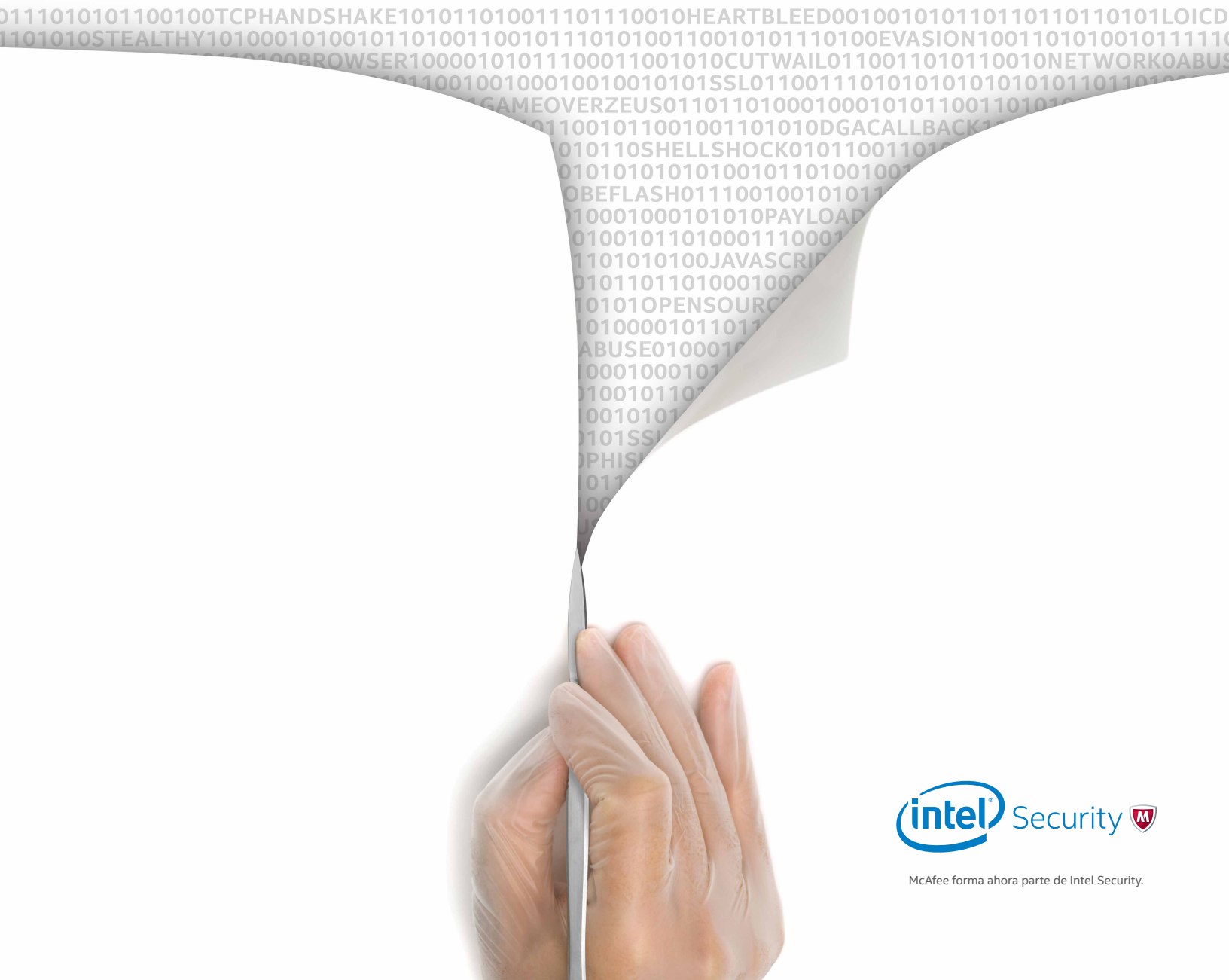
Informe

Análisis de los cinco principales métodos de ataque contra la red: El punto de vista del ladrón



intel Security

McAfee forma ahora parte de Intel Security.

