclusiva de Linux/CDorked es que se desplaza entre dominios de sitio web a las 24 horas, como promedio. Unos cuantos sitios comprometidos se utilizan durante más tiempo. De esta manera, aunque se informe acerca de un dominio con malware, los atacantes ya se habrán trasladado a otro. También en el caso de Linux/CDorked, los proveedores de alojamiento se cambian con frecuencia (cada dos semanas aproximadamente); de esta manera, se produce un desplazamiento entre los hosts comprometidos con el objetivo de evitar la detección. Los servidores de nombres comprometidos de estos mismos proveedores de alojamiento permiten que los sujetos malintencionados se trasladen de un host a otro sin perder el control de los dominios durante la transición. Una vez se encuentren en el nuevo host, los atacantes dan comienzo a un ciclo de nuevos dominios, normalmente mediante nombres de dominio con errores tipográficos deliberados (typosquatting)[22] en un intento de parecer legítimo ante los observadores eventuales.

CDorked y DarkLeech parecen formar parte de una estrategia mucho más amplia y complicada.

El análisis de los patrones de tráfico con CDorked efectuado por Cisco TRAC/SIO indica claramente la existencia de una conexión con DarkLeech. Esta URL de referencia especialmente codificada que emplea CDorked indica específicamente tráfico proveniente de DarkLeech. En cualquier caso, este no es el giro de acontecimientos más interesante en lo que respecta al malware: tanto CDorked como DarkLeech parecen formar parte de una estrategia mucho más amplia y complicada.

"El grado de sofisticación de estos ataques apuntan a que los ciberdelincuentes han obtenido un control considerable de miles de sitios web y de varios servidores de alojamiento, incluidos los servidores de nombres que emplean esos hosts", afirma Gavin Reid, director de inteligencia de amenazas de Cisco. "Combinado con el reciente aluvión de ataques de inicio de sesión por fuerza bruta contra sitios web individuales, parece que estamos siendo testigos de una inversión de la tendencia; ahora, la infraestructura de la Web se utiliza para formar lo que solo se puede describir como un Botnet muy grande —y muy potente—. Este überbot puede utilizarse para enviar spam, distribuir malware y poner en marcha ataques de DDoS a una escala inédita hasta el momento".

Se ha detectado tráfico malintencionado, con frecuencia un indicio de ataques selectivos, en todas las redes corporativas

Según un examen elaborado por Cisco de las tendencias de inteligencia de amenazas, el tráfico malintencionado es visible en la totalidad de las redes corporativas. Esto se traduce en que existen pruebas de que los delincuentes sofisticados u otros sujetos han penetrado estas redes, y podrían estar llevando a cabo sus actividades mientras pasan desapercibidos durante periodos prolongados.

Todas las organizaciones deben asumir que han sufrido un ataque de piratería o, al menos, aceptar que es cuestión de si constituirán el objetivo de una ofensiva, sino de cuándo y durante cuánto tiempo.

En un proyecto reciente que estudiaba las búsquedas de servicio de nombres de dominio (DNS, Domain Name Service) que se originan dentro de las redes corporativas, los expertos de inteligencia de amenazas de Cisco hallaron que en todos los casos, las organizaciones mostraban indicios de sus redes estaban comprometidas y habían sido objetos de un uso inapropiado (Figura 27). Por ejemplo, la totalidad de las redes empresariales analizadas por Cisco presentaban tráfico a sitios web que alojan malware, mientras que el 92% muestra tráfico a sitios web sin contenido, que normalmente alojan actividad malintencionada. El 96% de las redes estudiadas presentaban tráfico a servidores comprometidos.

Asimismo, Cisco detectó tráfico a sitios web militares o gubernamentales dentro de empresas que normalmente no trabajan con tales sectores, así como a sitios web de zonas geográficas de elevado riesgo, por ejemplo, de países que tienen prohibido desarrollar ningún tipo de actividad comercial con los Estados Unidos. Cisco ha observado que posiblemente se utilicen tales sitios debido a la elevada reputación, generalmente, de la que gozan las organizaciones públicas o gubernamentales. Es posible que el tráfico a estos sitios no constituya una señal definitiva de riesgo, pero, en el caso de las organizaciones que habitualmente no trabajan con el gobierno ni el ejército, podría indicar que los criminales están comprometiendo las redes con el objetivo de utilizarlas para acceder a otras redes y sitios web gubernamentales o militares.

A pesar de haber adoptado todas las medidas posibles para evitar que sus redes se enfrenten a amenazas malintencionadas, todas las organizaciones que Cisco examinó durante 2013 revelaron indicios de tráfico sospechoso. El tráfico identificado mediante las búsquedas de DNS puede aportar unos sólidos indicadores de riesgo; además, merecen una investigación más amplia por parte de las organizaciones que deseen detener a estos agentes de amenazas difíciles de detectar que actúan en sus redes. Se trata de un método orientado a aumentar la visibilidad de las actividades delictivas que, normalmente, resultan muy difíciles de localizar.

FIGURA 27

La ubicuidad del tráfico malintencionado

Malware de alto nivel de amenaza	Conexiones a dominios que son sitios o vectores de amenazas de malware conocidos.	100%
Gubernamental y militar	Tráfico excesivo y sospechoso dirigido a lugares con los que el público general normalmente no entra en contacto.	100%
Infraestructura tomada	Conexiones a infraestructura conocida o sitios comprometidos conocidos.	96%
Sitios sin contenido	Conexiones a sitios vacíos que podrían tener código para incrustar malware a los sistemas.	92%
FTP sospechoso	Conexiones inesperadas a sitios FTP irregulares.	88%
VPN sospechosa	Conexiones desde dentro de una organización a sitios VPN sospechosos.	79%
Educación a través amenazas	Conexiones a universidades desde lugares sospechosos que, en potencia, podrían servir de puntos de apoyo para otros tipos de malware.	71%
Pornografía	Un volumen muy alto de intentos de conexión a sitios pornográficos conocidos.	50%

ARTÍCULO ESPECIAL DE ESTUDIO DE SEGURIDAD DE CISCO:

Nuevas noticias sobre el bitsquatting y nuevas formas de detener ataques

Desde hace tiempo, el cybersquatting –la práctica de registrar nombres de dominio idénticos o equívocamente similares a una marca– ha constituido una herramienta de los delincuentes online. Recientemente, el denominado "bitsquatting", el registro de nombres de dominio que difieren en un dígito binario del dominio original, se ha convertido en otra forma de redireccionar tráfico de Internet a sitios que alojan malware o fraudes.

El bitsquatting constituye una vertiente del cybersquatting que tiene como objetivo los errores de bits que se producen en la memoria de los equipos. Un error de memoria se genera cuando el estado de uno o varios bits que se están leyendo en ella ha cambiado con respecto a lo que se había escrito con anterioridad. Tales errores se originan a causa de muchos factores, entre los que se incluyen los rayos cósmicos (partículas de gran energía que golpean a la Tierra con una frecuencia de 10 000 por metro cuadrado y segundo), que el dispositivo se utilice fuera de sus parámetros medioambientales recomendados, los defectos de fabricación e incluso las explosiones nucleares de baja potencia.

Con cambiar un único bit, un dominio como "twitter.com" puede convertirse en "twitte2.com", del que los atacantes sacan partido. Estos pueden simplemente registrar el dominio en cuestión, esperar a que se produzca un error de memoria y, a continuación, interceptar el tráfico de Internet.

Los investigadores de seguridad creen que los ataques de bitsquatting tienen más probabilidades de ocurrir contra nombres de dominio que se resuelven con frecuencia, dado que estos tendrán más posibilidades de aparecer en la memoria cuando se produzcan los fallos de bits. Sin embargo, un reciente estudio de Cisco prevé que los dominios que anteriormente no se consideraban lo suficientemente populares como para sufrir un ataque en realidad producirán un útil volumen de tráfico para el bitsquatting. Esto se debe a que la cantidad de memoria por dispositivo y el número de dispositivos conectados a Internet están aumentando; según las estimaciones de Cisco, en 2020, habrá 37 000 millones de "objetos inteligentes" conectados a Internet.[23]

Vectores de ataque de bitsquatting

Cisco TRAC/SIO ha identificado nuevos vectores de ataque de bitsquatting, entre los que se incluyen los siguientes:

- Bitsquatting de delimitador de subdominio: de acuerdo con la sintaxis adecuada para las etiquetas de nombres de dominio, los únicos caracteres válidos dentro de estos son A-Z, a-z, 0-9 y el guion. Sin embargo, cuando se busquen dominios relacionados con el bitsquatting, la limitación a estos caracteres deja de lado uno importante que también es válido dentro de sus nombres: el punto. Una nueva técnica de bitsquatting aprovecha los errores de bits que provocan que una letra "n" (01101110 en binario) se convierta en un punto "." (00101110 en binario) y viceversa.
- Delimitadores de subdominio en los que "n" se convierte en ".": en una variación de la técnica anterior, si un nombre de dominio de segundo nivel contiene la letra "n" y existen dos o más caracteres tras esa letra, entonces se trata de un "bitsquat" potencial. Por ejemplo, "windowsupdate.com" podría convertirse en "dowsupdate.com".
- Bitsquatting de delimitador de URL: un contexto popular para los nombres de dominio se encuentra dentro de una URL. Dentro de una URL habitual, los caracteres de barra inclinada, como "/", actúan como delimitadores y separan el esquema del nombre de host de la ruta URL. El carácter de barra inclinada (00101111 en binario) puede, con el cambio de un bit, convertirse en la letra "o" (01101111 en binario) y viceversa.

