Semestral 2014 de Cisco

Informe de seguridad

Resumen ejecutivo

Cualquier ciberataque, grande o pequeño, nace a partir de un eslabón débil en la cadena de seguridad. Los eslabones débiles pueden adoptar muchas formas: software desactualizado, código mal escrito, un sitio web abandonado, errores de desarrolladores, un usuario con confianza ciega. Los atacantes dedican todos sus esfuerzos a encontrar estos eslabones débiles, ya sea uno o todos, y a usarlos para su propio beneficio.

Desafortunadamente, los atacantes no tienen que buscar mucho ni esforzarse por encontrar debilidades en las organizaciones y los usuarios que se proponen como blancos. En el emergente mundo de Internet de todo que en última instancia se desarrolla sobre la base de la conectividad inherente a Internet de las cosas, su trabajo será aún más sencillo, ya que cualquier cosa conectada a una red, desde automóviles hasta sistemas de automatización de hogares, presenta una superficie que podría ser atacada.

Los efectos de los ciberataques son decepcionantes, tanto en términos de costos como en cuanto a pérdidas de productividad y reputación. Según el Instituto Ponemon, el costo promedio de una infracción de datos en organizaciones fue de USD 5,4 millones en el año 2014, cifra más elevada que los USD 4,5 millones del año 2013. Además, el informe ***Estimación del costo de la ciberdelincuencia y el ciberespionaje del Centro de Estudios Estratégicos e Internacionales*** estima que la economía de EE. UU. pierde USD 100 mil millones al año y que se pierden hasta 508 000 puestos de trabajo en EE. UU. debido a la actividad maliciosa en línea.[1]

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Inteligencia contra amenazas

Ir a Inteligencia contra amenazas

El ***Informe semestral de seguridad 2014 de Cisco*** examina la inteligencia contra amenazas y las tendencias de ciberseguridad para la primera mitad del año 2014. La investigación de Cisco ayuda a subrayar la gran cantidad de tipos de eslabones débiles presentes en los sistemas que usamos, incluida Internet misma, y qué podemos hacer para reducir su cantidad y sus efectos. Las conclusiones principales incluyen las siguientes:

Como parte del proyecto en curso de Cisco "Inside Out" ("De adentro hacia afuera") en el que se estudian las consultas al Sistema de nombres de dominio (DNS) (o el proceso de buscar la dirección del Protocolo de Internet [IP] asociada con un nombre de dominio) que se origina desde el interior de redes corporativas de ciertos clientes de Cisco, los investigadores que observan las redes de 16 grandes organizaciones multinacionales descubrieron que:

Se ha determinado que alrededor del 70% de las redes de ciertos clientes observadas por los investigadores de Cisco emiten consultas de DNS para DNS dinámico (DDNS).

Se ha determinado que más del 90% de las redes de ciertos clientes emiten solicitudes DNS para nombres de host asociados con la distribución de malware.

Se ha determinado que más del 40% de las redes de ciertos clientes emiten solicitudes DNS para sitios y dominios asociados con dispositivos que proporcionan servicios como VPN con Seguridad IP (IPsec), VPN con Capa de conexiones seguras (SSL), Protocolo de paquete seguro (SSH), Protocolo simple de transferencia de archivos (SFTP), FTP y FTP seguro (FTPS).

De las 2528 alertas de vulnerabilidades publicadas entre enero y junio de 2014, se determinó que se estaban vulnerando 28. Estas son las vulnerabilidades de alta prioridad o urgencia que se deben corregir con una respuesta acelerada.

Después de una reducción general en el año 2013, el volumen global de spam ha aumentado continuamente desde el pasado mes de octubre, pero no en todos los países.

Tendencias en la industria

Ir a Tendencias en la industria

En la primera mitad del año 2014, la industria farmacéutica y química, una vertical de alto nivel de ganancias, vuelve a ubicarse entre las primeras tres verticales de alto riesgo en cuanto a hallazgos de malware web.

La industria de los medios de comunicación y editorial ha presentado un índice significativamente más alto que el normal en malware web en comparación con lo observado anteriormente.

El año 2014 parece ser un año de mucha actividad de ataques de denegación de servicio distribuidos (DDoS) al Protocolo de hora de red (NTP). Uno de los ataques por amplificación de NTP más significativos que se observó en los primeros seis meses de 2014 fue sobre un cliente del proveedor de DNS a nivel global CloudFlare. En su pico máximo, el ataque del mes de febrero alcanzó casi 400 Gbps de tráfico del Protocolo de datagramas de usuarios (UDP).

La cantidad de kits de aprovechamiento de vulnerabilidades ha caído en un 87% desde el arresto del codificador, Paunch, el supuesto creador del altamente popular kit de aprovechamiento de vulnerabilidades Blackhole, el año pasado, según los investigadores de seguridad de Cisco.

Varios de los kits de aprovechamiento de vulnerabilidades observados en la primera mitad del año 2014 trataban de infiltrarse en el territorio antes dominado por Blackhole, pero aún no ha surgido ningún líder claro.

El aprovechamiento de vulnerabilidades de Puntos de venta (POS) está ganando favoritismo entre los delincuentes en el año 2014, por varios motivos:

La mayor probabilidad de que los sistemas POS estén conectados a Internet, que brinda a los delincuentes un punto de ingreso a redes corporativas.

La falta de consciencia de que la información de la tarjeta de crédito debería ser considerada como información crítica, que significa que está menos protegida.

El creciente uso por parte de las organizaciones de proveedores externos para todas o algunas de sus soluciones de POS, que ofrece más puntos de acceso a los delincuentes.

Una mirada hacia adelante

Ir a Una mirada hacia adelante

Riesgos de seguridad que Internet de las cosas probablemente genera y por qué las organizaciones deberían adoptar un enfoque proactivo para enfrentarlos.

El valor de utilizar análisis predictivos y aprendizaje de máquina para ayudar a identificar amenazas difíciles de detectar en la red.

Una tendencia entre organizaciones propensas a considerar la ciberseguridad tanto un riesgo estratégico como un proceso comercial.

La necesidad de soluciones de seguridad en las que la visibilidad sea la prioridad máxima, que estén enfocadas en las amenazas y basadas en plataformas que cubran toda la secuencia de un ataque (antes, durante y después del mismo) y que ayuden a cerrar brechas de seguridad y a reducir la complejidad causada por productos dispares.

Contenido

Introducción 7

Internet de las cosas: nuevas oportunidades, nuevos riesgos 7

Inteligencia contra amenazas 9

Un cambio de paradigma en el compromiso: mirar de adentro hacia afuera 10

Tendencias geopolíticas que se deben observar 14

Aprovechamiento de vulnerabilidades web: el aprovechamiento de vulnerabilidades Java sigue prevaleciendo 15

Actualización sobre vulnerabilidades: enfoque en los aprovechamientos de vulnerabilidades más comunes 17

Heartbleed: no es el único motivo para preocuparse 20

Informe de riesgos verticales en la industria: incrementos inusuales en algunos sectores 21

Detecciones de malware por región 23

Los 5 riesgos verticales principales por región 25

Actualización sobre spam: el spam “que promete solucionar problemas de la vida” pasa a ser más frecuente 26

Los delincuentes que se dedican al spam son cada vez más ágiles y cambian sus enfoques para mejorar sus índices de éxito 26

El volumen de spam a nivel mundial se duplicó con respecto al índice normal, pero en algunos países se ve una marcada disminución 27

Tendencias en la industria 28

Conexiones cifradas seguras comprometidas 29

Ataques por amplificación: atacantes que sincronizan relojes con NTP 31

Kits de aprovechamiento de vulnerabilidades: el campo se abre a la competencia 33

Publicidad maliciosa: un factor que altera la economía en Internet 35

Anuncios realmente malos: el rol de la publicidad maliciosa en el Ransomware 36

Vulnerabilidades de WordPress: ¿quién está atendiendo el negocio? 37

Ataques por POS: vector de amenaza popular para delincuentes que buscan datos sobre tarjetas usadas para pagos 38

Monitoreo más crítico de datos de tarjetas usadas para pagos 39

Ingeniería social: encontrar eslabones débiles en la persona 40

Una mirada hacia adelante 42

Ciberseguridad inteligente para el mundo real 43

Cómo hacer que la seguridad sea operativa: convertir a la seguridad en un proceso comercial 45

Comprender el riesgo cibernético en términos comerciales 47

Análisis predictivo: un detective que permite mejorar la seguridad 49

Acerca de Cisco 50

Notas 51

Este documento incluye contenido que permite búsquedas y se puede compartir

Hacer clic para abrir la función Buscar en Adobe Acrobat

Compartir contenido por correo electrónico y medios sociales

Software recomendado:

Adobe Acrobat versión 7.0 y superiores

Internet de las cosas: nuevas oportunidades, nuevos riesgos

Internet de las cosas "es la red de objetos físicos a los que se accede a través de Internet, según lo definido por los analistas y visionarios de la tecnología. Estos objetos contienen tecnología incrustada para interactuar con estados internos o con el entorno externo. En otras palabras, cuando los objetos pueden detectar y comunicarse, se cambia el cómo, el dónde y el quién de la toma de decisiones".[2]

Según Cisco, se espera que Internet de las cosas sume aproximadamente 50 mil millones de elementos al llegar el año 2020.[3] Ya está cambiando el panorama de seguridad, con lo que se está expandiendo exponencialmente la superficie de ataque. Internet de las cosas aumenta la importancia de la detección y la protección continuas y ubicuas, ya que tanto personas como procesos y datos cada vez están más conectados.

En este mundo de informática ubicua e interconectividad extrema en rápida evolución, cualquier elemento conectado a una red tiene una superficie pasible de ataque que puede ser aprovechada por delincuentes. Gran parte de lo que *podrían* hacer los atacantes sigue siendo hipotética, pero ya están haciendo planes, probando ideas y logrando cierto éxito.

Los piratas informáticos ya se han ocupado de los automóviles, los dispositivos médicos e incluso los monitores para bebés en su "investigación y desarrollo" de Internet de las cosas.[4–6]

La meta final de Internet de las cosas es aumentar la eficiencia operativa, posibilitar nuevos modelos empresariales y mejorar la calidad de vida. Dado que podemos conectar objetos cotidianos y reunirlos en una red, podemos combinar datos simples para generar inteligencia útil. Pero eso también quiere decir que hay más probabilidad de que haya más información personal y datos comerciales en la nube que se transmiten en un sentido y otro. Eso trae aparejado significativas repercusiones para aplicar medidas de seguridad correctas para proteger datos y para establecer políticas de privacidad que definan cómo se usan los datos.

La privacidad es una inquietud principal en Internet de las cosas. Incluso cuando los usuarios toman precauciones para asegurar su información y se abstienen de ser demasiado confiados, siguen en riesgo debido a enlaces débiles en la cadena de seguridad que escapan a su control (ver Conexiones cifradas seguras comprometidas, página 29). Cuando los atacantes llegan a un punto en el que pueden comenzar a correlacionar información de diferentes fuentes (un automóvil, un teléfono inteligente, un sistema de automatización de hogares), puede obtener un panorama mucho más completo de un usuario que si estuvieran viendo información desde un solo dispositivo, sistema o aplicación. Estos detalles sobre los usuarios, desde sus hábitos de compra hasta su ubicación física, permiten que los delincuentes inicien campañas altamente específicas y bien diseñadas con un nivel de sofisticación nunca antes visto.

A algunas personas podría parecerles exagerado pensar que algo tan mundano como un dispositivo en la ropa para controlar el estado físico o una videograbadora digital (DVR) pueda imponer un significativo riesgo de seguridad o que un pirata informático pudiera mostrar algún interés en él. Pero como los automóviles y otros dispositivos computarizados no tradicionales se asemejan cada día más a plataformas informáticas estándares, podrían ser más vulnerables a las mismas amenazas[7] que atacan a dispositivos informáticos tradicionales.

Los principales proveedores son conscientes de los problemas de seguridad en los dispositivos de Internet de las cosas y tienen los conocimientos y la experiencia necesarios para garantizar que la seguridad se incorpore a la arquitectura de sus productos. Las compañías emergentes pueden aprovechar lo que se aprendió en la industria de la ciberseguridad en los últimos 20 años y tratar de no cometer los mismos errores en sus innovaciones. Muchas de las mejores prácticas que se aplican a computadoras de uso general también se aplican a dispositivos de Internet de las cosas: instalar el software más reciente, por ejemplo. Pero en el mundo de Internet de todo al que nos está llevando Internet de las cosas, la seguridad será administrada en gran medida por sistemas, no por usuarios; por eso, la industria también tendrá que considerar eso cuando se diseñe tecnología segura para este entorno emergente. Esto incluye garantizar la transparencia para que los usuarios puedan estar seguros de que los dispositivos de Internet de las cosas mantendrán su seguridad automáticamente o de que sabrán cuándo podría ser necesario ejecutar alguna acción manual.

Siempre se agregará algo nuevo al ecosistema de Internet. Al mismo tiempo, también aumentará la cantidad de dispositivos abandonados y no administrados conectados a Internet. Al igual que los sitios web olvidados y descuidados de Internet actual (ver Vulnerabilidades de WordPress: ¿quién atiende el negocio?, pág. 37), estos dispositivos (desde electrodomésticos de cocina hasta cámaras de vigilancia o impresoras personales) serán eslabones débiles en la cadena de seguridad que ofrecerán a los piratas informáticos activos la posibilidad de desbloquear una cantidad prácticamente ilimitada de accesos, lo que podría dirigir al centro de datos.

Todos comprendemos las capacidades y motivaciones de los ciberdelincuentes: su creciente enfoque en Internet de las cosas es una progresión natural. A diferencia de la primera incursión de la comunidad global en un mundo conectado a Internet, todos tenemos el beneficio de la previsión: sabemos por experiencia que el entorno de Internet de las cosas presenta riesgos y que tanto organizaciones como usuarios serán víctimas de ataques. Ahora, un mayor riesgo es subestimar la laboriosidad de los atacantes y la extrema velocidad con la que tanto Internet de las cosas como Internet de todo están comenzando a tomar forma.

Inteligencia contra amenazas

Los investigadores de Cisco especializados en seguridad han reunido y analizado datos de seguridad correspondientes a la primera mitad del año 2014 basándose en el conjunto de datos de telemetría más grande disponible. Los expertos en seguridad de Cisco realizan investigaciones y análisis continuos de amenazas descubiertas, como tráfico de malware, que pueden proporcionar perspectivas sobre el posible comportamiento delictivo futuro y ayudar en la detección de amenazas.

Un cambio de paradigma en el compromiso: mirar de adentro hacia afuera

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

La inteligencia contra amenazas presentada en el ***Informe anual de seguridad 2014 de Cisco*** incluyó una conclusión clave de un proyecto "De adentro hacia afuera" reciente en el que los investigadores de Cisco especializados en seguridad revisaron búsquedas de DNS que se originaban desde el interior de redes corporativas.[8]

Los investigadores de Cisco especializados en seguridad descubrieron que había tráfico malicioso visible en el 100% de las redes muestreadas.[9]

Basándose en la actividad que observaron, los investigadores de Cisco también determinaron que este grupo en particular de redes corporativas que habían revisado probablemente había sido penetrado durante algún tiempo y que no se había detectado la infiltración central.