Ha llegado la hora de que sepa a qué (y a quién) se enfrenta

Según nuestros análisis, las fugas de datos (y los problemas que acarrean) son cada vez más generalizadas, y no muestran el más mínimo signo de remitir. Las amenazas a las que se enfrenta en la actualidad son obra de delincuentes experimentados, que se valen de técnicas avanzadas para atacar con precisión brechas en la red cuya existencia posiblemente desconoce. Si bien la situación es grave, con algunos cambios inteligentes en la red y una dosis adecuada de "conocimiento del enemigo", el pronóstico es bastante favorable.

La información es poder

Este informe incluye un análisis en profundidad de los cinco métodos de ataque contra la red más comunes empleados por los ladrones de datos. Asimismo proporciona una guía práctica sobre cómo ven los delincuentes su red y cómo utilizar esa información para mantener un perfil de seguridad dinámico, junto a formas de minimizar la probabilidad de una fuga y sus devastadoras consecuencias.

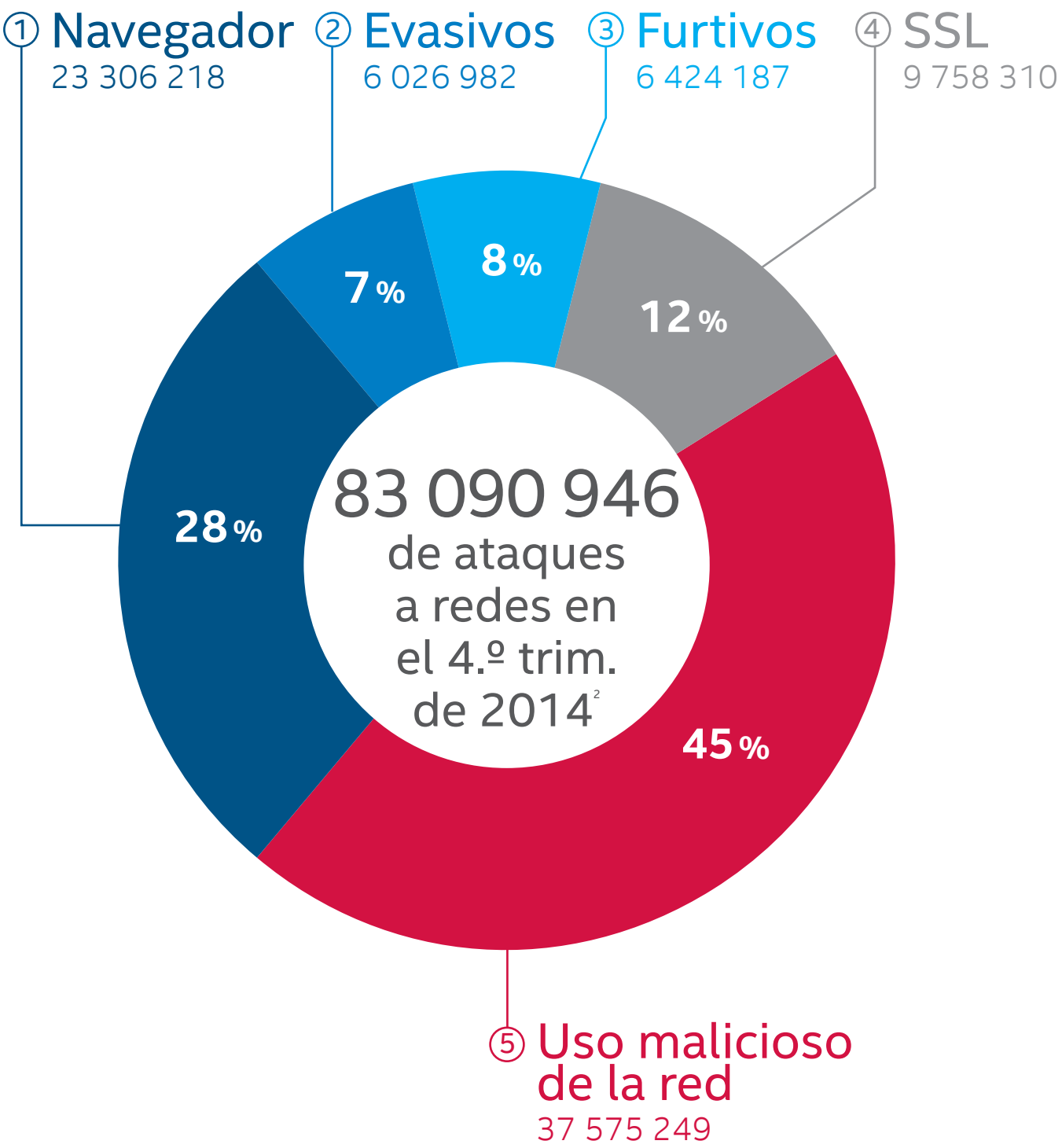
Grandes cifras que no cuadran

76 % de los asistentes a la conferencia Back Hat consideran que el malware avanzado es un problema grave o muy grave[1].

Asistentes que dedican 10 horas o más a la semana a luchar contra las amenazas[1]. **37 %**

Principales ataques a la red

Solamente en el 4.º trimestre de 2014 se produjeron más de 83 millones de ataques a redes[2].



1 Ataques al navegador

Usted ve un navegador, ellos una puerta

