Informe

Predicciones sobre amenazas para 2014 - McAfee® Labs

Índice

1: En el "mercado" de malware global en 2014, el malware para móviles será el motor del crecimiento tanto en cuanto a innovación tecnológica como en lo relativo al volumen de ataques.

En 2013 el ritmo de crecimiento de nuevo malware para móviles, dirigido casi exclusivamente a la plataforma Android, superó de largo al incremento del nuevo malware dirigido a PC. En los dos últimos trimestres, el crecimiento del nuevo malware para PC fue casi plano, mientras que se detectó un aumento del 33 % en nuevas muestras para Android.

Aunque McAfee Labs espera que esta tendencia continúe en 2014, las novedades no se ceñirán al crecimiento de nuevos ataques para móviles. Prevemos también que surjan tipos de ataques totalmente nuevos dirigidos a Android. Es muy probable que observemos los primeros ataques de ransomware reales dirigidos a dispositivos móviles, que cifrarán los datos clave en el dispositivo y los mantendrán retenidos a cambio de un rescate. La información solo se liberará si la víctima entrega al autor del ataque el dinero solicitado, ya sea en moneda real o virtual —como Bitcoin. También harán su aparición en el terreno de los móviles nuevas tácticas, como los ataques que aprovechan vulnerabilidades en las funciones de comunicaciones de campo cercano (NFC) que incorporan ahora muchos dispositivos móviles, así como otros que dañarán aplicaciones válidas con el fin de apropiarse de datos sin ser detectados.

Los ataques a dispositivos móviles afectarán también a la infraestructura de las empresas. Dichos ataques se valdrán del ya omnipresente fenómeno conocido como "BYOD" en sus siglas en inglés, o el uso de dispositivos personales en el trabajo, junto a la relativa inmadurez de la tecnología de seguridad en el área de los dispositivos móviles. Los usuarios que descarguen malware de manera involuntaria lo introducirán en el perímetro de la red empresarial de manera que podrá apropiarse de datos confidenciales. El fenómeno BYOD no va a desaparecer, por lo que las empresas deben implementar políticas y soluciones de administración de dispositivos globales que les permitan evitar convertirse en víctimas.

2: Gracias al uso de monedas virtuales, los ataques de ransomware maliciosos se extenderán por el mundo.

Los ataques de ransomware que cifran datos en los dispositivos de las víctimas no son una novedad. Sin embargo, tradicionalmente han sido vulnerables a las acciones de las fuerzas de seguridad contra los procesadores de pagos utilizados por los agresores.

Cuadro de diálogo de CryptoLocker.

Si bien es cierto que el incremento del uso de monedas virtuales beneficia y promueve la actividad económica, también ofrece a los ciberdelincuentes la infraestructura de pago anónima perfecta y no regulada que necesitan para cobrar el rescate a sus víctimas. Creemos que ataques como CryptoLocker seguirán proliferando mientras sigan siendo (muy) lucrativos. Asimismo, prevemos la aparición de nuevos ataques de ransomware dirigidos a empresas con el objetivo de cifrar activos de datos corporativos esenciales.

La ventaja, tanto para individuos como para empresas, es que aunque la carga útil del ransomware es exclusiva, los mecanismos de distribución (spam, descargas desapercibidas y aplicaciones infectadas) no lo son. Los particulares y las empresas que mantengan sus sistemas antimalware (endpoints y redes) actualizados estarán relativamente protegidos contra esta amenaza. Un sistema de copia de seguridad eficaz, ya sea personal o desplegado en la empresa, también aislará a las víctimas de la mayor parte de las consecuencias negativas del ransomware.

3: En el mundo de espionaje y contraespionaje de la ciberdelincuencia y la ciberguerra, las bandas de criminales y los estados desplegarán nuevos ataques ocultos que serán más difíciles de identificar y detener que nunca.

Al igual que las soluciones de seguridad de la información son cada vez más sofisticadas, los esfuerzos de la comunidad de ciberdelincuentes para sortear estas medidas han evolucionado también. Los ataques que incluyen técnicas de evasión avanzadas representan el frente más novedoso en la guerra de la protección de los datos empresariales. Una técnica de evasión popular que adoptará un buen número de ciberdelincuentes en 2014 es el uso de ataques que tienen la capacidad para detectar entornos aislados y que no se despliegan completamente hasta que no verifican que se están ejecutando directamente en un dispositivo no protegido.

Otras tecnologías de ataque que se perfeccionarán y desplegarán en 2014 son los ataques de programación orientados a retorno (o ROP) que consiguen que las aplicaciones legítimas se comporten de manera maliciosa, eliminando automáticamente el malware para ocultar su rastro tras hacerse con el objetivo, así como los ataques avanzados que afectan a sistemas de control industrial dedicados, con el potencial de dañar infraestructuras públicas y privadas.

Los ataques con motivaciones políticas seguirán aumentando, especialmente cuando se acerquen los Juegos Olímpicos de Invierno de Sochi de 2014 (en febrero) y la Copa del Mundo de la FIFA en Brasil (junio-julio). Los hacktivistas también aprovecharán estos eventos para divulgar sus ideas.

Las empresas de TI deberán responder a estas nuevas tácticas con el fin de garantizar que su defensa no dependa exclusivamente de medidas de seguridad que las bandas de ciberdelincuentes mundiales puedan sortear fácilmente.

4: Para finales de 2014 los "ataques sociales" serán algo totalmente habitual.