Cisco presenta algunas conclusiones adicionales en este informe del proyecto De adentro hacia afuera en curso. La información se basa en la revisión de datos analíticos recopilados de determinadas redes de clientes desde el comienzo del año 2014 por parte de los investigadores de Cisco especializados en amenazas. Los investigadores estudiaron de cerca 16 organizaciones multinacionales que, en conjunto, controlaron más de USD 4 billones en activos con ingresos por más de USD 300 mil millones en el año 2013. Este análisis arrojó tres datos de seguridad de peso que vinculan a esas empresas con el tráfico malicioso.

Solicitudes de DDNS

Descripción de la amenaza:

DDNS es un sistema que se usa normalmente para fines legítimos, a saber, usuarios particulares que necesitan la capacidad para asignar un nombre de dominio totalmente calificado (FQDN) estático, por ejemplo: homeserver.isp.com, a una cantidad o un grupo de direcciones IP asignadas dinámicamente por su Proveedor de servicios de Internet (ISP).

Desafortunadamente, DDNS, como muchas tecnologías y características desarrolladas para usos legítimos, puede ser muy popular entre los atacantes porque permite que los botnets y otras infraestructuras de ataque sean inmunes a la detección y a su posterior destrucción. La presencia de volúmenes inusualmente grandes de solicitudes de dominios usando proveedores de servicio DDNS, como nombre-servicios.com, podría indicar la posibilidad de que la red de una organización esté afectada. Aunque muchos de los pedido (y en ocasiones, todos) de una organización a proveedores DDNS son legítimos, estas solicitudes siempre se deben escudriñar para asegurarse de que, de hecho, sean legítimas.

Conclusiones

Se ha determinado que cerca del 70% (66,67%) de los pedidos muestreados en redes de clientes observados en el año 2014 como parte de este proyecto "De adentro hacia afuera" emiten solicitudes de DNS para DDNS. (Nota: Los investigadores de Cisco especializados en seguridad esperan que este porcentaje aumente con el paso del tiempo a medida que se incremente el tamaño de las muestras de las redes de clientes analizadas. Cisco recién acaba de iniciar el seguimiento de esta categoría nueva como un posible Indicador de compromiso (IOC); un IOC es un evento o artefacto que se observa en un sistema (a menudo sutil) que, cuando se correlaciona con otros IOC correspondientes a un sistema, indica un probable compromiso). Como ya se mencionó, esto de ninguna manera se traslada a todos y cada uno de los clientes afectados por malware que están usando proveedores de DDNS; sin embargo, Cisco ha sugerido que esos clientes analicen más de cerca estas solicitudes DDNS para asegurarse de que se estén ejecutando por motivos comerciales legítimos.

Solicitudes para sitios asociados con malware Eso incorpora la funcionalidad MiTB

Descripción de la amenaza:

Palevo, SpyEye y Zeus son familias de malware que incorporan la funcionalidad de hombre en el navegador (MiTB). Las búsquedas de DNS correspondientes a hosts afectados por Palevo, Zeus y SpyEye son consideradas como una amenaza muy grave. Palevo, SpyEye y Zeus son familias de malware que incorporan la funcionalidad de hombre en el navegador (MiTB). Se usan para ejecutar ataques de denegación distribuida de servicio (DDoS) y robar información ingresada en campos creados en tiempo real y agregados a un formulario existente. Palevo, Zeus y SpyEye se destacan porque representan una clase específica de malware que ataca información financiera y de otro tipo que se ingresa en formularios en línea de los navegadores usando el sistema operativo Windows.

Conclusiones

Se ha determinado que más del 90% (93,75%) de las redes de clientes observadas en el año 2014 tienen tráfico saliente a sitios web que alojan malware. Específicamente, se ha determinado que las redes emiten solicitudes DNS para nombres de dominio en los que la dirección IP en la que se resuelve el nombre del host se informa como infectada o asociada con la distribución de malware Palevo, Zeus o SpyEye.

Solicitudes DNS de FQDN, sitios y hosts asociados con protocolos administrativos

Descripción de la amenaza:

Las entidades maliciosas podrían usar canales de comunicación o protocolos de transferencia de datos cifrados y seguros para cubrir sus huellas al robar información; algunos ejemplos: VPN con Seguridad IP (IPsec), VPN con Capa de conexiones seguras (SSL), Protocolo de Intérprete de comandos seguro (SSH), Protocolo simple de transferencia de archivos (SFTP), FTP y FTP seguro (FTPS). Las organizaciones deben monitorear y validar estas comunicaciones periódicamente. Estos tipos de sitios se pueden usar para exfiltrar datos usando canales cifrados para evitar ser detectados.

Conclusiones

Se ha determinado que más del 40% (43,75%) de las redes de clientes observadas en el año 2014 emiten solicitudes DNS para sitios y dominios asociados con dispositivos que proporcionan servicios como VPN con IPsec, VPN con SSL, SSH, SFTP, FTP y FTPS.

Los investigadores de Cisco usaron búsquedas de DNS que se originan en el interior de redes corporativas para crear un snapshot de posibles compromisos de datos y vulnerabilidades. Los expertos en seguridad de Cisco analizaron la información basándose en listas de bloques y observaron tendencias en cibercompromisos, vulnerabilidades exclusivas que afectan verticales específicas y factores geopolíticos que podrían afectar a los actores y a la información objetivo. Los clientes de Cisco que participan del proyecto De adentro hacia afuera reciben un *Informe de ciberamenazas externas* elaborado y entregado por Cisco.

Tendencias geopolíticas que se deben observar

Los eventos geopolíticos en Europa Oriental y Oriente Medio están creando nuevas tendencias en el ámbito cibernético que están expandiendo el panorama del riesgo para empresas, gobiernos y otras organizaciones y usuarios individuales en todo el mundo, según los expertos en ciberseguridad de Cisco:

La inestabilidad política en Ucrania dio comienzo a una serie de ataques de DDoS y desacreditación de sitios web aparentemente calculada para complementar las acciones en tierra. Los problemas en Crimea y Kiev llevaron al descubrimiento de sofisticado malware de espionaje en redes ucranianas (llamado Ouroboros o Serpiente), que había pasado desapercibido durante meses o años.

En Oriente Medio, la invasión de secciones enteras del norte y el oeste de Irak por parte del Estado Islámico de Irak y el Levante (Islamic State of Iraq and the Levant, ISIL o ISIS) es acompañada por una campaña de sabotaje y guerra psicológica en los medios sociales.

Si miramos hacia adelante, las divisiones étnicas y religiosas de larga data se están profundizando en una parte del mundo que realmente está marcando el camino a seguir en el uso de las cibertácticas, tanto por parte de actores estatales como no estatales. En la segunda mitad del año 2014, las polémicas elecciones presidenciales de Turquía y las elecciones legislativas de los Estados Unidos, además del cese paulatino de las operaciones militares de Occidente en Afganistán, probablemente creen nuevas ondas expansivas en todo el panorama cibernético mundial.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Aprovechamiento de vulnerabilidades web: el aprovechamiento de vulnerabilidades Java sigue prevaleciendo

El aprovechamiento de vulnerabilidades del lenguaje de programación Java sigue liderando el *ránking* de IOC monitoreados por la plataforma de detección de malware avanzado Cisco® FireAMP. Estos ataques han extendido su aparentemente indiscutible liderazgo en la primera mitad del año 2014.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

FIGURA 1

Distribución semestral de compromiso de aplicaciones 2014

FUENTE: Cisco® FireAMP[10]

Los ataques a Java representaron el 91% de los IOC en noviembre de 2013, según el ***Informe semestral de seguridad 2014 de Cisco***; esa cifra se elevó ligeramente al 93% en mayo de 2014. La extensa superficie de ataque que presenta Java y el alto índice de rendimiento de la inversión son los factores que lo convierten en un favorito de los atacantes. (Si desea más detalles sobre el problema de Java y sugerencias para mitigarlo, lea el ***Informe anual de seguridad 2014 de Cisco***[11]***).***

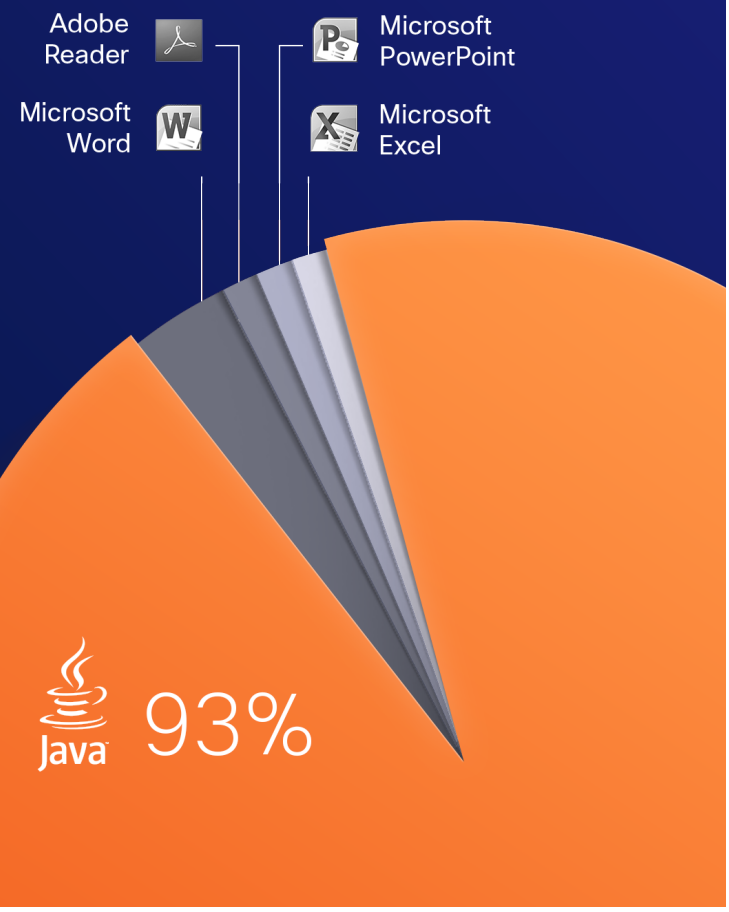


FIGURA 2

Hallazgos de malware web Java (Enero a mayo de 2014)

FUENTE: Cisco Cloud Web Security

Los hallazgos de malware web Java alcanzaron su pico máximo en marzo de 2014, con cerca de un 10% de todo el malware web encontrado.

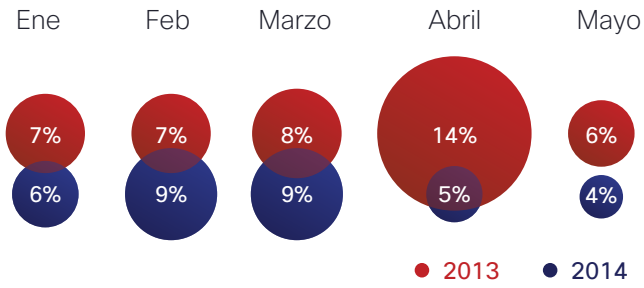


FIGURA 3

Hallazgos en Java, PDF y Flash (enero a mayo de 2014)

FUENTE: Cisco Cloud Web Security

Java, Flash y Adobe PDF son vectores populares para la actividad delictiva.

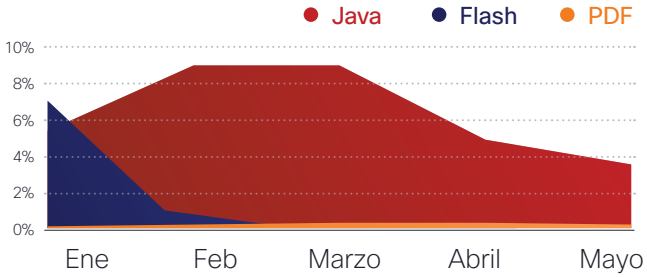
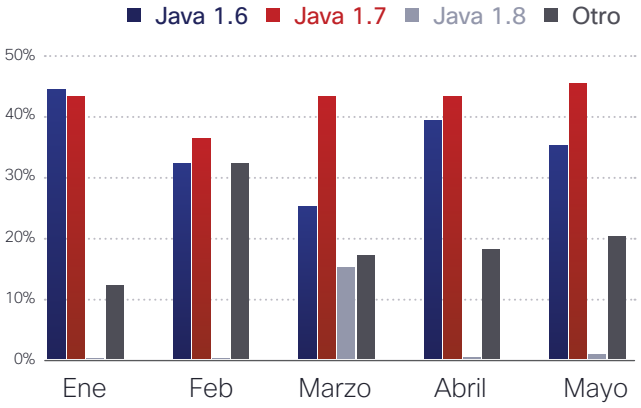


FIGURA 4

Hallazgos en Java por versión (enero a mayo de 2014)

FUENTE: Cisco Cloud Web Security

Los atacantes siguen destacándose en el aprovechamiento de las vulnerabilidades de las versiones anteriores de Java, particularmente Java 6 y 7. Se registró un importante aumento en los hallazgos de malware web con Java 8 en marzo, el mes en el que se lanzó la nueva versión. Sin embargo, la cantidad de detecciones correspondientes a Java 8 se redujo significativamente en el mes de abril y permaneció en un nivel muy bajo durante mayo. Debido al aumento en la cantidad de kits de aprovechamiento de vulnerabilidades que dependen primordialmente de vectores no Java, como Microsoft Silverlight, podríamos estar presenciando un alejamiento de Java 8 (que tiene controles de seguridad más sólidos) en favor de otro software que sea más propicio para un ataque.



Actualización sobre vulnerabilidades: enfoque en los aprovechamientos de vulnerabilidades más comunes

FIGURA 5

Estadísticas de alerta (enero a junio de 2014)

FUENTE: Cisco Intellishield®

Del 1 de enero de 2014 al 30 de junio de 2014, Cisco publicó miles de alertas multiproveedor sobre vulnerabilidades de seguridad conocidas. Pese a que la cantidad podría parecer intimidante, las vulnerabilidades extremadamente críticas suman aproximadamente el 1% de ese total. Según la investigación de Cisco, de las 2528 alertas sobre vulnerabilidades nuevas publicadas en ese período, solo se vulneraron efectivamente 28 poco después de publicados los informes.