Continúa en la siguiente página

Continuación de la página anterior

Prevención de los ataques de bitsquatting: creación de un RPZ "bitsquat"

Las dos técnicas de mitigación que se han utilizado habitualmente para evitar el bitsquatting ocupan su lugar en el arsenal de seguridad, pero ninguna resulta óptima:

- Utilizar memoria de corrección de errores (ECC): habría que actualizar toda la base de dispositivos instalados de forma simultánea en todo el mundo para convertir esta alternativa en una solución eficaz.
- Registrar el dominio "bitsquat", de modo que ningún otro tercero pueda hacerlo: esta alternativa no siempre resulta factible, puesto que ya se han registrado muchos dominios "bitsquat" populares. En función de la longitud del nombre de dominio, también podría suponer un elevado coste.

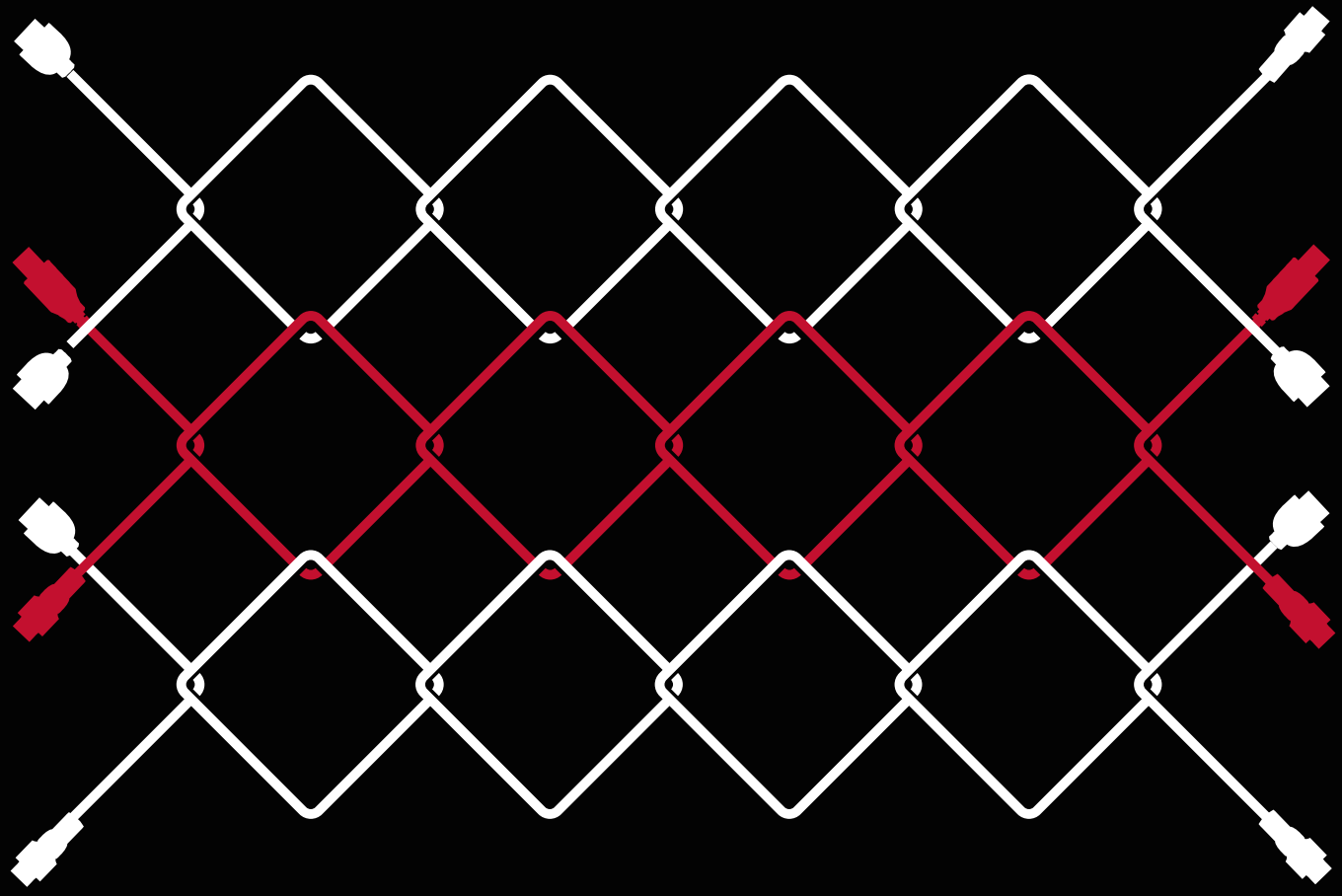
El lado bueno se encuentra en que estas técnicas de mitigación no representan las únicas que un profesional de seguridad puede implementar para proteger a los usuarios del redireccionamiento erróneo y accidental del tráfico de Internet. Con un grado de adopción suficiente, las nuevas mitigaciones podrían eliminar el problema del bitsquatting casi por completo.

Por ejemplo, las zonas de política de respuesta (RPZ) han figurado como una opción de configuración desde la versión 9.8.1 de BIND; además, existen parches para versiones anteriores de BIND. (BIND es un software de DNS de Internet muy utilizado). Los RPZ constituyen archivos de zona local que permiten que la resolución de DNS responda a solicitudes de DNS específicas afirmando que el nombre de dominio no existe (NXDOMAIN), redireccionando al usuario a un "espacio protegido" (una plataforma cerrada), o bien poniendo en práctica otras posibilidades.

Con el objetivo de mitigar los efectos de errores de un único bit para los usuarios de una resolución DNS, el administrador de resolución puede crear una RPZ que proteja frente al bitsquatting de nombres de dominio solo internos y aquellos que se resuelvan con frecuencia. Por ejemplo, la RPZ puede configurarse de modo que cualquier solicitud efectuada a la resolución de DNS para variantes "bitsquat" de estos dominios obtendrá una respuesta NXDOMAIN; de esta manera, se "corregirían" silenciosamente los errores de bit sin ningún esfuerzo por parte del cliente que experimenta el error de bit.[24]

Sector

Los investigadores de Cisco SIO llevan el debate a tendencias del sector que rebasan el ámbito de la telemetría de Cisco.



Los intentos de inicio de sesión por fuerza bruta suponen una táctica preferida para atacar sitios web

Aunque los intentos de inicio de sesión por fuerza bruta no suponen en absoluto una nueva táctica para los ciberdelincuentes, su uso se multiplicó por tres durante la primera mitad de 2013.

En el transcurso de la investigación, los investigadores de Cisco TRAC/SIO descubrieron una concentración de datos que se empleaba para efectuar tales acciones. En ella se incorporaban 8,9 millones de posibles combinaciones de nombres de usuario y contraseñas, incluidas contraseñas complejas; no solo las que se descubren con facilidad, del tipo "contraseña123". Las credenciales de usuario robadas contribuyen a mantener esta lista, y otras similares, bien provista.

FIGURA 28

Cómo funcionan los intentos de inicio de sesión por fuerza bruta

Los principales objetivos de recientes intentos de inicio de sesión por fuerza bruta son plataformas de sistemas de administración de contenido (CMS) ampliamente utilizadas, como WordPress y Joomla. Los intentos con éxito de obtener acceso no autorizado mediante un CMS dotan a los atacantes de la capacidad de cargar puertas traseras de PHP (preprocesador de hipertexto) y otros scripts malintencionados en los sitios web comprometidos. En determinados casos, la vulnerabilidad puede permitir que los atacantes encuentren el camino hasta un servidor de alojamiento, que, a continuación, pueden ocupar (Figura 28).

Teniendo en cuenta que existen más de 67 millones de sitios de WordPress en todo el mundo —y que los editores emplean la plataforma para crear blogs, revistas, redes sociales, así como sitios de noticias, deportivos y empresariales, entre otros— no sorprende, pues, que muchos delincuentes online tengan la vista puesta en obtener acceso a través de estos CMS.[25] Drupal, una plataforma de CMS que se desarrolla con celeridad, también ha constituido un objetivo este año; por ejemplo, en mayo, se recomendó a los usuarios que cambiaran sus contraseñas porque se había producido un acceso no autorizado (a Drupal) a través de un software de terceros instalado en la infraestructura de servidores de Drupal.org.[26]

Muchos delincuentes online tienen la vista puesta en obtener acceso a través de CMS.

No obstante, la popularidad de estos sistemas no es el único factor por el que resultan objetivos apetecibles. Los propietarios de estos sitios los han abandonado en gran medida —aunque continúan activos—. Posiblemente, existen millones de dominios adquiridos y blogs abandonados que están inactivos; ahora, muchos de ellos pertenecen probablemente a ciberdelincuentes. Los expertos de seguridad de Cisco señalan que el problema solo tiene visos de empeorar conforme más y más personas de los mercados emergentes de Internet de todo el mundo establezcan un blog o un sitio web para después olvidarlos.