Los ladrones saben que cuando sus empleados utilizan la Web, las decisiones sobre seguridad se alejan del departamento de TI. Por esa razón, utilizan una gran cantidad de mensajes de phishing, ataques de ingeniería social y descargas desapercibidas a través del navegador con el fin de engañar a los empleados con menos conocimientos técnicos y conseguir que divulguen datos. Es cuestión de probabilidad; si se sigue intentando, tarde o temprano, alguien termina cayendo.

Por lo tanto, en lugar de adquirir nuevas soluciones complementarias, más estáticas, es mejor elegir una solución de seguridad dinámica. Una solución que crezca a medida que cambian sus necesidades de seguridad, y que sea capaz de fortalecerse a medida que descubre qué debe protegerse y por qué.

Crecimiento del 87 %

El número URL sospechosas se disparó entre 2013 y 2014[3].

82 millones

de nuevas URL sospechosas detectadas en 2014[3].

El punto de vista del ladrón

"Sea cual sea el nuevo producto de seguridad, siempre consigo pasar. No es tanto una cuestión de tecnología, como de los usuarios; es muy fácil engañarlos."

Perfil de hacker:
Astuto

Método de ataque:
Navegador

Competencias:
JavaScript, Flash e ingeniería social

Motivación:
Crear ejércitos de robots

Las señas de identidad de un ataque al navegador

- **Cuanto menos sepa, mejor**
  Los hackers saben que los internautas de su empresa (a diferencia de los profesionales de seguridad) entran en contacto directo con contenido web malicioso.
- **El malware está bien oculto**
  Los navegadores copian en caché archivos y otro tipo de contenido de manera desapercibida para el usuario con el fin de mejorar su experiencia, lo que significa que el malware casi nunca resulta obvio para los más inexpertos.
- **Se aprovecha la ignorancia**
  Los agresores aprovechan esta realidad para transferir cargas útiles maliciosas y ejecutar secuencias de comandos de malware de manera encubierta.