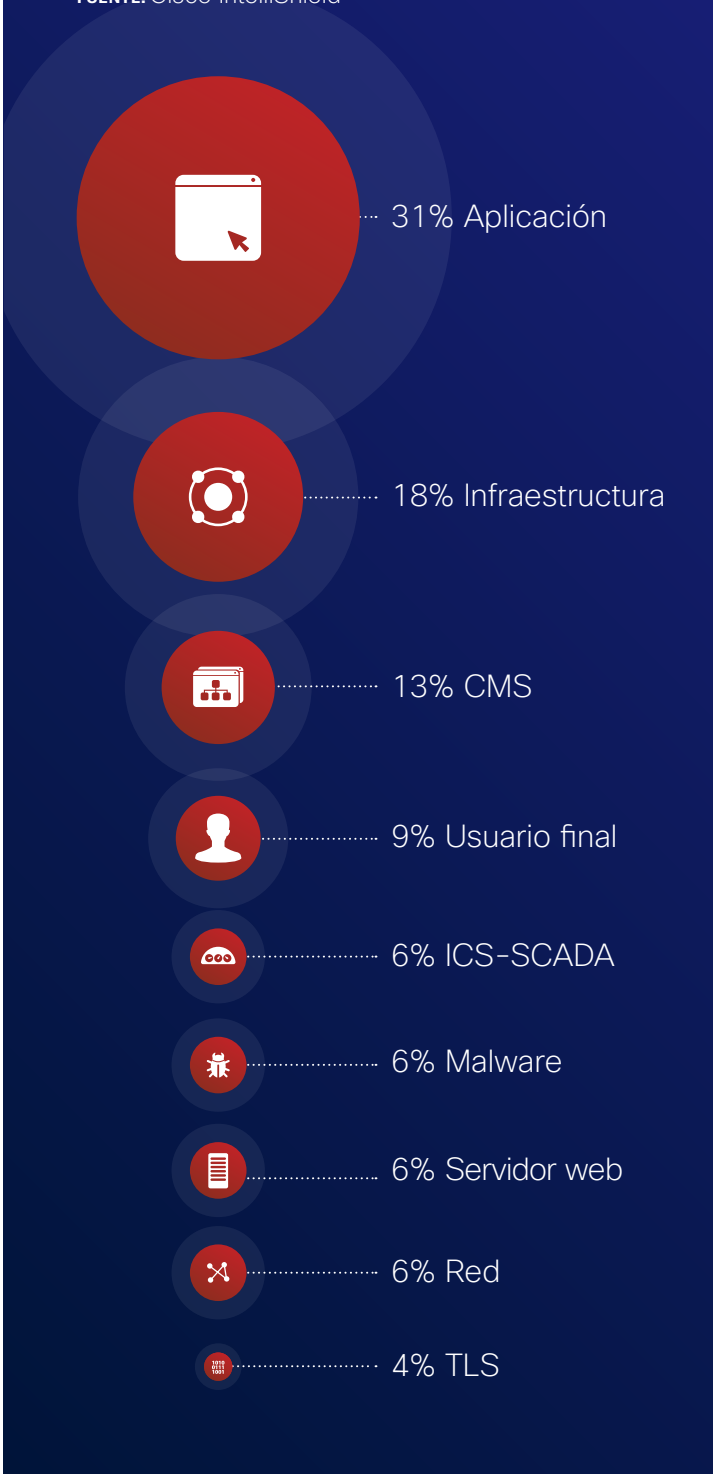
Los atacantes se concentran en vulnerabilidades comunes o “eslabones débiles” que saben son fáciles de vulnerar gracias a sus esfuerzos de “investigación y desarrollo”; luego, se incorporan los métodos de ataque exitosos a los kits de aprovechamiento de vulnerabilidades que se venden en el mercado clandestino. Los lenguajes de programación Java y Silverlight son ejemplos de vulnerabilidades que pueden encontrarse en varios kits de aprovechamiento de vulnerabilidades populares. (Ver Aprovechamiento de vulnerabilidades web: el aprovechamiento de vulnerabilidades Java sigue prevaleciendo en la página 15 y luego Kits de aprovechamiento de vulnerabilidades: el campo se abre a la competencia en la página 33.)

A medida que se publican los informes sobre vulnerabilidades, los profesionales de la seguridad y los medios tienden a enfocarse en las vulnerabilidades de día cero porque hay una necesidad aparentemente urgente de reaccionar ante noticias de tan alto perfil. Sin embargo, las organizaciones deberían priorizar sus inversiones de tiempo y dinero para corregir la pequeña cantidad de vulnerabilidades que los delincuentes están aprovechando más activamente.
Las otras vulnerabilidades se pueden manejar con procesos más rutinarios.

FIGURA 6

Principales productos que están siendo víctima de ataques

FUENTE: Cisco IntelliShield®



Es recomendable que las organizaciones tengan un "proceso de corrección para situaciones extremadamente urgentes" que se ejecutaría en paralelo con sus procesos de corrección estándares. Si se resuelven las vulnerabilidades prioritarias objetivo rápidamente, se pueden integrar otras vulnerabilidades menos urgentes al proceso de mantenimiento y corrección programado periódicamente. El resultado es una administración de riesgos más exacta: es mejor que tratar de instalar todos los parches o solo instalarlos en los períodos de mantenimiento programados periódicamente. Se necesita tener implementada una sólida inteligencia de seguridad para identificar vulnerabilidades de extrema urgencia para mantener un proceso de corrección de extrema urgencia con efectividad.

En la Figura 6 se muestran los principales productos que atacaron los delincuentes en el primer trimestre del año 2014. En la Figura 7 se ilustran algunas de las vulnerabilidades atacadas más comúnmente, según el Sistema de puntuación de vulnerabilidades comunes (CVSS).

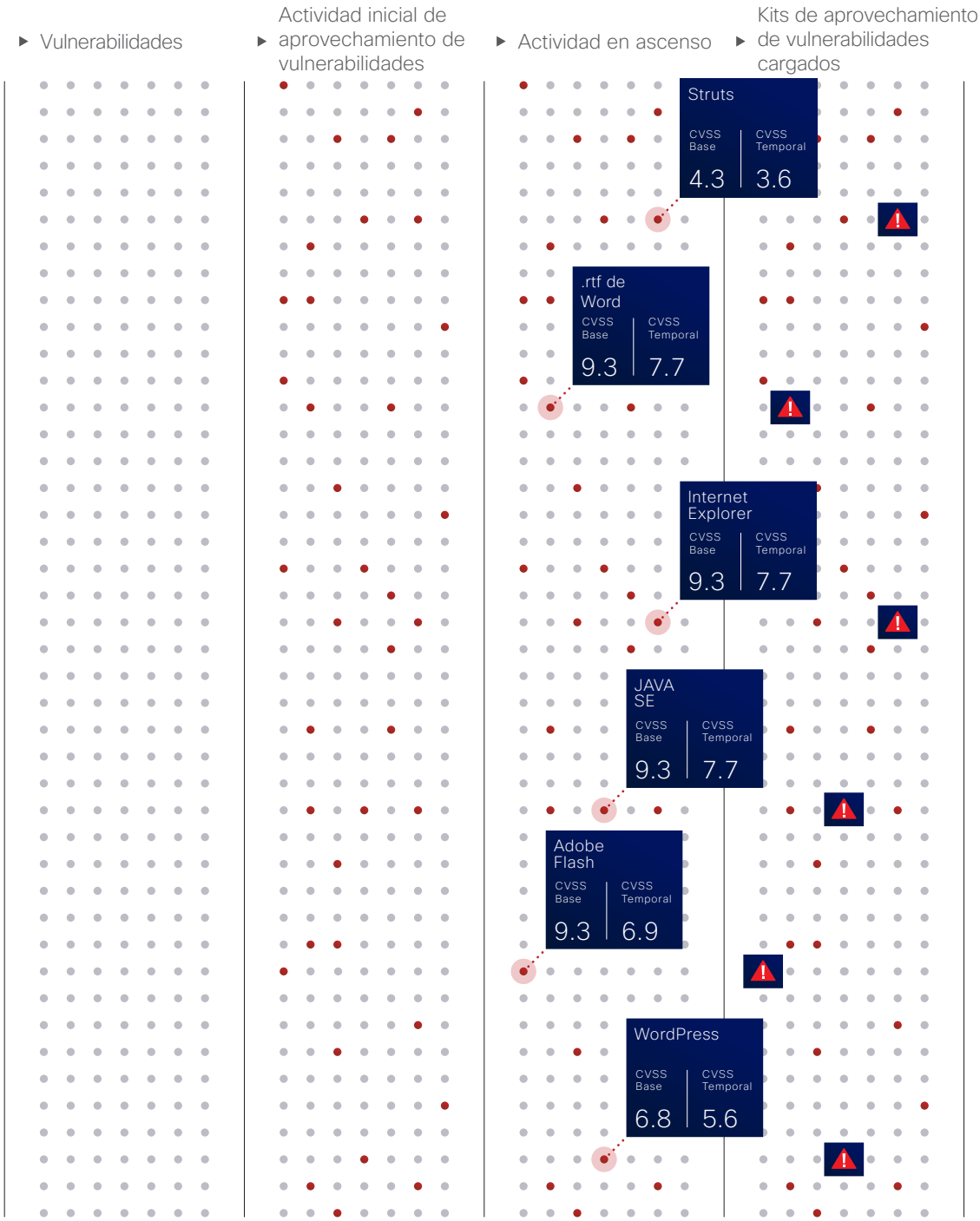
La puntuación de "Urgency" ("Urgencia") del cuadro del CVSS es útil porque indica las vulnerabilidades que están siendo atacadas, lo que se corresponde con las puntuaciones de "Temporal" ("Temporal") en las que se indican los métodos de ataque a vulnerabilidades activos. Además, si se estudia la lista de productos que están siendo víctima de los ataques, las empresas pueden determinar cuáles de esos productos están en uso y, en consecuencia, precisan ser monitoreados y corregidos.

Es importante comprender que las vulnerabilidades de la Figura 7 fueron las que mostraron señales iniciales de actividad maliciosa durante el período observado. La mayoría de estas vulnerabilidades todavía no se había convertido en "corriente", es decir, no había llegado a los kits de aprovechamiento de vulnerabilidades que se venden en el mercado.

FIGURA 7

Vulnerabilidades expuestas más comúnmente

FUENTE: Cisco IntelliShield®



COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Heartbleed: no es el único motivo para preocuparse

Algunas organizaciones no quedaron expuestas al "Heartbleed bug", una vulnerabilidad de seguridad en la biblioteca de criptografía de OpenSSL, porque estaban usando una versión anterior de OpenSSL que no incluía la vulnerabilidad.[12] La vulnerabilidad implica la implementación de la extensión heartbeat (RFC6520) de Seguridad de la capa de transporte (TLS) y podría permitir la fuga de claves secretas o información privada en comunicaciones cifradas con TLS.[13]

Sin embargo, es importante que esas organizaciones tengan presente que de enero a abril de 2014, hubo 16 vulnerabilidades de TLS y de validación de certificados *no* relacionadas con Heartbleed.

Estas vulnerabilidades podrían ponerlas en peligro. Los expertos en seguridad de Cisco también recomiendan que todos los usuarios se consideren con probabilidades de haber quedado expuestos a riesgos como resultado de Heartbleed y, en consecuencia, deberían tomar las medidas apropiadas como cambiar contraseñas o cerrar cuentas web.[14]

Desde que se descubrió Heartbleed, el proyecto OpenSSL (OpenSSL.org) ha informado varios defectos adicionales descubiertos en el software OpenSSL, algunos de los cuales "pueden permitir que un atacante cree una condición de denegación de servicio o, en determinadas situaciones, ejecución remota de códigos".[15] Algunos de estos defectos son debilidades ignoradas de larga data como, por ejemplo, la vulnerabilidad de inyección CCS, descubierta por un investigador de seguridad en Japón, es una falla de seguridad de 16 años de antigüedad en el software OpenSSL que permite que un atacante intercepte y descifre datos cifrados que viajan por Internet.[16]

Informe de riesgos verticales en la industria: incrementos inusuales en algunos sectores

En la primera mitad del año 2014, la industria farmacéutica y química, una vertical de alto nivel de ganancias, vuelve a ubicarse entre las primeras tres verticales de alto riesgo en cuanto a hallazgos de malware web; se ubicó en el primer lugar de la lista en el año 2013.[17] La industria de la aviación también vuelve a figurar entre los cinco primeros lugares, esta vez es la tercera de la lista.[18] Esto no debe sorprendernos por el valor de la propiedad intelectual que poseen las compañías de aviación.

Simultáneamente, la industria de los medios de comunicación y la editorial que actualmente figura en el primer lugar de la lista, presenta índices de hallazgos de malware web significativamente más elevados que los normales observados anteriormente por los investigadores de Cisco especializados en seguridad, quienes han venido compilando datos desde el año 2008.

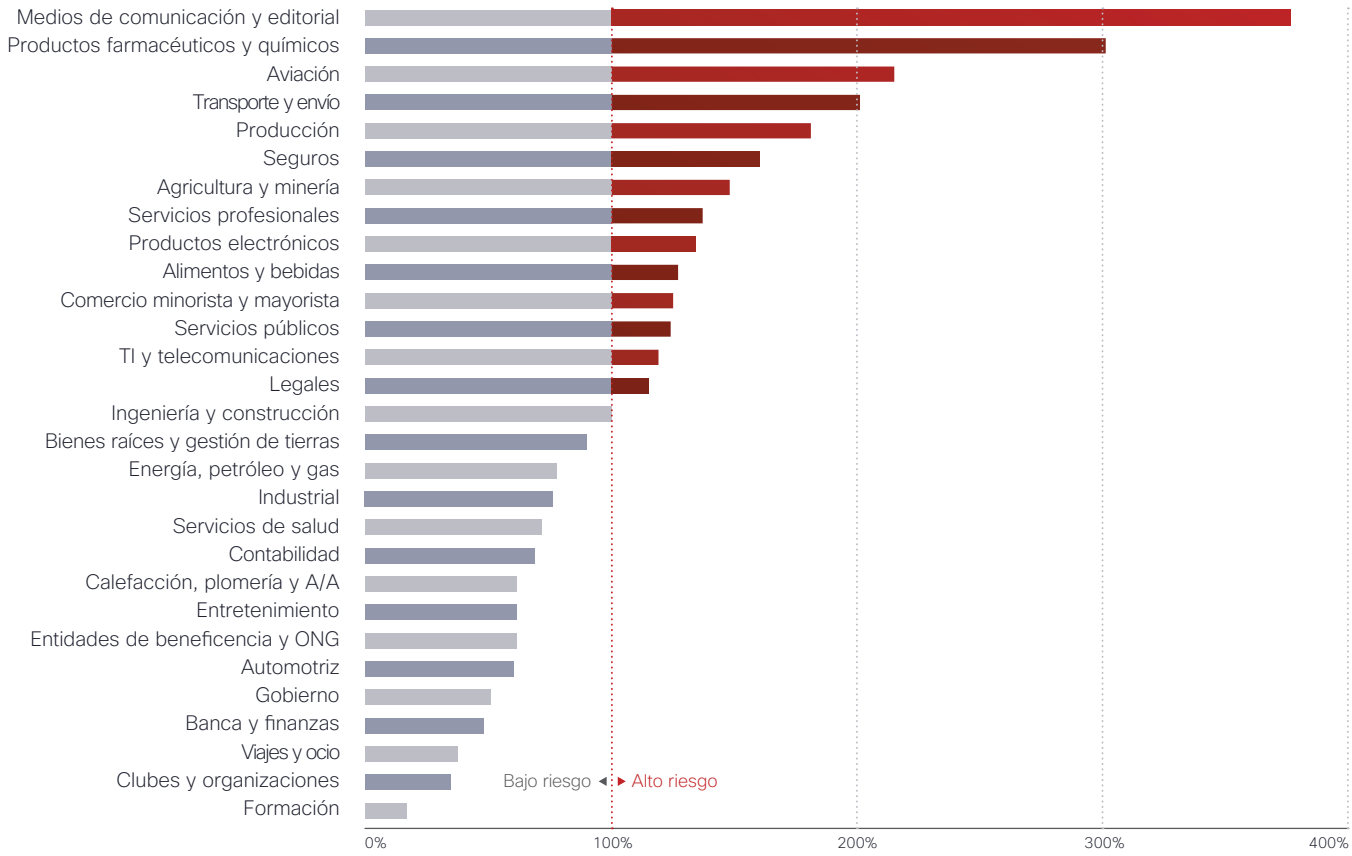
Los delincuentes que inician ataques y otros engaños en relación a eventos de alto perfil, como los Juegos Olímpicos de Invierno y la entrega de los Premios Oscar 2014, y noticias de alta repercusión como el misterio del Vuelo 370 de Malaysia Airlines y el desastre del ferry surcoreano, son probables motivos del aumento en la cantidad de detecciones en la industria de los medios de comunicación y la editorial Sus engaños pretenden aprovecharse del “eslabón débil” del ser humano: es decir, se induce a los usuarios a hacer clic e ingresar a sitios que alojan malware porque se los tienta con titulares captan su atención.