El uso generalizado de complementos, que están diseñados para ampliar la funcionalidad de un CMS y reproducir vídeos, animaciones y juegos, también está demostrando ser una bendición para los malhechores que desean obtener acceso no autorizado a plataformas como WordPress y Joomla. Muchas de las vulnerabilidades de CMS que han observado los investigadores de Cisco en 2013 se originan en complementos escritos en el lenguaje de scripting web PHP que se diseñaron de forma deficiente y sin ofrecer ninguna concesión a la seguridad.

AMPLIFICACIÓN DE DNS:

Técnicas de mitigación

Según los expertos de seguridad de Cisco, los ataques iniciados mediante la amplificación de DNS continuarán figurando como una preocupación en 2014. La iniciativa Open Resolver Project (openresolverproject.org) informa de que, a fecha de octubre de 2013, 28 millones de resoluciones abiertas en Internet presentan una "amenaza considerable" (tenga presente que el ataque de DDoS de Spamhaus de 300 Gbps solo empleó 30 000 resoluciones abiertas).

Si una resolución está abierta, implica que no filtra cuando envía respuestas. DNS utiliza el protocolo UDP, que no dispone de información de estado, lo que implica que se puede realizar una solicitud en nombre de otra parte. A continuación, esa parte recibe una cantidad de tráfico amplificada. Por este motivo, el sector estará haciendo frente a la identificación de resoluciones abiertas –y tomando medidas para cerrarlas– durante cierto tiempo.

Las empresas pueden reducir la probabilidad de recibir un ataque iniciado mediante amplificación de DNS de varias maneras, entre las que se incluyen la implementación de la mejor práctica actual (BCP, Best Current Practice) 38 del Grupo de trabajo de ingeniería de Internet para evitar ser el origen de los ataques. Esta BCP recomienda que los proveedores directos de paquetes de filtros de conectividad IP que accedan a sus redes desde clientes descendentes y que descarten todos los paquetes que

Continúa en la siguiente página

Ataques de DDoS: se vuelve a llevar lo antiguo

Las ofensivas de denegación de servicio distribuida (DDoS) –que interrumpen el tráfico entrante y saliente de los sitios web objetivos y pueden paralizar a los ISP (proveedores de servicios de Internet)– han estado aumentando tanto en volumen como en gravedad.

Puesto que los ataques de DDoS se han considerado durante mucho tiempo como un método arcaico en materia de técnicas de crimen online, muchas empresas tenían la tranquilidad de que las medidas de seguridad establecidas podrían proporcionar la protección adecuada. No obstante, esa confianza se ha tambaleado en vista de ataques de DDoS a gran escala en 2012 y 2013, entre los que se incluyen la Operación Ababil, que estaba dirigida contra varias instituciones financieras y, probablemente, contaba con una motivación de carácter político.[27]

"Los ataques de DDoS deben figurar como una de las principales preocupaciones de seguridad para las organizaciones de los sectores privado y público en 2014", afirma John N. Stewart, vicepresidente sénior y director de seguridad de Cisco. "Se espera que las campañas futuras sean más amplias y abarquen periodos prolongados. Las organizaciones, en especial aquellas que desarrollan su actividad o tienen intereses en los sectores que ya figuran entre los principales objetivos, como el energético y el de servicios financieros, deben formularse la siguiente pregunta: ¿podemos resistir un ataque de DDoS?".

Un nuevo giro: algunos ataques de DDoS se emplean probablemente para ocultar otras actividades dañinas,

Continuación de la página anterior

tengan una dirección de origen que no esté ubicada en ese cliente.[30] La BCP se elaboró en colaboración con Cisco, que ofrece directrices sobre la instalación de uRPF, su implementación.[31]

Otra técnica de mitigación consiste en configurar todos los servidores DNS autorizados para limitar la velocidad. El servidor de nombres autorizado, que publica el dominio de una empresa, está normalmente abierto a todas las solicitudes. El limitador de velocidad de recepción DNS (DNS RRL) constituye una función que puede activarse para evitar que un servidor DNS responda a la misma pregunta de la misma entidad demasiadas veces; de esta manera, se impide que se utilice a la empresa como intermediaria en ataques de DDoS. DNS RRL está habilitado en los servidores DNS y aporta una opción a los administradores de los servidores para limitar la eficacia en la que los atacantes pueden utilizar un servidor en ofensivas de amplificación. El limitador de velocidad de recepción DNS constituye una función más nueva y no es compatible con todos los servidores DNS; sin embargo, es compatible con ICS BIND, un popular servidor DNS.

Además, todos los servidores DNS recursivos deben configurarse con una lista de control de acceso (ACL), de modo que solo respondan a consultas de hosts de su propia red. Una ACL gestionada de forma errónea puede representar un factor principal en ataques de DNS, especialmente en servidores de gran envergadura

Continúa en la siguiente página

como fraude electrónico, tanto durante el despliegue de la campaña como en los momentos anterior y posterior (véase "DarkSeoul", página 58). Estos ataques pueden abrumar al personal bancario, evitar que se envíen notificaciones de transferencias a los clientes e impedir que estos denuncien el fraude. Y, para cuando la institución se recobra de tal suceso, le resulta imposible recuperar sus pérdidas financieras. El 24 de diciembre de 2012 se produjo una ofensiva de este tipo, que estaba dirigida contra el sitio web de una institución financiera de California regional y contribuyó a distraer a los empleados del banco de la intervención de una cuenta online de uno de sus clientes, un golpe que reportó a los ladrones más de 900 000 $.[28]

El rápido desarrollo de la experiencia en aprovechar las vulnerabilidades de servidores de alojamiento solo contribuirá a facilitar que los ciberdelincuentes pongan en marcha ataques de DDoS y roben a las organizaciones objetivo (véase "Fracturas en un ecosistema frágil", página 44). Al ocupar una parte de la infraestructura de Internet, los sujetos malintencionados pueden sacar partido de grandes cantidades de ancho de banda, puesto que les coloca en una posición aventajada para poner en marcha cualquier cantidad de potentes campañas. Ya está sucediendo: en agosto de 2013, el gobierno chino denunció que el ataque de DDoS de mayor envergadura que ha afrontado apagó el Internet chino durante unas cuatro horas.[29]

Incluso los spammers están utilizando ataques de DDoS para arremeter contra las organizaciones que creen que se están interponiendo en su generación de ingresos. En marzo de 2013, la organización sin ánimo de lucro Spamhaus — que efectúa un seguimiento de spammers y creó la lista de bloqueo de Spamhaus, un directorio de direcciones IP sospechosas— fue el objetivo de un ataque de DDoS que clausuró temporalmente su sitio web y ralentizó el tráfico de Internet en todo el mundo. Los atacantes estaban supuestamente afiliados con CyberBunker, un proveedor de alojamiento con unas condiciones de uso permisivas y sede en los Países Bajos, y STOPhaus, un grupo que ha expresado públicamente su aversión hacia las actividades

Continuación de la página anterior

con grandes cantidades de ancho de banda disponibles. Esta técnica contribuye asimismo a reducir las probabilidades de convertirse en un intermediario en un ataque de DDoS.

"Dado que existe un debate en el sector en torno a permitir que los servidores de nombres autorizados deshabiliten el servicio a entidades que acaban por convertirse en intermediarios de ataques de DDoS, las empresas deben poner en práctica las sencillas técnicas de mitigación descritas anteriormente", declara Gavin Reid, director de inteligencia de amenazas de Cisco.

Para obtener más información sobre las prácticas recomendadas de DNS, consulte "DNS Best Practices, Network Protections, and Attack Identification" (Prácticas recomendadas de DNS, protecciones de redes e identificación de ataques): http://www.cisco.com/web/about/security/intelligence/dns-bcp.html.

de Spamhaus. El ataque de DDoS se produjo después de que un servicio de Spamhaus muy extendido incluyó CyberBunker en su lista negra. En un acto manifiesto de represalia, los spammers sospechosos trataron de acabar con Spamhaus mediante un ataque de DDoS.

Este incidente de DDoS empleó una ofensiva de amplificación de DNS, que explota resoluciones DNS abiertas que responden a consultas incluso fuera de su intervalo de IP. Al enviar una consulta muy pequeña creada a propósito con una dirección de origen del objetivo falsificada a una resolución abierta, los atacantes pueden provocar una respuesta considerablemente mayor al blanco planteado. Después de que los intentos iniciales de dejar a Spamhaus sin conexión no dieran resultado, los delincuentes emplearon una ofensiva de amplificación de DNS dirigida contra proveedores de nivel 1 y otros directos de Spamhaus.

DarkSeoul

Como se señala en "Ataques de DDoS: se vuelve a llevar lo antiguo", el nuevo enfoque de los ciberdelincuentes orientado a comprometer servidores de alojamiento y el rápido crecimiento de la experiencia al respecto solo contribuyen a facilitar aún más que pongan en marcha ataques de DDoS y roben a organizaciones.

