Nadie está a salvo de la ciberdelincuencia

Las amenazas avanzadas se profundizan y amplían su alcance

Si bien los ataques informáticos por malware siguen teniendo predilección por las PC, en 2012 creció de manera notable la infección a dispositivos móviles, en especial aquellos bajo plataforma Android. Ofrecemos aquí un resumen de lo sucedido en los últimos meses del año anterior.

Al término del año 2012, el panorama de las amenazas seguía evolucionando en distintos frentes con riesgos tanto para particulares como para empresas. Las tres principales tendencias y eventos observados por los investigadores de los laboratorios McAfee Labs durante el cuarto trimestre fueron las siguientes:

- Un extraordinario crecimiento del malware dirigido a dispositivos basados en Android.
- La aparición de una nueva amenaza persistente avanzada dirigida contra empresas de servicios financieros y sus clientes.
- Las amenazas dirigidas a plataformas de PC vuelven a experimentar un crecimiento de dos cifras, y surgen tácticas y amenazas nuevas por parte de las bandas de ciberdelincuentes.

AMENAZAS CONTRA DISPOSITIVOS MÓVILES

Hasta hace muy poco, se daba por hecho que las amenazas de malware dirigido a dispositivos móviles sufrirían una evolución similar a la observada en las amenazas para PC de hace una década.

En esta suposición se subestimaron por completo la capacidad y las ambiciones de la comunidad de ciberdelincuentes. Según se aprecia en el siguiente cuadro, la evolución del segmento de amenazas de malware dirigidas a dispositivos móviles difiere claramente del crecimiento lineal experimentado por el segmento de los PC.

Los dispositivos móviles sufrieron un incremento en los ataques de malware, en especial aquellos basados en sistema operativo Android

El número de muestras de malware para dispositivos móviles descubierto por los laboratorios McAfee Labs en 2012 fue 44 veces superior a la cifra de 2011. Esto quiere decir que el 95 % del total de muestras de malware para dispositivos móviles desde sus inicios aparecieron el año pasado. El otro cambio observado en 2012 es que los ciberdelincuentes dedican en la actualidad prácticamente todos sus esfuerzos a los ataques a Android: el 97 % de las muestras de malware detectadas el año pasado iban dirigidas a esta plataforma. Solo en el cuarto trimestre, el número de nuevas muestras de malware basadas en Android creció un 85 %.

AMENAZAS PERSISTENTES AVANZADAS

Tras una ligera tregua en los inicios de Stuxnet, la aparición de nuevas amenazas persistentes avanzadas (APT) se aceleró en la segunda mitad de 2012. La primera APT anunciada en 2012 fue Operation High Roller. Diseñada originalmente para atacar sistemas de transferencia automática (ATS) en Europa, los investigadores de los laboratorios McAfee Labs observaron nuevos ataques basados en High Roller dirigidos a empresas de fabricación e importación/exportación de Estados Unidos y Latinoamérica.

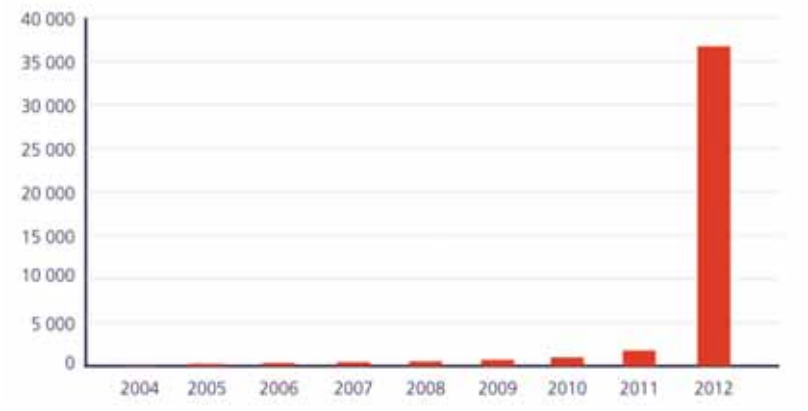
Todo indica que aparecerán nuevas variantes de High Roller dirigidas contra la infraestructura del sistema de pagos electrónicos Automated Clearing House (ACH) utilizado para procesar la gran mayoría de las transacciones de comercio electrónico a nivel mundial.

En el cuarto trimestre asistimos a la aparición de una nueva APT llamada Blitzkrieg. A diferencia de High Roller, cuyo objetivo principal son las infraestructuras de servicios financieros, Blitzkrieg ataca tanto a particulares como a instituciones bancarias. Blitzkrieg ataca en primer lugar los equipos de los usuarios a través de phishing e instala un troyano conocido como Prinimalka. A partir de ahí, el troyano supervisa las acciones de los usuarios y el tráfico web con el fin de detectar el uso de credenciales de conexión a la banca electrónica. Los autores de Blitzkrieg exportan entonces estas credenciales a un servidor de control y las utilizan para llevar a cabo transferencias electrónicas de fondos ilícitas.

MALWARE

Tras el ligero descenso experimentado en el tercer trimestre, el número de nuevas muestras de malware detectadas mostró un importante crecimiento durante el cuarto trimestre, con un aumento del 35 % respecto al trimestre anterior. A lo largo del año, el número de muestras de malware detectadas aumentó un 50 %, con lo que se superan los 120 millones de muestras en el "zoológico" de McAfee Labs.