Los sitios de medios de comunicación y editoriales, sean grandes o pequeños, pueden atraer a una amplia variedad de personas, desde consumidores particulares hasta organizaciones en todo el mundo. También dependen en gran medida de la publicidad para subsistir. Por es motivo en particular, es probable que el aumento de la publicidad maliciosa sea responsable en parte del incremento en los hallazgos de malware web en la industria de los medios de comunicación y la editorial en la primera mitad del año 2014. (Ver Publicidad maliciosa: un factor que altera la economía en Internet, en la página 35.)

FIGURA 8

Riesgo vertical de hallazgos de malware web, primera mitad del año 2014

FUENTE: Cisco Cloud Web Security



Para determinar los índices de hallazgos de malware específicos de un sector, los investigadores de Cisco especializados en seguridad comparan el índice mediano de hallazgos correspondiente a todas las organizaciones que transmiten a través de Cisco Cloud Web Security con el índice mediano de hallazgos correspondiente a todas las compañías de un sector específico que transmiten a través del servicio. Un índice de hallazgos de la industria superior al 100% refleja un riesgo mayor de lo normal de hallazgos de malware web, mientras que un índice inferior al 100% refleja un riesgo menor. Por ejemplo, una compañía con un índice de hallazgos del 170% tiene un riesgo de un 70% por arriba de la mediana. A la inversa, una compañía con un índice de hallazgos del 70% se encuentra un 30% por debajo de la mediana.

Hallazgos de malware por región

Por primera vez, los investigadores de Cisco especializados en seguridad están presentando datos sobre riesgos de hallazgos de malware web para verticales de la industria por región. Las tres regiones se definen de la siguiente manera: AMER (Norteamérica, Centroamérica y Latinoamérica), APJC (Asia Pacífico, China, Japón e India) y EMEAR (África, Europa y Oriente Medio).

En la región AMER, tal como se indica en la Figura 9, la aviación supera a las demás industrias por un importante margen.

El riesgo vertical en una región en particular se verá influenciado por el producto bruto interno de esa región. Habitualmente, cuanto mayor sea el valor de los bienes y servicios, o de la propiedad intelectual, de una vertical en particular, mayor será el riesgo de hallazgos de malware correspondiente a esa industria.

Una vertical en particular también podría estar representada por una cifra menor en una región que no suele tener producción en ese sector específico. Este es un motivo para el riesgo "de la granja a la mesa" que suelen padecer compañías en las industrias de la agricultura, los alimentos y las bebidas, y el transporte. También es el probable motivo para que en la industria de los alimentos y las bebidas se registrara la mayor cantidad de hallazgos de malware web en la región EMEAR. Las recientes sequías, inundaciones y disturbios en esa región han afectado la disponibilidad de suministros e infraestructuras básicos para sus habitantes.

Hallazgo versus compromiso

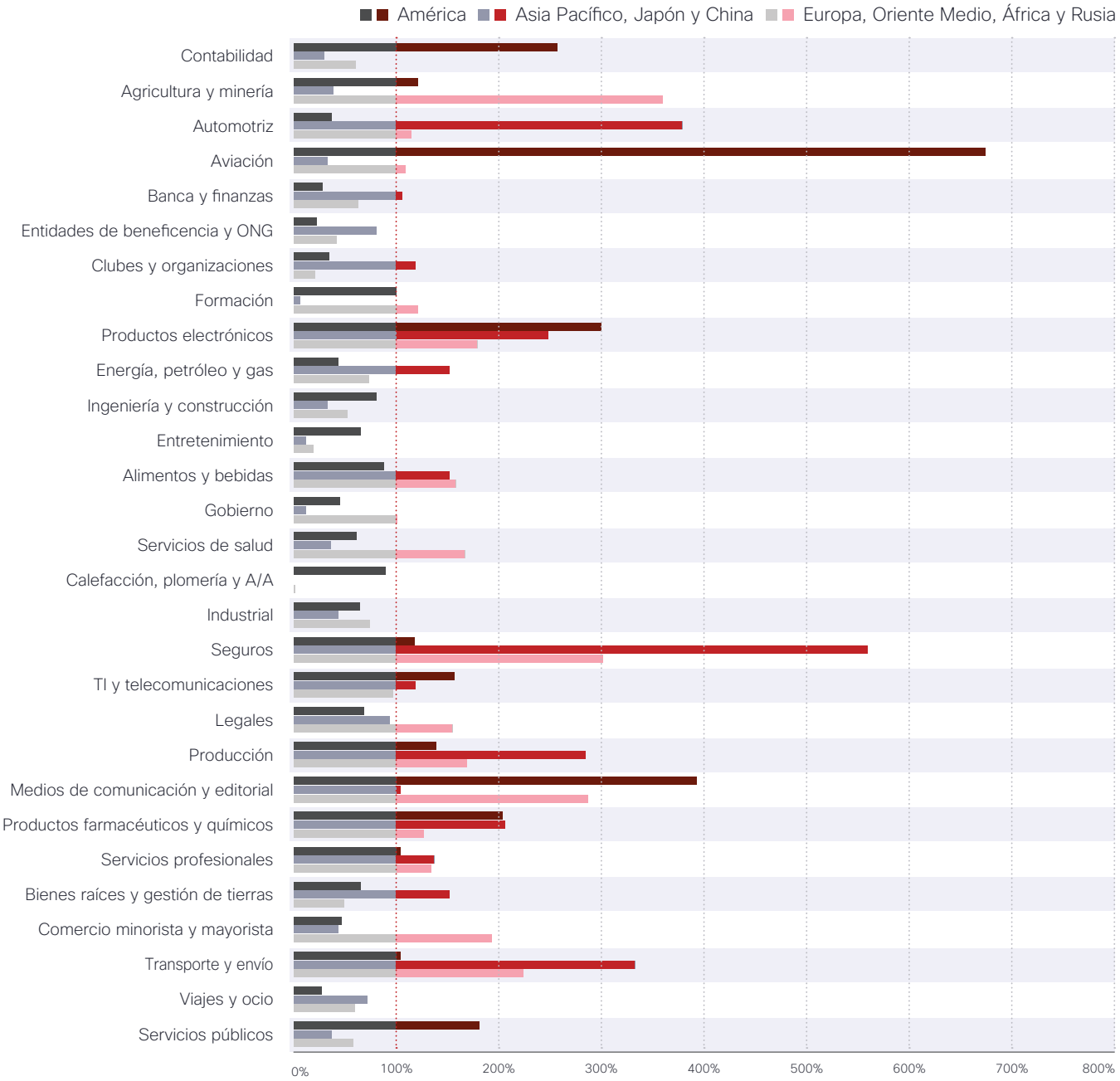
Un "hallazgo" es una instancia en la que se bloquea malware. A diferencia de un "compromiso", el usuario no se infecta durante un hallazgo porque no se descarga ningún código binario.

En la región APJC, la vertical de mayor riesgo fueron los seguros, seguida por la industria farmacéutica y química, y las verticales relacionadas con la electrónica. Los recientes problemas en la región APJC, como el devastador terremoto, tsunami y desastre nuclear de Japón en el año 2011, y el subsiguiente ajuste del mercado de los seguros, son probables factores para que la industria de los seguros se convierta en un objetivo clave para los atacantes. Es más, como la industria de los seguros es un proveedor de servicios de corporaciones importantes y otras entidades, los delincuentes podrían pretender atacar a las aseguradoras como un modo de obtener información confidencial sobre sus clientes o de encontrar una ruta hasta sus redes y centros de datos.

FIGURA 9

Riesgo vertical de hallazgo de malware web por región

FUENTE: Cisco Cloud Web Security



Las cinco verticales principales del riesgo por región

En la Figura 10 se proporciona un desglose de las cinco verticales principales de riesgo correspondientes a cada región: AMER, APJC y EMEAR. iFrames y los scripts maliciosos dominan todas las industrias representadas, aunque los actores maliciosos de las tres regiones parecen depender en gran medida de aprovechamientos de vulnerabilidades para atacar industrias específicas. En APJC, los engaños, la suplantación de identidad y el fraude por clic en publicidad se usan con frecuencia para aprovecharse de la confianza de los usuarios en las industrias del transporte y los envíos.

Aparentemente, incluso pocos delincuentes tratan de aprovechar las cinco verticales de riego principales en cualquiera de las tres regiones con técnicas como el ransomware y el scareware o con virus y gusanos. La cantidad de hallazgos de malware web en dispositivos móviles también es bastante baja en todas las regiones.

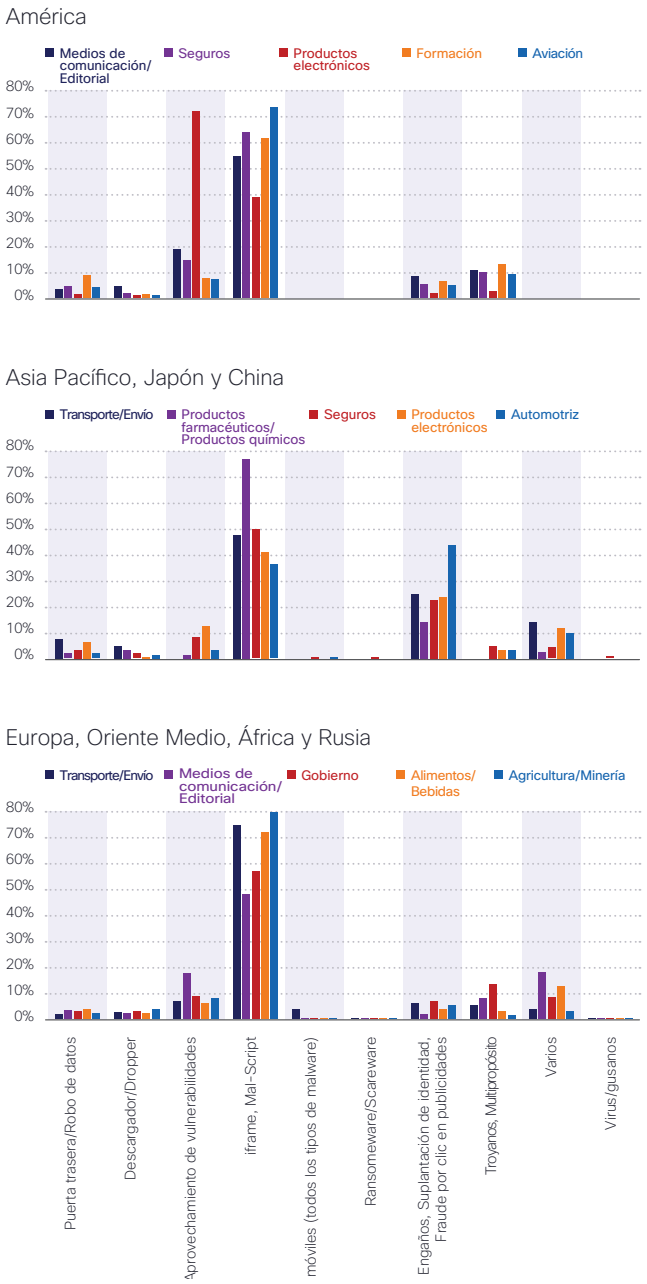
Los hallazgos que se presentan en estos cuadros se basan primordialmente en los sitios en los que se registraron los bloqueos de malware web (es decir, los hallazgos), según datos de Cisco Cloud Web Security, y no en tipos de amenazas en la red.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

FIGURA 10

Riesgo vertical de malware web

FUENTE: Cisco Cloud Web Security



Actualización sobre spam: el spam “que promete solucionar problemas de la vida” pasa a ser más frecuente

Los delincuentes que crean spam tradicionalmente han utilizado trucos de ingeniería social para convencer a sus víctimas de que abran los mensajes y hagan clic en los enlaces, que suelen dirigirlos a sitios comprometidos o de malware. Las entregas de paquetes falsas o los falsos asuntos impositivos urgentes son ardides comunes, pero ahora los profesionales especializados en seguridad ven una tendencia a usar spam que “soluciona problemas de la vida” o “adversidades”. Este tipo de spam recurre a la emoción para obtener resultados.

Por ejemplo: el spam que “soluciona problemas de la vida” podría enfocarse en el tratamiento o la recuperación de una enfermedad potencialmente mortal y el spam de las “adversidades” podría mencionar los temas del desalojo o la bancarrota. Ambos pueden ejercer gran presión para que el destinatario abra el mensaje, mucho más que un mensaje sobre la entrega express de un paquete.

El spam que “soluciona problemas de la vida” y “adversidades” se enfoca en un eslabón débil común de la cadena de seguridad: el usuario, quien, incluso con conocimientos sobre ingeniería social, tiende a responder a un mensaje que promete resolver adversidades personales.

Al igual que en la lucha contra cualquier campaña de spam, la clave para mitigar el spam que promete solucionar problemas de la vida es el uso de tecnología para el bloqueo de spam que se puede actualizar dinámicamente.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Los delincuentes que se dedican al spam son cada vez más ágiles y cambian sus enfoques para mejorar sus índices de éxito

Los delincuentes que se dedican al spam reaccionan rápidamente a los avances en la tecnología que bloquea sus mensajes. Ajustan el texto, las imágenes y los nombres de dominio para evadir los filtros de spam. Y, cuando cae la eficacia de los mensajes, vuelven a hacer todos los cambios que sean necesarios.

Los investigadores de Cisco especializados en seguridad monitorean diversos tipos de spam y la evolución de los mensajes para informar a los clientes sobre las nuevas tácticas que utilizan los delincuentes dedicados al spam para obtener acceso a las redes o robar información. En algunos casos, las notas de cobertura correspondientes a un tipo de spam específico (como un anuncio falso sobre un pago electrónico) podrían ser actualizadas decenas de veces por los investigadores de Cisco a medida que los delincuentes cambian sus tácticas.