Salve a sus empleados de ellos mismos

- **Minimice las decisiones equivocadas**
  Empiece por filtrar el contenido web y las URL. De esta forma, protege a los usuarios de los rincones oscuros de la Web y, además, es más fácil sentar la norma.
- **Profundice en el análisis**
  Adelántese a las últimas amenazas identificando el malware que se oculta en el contenido más sofisticado del navegador, como JavaScript y Adobe Flash.
- **Descubra las intenciones**
  Para disponer de la máxima protección, utilice los entornos de navegador simulados, denominados de emulación. Gracias a estas tecnologías descubrirá de manera inmediata la intención de los archivos entrantes.
- **Adopte una visión integral**
  Reduzca al mínimo el gasto en medidas reactivas. Garantice su seguridad en el futuro mediante la adopción de una solución de próxima generación que crece a la par que sus necesidades.

2 Ataques evasivos

Si existe un fallo, los ciberdelincuentes lo encontrarán

Las soluciones de seguridad son más sofisticadas e inteligentes que nunca. Pero, por desgracia, los ciberdelincuentes también. Los ingeniosos ladrones emplean técnicas de evasión que desafían más que nunca la seguridad de la red, aprovechando el más mínimo fallo en cada nivel de la infraestructura.

Gracias a sus técnicas evasivas, los ciberdelincuentes despistan a los dispositivos de red, eluden las inspecciones o encubren su presencia. Los ladrones de datos están ávidos de innovaciones sobre técnicas de evasión y saben que la mejor forma de vencer a los sistemas de seguridad es no oponer resistencia.

El **22 %** de los CIO y responsables de seguridad admiten que sus redes han sufrido ataques en los últimos 12 meses.

El **40 %** de los que han sufrido ataques consideran que las AET han sido determinantes.

Y SIN EMBARGO[4]

El **63 %** tiene dificultades para convencer a los directivos de la existencia de las AET y de su coste económico.

El **39 %** carece de métodos para detectar y rastrear las AET.

El punto de vista del ladrón

"La mayor parte de mis objetivos están convencidos de que la técnicas de evasión no son un peligro real. Ojos que no ven, corazón que no siente... justo como mis ataques. Su ceguera juega a mi favor."

Perfil de hacker:
Innovador

Competencias:
Redes, creación de malware

Método de ataque:
Técnicas de evasión

Motivación:
Control de endpoints y creación de redes de bots

Lo que debe saber

Cómo eluden los ciberdelincuentes los sistemas de seguridad

- **Ocultan su presencia durante las transferencias a través de la red**
  Gracias al uso de técnicas de evasión avanzada (AET), los ciberdelincuentes más astutos consiguen eludir la detección en las redes mediante la división de los paquetes de archivos (malware) en patrones difíciles de inspeccionar.
- **Permanecen inactivos durante el análisis**
  Para evitar ser detectados en entornos aislados (entornos de seguridad restringidos que analizan en detalle el comportamiento de archivos sospechosos), los archivos maliciosos los identifican y pasan a modo inactivo.
- **Permanecen ocultos durante las devoluciones de llamadas**
  Una vez en el endpoint elegido, el malware más sofisticado evita comportamientos anómalos o usa conexiones de devolución de llamada aleatorias con el fin de sortear los dispositivos de seguridad y continuar con su actividad maliciosa.

No permita a los delincuentes campar a sus anchas

- **Identifique los patrones de transferencia ocultos**
  Mediante el seguimiento y la inspección continuos de las sesiones de red, de principio a fin, se pueden detectar y bloquear patrones complejos de conexiones evasivas.
- **Intensifique los análisis**
  El análisis del código de archivos latente en el malware permite a los entornos aislados identificar comportamientos maliciosos ocultos y mejorar las tasas de detección.
- **Bloquee las devoluciones de llamadas**
  Mediante el seguimiento inteligente de las conexiones se pueden identificar y bloquear los patrones de devolución de llamada encubiertos. Asociar el tráfico de red a los procesos de los endpoints que lo originan permite localizar las conexiones maliciosas que, por lo general, pasan desapercibidas cuando se emplean métodos menos inteligentes.
- **Exija experiencia demostrada**
  Al planificar su estrategia de defensa, opte por tecnologías y soluciones con una trayectoria probaba y cuantificable en cuanto a neutralización de ataques evasivos. Nada puede sustituir a la experiencia.