Los investigadores de seguridad de Cisco advierten de que las campañas de DDoS futuras podrán crear interrupciones y daños considerables, incluidas pérdidas financieras debidas a robos.

Los ataques selectivos de DarkSeoul de marzo de 2013 involucraron un malware "wiper" (borrador) diseñado para destruir los datos de los discos duros de decenas de miles de PC y servidores. La ofensiva estaba dirigida contra

instituciones financieras y compañías de medios de comunicación de Corea del Sur y la carga estaba fijada para activarse al mismo tiempo. Sin embargo, este malware wiper parece suponer únicamente una faceta del ataque. A la vez que se activaba el malware, se inició una ofensiva contra el sitio web del proveedor de red coreano LG U+ y las redes de otras organizaciones objetivo comenzaron a caer, unas capacidades que se encuentran en el malware wiper.[32]

Algunos mantienen que estos ataques fueron consecuencia de una guerra cibernética que ha iniciado Corea del Norte para obstaculizar económicamente a su vecina del sur, o bien un acto de sabotaje por parte de otra nación. Sin embargo, existe la posibilidad de que los ataques de DarkSeoul estuvieran destinados a ocultar unas ganancias económicas.[33]

Los investigadores de seguridad aún tratan de comprender estos ataques –y de descubrir quién estuvo tas ellos–, pero los indicios apuntan a que los planes para DarkSeoul podrían haberse puesto en marcha mucho antes, en 2011. En ese año, la Oficina Federal de Investigación (FBI) estadounidense advirtió por primera vez de la aparición de troyanos bancarios diseñados para ocultar la transferencia de fondos fraudulentos de las cuentas de las víctimas.[34] A continuación, en 2012, la empresa de seguridad RSA informó sobre una nueva categoría de ciberdelincuentes que estaban construyendo una sofisticada campaña de troyanos que lanzarían un ataque en un día programado y tratarían de hacerse con los fondos de tantas cuentas comprometidas como les resultara posible antes de que los sistemas de seguridad detuvieran la operación.[35] Y en la Nochebuena de 2012, los ladrones online utilizaron un ataque de DDoS como tapadera mientras robaban a una institución financiera regional de California.[36]

De acuerdo con los investigadores de Cisco TRAC/SIO, un archivo binario de malware identificado en los ataques de DarkSeoul dirigidos contra organizaciones de medios de comunicación e instituciones financieras es un troyano bancario que atacaba específicamente a clientes de los mismos bancos coreanos. Ese hecho, junto con el cronograma de las tendencias de crimen online que desembocaron en DarkSeoul, indica que la campaña podría haber servido para hacer que un robo pareciera otra actividad.

Ransomware

Durante todo el 2013, los atacantes se han distanciado cada vez más de las infecciones impulsadas por Botnet tradicionales en PC. Parte de este cambio incluía un aumento del uso de ransomware como la carga final de malware de sitios web comprometidos, mensajes de correo electrónico malintencionados y troyanos descargadores. El ransomware consiste en una categoría de malware que impide que los sistemas infectados funcionen con normalidad hasta que se abone una cuota prescrita.

Durante todo el 2013, los atacantes se han distanciado cada vez más de las infecciones impulsadas por Botnet tradicionales en PC.

El ransomware proporciona una fuente de ingresos directa y difícil de seguir, aunque inmediata, para los atacantes sin necesidad del uso de servicios intermediarios alquilados, como los que proporcionan los Botnets tradicionales. Los adversarios imitan economías locales legítimas que han presenciado un aumento considerable de propiedad exclusiva como consecuencia de pérdidas de empleos y declives económicos, pero la motivación de los ciberdelincuentes es la pérdida de disponibilidad de Botnet y de kits de explotación accesibles debido a desmantelamientos.

En otoño de 2013, un nuevo tipo de ransomware, denominado CryptoLocker, comenzó a cifrar los archivos de las víctimas con una combinación de pares de claves de 2048 bits de RSA y AES-256, considerada imposible de descifrar. En acción, CryptoLocker no se limita al equipo local, sino que incluye los tipos de archivos coincidentes de cualquier unidad asignada en la que se pueda escribir. Tras completar el cifrado, a las víctimas se les presenta una serie de cuadros de diálogo que proporcionan unas instrucciones detalladas para el pago del rescate (Figura 29). Se presenta asimismo un temporizador que insta a la víctima a pagar en un plazo específico (que va de 30 a 100 horas). El cuadro de diálogo continúa advirtiendo de que, en el caso de no abonar el rescate en el intervalo especificado, la clave privada se eliminará del servidor de control y mando, después de lo cual se perderá la posibilidad de descifrar los archivos.

El uso de CryptoLocker aumentó repentinamente a mediados de octubre, posiblemente como represalia por la pérdida de los kits de explotación Blackhole y Cool tras el arresto del supuesto autor de esos marcos.

FIGURA 29

Instrucciones de rescate de CryptoLocker

La laguna de soluciones y la escasez personas competentes en el tema de la seguridad

[La sofisticación de la tecnología y las tácticas utilizadas por delincuentes online —y sus intentos incansables de infringir la seguridad de las redes y robar datos— han sobrepasado la capacidad de los profesionales de la seguridad y de TI para abordar las amenazas. La mayoría de las organizaciones no cuentan con el capital humano ni los sistemas para supervisar las redes continuamente y determinar cómo se están infiltrando en ellas.]

La escasez de personas competentes en el tema de la seguridad empeora el problema: incluso cuando los presupuestos lo permiten, a los directores de seguridad de la información les resulta difícil contratar a personas con conocimientos de seguridad actualizados. Se estima que para 2014, al sector aún le faltará más de un millón de profesionales de la seguridad en todo el mundo. También muy solicitados se encuentran los profesionales de la seguridad con conocimientos de la ciencia de los datos; comprender y analizar los datos de seguridad puede contribuir a mejorar la armonización con los objetivos empresariales (véase el apéndice de la página 69, "Las organizaciones precisan científicos de los datos: Herramientas de análisis de datos introductorias para los encargados de la seguridad".)

A los CISO les resulta difícil contratar a personas con conocimientos de seguridad actualizados.

La nube como un nuevo perímetro

Tal y como declaran los directores de seguridad de la información a los expertos de seguridad de Cisco (véase la página 18), trasladar cantidades cada vez mayores de datos críticos empresariales a la nube supone una preocupación de seguridad creciente.

Según Michael Fuhrman, vicepresidente de ingeniería de Cisco, la revolución de la nube es comparable al auge de las soluciones basadas en la Web de finales de la década de 1990.

"Este fue un cambio radical en el uso empresarial de las nuevas tecnologías y, al mismo tiempo, presenciamos un aumento de los ataques online de delincuentes", apunta Fuhrman. "En la actualidad, el cambio radical proviene de la nube. Las empresas no solo alojan muchas de sus aplicaciones esenciales en la nube, sino que también la utilizan para consumir y analizar información empresarial vital".

El auge del Cloud Computing es innegable e imparable.

El auge del Cloud Computing es innegable e imparable. Cisco prevé que el tráfico de red en la nube experimente un aumento superior al triple en 2017.[37]

En 2014 y en adelante, los profesionales de la seguridad podrán ver cómo se trasladan perímetros corporativos al completo a la nube. Estos extremos de la red han pasado a estar mucho menos definidos en los últimos años. Pero con tantas aplicaciones y tantos datos en la nube, las organizaciones están perdiendo rápidamente la capacidad de ver quién y qué entra y sale de las fronteras corporativas, así como qué acciones están realizando los particulares.

Esta transición a la nube cambia las reglas del juego porque redefine el lugar en el que los datos se almacenan, al que se trasladan y desde el que se accede; además, genera mayores oportunidades para los adversarios.

La carencia de información acerca de cómo los proveedores de nube defienden sus productos contra violaciones de la seguridad agudiza los temores que penden sobre la cesión del control de los datos a la nube. Las organizaciones normalmente no formulan las suficientes preguntas

sobre qué se describe en los acuerdos de nivel de servicio de sus proveedores, o con qué frecuencia actualizan su software de seguridad o aplican parches a las vulnerabilidades.

Las organizaciones precisan la garantía de que un proveedor de nube utiliza las estrategias y las herramientas más sofisticadas disponibles para frustrar ataques, o bien detectarlos y detenerlos mientras se estén produciendo. En el caso de los equipos de seguridad de la información, la decisión de avanzar se reduce con frecuencia a una pregunta: "¿qué controles debo buscar en un proveedor con el objetivo de confiar en él para administrar y proteger mis datos?".

Por otra parte, los proveedores de nube afrontan dificultades para identificar e implementar un conjunto de controles fáciles de gestionar dedicados a un número en aumento de regulaciones internacionales, que se precisan para hacer frente a un entorno de amenazas cada vez más hostil.

"Cuando elegimos proveedores para infraestructuras vitales y de seguridad, con frecuencia nos decidimos por uno según la reputación y las cualificaciones técnicas", señala John N. Stewart, vicepresidente sénior y director de seguridad de Cisco. "Últimamente, el proceso y un planteamiento hacia la seguridad que evolucione del proveedor también se han convertido en factores que cada vez revisten una mayor importancia".