El volumen de spam a nivel mundial se duplicó con respecto al índice normal, pero en algunos países se ve una marcada disminución

FIGURA 11

Volumen de spam a nivel mundial (Enero de 2014 a mayo de 2014)

FUENTE: Plataforma de inteligencia contra amenazas de Cisco

Después de una reducción general en el año 2013, el volumen global de spam ha aumentado continuamente desde el pasado mes de octubre. De acuerdo con la investigación de Cisco, los volúmenes de spam han aumentado al punto de que, ahora, el spam ha alcanzado su nivel máximo desde finales del año 2010. De junio de 2013 a enero de 2014, la cantidad promedio de mensajes de spam fue de 50 mil millones a 100 mil millones por mes. Sin embargo, a marzo de 2014, los volúmenes alcanzaron picos de más de 200 mil millones de mensajes por mes, dos veces por encima de los índices normales.[19]

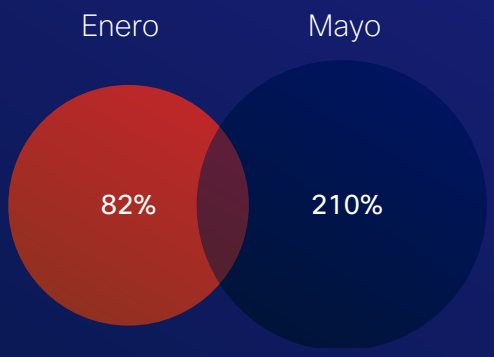
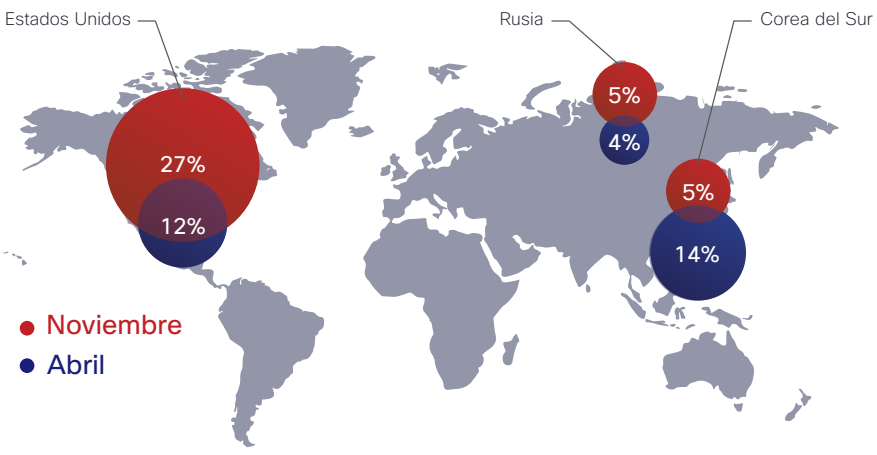


FIGURA 12

Tendencias de volumen por país, (Noviembre de 2013 a abril de 2014)

FUENTE: Plataforma de inteligencia contra amenazas de Cisco

Además, pese a que el volumen de spam a nivel mundial está aumentando, ese aumento no se registra en todos los países. De hecho, tanto en Rusia como en Estados Unidos se han visto marcadas reducciones en el volumen de spam desde noviembre de 2013. Mientras tanto, en Corea del Sur se ha registrado un pico importante en el volumen de spam, en comparación con los otros 10 países principales monitoreados por los investigadores de Cisco especializados en seguridad.



Argentina	2%	7%	Alemania	2% | 6%
China	11%	5%	Irán	1% | 4%
Japón	2%	7%	España	3% | 7%
Reino Unido	2%	4%		

Tendencias en la industria

Los expertos en seguridad de Cisco ofrecen datos y análisis de amenazas y tendencias de seguridad observadas durante la primera mitad del año 2014, así como proyecciones para lo que se espera en los próximos meses.

Conexiones cifradas seguras comprometidas

Ataques recientes de alto perfil que aprovechaban vulnerabilidades en certificados de cifrado y seguridad, como "goto fail" de Heartbleed y Apple[20] han revelado que muchas implementaciones populares de TLS representan el eslabón más débil para todos los usuarios. Es una ironía que medidas de seguridad como el cifrado y la criptografía se hayan convertido en eslabones débiles. Durante años, se ha instado a los consumidores a que busquen el símbolo del candado en línea como un modo de confirmar que estaban por completar una transacción "segura". Muchos usuarios también han confiado en que su información estuviera bien protegida en el punto de venta (POS) sin conexión, porque creían que no se llevaba a cabo ningún cifrado de extremo a extremo, si es que incluso pensaban en eso.

Lo que nos han demostrado estos últimos seis meses, sin embargo, es que, independientemente de lo alerta o precavidos que sean los usuarios, o de la cantidad de protecciones de seguridad que se implementen, los eslabones débiles que escapan a su control todavía los dejan expuestos a un gran riesgo.

Obviamente, abordar el problema de las conexiones cifradas seguras comprometidas es imperioso para cualquier empresa que acepte pagos. Para eso se requiere un estudio más cercano de los procesos de la industria que ayudan a llevar productos de cifrado y otros productos de seguridad al mercado.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Heartbleed y eventos similares ponen de manifiesto que muchas organizaciones que utilizan conexiones cifradas seguras y tecnologías relacionadas asumen lo siguiente:

- Los protocolos criptográficos que se basan en códigos abiertos estándares y populares proporcionan seguridad sólida.
- Todo el código fuente incrustado en productos y servicios de seguridad, incluido el provisto por terceros, ha sido investigado profundamente por expertos en seguridad.

Ninguna de las suposiciones es verdadera, pero ambas son factores para la implementación exitosa de ataques como Heartbleed que explotan las vulnerabilidades y otras fallas de seguridad y se aprovechan de la confianza de los usuarios.

Mejorar los procesos de la industria no será fácil. De acuerdo con los expertos en seguridad de Cisco, en su estado actual OpenSSL es complejo y difícil de implementar correctamente, además de probarlo en busca de vulnerabilidades. El proceso de investigación actual del código abierto y patentado necesita un enfoque más robusto, pero todavía no se sabe quién debería desarrollar y mantener ese enfoque. Mientras tanto, la comunidad de seguridad está debatiendo si se puede corregir siquiera el sistema de autoridades de certificados vulnerado.

En el mundo de la seguridad, la simplicidad es prioritaria; minimizar la cantidad de código necesaria para ser confiable es un paso importante para crear implementaciones seguras. Los expertos en seguridad de Cisco anticipan que para mejorar las bibliotecas e seguridad SSL/TLS de código abierto se necesitará lo siguiente, como mínimo:

- Reducir la complejidad de los protocolos y sus implementaciones
- Validar que el código se haya implementado correctamente, esté libre de vulnerabilidades y no contenga fallas ocultas
- Asegurarse de que quienes prueben y validen el código estén debidamente calificados

Una salida positiva de eventos recientes como Heartbleed: muchas personas pertenecientes a la comunidad de desarrolladores están buscando proactivamente en su código fallas que deben corregir. La Fundación Linux también acaba de anunciar la formación de la Iniciativa de Infraestructura Central, que "permite que las compañías de tecnología determinen y financien en conjunto proyectos de código abierto que precisen asistencia y, a la vez, permite que los desarrolladores continúen con su trabajo según las normas de la comunidad que han convertido al código abierto en un éxito de semejante magnitud".[21] OpenSSL fue uno de los primeros proyectos que se consideró para que recibiera fondos de la Iniciativa de infraestructura central. Cisco es uno de los patrocinadores fundadores de la Iniciativa.

Ataques por amplificación: atacantes que sincronizan relojes con NTP

Los expertos en seguridad de Cisco advirtieron en el *Informe anual de seguridad 2014 de Cisco* que los ataques de DDoS, es decir, los iniciados a través de amplificación de DNS, seguirían siendo una de las principales preocupaciones de seguridad para las organizaciones en el año 2014.[22] Pero incluso antes de eso, los investigadores de Cisco afirmaron que el NTP, que está diseñado para sincronizar los relojes de las computadoras por una red, era un eslabón débil y posicionado para convertirse en un vector de ataques de DDoS amplificados. Basaron su proyección en sus observaciones: las herramientas de ataque diseñadas para utilizar la creciente cantidad de servidores NTP vulnerables se estaban comenzando a distribuir entre la comunidad de piratas informáticos.[23]

FIGURA 13

Ataque de DDoS al NTP de CloudFlare, 2014

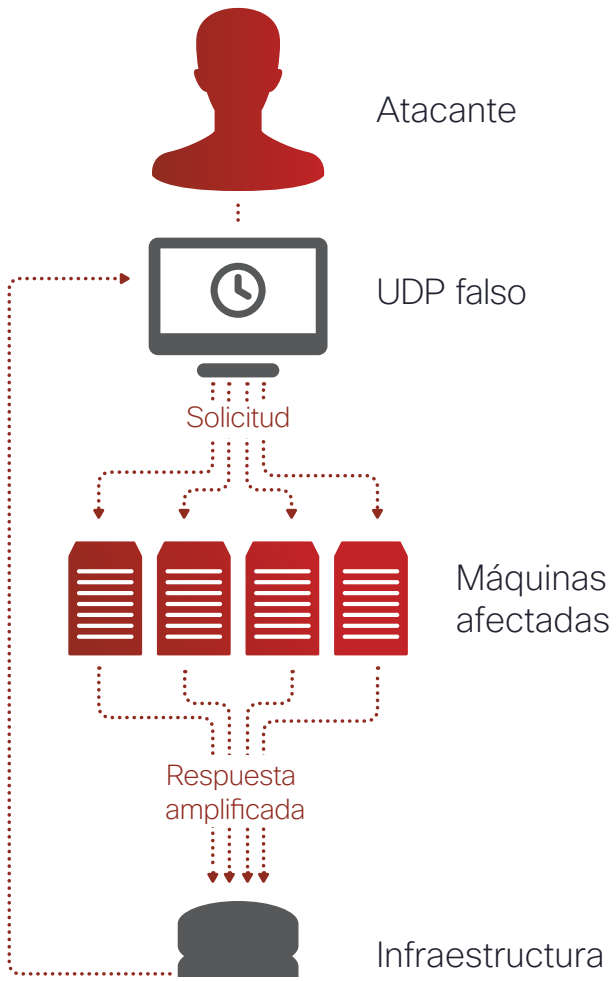
FUENTE: Plataforma de inteligencia contra amenazas de Cisco

Uno de los ataques por amplificación de NTP más significativos que se observó en los primeros seis meses de 2014 fue sobre un cliente del proveedor de DNS a nivel global CloudFlare (ver la Figura 13). En su pico máximo, el ataque del mes de febrero alcanzó casi 400 Gbps de tráfico UDP, sobrepasando así el ataque de DDoS Spamhaus de marzo de 2013 de 300 Gbps que implicó a 30 000 resolvedores de DNS abiertos.[24]

Es fácil comprender por qué algunos atacantes están experimentando con NTP como herramienta para sus ataques de DDoS: OpenNTPProject.org, un proyecto de escaneo de NTP diseñado para aumentar el conocimiento sobre el problema de NTP, ha detectado más de 1 millón de servidores NTP vulnerables.[25] Combinados, el ancho de banda de estos servidores probablemente sea mayor que cualquier ataque de DDoS visto a la fecha.

FIGURA 14

Ejecución de un ataque al NTP



COMPARTIR EL INFORME SEMESTRAL DE SEGURIDA 2014 DE CISCO

Para ejecutar un ataque por amplificación del NTP, el delincuente envía pequeñas solicitudes a máquinas NTP vulnerables; para ello, falsifica la dirección del paquete UDP para que las solicitudes parezcan provenir del objetivo que está tratando de desconectar. El UDP no reconoce estados; la capacidad de falsificar la dirección UDP es un componente necesario en ataques por amplificación de DNS y de NTP. Los servidores NTP implicados en el ataque devuelven una respuesta muy larga a las solicitudes pequeñas y envían toda la información de regreso al objetivo cuya máquina queda inundada y desconectada. (Actualmente, en la industria se está trabajando para prevenir la falsificación de UDP; dichos trabajos deben continuar.)

Es necesario actualizar los servidores NTP en contacto con el público a la versión de NTP más reciente para prevenir un posible ataque por amplificación de NTP. Al momento de redactar este documento, esa versión es la 4.2.7. Esta actualización elimina el soporte para el comando MON_GETLIST o “monlist”, que es un comando remoto que devuelve las direcciones de las últimas 600 máquinas con las que interactuó el servidor NTP. Si no es posible realizar la actualización, usar la opción *noquery* en la configuración del NTP también impedirá consultas monlist.

Aunque los ataques por amplificación de NTP podrían ser un nuevo tipo de ataque de DDoS, anticipamos que la amplificación de DNS seguirá siendo una técnica obligada para muchos atacantes. De acuerdo con el proyecto Open Resolver, hasta el mes de octubre de 2013, 28 millones de resolvedores abiertos imponían una amenaza significativa.[26]

Kits de aprovechamiento de vulnerabilidades: el campo se abre a la competencia

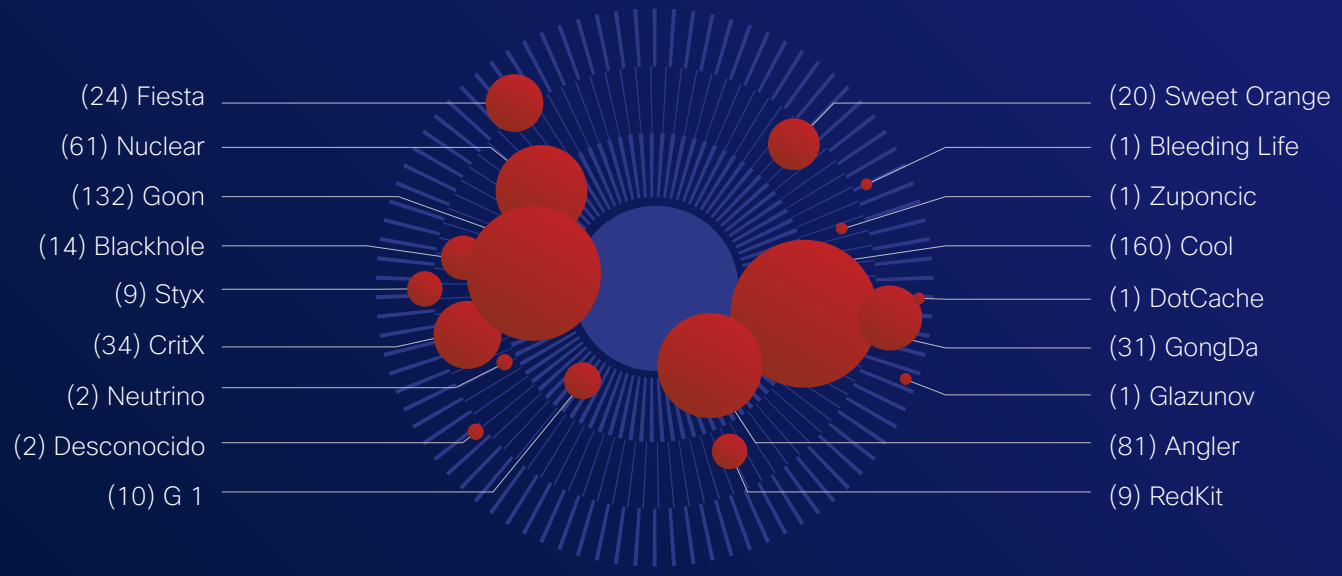
Cuando el "cerebro del malware conocido como 'Paunch,' el supuesto creador y distribuidor del kit de aprovechamiento de vulnerabilidades Blackhole" fue arrestado en Rusia el mes de octubre de 2013,[27] en muy poco tiempo los autores de kits de aprovechamiento de vulnerabilidades comenzaron a señalar sus reclamos por el territorio que antes dominaba su kit.

Blackhole era indudablemente el kit de aprovechamiento de vulnerabilidades más usado y mejor mantenido. Cuando Paunch y Blackhole fueron dejados fuera de servicio por las autoridades, los atacantes posaron su atención en nuevos kits de aprovechamiento de vulnerabilidades. Según los investigadores de Cisco especializados en seguridad, muchos contendientes se disputaron el primer puesto en la primera mitad del año 2014; sin embargo, todavía no ha surgido ningún líder claro.