3 Ataques furtivos

Conseguir saberlo todo de usted

Según las estimaciones, los hackers consiguieron el año pasado unos beneficios de 2500 millones de dólares gracias a su actividad delictiva[5]. A la vista de semejantes ganancias, atacar su red nunca ha sido más atractivo.

Esto justifica el surgimiento de amenazas avanzadas, extremadamente complejas, capaces de vencer a cualquier solución aislada que se utilice contra ellas. Los ciberdelincuentes son conscientes de sus puntos débiles, conocen todos los aspectos de su enfoque de seguridad y saben disimular su identidad a la perfección. Detenerles requiere un trabajo coordinado de toda su red de seguridad.

1367
brechas de seguridad confirmadas en 2013[6].

Protección de la propiedad intelectual

Cada día casi cuatro empresas sufren pérdidas de propiedad intelectual[6].

El punto de vista del ladrón

"Me encanta introducirme en una empresa que invierte enormes cantidades de dinero en tecnología, pero que no consiguen que funcione. Sé que dejo rastro, pero para cuando los administradores consiguen unir todos los cabos, ya hace tiempo que he desaparecido."

Perfil de hacker:
Beneficio económico

Método de ataque:
Furtivo

Competencias:
Planificación y desarrollo de ataques

Motivación:
Su propiedad intelectual

Lo que debe saber

Indicios de ataque furtivo

- **El engaño es habitual**
  Los ataques furtivos enmascaran sus intenciones hasta que alcanzan el endpoint elegido.
- **No hay lugar para la improvisación**
  Los ciberdelincuentes dedican meses a la preparación de sus ataques a fin de adquirir un conocimiento profundo de la red y de la infraestructura.
- **Cuidado con los dispositivos personales**
  Los agresores aprovechan los dispositivos personales utilizados en el lugar trabajo (que cuentan con menos protección), para infiltrarse desde el interior en la red protegida.
- **Aprovechan la sobrecarga de información y las soluciones de seguridad aisladas**
  Los ataques se recrudecen debido a que el personal de TI, que está sobrecargado, pasa por alto a menudo las señales sutiles de estos ataques selectivos.

La estrategia de aislamiento

- **Identifique los ataques desconocidos**
  La tecnología de análisis en entornos aislados (sandboxing) permite conocer las intenciones de los archivos entrantes y detectar malware desconocido y sigiloso.
- **La correlación es esencial**
  Todos los dispositivos de seguridad de red del perímetro deben comunicarse con las tecnologías de sandboxing para garantizar la impermeabilidad de la red.
- **Cree un sistema de protección cohesionado**
  Debe acabar con el aislamiento de los dispositivos de seguridad; deben compartir sus contenidos y aprender los unos de los otros en tiempo real.
- **Aléjese de las soluciones aisladas tradicionales**
  Si bien hay tecnologías específicas capaces de identificar los ataques, solo un enfoque conectado que comparta la información y aprenda del contexto le permitirá detener las amenazas avanzadas y evitar las fugas.

4 Ataques SSL

A veces, los ciberdelincuentes se ocultan delante de sus narices

Para bloquear eficazmente los ataques, la visibilidad es esencial. Aunque el protocolo SSL y el cifrado han sido la base de las comunicaciones seguras, también ofrecen nuevas vías de entrada a los ciberdelincuentes.

Desde el punto de vista del ladrón, el uso de los canales cifrados ya disponibles en su red es una forma extraordinaria de ocultar los ataques. En otras palabras, los hackers básicamente vuelven sus defensas contra usted. ¿Se puede evitar esta situación? Sí. Pero debe encontrar un equilibrio entre emplear funciones de inspección eficaces y reducir el rendimiento de la red, algo que puede resultar complicado.