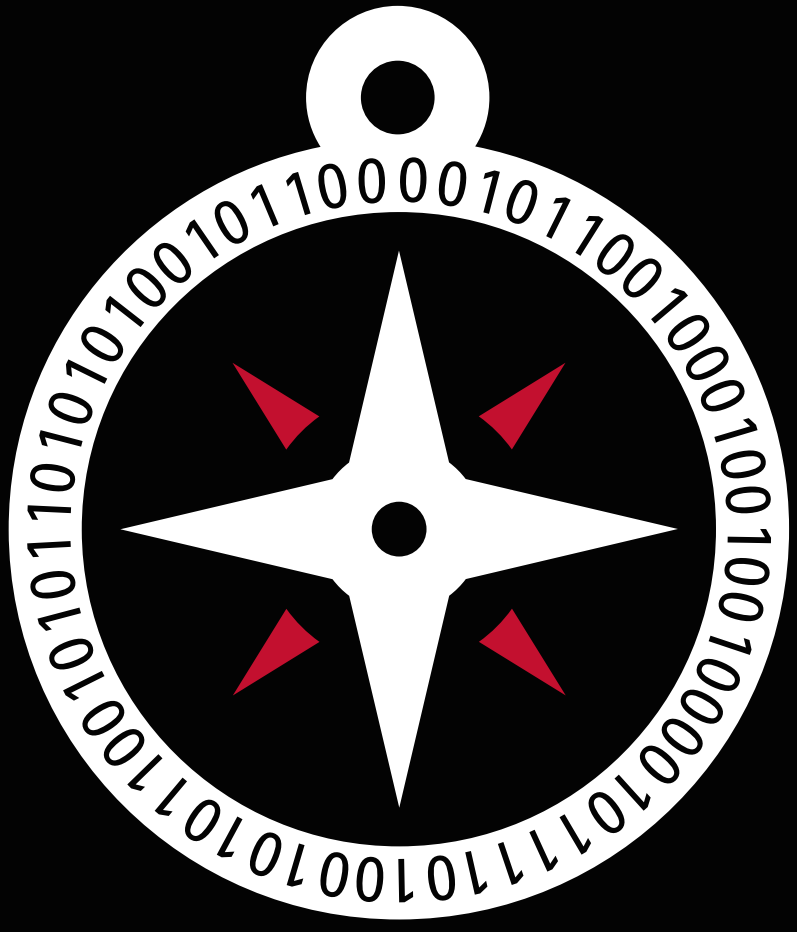
Casualmente, los mismos aspectos que convierten a la nube en una amenaza —como la ubicación externa al perímetro de la red y el aumento del uso de la nube para datos vitales de la empresa— puede posibilitar que las organizaciones consigan que el proceso de toma de decisiones en materia de seguridad resulte más preciso y se produzca en prácticamente tiempo real. Puesto que cada vez pasa más tráfico por la nube, las soluciones de seguridad también pueden utilizarla para analizar rápida y fácilmente este tráfico, y sacar partido de esta información complementaria. Además, en el caso de las organizaciones pequeñas o aquellas con limitaciones presupuestarias, un servicio en la nube bien protegido y gestionado puede ofrecer más garantías de seguridad que los propios servidores y firewalls de una empresa.

"Cuando elegimos proveedores para infraestructuras vitales y de seguridad, con frecuencia nos decidimos por uno según la reputación y las cualificaciones técnicas. Últimamente, el proceso y un planteamiento hacia la seguridad que evolucione del proveedor también se han convertido en factores que cada vez revisten una mayor importancia".

John N. Stewart, vicepresidente sénior y director de seguridad de Cisco

Recomendaciones

Muchas organizaciones encuentran dificultades para consolidar una visión de seguridad respaldada por una estrategia eficaz que emplee nuevas tecnologías, simplifique su arquitectura y sus operaciones, y fortalezca sus equipos de seguridad.



Objetivos para 2014: verificar la fiabilidad y mejorar la visibilidad

En la actualidad, en un entorno en el que el nivel de confianza asociada con una red o un dispositivo debe evaluarse de forma dinámica, las organizaciones se enfrentan a modelos de seguridad fragmentados que aplican las políticas de un modo poco uniforme, a inteligencia de amenazas aislada y a la proliferación de proveedores y productos que se deben administrar.

Las conexiones entre las organizaciones, los datos y los ataques avanzados que ponen en marcha sujetos malintencionados resultan sencillamente demasiado complejas para que un único dispositivo haga frente a ellas. Lo que es más, la mayoría de las organizaciones carecen del personal de seguridad con la experiencia y los conocimientos suficientes para ayudarles a adaptar sus modelos de seguridad a los retos –y las oportunidades– que presentan el Cloud Computing, la movilidad y las nuevas maneras de desarrollar la actividad comercial impulsadas por los avances tecnológicos.

En el último año se ha presenciado como organizaciones de todos los tipos experimentaban dificultades para adoptar la innovación sin crear nuevas lagunas de seguridad o ampliar las que ya se conocían. El año 2013 también sacó a relucir el problema de la confianza. Ahora, resulta aún más probable que los usuarios de todos los tipos pongan en duda la fiabilidad de la tecnología de la que dependen cada día, tanto el ámbito profesional como en el personal. Por tanto, resulta más importante que nunca que los proveedores de tecnología contribuyan a asegurar a los clientes que la seguridad figura como una prioridad en sus procesos de fabricación y que estén preparados para respaldar tales garantías.

"Nos encontramos en una transición de mercado en la que la confianza reviste importancia, y el proceso y la tecnología deben representar unas características integrales del diseño de productos para que un proveedor satisfaga las necesidades que crean las amenazas de la actualidad", explica el director de seguridad de Cisco, John N. Stewart. "La palabra de una empresa no es suficiente. Las compañías precisan recibir una garantía por medio de productos certificados, procesos de desarrollo integrados, tecnología innovadora y una reputación respectada en el sector. Las organizaciones también deben convertir la verificación de la credibilidad de los productos tecnológicos que utilizan y de los proveedores que los suministran en una prioridad constante.

Mejorar la armonización entre las operaciones de seguridad y los objetivos empresariales también supone una importante medida para fortalecer la seguridad de la empresa. En una coyuntura de recursos limitados y presupuestos anémicos, esta armonización puede contribuir a que los directores de seguridad de la información y otros ejecutivos del mismo tipo identifiquen los riesgos clave y los planteamientos de mitigación adecuados. Aceptar que la realidad es que no se pueden proteger todos los recursos corporativos en todo momento forma parte de este proceso. "Alcanzar un acuerdo en lo que respecta a lo que reviste la mayor importancia desde la perspectiva de la seguridad cibernética", subraya Gavin Reid, director de inteligencia de amenazas de Cisco. "Se trata de un enfoque más productivo que esperar hallar una panacea que lo solucione todo".

Para hacer frente a los retos de seguridad de la actualidad directamente, las organizaciones deben examinar su modelo de seguridad de forma holística y obtener visibilidad de todo el proceso del ataque:

- **Antes de una ofensiva:** para defender las redes, las organizaciones deben ser conscientes de qué se encuentra en ellas, como dispositivos, sistemas operativos, servicios, aplicaciones, usuarios, etc. Asimismo, deben implementar controles de acceso, aplicar políticas de seguridad, así como bloquear aplicaciones y el acceso global a los recursos esenciales. No obstante, las políticas y los controles solo constituyen una pequeña parte de una perspectiva más amplia. Estas medidas pueden contribuir a reducir la superficie de ataque, pero siempre existirán lagunas que los delincuentes hallarán y de las que se aprovecharán para lograr sus metas.
- **Durante una ofensiva:** las organizaciones deben hacer frente a un amplio abanico de vectores de ataque con soluciones que puedan funcionar allí donde la amenaza se pueda manifestar, es decir, en la red, en los terminales, en los dispositivos móviles y en los entornos virtuales. Si se ha establecido soluciones eficaces, los profesionales de la seguridad se encontrarán en una posición mucho mejor para bloquear las amenazas y contribuir a defender el entorno.
- **Después de una ofensiva:** es una realidad, muchos ataques penetrarán la red. Esto implica que las organizaciones deben contar con un plan oficial que les permitirá determinar el alcance de los daños, contener el suceso, solventar los problemas y conseguir que las operaciones vuelvan a la normalidad lo antes posible.

"Los atacantes y sus herramientas han avanzado para eludir las defensas tradicionales. La realidad es que ya no se trata de si se infiltrarán, sino cuándo", apunta Marty Roesch, Arquitecto de seguridad principal del Grupo de seguridad de Cisco. "Se precisa un planteamiento de seguridad centrado en las amenazas e impulsado por la visibilidad para proteger a los usuarios en el proceso del ataque: tanto en el despliegue de este como en los momentos anterior y posterior".

Cómo los servicios contribuyen a cumplir los retos de seguridad

Con una mayor superficie de ataque, el aumento de la proliferación y de la sofisticación de los modelos de ataque, y la creciente complejidad dentro de la red, más organizaciones encuentran dificultades para consolidar una visión de seguridad que emplee las nuevas tecnologías, simplifique su arquitectura y sus operaciones, y fortalezca sus equipos.