FIGURA 15

Kits de aprovechamiento de vulnerabilidades observados desde enero de 2014

FUENTE: Plataforma de inteligencia contra amenazas de Cisco



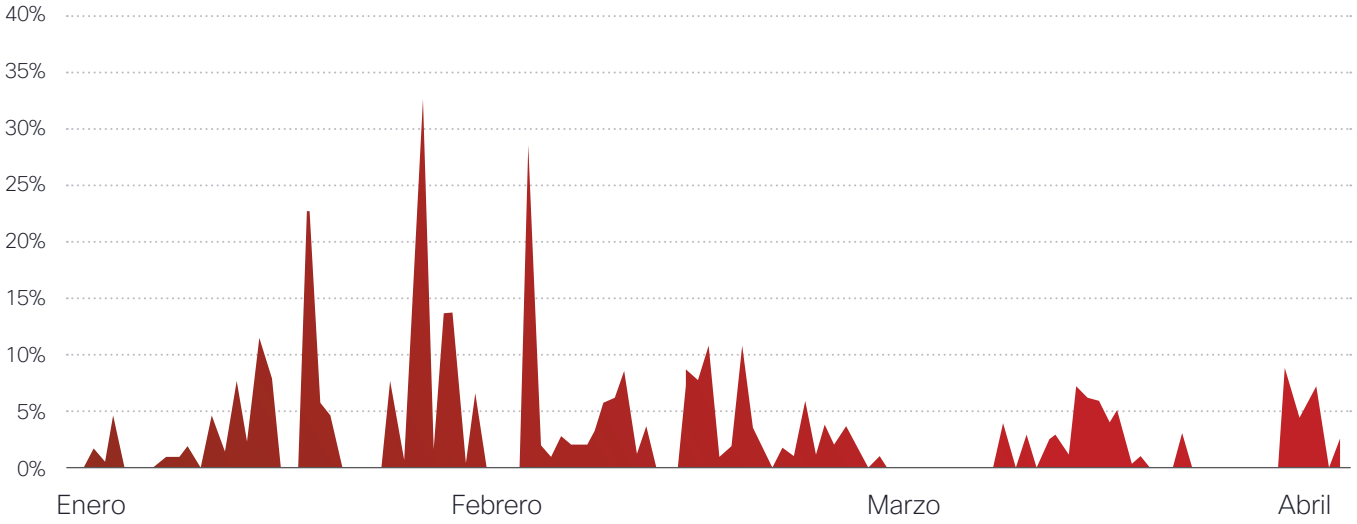
(Cantidad de ataques) Nombre del kit de aprovechamiento de vulnerabilidades

Pese a la mayor competencia, la cantidad de kits de aprovechamiento de vulnerabilidades ha caído un 87% desde el arresto de Paunch el año pasado, según los investigadores de Cisco especializados en seguridad (ver la Figura 16).

FIGURA 16

Reducción en la cantidad de kits de aprovechamiento de vulnerabilidades (Enero a abril de 2014)

FUENTE: Plataforma de inteligencia contra amenazas de Cisco



Los atacantes también están usando kits de aprovechamiento de vulnerabilidades para campañas más específicas y sofisticadas, están enfocándose en atacar a usuarios específicos con el objetivo de dejar al descubierto vulnerabilidades en aplicaciones, programas y sistemas que les ofrezcan una ruta directa a las infraestructuras. Por ejemplo, los kits de aprovechamiento de vulnerabilidades “LightsOut” o “Hello” están destinados específicamente a la industria de la energía.

Publicidad maliciosa: un factor que altera la economía en Internet

Actualmente, el gasto en publicidad por Internet deja atrás a todas las demás formas de medios de comunicación.[28] Si consideramos los humildes orígenes de la publicidad en Internet (un simple anuncio con banners de Hotwired en 1994) estamos ante una escalada bastante impresionante en dos décadas. La publicidad en Internet, que puede ser molesta para los usuarios, es importante porque permite que las personas consuman libremente la amplia mayoría de la red. Si ese modelo cambiara o si la gente dejara de confiar en la publicidad en Internet, las repercusiones para la red serían monumentales.

La "publicidad maliciosa", publicidad en línea usada para diseminar malware, es una amenaza a ese modelo y a la confianza de los usuarios. Afecta a todos los usuarios de Internet y es un factor que altera la economía de Internet. Según los expertos en seguridad de Cisco, la publicidad maliciosa remarca la sofisticación de la economía de los ciberdelincuentes modernos en términos de división de mano de obra, cooperación y especialización en toda la cadena de ataque.

La publicidad maliciosa se está volviendo más frecuente y los delincuentes pueden lanzar campañas con objetivos muy específicos. Un delincuente dedicado a la publicidad maliciosa que quiere atacar a una población específica en un momento determinado (por ejemplo: fanáticos del fútbol en Alemania mientras miran un juego de la Copa del Mundo) pueden recurrir a un intercambio de anuncios legítimo para cumplir con su objetivo. Al igual que los anunciantes legítimos, se ponen en contacto con compañías que actúan como controladores de los intercambios de anuncios. Pagan la publicidad por adelantado, quizás USD 2000 o más por anuncio y piden a las compañías que les digan a las plataformas de intercambio de anuncios que los entreguen lo más rápidamente posible para que haya muy poco tiempo (o nada) para inspeccionar el contenido del anuncio.

Las víctimas de publicidades maliciosas quedan infectadas con malware mientras navegan normalmente por Internet y, por lo tanto, no tienen idea de dónde o cómo se infectaron. Rastrear el origen es prácticamente imposible, porque el anuncio que descargó el malware ha desaparecido hace mucho tiempo.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Anuncios realmente malos: el rol de la publicidad maliciosa en el Ransomware

Tal como se informó en el ***Informe anual de seguridad 2014 de Cisco***, la publicidad maliciosa fue clave en la distribución del ransomware CryptoLocker. El ransomware (software de rescate) es tan siniestro como lo indica su nombre: es un tipo de malware que cifra archivos o las computadoras de las víctimas hasta que paguen un rescate.[29]

CryptoLocker fue neutralizado recientemente: El Departamento de Justicia de EE. UU. informó en junio que estaba trabajando con agencias de cumplimiento de la ley en otros países y con compañías de tecnología para desmantelar un enorme botnet de dos años de antigüedad conocido como "Gameover Zeus", un principal vehículo de distribución de CryptoLocker.[30] Pero en poco tiempo una nueva marca de ransomware, "CryptoWall", ocupó su lugar.

Durante la primera mitad del año 2014, los investigadores de Cisco examinaron minuciosamente campañas de ataque que usaban la red, específicamente las que usaban publicidad maliciosa para redireccionar a los usuarios a sitios web que alojaban kits de aprovechamiento de vulnerabilidades (alquilados o comprados por el atacante) que colocaban un "dropper" en los sistemas de los usuarios e infectaban a los sistemas vulnerables. Como parte de esa investigación, los expertos en seguridad de Cisco observaron niveles elevados de tráfico consistentes con un nuevo kit de aprovechamiento de vulnerabilidades conocido como "RIG", que fue observado por primera vez en foros especializados en delitos en el mes de abril de 2014.[31] RIG utiliza la publicidad maliciosa para ejecutar un ataque con descarga en paralelo de código malicioso sobre personas que visitan sitios web legítimos de alto perfil. Los delincuentes están usando el kit de herramientas de ataque para distribuir el ransomware CryptoWall.

A principios de junio, Cisco había bloqueado solicitudes a muchos sitios WordPress comprometidos que estaban siendo redireccionadas por publicidad maliciosa.

(Ver Vulnerabilidades de WordPress: ¿quién atiende el negocio?, página 37.)

Las páginas de bienvenida de los sitios alojan métodos de ataque para Java, Flash y el protocolo multimedia Microsoft Silverlight. Según los investigadores de Cisco, el uso del último plug-in para ayudar a iniciar ataques parece estar ganando favoritismo en la comunidad de ciberdelincuentes. Fiesta fue el primer kit de aprovechamiento de vulnerabilidades conocido que incorporó un exploit para Silverlight en el año 2013. RIG y otro kit de aprovechamiento de vulnerabilidades, Angler, pronto siguieron el ejemplo para no perder competitividad en el mercado de kits de aprovechamiento. (Ver Kits de aprovechamiento de vulnerabilidades: el campo se abre a la competencia, página 33.)

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Vulnerabilidades de WordPress: ¿quién atiende el negocio?

Empresas de todas las magnitudes confían en WordPress, el software web que es, esencialmente, una recopilación de scripts y complementos que permite que los usuarios hagan fácilmente todo lo que quieran hacer con sus sitios web: blogs, alojar foros y realizar comercio electrónico, entre otros.

WordPress fue diseñado pensando en la funcionalidad, no en la seguridad.

La mayoría de los usuarios de WordPress carece del conocimiento o de las habilidades que se necesitan para asegurarlo correctamente. Y, con bastante frecuencia, los usuarios que configuran un sitio web con el sistema de administración de contenido (CMS) de WordPress y sistemas similares lo abandonan con el tiempo.

En la red podemos encontrar innumerables sitios como estos, que son un importante eslabón débil en la cadena de seguridad. Los atacantes que se infiltran en estos sitios olvidados pueden cargar códigos binarios maliciosos y usarlos como sitios para la implementación de aprovechamiento de vulnerabilidades. Los usuarios encuentran estos sitios mientras navegan por sitios web activos y legítimos que también han sido infiltrados; un iFrame recoge contenido del sitio abandonado y se lo presenta a usuarios en el sitio legítimo.

WordPress no es el único CMS con este problema, pero se destaca de otros como Joomla y e107 debido a su popularidad. Los sitios web abandonados imponen un alto riesgo sobre la seguridad general de Internet y, como nadie está atendiendo el negocio, limpiar o desmantelar estos sitios no es fácil. Incluso si los propietarios del sitio piensan en tomar alguna medida, la mayoría corrige el punto de ingreso y no verifican si ya están afectados. No encuentran la puerta trasera ni la eliminan de su sitio.

Actualmente, muchos proveedores de alojamiento líderes están ofreciendo servicios de instalación de WordPress administrados y de bajo costo para sitios web comerciales como parte de su paquete de oferta de alojamiento. Los proveedores se aseguran de que se apliquen todos los parches y de que se implementen todos los ajustes de seguridad correctos. En el futuro, a medida que más personas hagan uso de este tipo de servicio, esto ayudará a reducir la cantidad de sitios con vulnerabilidades de WordPress.

Ataques por POS: vector de amenaza popular para delincuentes que buscan datos sobre tarjetas usadas para pagos

Varias tendencias de intersección han convertido a los sistemas POS en una víctima atractiva para los delincuentes que pretenden robar grandes cantidades de datos de tarjetas de crédito y convertirlas rápidamente en dinero. Las recientes infracciones a la seguridad de alto perfil en importantes negocios minoristas señalan el hecho de que estos tipos de ataques pueden llevarse a cabo con éxito y sencillez. Examinar las capacidades de detección antes de un ataque a los datos de tarjetas usadas para pagos es una buena idea desde el punto de vista comercial, junto con reducir los tiempos de corrección durante y después de un ataque.

Los ataques implican el robo de los datos que están presentes en las franjas magnéticas de las tarjetas usadas para pagos. Una vez robados, estos datos se pueden usar para crear tarjetas de crédito falsas que pueden servir para compras fraudulentas en los negocios. El malware por POS permite extraer datos de la memoria, evadiendo así datos cifrados en discos o en la red. Entre las tendencias que están permitiendo ejecutar este exploit en mayor escala se incluyen las siguientes:

Conexión a Internet de los sistemas POS

La mayor probabilidad de que los sistemas POS estén conectados a Internet, lo que brinda a los delincuentes un punto de ingreso a redes corporativas

Falta de consciencia

La falta de consciencia por parte de muchas organizaciones de que la información de tarjetas usadas para pagos debería ser considerada como datos críticos, lo que quiere decir que está menos protegida.

Proveedores externos

El creciente uso por parte de las organizaciones de proveedores externos para todas o algunas de sus soluciones de POS, lo que ofrece más puntos de acceso a los delincuentes.

Los datos presentes en una tarjeta usada para pagos es una mercancía muy valiosa en el mercado de la delincuencia en línea y son muy rentables. Los delincuentes creen que robar datos de sistemas POS es más efectivo que hacerlo directamente de negocios de comercio electrónico; los bancos ahora son más hábiles para detectar y detener este tipo de robo.

Además, como la de Estados Unidos es una de las pocas economías líderes cuyas tarjetas para pagos habitualmente tienen franjas magnéticas (en lugar del sistema de “chip y PIN” más seguro), los datos presentes en la franja magnética son fáciles de convertir en dinero. (Sin embargo, sin cifrado de extremo a extremo de los datos de la tarjeta, se pueden robar los números y las fechas de vencimiento de la tarjeta para usarlos en transacciones en línea, incluso con los sistemas de chip y PIN.)

Monitoreo más crítico de datos de tarjetas usadas para pagos

Para evitar el robo de datos de tarjetas usadas para pagos y otra información confidencial en los sistemas POS, las organizaciones deben invertir más en barreras tecnológicas que impidan el ingreso de los delincuentes. También deben reconocer que los datos presentes en las tarjetas usadas para pagos merecen más atención por parte de los profesionales de seguridad que contratan en sus empresas.

Algunas organizaciones optan por agregar dispositivos de cifrado por hardware en el sistema POS; esto puede ayudar a evitar la intercepción de los datos de las tarjetas usadas para pagos en su paso de una red a otra. Si esto es considerado un gasto excesivo, al menos las organizaciones deberían marcar estos datos como "críticos" y monitorearlos para detectar cualquier acceso no autorizado y movimientos irregulares en los datos. Hay demasiadas maneras de comprometer inicialmente una red y las organizaciones generalmente deberían asumir que los atacantes ya saben cómo ingresar a una red.

Los IOC más lógicos que evidenciarían un posible robo de datos presentes en tarjetas usadas para pagos son los siguientes: importación de un conjunto de herramientas, un proceso nuevo que se ejecuta en un terminal de POS y la exfiltración de archivos comprimidos con tamaño y frecuencia uniformes. Se debería considerar a los sistemas que pueden analizar estas conductas en toda la red extendida.

También es recomendable realizar una detección de cambios en aplicaciones y procesos en todos los sistemas de procesamiento de tarjetas usadas para pagos. Cualquier cambio en un terminal debería ser causa para un análisis inmediato. Además, aunque la mayoría de los protocolos tienden a usar la compresión por motivos de eficiencia y velocidad, las herramientas de compresión en sí mismas deberían ser parte de la "lista blanca de aplicaciones" de una organización.

Finalmente, las redes se deberían segmentar para que las empresas no faciliten el acceso de los criminales a tesoros escondidos de datos: los sistemas POS deberían estar en un segmento de la red separado de la red empresarial para limitar el acceso y rechazar ataques a los sistemas POS.

Con el aumento exponencial en la cantidad de dispositivos móviles y su proliferación en las redes empresariales, la segmentación debería incluir fuertes capacidades de identificación que puedan detectar de qué usuario se trata, el tipo de dispositivo que está utilizando el usuario para acceder a la red y el método por el cual se está accediendo a la red. Por ejemplo: se podría permitir el acceso a través de una computadora portátil privada en la LAN inalámbrica del campus de la empresa, pero se podría denegar el acceso usando una tablet a través de una VPN de acceso remoto debido a la sensibilidad de los datos del sistema POS.