24 000 000

de ataques SSL detectados por McAfee solamente en 2014. Los ataques SSL se dispararon en el 3.er y 4.º trimestre de 2014, probablemente debido a la aparición de Heartbleed[7].

El punto de vista del ladrón

"¿Por qué no ocultarme en el tráfico cifrado? La mayoría de las empresas no disponen del equipo necesario para inspeccionarlo. Y como no pueden verlo, puedo emplear incluso ataques sencillos."

Perfil de hacker:
Eficaz

Competencias:
Cifrado, vulnerabilidades de aplicaciones

Método de ataque:
SSL/tráfico cifrado

Motivación:
Económica

Cuestionamiento del protocolo SSL

- **El problema es cada vez mayor**
  En la medida en que cada vez más aplicaciones empresariales (en la nube, en los medios sociales) adoptan el cifrado, los hackers disponen de muchos sitios donde esconderse.
- **Consiguen sortear la inspección in situ**
  Los archivos maliciosos y las cargas útiles pueden distribuirse a través del cifrado y, por lo tanto, eludiendo las inspecciones in situ.
- **El lobo con piel de oveja**
  Los ciberdelincuentes son todavía más eficaces ya que pueden lanzar ataques rudimentarios y sencillos a través de conexiones SSL que no pueden inspeccionarse.

La estrategia para estar protegido

- **Combine visibilidad e integración**
  En pocas palabras, necesita una mayor visibilidad del tráfico cifrado.
- **Adopte un enfoque equilibrado**
  Ser capaz de inspeccionar el tráfico cifrado no debe suponer un deterioro del rendimiento de la red. El rendimiento de los segmentos de red importantes no debería verse afectado.
- **Combine recursos**
  La inspección SSL integrada con otras tecnologías de seguridad permite la inspección avanzada de ataques ocultos.

5 Uso malicioso de la red

A los ciberdelincuentes les gusta dar donde más duele

Lo más probable es que Internet juegue un papel fundamental en la mayor parte de sus operaciones cotidianas, y le permita recopilar datos y desarrollar la actividades comerciales. Entonces, si desapareciera su sitio web de la noche a la mañana, ¿qué consecuencias tendría?

¿Enormes? Tenga la certeza. Los ciberdelincuentes también lo saben. Esa es la razón por la que el uso malicioso de la red y de los recursos sigue siendo uno de los tipos más comunes de ataques contra la red. Además, implementar una solución de detección eficaz puede ser un verdadero reto. En la medida en que los ciberdelincuentes utilizan el tráfico normal de forma maliciosa, nada hace pensar que hay algo anormal en el propio tráfico. Tiene que mantener los ojos bien abiertos.

109 000 000

de ataques DDoS fueron detectados en 2014[8].

62 millones

de ataques de fuerza bruta maliciosos fueron detectados en 2014[9].

El punto de vista del ladrón

"Por el equivalente a 6 dólares en bitcoins, puedo alquilar una herramienta de DDoS y colapsar la mayoría de los sitios web. Mejor aún, si envío el tipo de paquete adecuado a sus servidores web, puedo paralizar el sitio web gratis."

Perfil de hacker:
Destructor y ladrón

Competencias:
Redes y servidores web

Método de ataque:
Uso malicioso de la red

Motivación:
Ciberactivismo o diversión

Signos de uso malicioso

- **El invitado inoportuno**
  En un ataque de denegación de servicio distribuido (DDoS), un servidor recibe un flujo de solicitudes de conexión o bien solicitudes de conexión especialmente diseñadas.
- **Se intenta abarcar demasiado**
  Los recursos del servidor se encuentran sobrecargados o totalmente inutilizados, lo que impide la gestión normal del tráfico.
- **La motivación real**
  Los agresores a menudo utilizan los ataques DDoS para distraer la atención de los administradores de TI mientras se infiltran de manera furtiva.
- **Chantaje**
  Los ataques DDoS, generalmente lanzados con fines delictivos, pueden venir acompañados en ocasiones por solicitudes de rescate.