La falta de personas competentes en el tema de la seguridad, que se trató en la página 61, complica estos problemas. Además, el sector de seguridad innova a un ritmo superior al que las organizaciones pueden adoptar y gestionar estas nuevas herramientas.

Hallar la persona competente adecuada para abordar el panorama de seguridad en evolución puede suponer un reto. La contratación de recursos externos complementarios no solo puede contribuir a reducir los costes, sino que también permite que la empresa libere recursos para centrarse en prioridades más importantes.

Fortalecimiento de la cadena en sus puntos débiles

La prevención de las amenazas resulta sin lugar a dudas fundamental para mantener la seguridad cibernética. Por este motivo, dado que más delincuentes online están dirigiendo sus miras a comprometer la infraestructura de Internet en lugar de equipos individuales, los expertos de seguridad de Cisco recomiendan que los ISP y las empresas de alojamiento desempeñen un papel más activo a la hora de proteger la integridad de Internet.

La identificación de amenazas difíciles de detectar, como DarkLeech y Linux/CDorked (véase la página 46), requiere mucha más "capacidad de respuesta humana" por parte de los proveedores de alojamiento. En esta capacidad de respuesta se incluyen investigar completamente las denuncias de los usuarios y tomarlas en serio. Asimismo, los proveedores deben establecer mejores controles para garantizar que pueden verificar la integridad de sus instalaciones de sistemas operativos de servidores. Los investigadores de Cisco afirman que en los casos de malware sigiloso, como CDorked, los equipos de seguridad no habrían podido saber que el binario se había sustituido si no hubieran contado con un control orientado a verificar la integridad de la instalación.

Por supuesto, los sistemas de usuarios individuales son susceptibles de sufrir una violación de la seguridad, pero la debilitación de la cadena comienza a menudo mucho antes de que la amenaza llegue a ellos. Ahora, el ataque se produce con más frecuencia en el medio de la cadena; por este motivo, los proveedores deben tomar una mayor consciencia de las amenazas potenciales que atacan la infraestructura de Internet.

Apéndice

Las organizaciones de seguridad precisan científicos de los datos

Herramientas de análisis de datos introductorias para los encargados de la seguridad

Los equipos de directores de seguridad están recopilando una cantidad de datos sin precedentes y la inteligencia que se encuentra en ellos presenta un valor demasiado elevado para permitir que se desaprovechen. El análisis de los datos relevantes para la seguridad proporciona pistas sobre las actividades de los atacantes y aporta una perspectiva interactiva acerca de cómo frustrar las ofensivas.

Los análisis de datos no resultan un aspecto novedoso para el encargado de la seguridad. Existe asimismo cierta expectativa entre los profesionales de la seguridad de que se generarán y etiquetarán registros. Los encargados de desarrollar las pruebas de penetración crean un registro de investigación después de una evaluación. Los diseñadores de sistemas operativos implementan subsistemas de auditorías. Los desarrolladores de aplicaciones compilan programas que generan registros.

Con independencia del nombre que porten los datos, no cabe duda de que los encargados de la seguridad cuentan con abundante información; en este sentido, su análisis puede desembocar en descubrimientos importantes.

Los encargados de la seguridad cuentan con abundante información; en este sentido, su análisis puede desembocar en descubrimientos importantes.

Aunque el análisis de datos en sí mismo no es nuevo, la evolución del panorama de seguridad ha repercutido en el proceso del análisis de datos, lo que se ha visto reflejado en los siguientes ámbitos:

- El enorme volumen de datos generados es sorprendente.
- La frecuencia con la que se precisa el análisis de datos ad hoc está aumentando.
- Los informes estandarizados, a pesar de su utilidad, resultan insuficientes.

Por suerte, la barrera de entrada para que los profesionales de la seguridad efectúen análisis de datos, incluso en este entorno más complejo, es reducida y el ecosistema de herramientas de análisis de datos presenta una amplia gama de posibilidades. A continuación se aporta una descripción general de solo algunas de las herramientas disponibles gratuitamente que los profesionales pueden utilizar para comenzar a analizar datos.

Análisis del tráfico con Wireshark y Scapy

Dos herramientas sobresalientes a la hora de efectuar análisis del tráfico son Wireshark y Scapy. Wireshark no necesita presentación. Scapy consiste en una herramienta basada en Python que se puede utilizar, como un módulo de Python o de forma interactiva, para elaborar o inspeccionar el tráfico.

El amplio conjunto de herramientas de línea de comandos y de disectores de protocolos de Wireshark lo convierten en una utilidad indispensable. Por ejemplo, por medio del campo de filtro de visualización tcp.stream de Wireshark, un archivo PCAP que contenga varios flujos de TCP puede fraccionarse en archivos más pequeños que presenten cada uno todos los paquetes pertenecientes a un único flujo de TCP.

La figura A1 muestra este comando, que imprime el índice de flujo de TCP de los primeros cinco paquetes de TCP en traffic_sample.pcap.

FIGURA A1

El comando tshark para extraer el índice tcp.stream

```
tshark -r traffic_sample.pcap -T fields -e tcp.stream tcp | head -n 5
```

tshark constituye una de las herramientas de línea de comandos de Wireshark.

tcp.stream hace referencia al campo de índice de flujos de filtros de visualización de TCP.

Con ese conocimiento, es posible escribir un script que divida traffic_sample.pcap en archivos PCAP independientes:

```
$ cat ~/bin/uniq_stream.sh
#!/bin/bash

function getfile_name() {

                orig_name=$1
                stream=$2
                file_name="$(echo $orig_name | cut -d'.' -f1)"
                file_name+="-${stream}.pcap"

                echo "${file_name}"

                return 0
}

streams=$(tshark -r ${1} -T fields -e tcp.stream | sort -un | tr '\n' ' ')

for x in ${streams}
do
                file_name=$(getfile_name ${1} ${x})
                echo "Creating ${file_name}..."
                tshark -r ${1} -w $file_name tcp.stream eq ${x}
done
$
```

Este script crea un único archivo PCAP para cada uno de los 147 flujos de TCP presentes en traffic_sample.pcap. Ahora, resulta más sencillo efectuar un análisis más detallado de cada flujo de TCP. Tenga presente los paquetes que no sean de TCP presentes en traffic_sample.pcap no se encontrarán en ninguno de los nuevos archivos PCAP:

```
$ /bin/uniq_stream.sh traffic_sample.pcap
Creating traffic_sample-1.pcap...
Creating traffic_sample-2.pcap...
...
...
Creating traffic_sample-146.pcap...
Creating traffic_sample-147.pcap...
```

Scapy cuenta con sus propios puntos fuertes. Dado que está desarrollado en Python, es posible utilizar todas las funciones del lenguaje Python y otras herramientas de este. El siguiente fragmento de código demuestra cómo Scapy utiliza la sobrecarga del operador, de modo que la creación del tráfico pueda realizarse de forma rápida e intuitiva:

```
# scapy

>>> dns_query = IP()/UDP()/DNS()

>>> from socket import gethostbyname,gethostname

>>> dns_query[IP].src = gethostbyname(gethostname())

>>> dns_query[IP].dst = “8.8.8.8”

>>> import random

>>> random.seed()

>>> dns_query[UDP].sport = random.randint(0, 2**16)

>>> dns_query[DNS].id = random.randint(0, 2**16)

>>> dns_query[DNS].qdcount = 1

>>> dns_query[DNS].qd = DNSQR(qname=“www.cisco.com”)

>>> scapy.sendrecv.sr1(dns_query)

>>> response = scapy.sendrecv.sr1(dns_query)

Begin emission:

.....Finished to send 1 packets.

.*

Received 14 packets, got 1 answers, remaining 0 packets

>>> response[DNS].ar[DNSRR].rdata

‘64.102.255.44’

>>>
```

Este ejemplo muestra cómo se pueden construir los paquetes y cómo se puede analizar el tráfico en directo. Sin embargo, también es posible utilizar Scapy para analizar archivos PCAP con la misma facilidad.

Análisis de datos en formato CSV

Los archivos de valores separados por comas (CSV) representan un formato popular de intercambio de datos. Muchas herramientas (tshark incluida) permiten que el usuario exporte datos en formato CSV. Normalmente, los profesionales de la seguridad utilizan programas de hojas de cálculo, como Excel, para analizar los datos en CSV. Con frecuencia, también se pueden utilizar herramientas de línea de comandos, como grep, cut, sed, awk, uniq y sort.