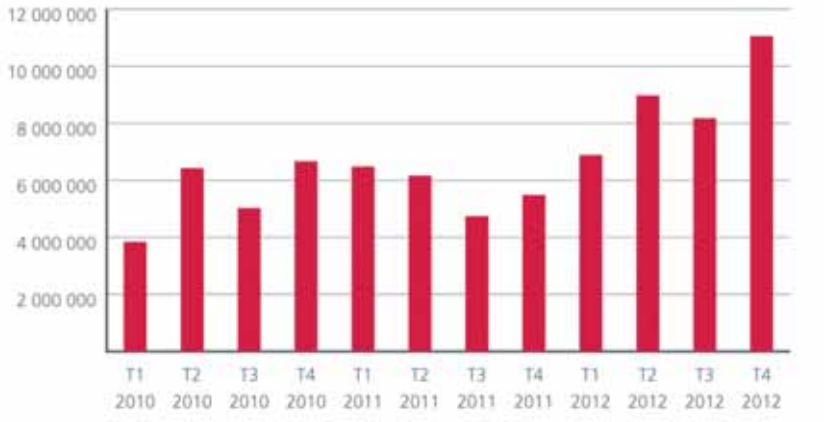
Además de más abundantes, las amenazas dirigidas a usuarios de PC siguen siendo cada vez más



peligrosas y sofisticadas. Por ejemplo, los casos de troyanos ladrones de contraseñas nuevos y exclusivos aumentaron un 72 % durante el cuarto trimestre. Los ciberdelincuentes tienen claro que las credenciales de autenticación de los usuarios constituyen algunos de los activos de propiedad intelectual más valiosos que pueden encontrar en la mayoría de los ordenadores.

También han descubierto que una de las mejores formas de eludir la seguridad estándar de los sistemas es "firmar" electrónicamente el malware valiéndose de certificados robados o creados a tal efecto.

Durante el cuarto trimestre, se produjo un pronunciado crecimiento de esta táctica, período en el que los casos de binarios de malware firmados se multiplicaron por tres.



Además de sus objetivos habituales, es decir, el sistema operativo y las aplicaciones, ahora los ciberdelincuentes atacan con fuerza la base del sistema: la BIOS y las pilas de almacenamiento. Los ataques a subsistemas de almacenamiento fueron particularmente populares durante el cuarto trimestre. Uno de los métodos más utilizados es el ataque al registro de inicio maestro (MBR) de la unidad de disco del sistema.

Una de las formas de ataque más insidiosas que experimentaron un importante crecimiento durante 2012 es el ransomware. Los ataques de ransomware suelen presentarse de dos formas. En el primer caso, el ciberdelincuente se apodera de información confidencial del sistema de un usuario o de la infraestructura de TI de una empresa y, a continuación, exige el pago de una cantidad de dinero a cambio de no hacer públicos los datos.

En la segunda forma de ataque, el ciberdelincuente se hace con el control del sistema (o dispositivo móvil) de un usuario, cifra sus datos y exige una suma de dinero por la clave de cifrado. Desgraciadamente, ni siquiera los usuarios que acceden a las demandas de "rescate" tienen la seguridad de que vayan a recibir la clave de cifrado prometida.

El tramo final de crecimiento de malware dirigido a PC detectado durante el cuarto trimestre de 2012 corresponde a un marcado incremento de las amenazas basadas en la Web. El mecanismo básico de infección permite a un ciberdelincuente descargar malware de manera furtiva desde un sitio web sin conocimiento del usuario. El malware intenta, entonces, añadir el sistema a una red de bots o robar datos del sistema del usuario.

La distribución de malware de sitios web infectados se convirtió en una táctica cada vez más popular en 2012 debido, principalmente, a las actuaciones de las fuerzas de seguridad, que consiguieron desactivar algunas de las redes de bots más importantes. McAfee Labs también ha detectado una nueva tendencia mediante la cual las bandas criminales crean un "superdominio" de sitios web infectados.

Gracias a esta técnica, consiguen incluir cientos o miles de sitios web distintos tras una sola dirección IP.

Esta dirección se cambia con frecuencia con el fin de evitar la detección y el tráfico se dirige a la misma a través del envenenamiento de DNS y otras técnicas.

OTRAS TENDENCIAS

Aunque las tres tendencias descritas conforman la mayor parte de las "novedades" en el panorama de las amenazas del cuarto trimestre, hay otras tres que merece la pena mencionar. En primer lugar, el descenso continuado del volumen de spam y el número de sistemas infectados controlados por operadores de redes de bots. En lo que se refiere a las redes de bots, la situación se explica en parte por las acciones de las fuerzas de seguridad, mencionadas anteriormente, pero también por la pérdida de atractivo de este modelo de negocio. Los volúmenes de spam reflejan por lo general la actividad de las redes de bots y el cuarto trimestre evidencia este hecho. La tendencia descendente continuada de los volúmenes de spam es síntoma de que muchos creadores de spam optan por otras formas de ciberdelincuencia o centran sus esfuerzos en ataques de phishing mucho más selectivos dirigidos a grupos de víctimas específicos.

En segundo lugar, McAfee Labs detectó un importante crecimiento del uso de Internet para vender documentos falsos: pasaportes, documentos de identidad, facturas y otros certificados expedidos oficialmente. Aunque preocupante, esta tendencia no es más que la aplicación de la tecnología del comercio electrónico a una actividad que es muy anterior a la aparición de Internet.

Por último, el hacktivismo experimentó un moderado ascenso durante el cuatro trimestre; se observaron ataques contra objetivos del sector público y privado en Israel, Siria, Reino Unido y Estados Unidos.

Si bien durante 2013 es probable que los ataques de hackers que dicen estar relacionados co el sindicato Anonymous sigan contándose entre las amenazas, McAfee Labs prevé un descenso a lo largo del año, ya que dichos ataques serán sustituidos por otros financiados y perpetrados por ciberdelincuentes al servicio de estados. ■

Fuente:

McAfee
An Intel Company