Cisco anticipa que los atacantes que buscan datos de tarjetas usadas para pagos sigan enfocando sus esfuerzos en los sistemas POS. Sin embargo, contar con detallados sistemas de detección y alerta, además de la implementación de cifrado por hardware, puede ayudar a prevenir la ejecución de dichos ataques.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Ingeniería social: encontrar eslabones débiles en la persona

Una empresa puede pagar cientos de miles de dólares, o más, por el software de seguridad más reciente y pensar que está protegida de ataques a objetivos específicos que ingresan a través de la red. Pero si la amenaza es una persona real que ingresa por la puerta principal de una oficina o de una torre de servidores, ¿qué puede hacer el software del perímetro de la red?

Los delincuentes inteligentes tienen más beneficios si se presentan in situ para conectarse físicamente a una red en lugar de elaborar mensajes de correo electrónico de suplantación de identidad con enlaces que llevan a sitios web comprometidos. (No estamos diciendo que el spam y otras campañas de ingeniería social en línea hayan desaparecido; ver la página 26 para leer más.) El solo hecho de poder conectarse a una conexión Ethernet o desconectar un teléfono IP y usar ese cable para acceder a información de a red puede tener graves consecuencias. La ingeniería social es el acto de atacar las vulnerabilidades de las personas. En consecuencia, la gente (sus empleados) se convierte en el eslabón más débil de su postura de seguridad, tanto física como digital.

Los delincuentes usan tácticas similares para diseñar la ingeniería social de una visita en persona de la misma manera que en el caso de mensajes de correo electrónico y sitios web comprometidos. El objetivo es generar confianza (aunque no retribuida) en una persona que pueda otorgarles acceso a las instalaciones de la compañía.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

Si investiga a un empleado específico en LinkedIn (por ejemplo: averiguar todo, desde sus tareas laborales hasta la universidad en la que estudió y los equipos deportivos con los que simpatiza), el delincuente puede presentarse como una persona que la víctima podría conocer o tener motivos para confiar en ella.

Gracias a la popularidad de las redes sociales, especialmente entre profesionales, hay gran cantidad de información y fotos a la vista de cualquiera que necesite poner literalmente un pie en la puerta.

Equipado con información recopilada en búsquedas en línea, un delincuente puede simular ser un periodista y solicitar una entrevista o asegurar ser un posible socio o cliente y pedir una visita en persona. El delincuente también podría llevar una insignia falsa para dar la impresión de autoridad.

Los delincuentes también han descubierto que no necesitan iniciar semejantes engaños en la puerta principal de la organización que pretenden atacar. En cambio, se enfocarán en un eslabón más débil; es decir, un socio comercial o proveedor menos seguro que tenga acceso o conectividad con su objetivo real: la red. Esta es una técnica especialmente efectiva que se usa cuando la seguridad de un objetivo es elevada, pero la de un socio comercial de confianza del objetivo no lo es. Los piratas informáticos siempre tratan de encontrar la forma más fácil de ingresar.

Un enfoque para mitigar las infracciones a la seguridad basadas en la ingeniería social que implica obtener acceso físico a la red es asegurarse de que en los puertos de acceso a la red se hagan cumplir los procesos de autenticación y autorización antes de otorgar acceso a la red. Además, las organizaciones pueden crear “dominios de seguridad dinámicos” por usuario, por dispositivo, por usuario y dispositivo, o con cualquier otra configuración necesaria. Estos dominios de seguridad dinámicos pueden usar tecnología como 802.1x, listas de control de acceso (ACL) a puertos, VPN y evaluación de posturas de hosts.

Solución

Independientemente del método de acceso que emplee un atacante (red cableada, inalámbrica o VPN), los profesionales de seguridad pueden crear dinámicamente un dominio (o “burbuja”) de seguridad hecho especialmente para él. Si un delincuente conecta una computadora portátil a un puerto in situ, la red detendrá a la persona, la autenticará, elaborará su perfil, evaluará su postura, observará su comportamiento y, luego, proporcionará al usuario derechos de autorización muy específicos y dinámicos que le restringen el acceso a la red en función de una política contextual.

Una mirada hacia adelante

Los expertos de Cisco especializados en seguridad ofrecen su opinión sobre la manera en la que las empresas pueden mejorar la seguridad considerándola como un proceso comercial, aumentando el diálogo entre los líderes comerciales y tecnológicos en la organización y usando soluciones de tecnología emergentes que proporcionan más visibilidad de las amenazas cada vez más difíciles de detectar.

Ciberseguridad inteligente para el mundo real

Fortalecer los eslabones débiles en toda la cadena de seguridad depende en gran medida de la capacidad que tengan las organizaciones individuales y la industria para crear consciencia sobre el riesgo cibernético a nivel de las juntas directivas y de convertir a la ciberseguridad en un factor imperioso para el negocio. Alinear la estrategia comercial, las operaciones de seguridad y los controles que posibilitan la capacidad de recuperación cibernética también es fundamental porque es la cualidad para crear visibilidad de red en toda una red "ruidosa" empleando soluciones emergentes e inteligentes como el análisis predictivo.

Para cubrir toda la continuidad de un ataque (antes, durante y después del mismo) las organizaciones deben ocuparse de una amplia gama de vectores de ataque con soluciones de seguridad que funcionan en todo lugar donde se pueda manifestar una amenaza. Esto incluye la red, los dispositivos móviles, los entornos virtuales y en la nube o el centro de datos.

Reducir las brechas de seguridad (independientemente de que sean vulnerabilidades conocidas y aprovechadas activamente en Java, Flash o Adobe PDF, sitios web abandonados creados en WordPress, fallas de seguridad ignoradas desde hace tiempo en el software OpenSSL, acceso físico no protegido a redes o servidores NTP vulnerables) y la complejidad causada por productos dispares y soluciones inconexas. Para asegurarse de que la red tenga la flexibilidad necesaria para admitir el negocio, también es fundamental evaluar el estado del ciclo de vida de los dispositivos de red detectados, las posibles vulnerabilidades de seguridad y la administración de versiones del sistema operativo.[32]

La estrategia de Cisco para ayudar a las organizaciones a hacer frente a estos desafíos de seguridad conocidos y emergentes se basa en tres aspectos clave estratégicos:

Visibilidad como prioridad máxima

Cuanto más podamos ver, estaremos en mejores condiciones para correlacionar información y aplicar inteligencia para comprender el contexto, tomar mejores decisiones y tomar medidas, ya sea manual o automáticamente.

Enfoque en las amenazas

Debemos enfocarnos en detectar, comprender y detener amenazas mediante un análisis continuo e inteligencia de seguridad en tiempo real que se proporciona desde la nube y se distribuye entre todas las soluciones de seguridad para mejorar la eficacia.

Con base en plataformas

Ahora la seguridad es más un problema de red. Requiere un sistema integrado de plataformas ágiles y abiertas que cubran los dispositivos de red, y la nube.

La ciberseguridad inteligente para el mundo real nos ayudará a posibilitar una Internet de las cosas segura y a formar la base de una Internet de todo en la que la seguridad, al igual que la informática, será potente y ubicua, además de perfecta para los usuarios finales.

cómo hacer para que la seguridad sea operativa: convertir a la seguridad en un proceso comercial

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

A menudo, las evaluaciones de seguridad revelan que la causa raíz de un problema es una falla operativa responsabilidad de la empresa y una falla técnica. Carencia de madurez operativa o de capacidad operativa (o ambas) que deriva en controles de seguridad débiles o inexistentes.

A medida que la ciberseguridad pasa a ser más un riesgo estratégico para las empresas de la actualidad, cada vez es más importante alcanzar la "madurez en operaciones de seguridad", punto en el que la organización tiene una visión holística de los riesgos de ciberseguridad y mejora continuamente las prácticas de ciberseguridad.

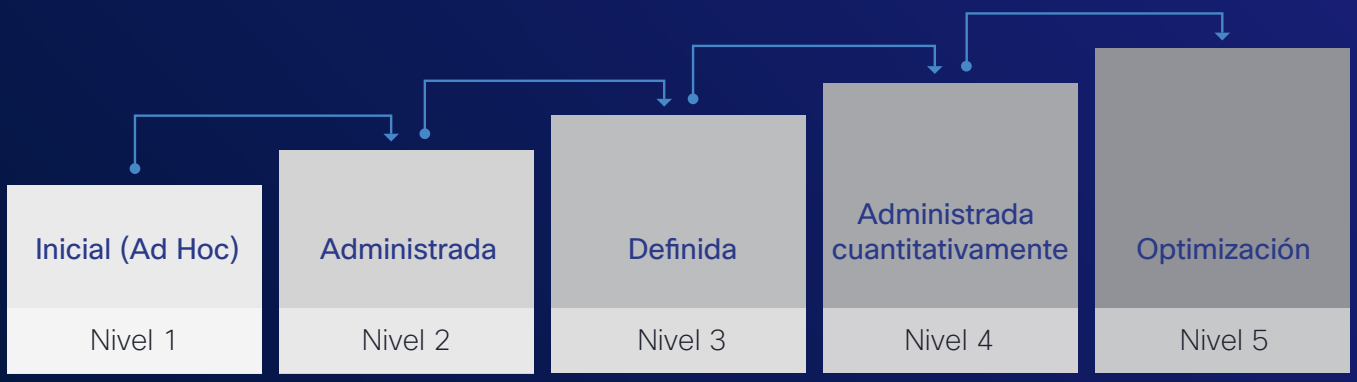
Con la ayuda de los proveedores de servicios que trabajan en este ámbito, muchas organizaciones están trabajando en pos de convertir a la seguridad en un proceso (o conjunto de procesos) altamente estandarizado y con diversidad de mediciones, que es revisado periódicamente para asegurarse de que se estén cumpliendo los objetivos estratégicos. La decisión de ver a la seguridad como un proceso comercial a menudo surge de iniciativas comerciales más extensas diseñadas para mejorar el control, el riesgo y el cumplimiento (GRC) en toda la organización. Muchas empresas descubren, a menudo demasiado tarde, que, en todo lo referido a seguridad de TI, el cumplimiento no basta.

Las organizaciones que convierten a la seguridad en un proceso operativo pueden entender mejor:

1. Lo que necesitan proteger
2. El buen (o mal) funcionamiento de sus medidas de seguridad actuales
3. Lo que necesitan lograr en términos de ciberseguridad

FIGURA 17

Modelo CMMI



Convertir a la seguridad en un proceso operativo deriva en una mejor visibilidad de lo que está sucediendo con la seguridad de TI en toda la organización: qué empleados son sus responsables, si son las personas correctas para ocuparse de esa responsabilidad y, de ser así, si están haciendo bien su trabajo. Las empresas que convierten a la seguridad en un proceso operativo pueden determinar si se están desplegando y usando efectivamente los recursos de TI.

Un componente fundamental para convertir a la seguridad en un proceso operativo es un diálogo productivo entre los líderes de seguridad, como los directores de información (CIO), los directores de seguridad de la información (CISO) y los líderes comerciales. Para convertir a la ciberseguridad en un proceso comercial formal es preciso que estos dos grupos de liderazgo trabajen más estrecha y frecuentemente para definir niveles de riesgo aceptables y para delinear objetivos estratégicos en torno a la seguridad para la organización. A fin de impulsar este diálogo, los CISO deben encontrar maneras de presentar información de ciberseguridad en términos que los líderes comerciales puedan comprender claramente; las cifras, por ejemplo, pueden ayudar a traducir el valor de los pasos que da la empresa para evitar un riesgo de ciberseguridad en particular.

Convertir a la seguridad en un proceso operativo también implica seguir un “modelo de madurez”. La Integración del modelo de madurez de capacidades (CMMI) de Carnegie Mellon es un ejemplo. Este modelo ampliamente usado comenzó como un proyecto en el Instituto de Ingeniería de Software de la universidad en la década de 1980. Tal como se ilustra en la Figura 17, el punto de inicio del modelo de madurez es la frase “ad hoc”, que esencialmente es un modo “para combatir incendios”. Cuando una organización alcanza la última fase, está usando procesos estandarizados y posibles de repetir y medir.

Comprender el riesgo cibernético en términos comerciales

Muchas compañías están apostando el futuro de sus modelos comerciales basándose en la conectividad ubicua que promete el mundo de Internet de las cosas. Pero para prepararse y tener éxito a largo plazo en este entorno de rápida emergencia, la cúpula ejecutiva debe comprender, en términos comerciales, los riesgos cibernéticos asociados con desarrollar dependencia en la red.

No analizar problemas de ciberseguridad en público ha sido desde hace mucho tiempo el status quo para muchas organizaciones, pero todo está cambiando. Cada vez más líderes comerciales comienzan a entender que los riesgos de ciberseguridad son desafíos comunes para todas las organizaciones, especialmente a medida que las empresas se vuelven más digitalizadas y los activos de información se convierten cada vez más en activos estratégicos.

Estos ejecutivos también están empezando a reconocer que en un mundo de Internet de las cosas, es necesario tener un diálogo honesto acerca de las amenazas y las mejores prácticas para mitigarlas en la empresa, entre empresas (incluidos los competidores) y entre los sectores público y privado. La creciente presión que ejercen los directorios, que buscan comprender los posibles efectos comerciales de los riesgos de ciberseguridad, está ayudando a elevar este punto de vista al nivel de las cúpulas directivas.

Las medidas recientes tomadas por la Comisión de Valores y Bolsa (Securities and Exchange Commission, SEC) de EE. UU. han ayudado a que la ciberseguridad se convierta en un tema prioritario para los directorios. La SEC publicó requisitos para informes de ciberseguridad para compañías que cotizan en bolsa en el año 2011,[33] de estos requisitos exigen que estas compañías informen a sus accionistas sobre "instancias significativas de robos o ataques cibernéticos o, incluso, ante situaciones en la que existe un riesgo material de dicho suceso".[34] La SEC también organizó una mesa redonda sobre ciberseguridad este año "para debatir la ciberseguridad y los problemas y desafíos que presenta para los participantes del mercado y las compañías que cotizan en bolsa, y cómo están abordando estas inquietudes".[35]

En el marco global, el Foro Económico Mundial (World Economic Forum, WEF), una institución internacional comprometida con la mejora del estado del mundo a través de la cooperación entre los sectores público y privado, ha presentado su concepto de "capacidad de recuperación cibernética" en el año 2011 como un modo de elevar problemas de ciberseguridad y de otro tipo al nivel de temas de directorio. El WEF promueve la capacidad de recuperación cibernética como un ecosistema interdependiente en el que la organización más fuerte lo es tanto como el eslabón más débil de la cadena de seguridad. Esto se delinea en uno de los cuatro principios orientadores de la iniciativa "Asociarse para la capacidad de recuperación cibernética"[36] del WEF:

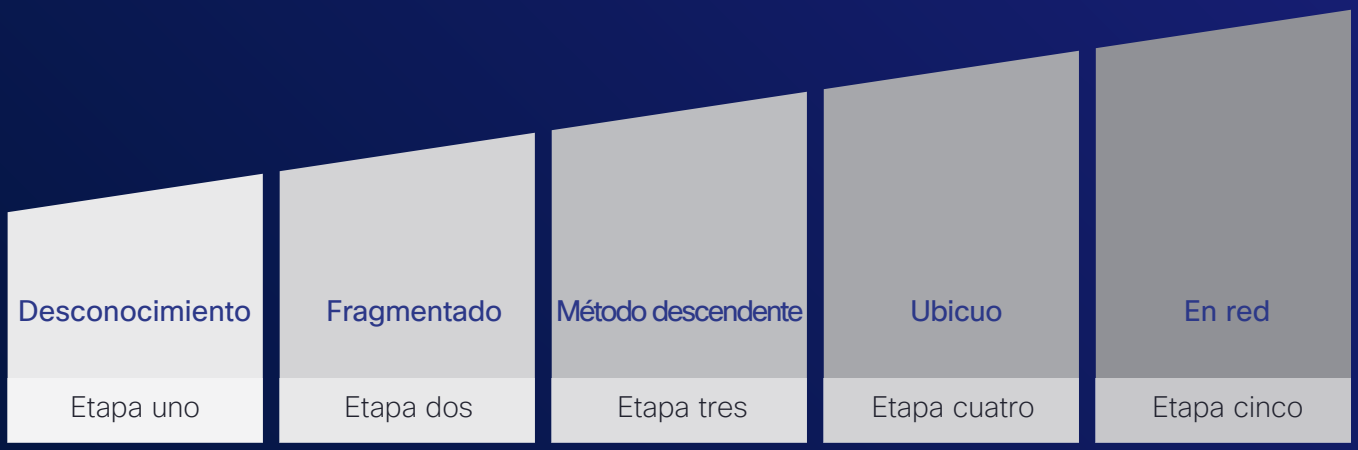
Todos somos tan fuertes como el eslabón más débil de las cadenas de las que dependemos; cada uno aporta a la seguridad de nuestro mundo hiperconectado. Un espacio en línea abierto, seguro y con capacidad de recuperación es un bien público; todos los actores comparten la responsabilidad de crear y apoyar este recurso.