Protéjase

- **Conozca su tráfico**
  Para poder conocer plenamente el tráfico abusivo que golpea su servidor web, es necesario llevar a cabo una inspección profunda de los paquetes in situ.
- **Preste atención al volumen**
  Es imprescindible llevar a cabo un análisis volumétrico para identificar los pequeños cambios, a menudo enmascarados, en los patrones de tráfico.
- **Consiga visibilidad total**
  Necesita disponer de visibilidad total del tráfico SSL, ya que los ataques se suelen ocultar en el tráfico cifrado.
- **Actúe de manera eficaz e inteligente**
  Combine el poder del filtrado del tráfico malicioso con las últimas tecnologías de inspección y benefíciese de la mejor solución de protección.

Es responsabilidad de todos

En un momento en que las fugas de datos se han vuelto algo cotidiano, las empresas se esfuerzan en aportar respuestas eficaces a los problemas de seguridad. Ha llegado la hora de abordar el problema desde otro punto de vista y replantearse por completo la seguridad de la red.

Lo nuevo no es siempre lo mejor

Los importante es que todos participemos en el debate. Resulta fundamental comprender a lo que nos enfrentamos y cómo podemos combatir estos cinco métodos de ataque. Utilizar sistemáticamente las últimas novedades parar resolver el problema es una actitud avocada al fracaso. La multiplicación de las herramientas y soluciones no va a reducir el número de vectores de amenazas. Resulta más eficaz mejorar la comunicación y la coordinación entre las soluciones de seguridad de las que ya dispone.

Los ladrones no son infalibles

La constante evolución de las amenazas obliga a utilizar una plataforma capaz de crecer a medida que lo hacen sus necesidades. Y cuando vaya adquirir esa plataforma, asegúrese de que elige un proveedor que invierte en tecnología y que cuenta con una trayectoria de éxito demostrada en materia de seguridad.

Más información

Para conocer las últimas innovaciones de Intel Security, le invitamos a que nos visite en www.mcafee.com/es/products/network-security/index.aspx. También puede utilizar la información contenida en este documento para iniciar los debates necesarios entre las partes interesadas de su empresa. Únase al debate #puntodevistadelladron.

Siga la seguridad de red

Acerca de Intel Security

McAfee forma ahora parte de Intel Security. Con su estrategia Security Connected, su innovador enfoque de seguridad reforzada por hardware y su exclusiva red Global Threat Intelligence, Intel Security trabaja sin descanso para desarrollar soluciones y servicios de seguridad proactivos que protejan los sistemas, las redes y los dispositivos móviles de uso personal y empresarial en todo el mundo. Intel Security combina la experiencia y los conocimientos de McAfee con la innovación y el rendimiento demostrado de Intel para hacer de la seguridad un ingrediente fundamental en todas las arquitecturas y plataformas informáticas. La misión de Intel Security es brindar a todos la tranquilidad para vivir y trabajar de forma segura en el mundo digital.

www.intelsecurity.com

1. Cifras basadas en una encuesta de Intel® Security realizada entre los asistentes a la conferencia Black Hat de 2014
2. Informe de McAfee Labs sobre amenazas (4.º trimestre de 2014)
3. Ibid.
4. http://www.mcafee.com/es/resources/reports/rp-security-industry-dirty-little-secret.pdf
5. http://www.darkreading.com/russian-hackers-made-$25b-over-the-last-12-months-/d/d-id/1316631
6. Verizon. *2014 Data Breach Investigations Report* (Informe de Verizon sobre las investigaciones de fugas de datos de 2014)
7. Informe de McAfee Labs sobre amenazas (4.º trimestre de 2014)
8. Ibid.
9. Datos de McAfee Labs sobre ataques: 1er-4.º trimestre de 2014

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com