Considere utilizar csvkit como una alternativa. Csvkit proporciona varias herramientas que facilitan procesar los datos de CSV de la línea de comandos. Examine el siguiente archivo CSV y observará lo sencillo que resulta encontrar todas las líneas que tienen el host tty.example.org en la columna scr:

```
$ head -n 3 tcp_data.csv
src,srcport,dst,dstport
“tty.example.org”,“51816”,”vex.example.org”,”443”
“vex.example.org”,”443”,”tty.example.org”,”51816”

$ csvgrep -n tcp_data.csv
        1: src
        2: srcport
        3: dst
        4: dstport

$ csvgrep -c 1 -r ‘tty\.example\.org’ tcp_data.csv | head -n 5
src,srcport,dst,dstport
tty.example.org,51816,vex.example.org,443
tty.example.org,51816,vex.example.org,443
tty.example.org,51427,paz.example.org,5222
tty.example.org,51767,bid.example.org,80
```

Csvkit incluye un amplio abanico de utilidades. Csvstat resulta de especial utilidad porque procesa automáticamente varias estadísticas. Por ejemplo, resulta sencillo procesar la frecuencia de los cinco primeros hosts src:

```
$ csvstat -c 1 tcp_data.csv
  1. src
  <type 'unicode'>
  Nulls: False
  Unique values: 55
  5 most frequent values:
                tty.example.org:        2866
                lad.example.org:        1242
                bin.example.org:        531
                trw.example.org:        443
                met.example.org:        363
Max length: 15

Row count: 6896
```

Matplotlib, pandas, IPython y otros

Se encuentra disponible un completo conjunto de herramientas de visualización y análisis de datos basados en Python. Un lugar fenomenal para descubrir estas herramientas es el sitio SciPy (http://www.scipy.org). Los paquetes de IPython, pandas y Matplotlib resultan de especial interés:

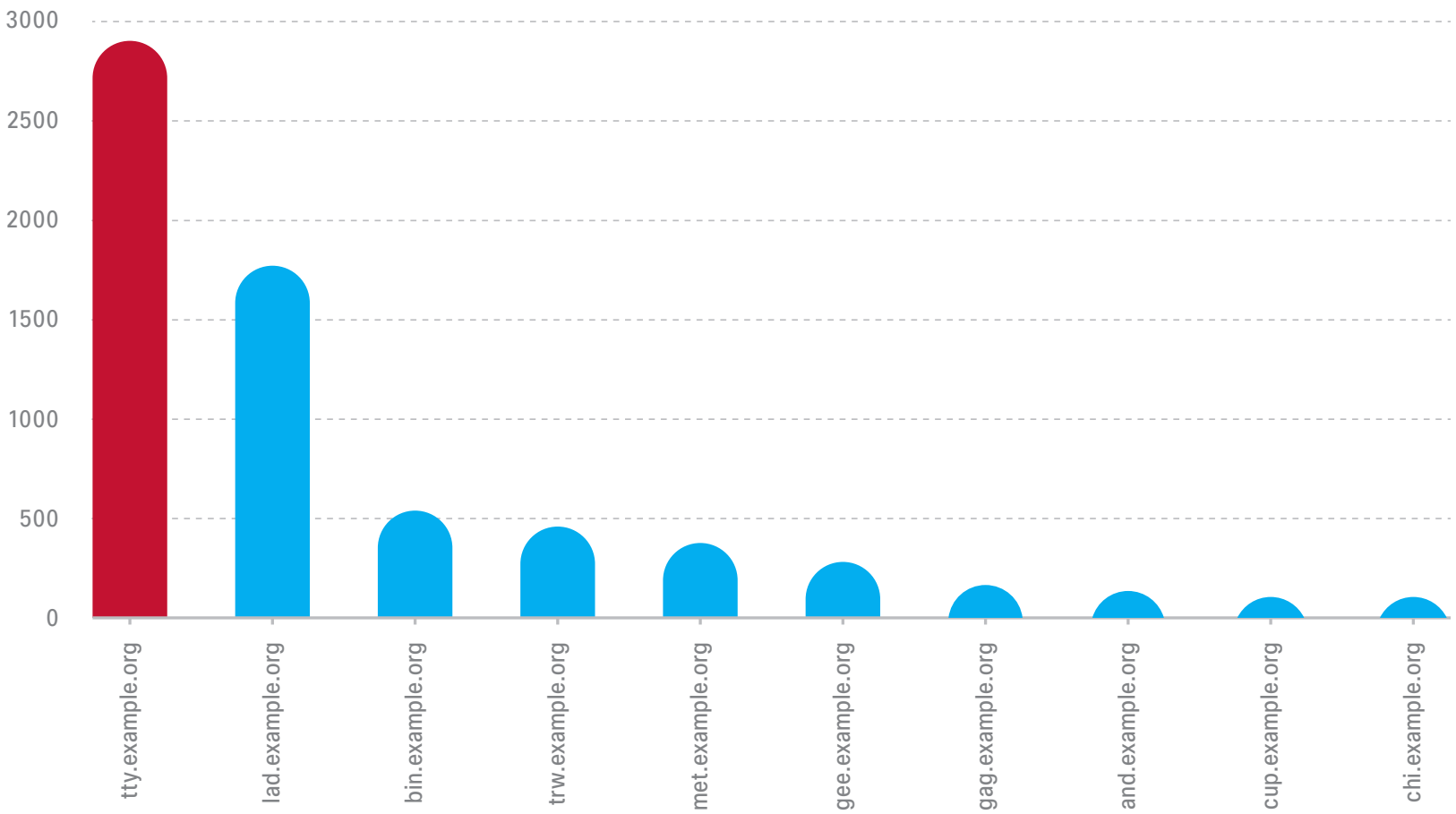
- Matplotlib posibilita una virtualización flexible y sencilla.
- pandas proporciona las herramientas para manipular y examinar datos sin procesar.
- IPython aporta funciones al intérprete de Python que facilitan el análisis de datos interactivo.

El siguiente código demuestra cómo los encargados de la seguridad pueden utilizar estas tres herramientas para obtener un gráfico de los principales hosts de tcp_data.csv:

```
In [3]: df = read_csv("/Users/shiva/tmp/data_analysis/tcp_data.csv")
In [4]: df
Out[4]:
<class 'pandas.core.frame.DataFrame'>
Int64Index: 6896 entries, 0 to 6895
Data columns (total 4 columns):
src 6896 non-null values
srcport 6896 non-null values
dst 6896 non-null values
dstport 6896 non-null values
dtypes: int64(2), object(2)
In [5]: df['src'].value_counts()[0:10]
Out[5]:
tty.example.org 2866
lad.example.org 1242
bin.example.org 531
trw.example.org 443
met.example.org 363
gee.example.org 240
gag.example.org 126
and.example.org 107
cup.example.org 95
chi.example.org 93
dtype: int64
In [6]: df['src'].value_counts()[0:10].plot(kind="bar")
Out[6]: <matplotlib.axes.AxesSubplot at 0x8479c30>
```

FIGURA A2

Gráfico generado mediante Plot ()



La grandeza de pandas se encuentra en cómo permite que los usuarios exploren los datos. Por ejemplo, no supone mucho esfuerzo encontrar el número de srcports únicos desde los que se conecta tty.example.org para cada combinación de dst y dstport única con la que se comunica:

```
In [229]: tty_df = df[df.src == “tty.example.org”]
In [230]: num_ports = lambda x: len(set(x))
In [231]: pivot_table(tty_df, rows=[‘dst’,‘dstport’], values=‘srcport’, aggfunc=num_ports)
Out[231]:
dst dstport
add.example.org 80 2
ala.example.org 80 3
and.example.org 80 1
auk.example.org 80 2
bid.example.org 80 1
…
```

Comience a analizar datos

Los ejemplos de las páginas anteriores no representan más que una parte ínfima de las funciones y hacen justicia a las herramientas mencionadas. Sin embargo, bastan para que los profesionales de la seguridad comiencen a realizar análisis de datos significativos.

Los directores de seguridad tienen que conseguir que los encargados de la seguridad trabajen como científicos de los datos. El examen de los datos disponibles aportará perspectivas que no se pueden obtener de ninguna otra manera. Con el tiempo, se desarrollará una intuición sobre qué partes de los datos se deben explorar. Es posible que determinadas organizaciones se percaten de que pueden beneficiarse de contar con científicos de los datos dedicados en sus equipos.

Información sobre Cisco SIO

Cisco SIO

La protección y administración de las redes actuales, tan ágiles y distribuidas, se están convirtiendo un desafío cada vez más difícil.

Los delincuentes online siguen aprovechándose de la confianza de los usuarios en aplicaciones y dispositivos de consumo, lo que aumenta los riesgos para organizaciones y empleados. La seguridad tradicional, que se basa en la distribución en capas de los productos y el uso de múltiples filtros, es una protección insuficiente contra la última generación de malware, que tiene objetivos globales y se propaga rápidamente utilizando numerosos vectores.

Cisco le toma la delantera a las posibles amenazas gracias al sistema de inteligencia de amenazas en tiempo real de Cisco Security Intelligence Operations (SIO). Cisco SIO es el ecosistema de seguridad basado en la nube más grande del mundo. Utiliza más de 75 terabytes de fuentes de datos activas procedentes de las soluciones de correo electrónico, sitios web, firewalls y sistemas de prevención de intrusiones (IPS) de Cisco implementadas.

Cisco SIO sopesa y procesa los datos y, automáticamente, clasifica las amenazas y crea reglas a partir de más de 200 parámetros. Los investigadores de seguridad recopilan y proporcionan información sobre eventos de seguridad que, potencialmente, podrían afectar a las redes, aplicaciones y dispositivos. Las reglas se envían de forma dinámica a los dispositivos de seguridad de Cisco implementados cada tres o cinco minutos.

La seguridad tradicional supone una protección insuficiente contra la última generación de malware.