COMPARTIR EL INFORME SEMESTRAL DE SEGURIDAD 2014 DE CISCO

La iniciativa de capacidad de recuperación cibernética del WEF está diseñada para ayudar a los directores ejecutivos y a otros líderes de las cúpulas directivas (incluidos los CIO y los CISO) a impulsar el debate sobre la ciberseguridad en sus organizaciones y a hablar en términos comerciales sobre los riesgos cibernéticos y las oportunidades. Por ejemplo: "¿Qué costo afrontará la empresa si decidimos no invertir en una tecnología que produzca valor debido a inquietudes relacionadas con el riesgo cibernético?"

FIGURA 18

Modelo de madurez para la capacidad de recuperación cibernética en la organización



Según el WEF, para alcanzar la capacidad de recuperación cibernética es necesario que las organizaciones adopten un enfoque basado en riesgos con respecto a la ciberseguridad, un enfoque válido para cualquier empresa que pretenda mejorar su ciberseguridad. La institución ofrece este modelo de madurez, que ilustra un camino para llegar a la capacidad de recuperación cibernética.

A través de esta iniciativa de capacidad de recuperación cibernética, el WEF enfatiza que la ciberseguridad no es algo que pueda lograr un único departamento de una organización, más específicamente, TI. Esto se debe a que las capacidades de ciberseguridad no son solo técnicas sino también institucionales. Además, el WEF destaca que promover la consciencia sobre ciberseguridad en la organización es, en gran medida, responsabilidad del director ejecutivo, quien, además, es el máximo responsable de ayudar a que la empresa logre la capacidad de recuperación cibernética necesaria.

Análisis predictivo: un detective que permite mejorar la seguridad

Es un círculo vicioso: la industria de la seguridad desarrolla una respuesta específica para una amenaza de ciberseguridad en particular y los atacantes encuentran una nueva manera de evitar ser detectados. Los atacantes están trabajando anticipadamente para saber qué tipo de soluciones de seguridad se están desplegando y están optando por patrones de comportamientos menos visibles y con menor capacidad de detección por contenido para ocultar bien sus amenazas. Ahora, hay menos "manzanas podridas evidentes" para que las detecten las soluciones y los profesionales de seguridad; en su lugar, hay más tráfico cifrado, más confusión y más aleatorización de parte de los actores maliciosos para que sus comportamiento de comando y control pasen desapercibidos entre el tráfico real.

La poca visibilidad que tienen las organizaciones de las redes "ruidosas" de la actualidad significa que las amenazas omnipresentes tengan muchos lugares donde ocultarse. Para atravesar ese ruido y saber si está sucediendo algo anómalo en una red es necesario conocer el aspecto real de lo "normal". El análisis predictivo es una capacidad de detección emergente que proporciona este tipo de información y ayuda a que las organizaciones aumenten la flexibilidad de sus soluciones de seguridad. Es una herramienta para detectar comportamientos inusuales en una red (los síntomas de una infección) a través de análisis de comportamientos y detección de anomalías.

Mediante el uso del análisis predictivo, las organizaciones pueden evaluar el comportamiento de las entidades (servidores host y usuarios) en la red. Se crea y usa un modelo, derivado de muchos modelos más pequeños y una representación concisa de comportamiento pasado, para predecir cómo se deberían comportar las entidades en el futuro. En condiciones ideales, los datos se correlacionan en la nube para mejorar la velocidad, la agilidad y la profundidad de la detección de amenazas. Si hay alguna discrepancia con respecto al comportamiento esperado que sea significativa o se sostenga en el tiempo, se la marca para su investigación.

El análisis predictivo ayuda a aumentar la exactitud de las técnicas de seguridad existentes, además de incrementar su capacidad de detectar comportamientos desconocidos o inusuales en la red. Implica algoritmos avanzados para la toma de decisiones que analizan varios parámetros e incorporan datos de tráfico en vivo; las capacidades de aprendizaje de máquina permiten que el sistema aprenda y se adapte en función de lo que ve.

Los sistemas de aprendizaje de máquina son como detectives. Buscan en los lugares donde podría haber peligros y evidencias de que se ha registrado un incidente, de que está por suceder o de que podría ser inminente. Y, pese a que no necesariamente manejan la seguridad o el cumplimiento de políticas, otorgan las herramientas necesarias a otros sistemas para encontrar amenazas inesperadas y tomar medidas de corrección. A fin de proporcionar valor y ayudar a la organizaciones a elevar su eficacia en seguridad, el análisis predictivo se debe desplegar junto con soluciones de seguridad basadas en el contenido, soluciones de administración perimetral y soluciones de administración de políticas.

Acerca de Cisco

Cisco ofrece ciberseguridad inteligente para el mundo real. La visión se basa en un enfoque hacia la seguridad centrado en las amenazas que reduce la complejidad, al tiempo que proporciona más visibilidad, control continuo y protección contra amenazas avanzadas en toda la continuidad del ataque. Con este modelo de seguridad centrado en las amenazas, las organizaciones pueden actuar rápidamente antes, durante y después de un ataque.

Los investigadores especializados en amenazas del ecosistema de Inteligencia en seguridad colectiva de Cisco aportan profundos conocimientos y sofisticados sistemas de datos masivos a la detección, el análisis y la protección contra amenazas, tanto conocidas como emergentes. Los reconocidos expertos en seguridad de Cisco están respaldados por infraestructura y sistemas sofisticados que proporcionan un nivel inigualable de visibilidad a partir de la suma total de datos y el análisis de la incomparable telemetría Cisco de miles de millones de solicitudes y mensajes de correo electrónico, millones de muestras de malware, conjuntos de datos de código abierto y miles de intrusiones a redes.

El resultado es “inteligencia masiva”: inteligencia que ofrece mayor efectividad en seguridad y que protege inmediata y ubicuamente redes extendidas por todo el mundo.

Para más información sobre el enfoque centrado en amenazas de Cisco, visite www.cisco.com/go/security.

Notas

1 *Estimación del costo de la ciberdelincuencia y el ciberespionaje*, Centro de Estudios Estratégicos e Internacionales (CSIS), Julio de 2013: https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage.

2 "Internet de las cosas", Cisco.com: http://www.cisco.com/web/solutions/trends/iot/overview.html.

3 Infografía "Internet de las cosas", Grupo de soluciones comerciales para Internet de Cisco: http://share.cisco.com/internet-of-things.html.

4 "Hackers Reveal Nasty New Car Attacks–With Me Behind The Wheel" ("Piratas informáticos demuestran nuevos ataques muy peligrosos a automóviles: conmigo detrás del volante"), por Andy Greenberg, *Forbes*, 12 de agosto de 2013: http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

5 "Hackers Reportedly Targeted Three Large Medical Device Makers" ("Se informa que piratas informáticos atacan a tres grandes fabricantes de dispositivos médicos"), iHealthBeat.com, 11 de febrero de 2014: www.ihealthbeat.org/articles/2014/2/11/hackers-reportedly-targeted-three-large-medical-device-makers.

6 "¿Qué tan seguro es su monitor para bebés? What can happen when the 'Internet of Things' gets hacked" ("¿Qué puede suceder cuando un pirata ataca 'Internet de las cosas'"), por Matt Hartley, *Financial Post,* 3 de mayo de 2014: http://business.financialpost.com/2014/05/03/how-secure-is-your-baby-monitor-what-can-happen-when-the-internet-of-things-gets-hacked/?__lsa=bc1b-f93e.

7 "The Internet of Everything, Including Malware" ("Internet de las cosas, incluido el malware"), por Craig Williams, blog de seguridad de Cisco, 4 de diciembre de 2014: http://blogs.cisco.com/security/the-internet-of-everything-including-malware/.

8 El punto central de este informe es destacar la cantidad de solicitudes para FQDN, dominios, sitios y otros elementos potencialmente maliciosos que están generándose desde el cliente.

9 *Informe anual de seguridad 2014 de Cisco:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

10 Los clientes que estén interesados en compartir inteligencia directa con el programa AEGIS en el Equipo de Investigación de Vulnerabilidades deben escribir a threatintel@cisco.com.

11 Ibídem.

12 Para más información sobre Heartbleed, visite www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.

13 "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations" ("Vulnerabilidad Heartbleed en OpenSSL CVE-2014-0160 – Productos y soluciones de mitigación Cisco"), por Pano Kampanakis, blog de seguridad de Cisco, 9 de abril de 2014: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations.

14 Para más información sobre la mitigación de la vulnerabilidad Heartbleed en OpenSSL, consulte "Cisco Event Response: OpenSSL Heartbleed Vulnerability CVE-2014-0160" ("Respuesta de Cisco ante eventos: vulnerabilidad Heartbleed en OpenSSL CVE-2014-0160"), 22 de abril de 2014, Cisco.com: www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html.

15 "New OpenSSL Defects – Another Heartbleed? Tor Stripped?" ("Nuevos defectos en OpenSSL – ¿Otro Heartbleed? ¿Tor vulnerado?"), por James Lyne, *Forbes*, 5 de junio de 2013: www.forbes.com/sites/jameslyne/2014/06/05/new-openssl-defects-another-heartbleed.

16 "Severe OpenSSL Security Bug Uncovered by Japanese Researcher Months After Heartbleed" ("Grave problema de seguridad en OpenSSL descubierto por investigador japonés meses después de Heartbleed,"), por Luke Villapaz, *International Business Times*, 5 de junio de 2014: www.ibtimes.com/severe-openssl-security-bug-uncovered-japanese-researcher-months-after-heartbleed-1594989.

17 *Informe anual de seguridad 2014 de Cisco:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

18 Ibídem.

19 "Spam Hits Three Year High-Water Mark" ("Spam alcanza su punto máximo en tres años"), blog de seguridad de Cisco, 2 de mayo de 2014: http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark.

20 "Major Apple security flaw: Patch issued, users open to MITM attacks" ("Importante falla de seguridad en Apple: corrección publicada, usuarios expuestos a ataques de MITM"), por Violet Blue, blog "Zero Day" ("Día Cero"), *ZDNet*, 22 de febrero de 2014: http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/.

21 "Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects" ("Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware y la Fundación Linux forman nueva iniciativa para apoyar proyectos críticos de código abierto"), comunicado de prensa, Fundación Linux, 24 de abril de 2014. Para más información sobre la Iniciativa, visite http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel.

22 *Informe anual de seguridad 2014 de Cisco:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

23 "When Network Clocks Attack" ("Cuando atacan los relojes de la red"), por Jaeson Schultz, blog de seguridad de Cisco, 10 de enero de 2014: http://blogs.cisco.com/security/when-network-clocks-attack/.

24 "Chronology of a DDoS: Spamhaus" ("Cronología de una DDoS: Spamhaus"), por Seth Hanford, blog de seguridad de Cisco, 28 de marzo de 2013: http://blogs.cisco.com/security/chronology-of-a-ddos-spamhaus/.

25 Si quiere saber si su servidor NTP es vulnerable, visite openntpproject.org. Para más información sobre las mejores prácticas de DNS, consulte "DNS Best Practices, Network Protections, and Attack Identification" ("Mejores prácticas de DNS, protecciones de red e identificación de ataques"): http://www.cisco.com/web/about/security/intelligence/.

26 Proyecto Open Resolver: www.openresolverproject.org.

27 "Meet Paunch: The Accused Author of the Blackhole Exploit Kit" ("Le presentamos a Paunch: el supuesto autor del kit de aprovechamiento de vulnerabilidades Blackhole"), por Brian Krebs, blog KrebsOnSecurity, 6 de diciembre de 2013: http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.

28 "Global Internet Ad Spend Sees Double-Digit Growth, Outpaces Other Media" ("El gasto mundial en anuncios de Internet aumenta con porcentajes de dos dígitos y supera a los demás medios de comunicación"), *Nielsen,* 10 de julio de 2012: http://www.nielsen.com/us/en/newswire/2012/global-internet-ad-spend-sees-double-digit-growth-outpaces-other-media.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+(Nielsen+Wire).

29 *Informe anual de seguridad 2014 de Cisco:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

30 "Malicious Advertisements on Major Websites Lead to Ransomware" ("Publicidades maliciosas en importantes sitios web derivan en Ransomware"), por Jeremy Kirk, Servicio de noticias de IDG, 6 de junio de 2014: http://www.pcworld.com/article/2360820/malicious-advertisements-on-major-websites-lead-to-ransomware.html.

31 "RIG Exploit Kit Strikes Oil" ("El kit de aprovechamiento de vulnerabilidades RIG golpea a la industria del petróleo"), por Andrew Tsonchev, blog de seguridad de Cisco, 5 de junio de 2014: http://blogs.cisco.com/security/rig-exploit-kit-strikes-oil/.

32 Informe Network Barometer: evaluación de la preparación de las redes globales para apoyar los negocios, *Dimension Data,* 2013: http://www.dimensiondata.com/Global/Documents/Network%20Barometer%20Report%202013.pdf.

33 "CF Disclosure Guidance: Topic No. 2: Cybersecurity" ("Pautas sobre obligaciones de divulgación propuestas por la División de Finanzas de Corporaciones: Tema N.° 2: Ciberseguridad"), División de Finanzas de Corporaciones, SEC, 13 de octubre de 2011: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

34 "Cybersecurity: SEC outlines requirement that companies report data breaches" ("Ciberseguridad: la SEC delinea un requisito que obliga a las compañías a informar infracciones a la seguridad de los datos"), por Ellen Nakashima y David S. Hilzenrath, *The Washington Post,* 14 de octubre de 2011: http://www.washingtonpost.com/world/national-security/cybersecurity-sec-outlines-requirement-that-companies-report-data-breaches/2011/10/14/gIQArGjskL_story.html.

35 "Cybersecurity Roundtable" ("Mesa redonda sobre ciberseguridad"), SEC: http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

36 Para más información sobre la iniciativa Asociarse para la capacidad de recuperación cibernética del WEF, vaya a http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience.

CISCO