Además, el equipo de Cisco SIO publica recomendaciones sobre las prácticas de seguridad adecuadas, así como directrices tácticas para desarticular las amenazas. Cisco se compromete a ofrecer soluciones de seguridad completas que sean integradas, completas y efectivas y que permitan una seguridad holística para organizaciones de todo el mundo. Con Cisco las organizaciones pueden ahorrar tiempo en la investigación de amenazas y vulnerabilidades y concentrarse en aplicar un enfoque activo de la seguridad.

Si desea conocer más sobre información inmediata y análisis de vulnerabilidades y amenazas, así como las soluciones de mitigación de Cisco visite: www.cisco.com/go/sio.

Notas finales

1 Para obtener más información sobre la evolución de cualquiera a cualquiera, consulte "El nexus de dispositivos, nubes y aplicaciones" en el *Informe anual de seguridad de Cisco 2013*: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

2 Ibídem.

3 *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security* (Se acabaron los centros duros: presentación del modelo de confianza cero de la seguridad de la información), de John Kindervag, Forrester, 12 de noviembre de 2012.

4 "Timeline of Edward Snowden's Revelations" (Cronograma de las revelaciones de Edward Snowden) *Al Jazeera America*: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html.

5 "NSA collecting phone records of millions of Verizon customers daily" (La NSA recopila los registros telefónicos de millones de clientes de Verizon a diario) de Glenn Greenwald, *The Guardian*, 5 de junio de 2013: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

6 GCHQ: Government Communications Headquarters (Cuartel General de Comunicaciones del Gobierno), una agencia de inteligencia británica.

7 "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say" (La NSA infiltra enlaces en los Data Centers de Yahoo y Google en todo el mundo, según los documentos de Snowden), de Barton Gellman y Ashkan Soltani, *The Washington Post*, 30 de octubre de 2013: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

8 Para obtener más información, consulte "Cisco Secure Development Life cycle (CSDL)": http://www.cisco.com/web/about/security/cspo/csdl/index.html.

9 Ibídem.

10 Cisco define el Internet of Everything como la siguiente oleada de crecimiento drástico de Internet que se generará a partir de la confluencia de las personas, los procesos, los datos y las cosas.

11 "Massive Spam and Malware Campaign Following the Boston Tragedy" (Masiva campaña de malware y spam tras la tragedia de Boston), *Blog de seguridad de Cisco*, 17 de abril de 2013: http://blogs.cisco.com/security/massive-spam-and-malware-campaign-following-the-boston-tragedy/.

12 Ibídem.

13 Ibídem.

14 Página de "Acerca de" del sitio web de Java: http://www.java.com/en/about/.

15 Para obtener más información sobre la "evolución de cualquiera a cualquiera", consulte el *Informe anual de seguridad de Cisco 2013*: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

16 "Department of Labor Watering Hole Attack Confirmed to be 0-Day with Possible Advanced Reconnaissance Capabilities" (Se confirma que el ataque "watering hole" contra el Departamento de trabajo fueron de día cero con posibles capacidades avanzadas de reconocimiento),
de Craig Williams, *Blog de seguridad de Cisco*, 4 de mayo de 2013: http://blogs.cisco.com/security/department-of-labor-watering-hole-attack-confirmed-to-be-0-day-with-possible-advanced-reconnaissance-capabilities/.

17 "Watering-Hole Attacks Target Energy Sector" (Los ataques "watering hole" están dirigidos contra el sector energético), de Emmanuel Tacheau, *Blog de seguridad de Cisco*, 18 de septiembre de 2013: http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/.

18 "Apache DarkLeech Compromises" (Vulnerabilidades de Apache aprovechadas por DarkLeech), de Mary Landesman, *Blog de seguridad de Cisco*, 2 de abril de 2013: http://blogs.cisco.com/security/apache-DarkLeech-compromises/.

19 "Ongoing malware attack targeting Apache hijacks 20,000 sites" (Un ataque de malware continuo dirigido contra Apache se hace con 20 000 sitios), de Dan Goodin, *Ars Technica*, 2 de abril de 2013: http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/.

[20] "Linux/CDorked FAQS" (Preguntas frecuentes de Linux/CDorked), de Mary Landesman, *Blog de seguridad de Cisco*, 1 de mayo de 2013: http://blogs.cisco.com/security/linuxcdorked-faqs/.

[21] "DarkLeech Apache Attacks Intensify" (Los ataques a Apache de DarkLeech se intensifican), de Matthew J. Schwartz, *InformationWeek*, 30 de abril de 2013: http://www.informationweek.com/security/attacks/DarkLeech-apache-attacks-intensify/240153922.

[22] Typosquatting consiste en la práctica de registrar nombres de dominio que difieren en un carácter de nombres de dominio populares.

[23] "Thanks to IoE, the next decade looks positively 'nutty'" (Gracias a IoE, la siguiente década parece una locura positiva), de Dave Evans, *Blog de la plataforma Cisco*, 12 de febrero de 2013: http://blogs.cisco.com/news/thanks-to-ioe-the-next-decade-looks-positively-nutty/.

[24] Para obtener más información acerca de estrategias de mitigación para el bitsquatting, lea el informe técnico de Cisco, *Examining the Bitsquatting Attack Surface* (Análisis de la superficie de ataque de bitsquatting), 2013: http://blogs.cisco.com/wp-content/uploads/Schultz-Examining_the_Bitsquatting_Attack_Surface-whitepaper.pdf.

[25] "WordPress Sites in the World" (Sitios de WordPress en el mundo) y "A Look at Activity Across WordPress.com" (Un vistazo a la actividad de WordPress), WordPress.com: http://en.wordpress.com/stats/.

[26] "Important Security Update: Reset Your Drupal.org Password" (Aviso importante de seguridad: Restablezca su contraseña de Drupal.org), Drupal.org, 29 de mayo de 2013: https://drupal.org/news/130529SecurityUpdate.

[27] Es posible encontrar un informe detallado de los patrones y las cargas de la campaña Operación Ababil en "Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions" (Respuesta a eventos de Cisco: Ataques de negación de servicio distribuida contra instituciones financieras): http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[28] "DDoS Attack on Bank Hid $900,000 Cyberheist" (Un ataque de DDoS a un banco ocultó un golpe cibernético de 900 000 $), de Brian Krebs, Blog *KrebsonSecurity*, 19 de febrero de 2013: http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[29] "Chinese Internet Hit by Attack Over Weekend" (El Internet chino sufre un ataque durante el fin de semana), de Paul Mozer, *China Real Time Report*, WSJ.com, 26 de agosto de 2013: http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend/.

[30] Fuente: Wikipedia: "Ingress Filtering" (Filtro de entrada): http://en.wikipedia.org/wiki/Ingress_filtering.

[31] "Understanding Unicast Reverse Path Forwarding" (Examen de Unicast Reverse Path Forwarding), sitio web de Cisco: http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html.

[32] "Your Hard Drive Will Self-Destruct at 2 p.m.: Inside the South Korean Cyberattack" (Su disco duro se autodestruirá a las 14:00: Dentro del ataque cibernético de Corea del Sur), de Sean Gallagher, *Ars Technica*, 20 de marzo de 2013: http://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/.

[33] "Thoughts on DarkSeoul: Data Sharing and Targeted Attackers" (Opinión sobre DarkSeoul: Uso compartido de datos y atacantes seleccionados), de Seth Hanford, *Blog de seguridad de Cisco*, 27 de marzo de 2013: http://blogs.cisco.com/tag/darkseoul/.

[34] Ibídem.

[35] "Cyber Gang Seeks Botmasters to Wage Massive Wave of Trojan Attacks Against U.S. Banks" (Una banda cibernética busca dueños de bots para lanzar un ataque de troyanos masivo contra bancos estadounidenses), de Mor Ahuvia, RSA, 4 de octubre de 2012: https://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/.

[36] "DDoS Attack on Bank Hid $900,000 Cyberheist" (Un ataque de DDoS a un banco ocultó un golpe cibernético de 900 000 $), de Brian Krebs, Blog *KrebsonSecurity*, 19 de febrero de 2013: http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[37] "Cisco projects data center-cloud traffic to triple by 2017" (Cisco prevé que el tráfico entre el Data Center y la nube se triplique para 2017), ZDNet, 15 de octubre de 2013: http://www.zdnet.com/cisco-projects-data-center-cloud-traffic-to-triple-by-2017-7000021985/.

Sede central en América
Cisco Systems, Inc.
San José, CA (EE. UU.)

Sede central en Asia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International
BV Amsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, y los números de teléfono y fax se pueden consultar en la Web de Cisco en **www.cisco.com/go/offices**.

Todo el contenido está protegido por Copyright © 2011–2014 Cisco Systems, Inc. Todos los derechos reservados. Este documento es información pública de Cisco. Cisco y el logotipo de Cisco son marcas comerciales de Cisco Systems, Inc. y/o de sus filiales en Estados Unidos y en otros países. Puede consultar una lista de las marcas comerciales de Cisco en www.cisco.com/go/trademarks. Todas las marcas comerciales de terceros mencionadas en este documento pertenecen a sus respectivos propietarios. El uso de la palabra " partner" no implica la existencia de una asociación entre Cisco y cualquier otra empresa. (012114 v1)