Los ataques a plataformas de redes sociales son los que aprovechan las bases de usuarios más numerosas, como Facebook, Twitter, LinkedIn, Instagram, etc. Muchos de estos ataques copian las tácticas de otro malware, como Koobface, y se limitan a utilizar las plataformas sociales como mecanismo de distribución. Sin embargo, en 2014 aparecerán ataques que emplearán funciones que son exclusivas de las plataformas sociales con el fin de proporcionar datos sobre los contactos, la ubicación o la actividad profesional de los usuarios, que podrán utilizarse para enviar publicidad o para delitos virtuales o reales.

Uno de los ataques a plataformas más conocido simplemente roba las credenciales de autenticación de los usuarios y posteriormente las utiliza para obtener información personal de sus "amigos" o colegas, que no sospechan nada. La red de bots Pony[1], que consiguió más de dos millones de contraseñas de los usuarios de Facebook, Google o Yahoo, entre otros, es solo la punta del iceberg. Facebook estima que de 50 a 100 millones de las cuentas de sus usuarios activos mensuales (MAU, por sus siglas en inglés) corresponden a duplicados y que hasta 14 millones de estos usuarios se consideran "no deseados". Según un estudio reciente de Stratecast, el 22 % de los usuarios de medios sociales han sufrido algún incidente relacionado con la seguridad[2].

Tanto las empresas privadas como los entes públicos emplearán también las plataformas sociales para lanzar "ataques de reconocimiento" contra sus competidores y rivales, ya sea directamente o a través de terceros. Los líderes más prominentes de los sectores público y privado han sufrido este tipo de ataques en 2013. Podemos prever un aumento de la frecuencia y el alcance de estos ataques en 2014.

La otra modalidad de ataques sociales cuyo volumen puede crecer en 2014 es la conocida como de "bandera falsa", que engañan al usuario para que revele información personal o credenciales de autenticación. Uno de los ataques más populares será una solicitud "urgente" para restablecer la contraseña del usuario. El agresor se apropiará de las credenciales de nombre de usuario y contraseña, y utilizará la cuenta del usuario para obtener información sobre él y sobre sus contactos.

Para evitar los ataques a través de plataformas sociales y de bandera falsa, los individuos y las empresas deberán mejorar sus soluciones y políticas de seguridad para incrementar la vigilancia, y asegurarse de que el uso que los empleados hacen de las plataformas de medios sociales no provoque fugas de datos materiales.

5: Los nuevos ataques contra PC y servidores aprovecharán vulnerabilidades en capas superiores e inferiores al sistema operativo.

Aunque muchos grupos de ciberdelincuentes centrarán su atención en los dispositivos móviles, otros seguirán atacando los PC y los servidores. Sin embargo, los nuevos ataques que veremos en 2014 no afectarán solamente al sistema operativo, sino que aprovecharán vulnerabilidades por encima y por debajo de este.

En 2014 muchos de los nuevos ataques a PC aprovecharán vulnerabilidades del lenguaje HTML5, que permite publicar los sitios web con sofisticadas funciones de interacción y personalización para programadores. Sin embargo, HTML5 también revela algunas superficies de ataque nuevas. Con HTML5, los investigadores ya han demostrado cómo supervisar el historial de navegación del usuario para dirigir mejor las campañas publicitarias. Muchas de las aplicaciones basadas en HTML5 han sido diseñadas para dispositivos móviles, por lo que prevemos que surjan ataques que entren en el entorno aislado del navegador y proporcionen a los agresores acceso directo a los dispositivos y sus servicios. Muchas empresas diseñarán también aplicaciones empresariales basadas en HTML5. Para impedir la fuga de datos utilizados por estas aplicaciones, es preciso incorporar la seguridad a estos nuevos sistemas desde el primer día.

Cada vez más, el objetivo de los ciberdelincuentes serán las vulnerabilidades debajo del sistema operativo, en la pila de almacenamiento e incluso en la BIOS. Para mitigar estos ataques de bajo nivel en el entorno empresarial se deberán desplegar medidas de seguridad asistidas por hardware que funcionen también por debajo del nivel del sistema operativo.

6: La evolución del panorama de amenazas obligará a la adopción de analíticas de seguridad de los grandes volúmenes de datos, o Big Data, para satisfacer los requisitos de detección y rendimiento.

Históricamente, la mayoría de las soluciones de seguridad de la información han dependido de la identificación de cargas útiles maliciosas (listas negras) o del seguimiento de las aplicaciones válidas (listas blancas). El desafío actual al que se enfrentan los responsables de la seguridad de la información implica la identificación y el procesamiento adecuado de las cargas útiles "grises". Para ello es necesario aplicar varias tecnologías de seguridad en coordinación con sólidos servicios de reputación de amenazas.

Los servicios de reputación de amenazas ya han demostrado su utilidad a la hora de detectar malware, sitios web maliciosos, spam y ataques a redes. En 2014, los proveedores de seguridad incorporarán nuevos servicios de reputación de amenazas que les permitirán, tanto a ellos como a sus usuarios, identificar amenazas persistentes avanzadas sigilosas de una forma más rápida y más precisa que en la actualidad. Los análisis de Big Data permitirán a los profesionales de la seguridad identificar ataques mediante técnicas de evasión avanzadas y con un alto grado de sofisticación, así como amenazas persistentes avanzadas capaces de perturbar procesos empresariales críticos.

7: El despliegue de aplicaciones empresariales basadas en la nube creará nuevas superficies de ataque que serán aprovechadas por los ciberdelincuentes.

A Willie Sutton, de quien se dice que participó en el robo de 100 bancos a principios del siglo 20, se le atribuye la afirmación de que robaba bancos sencillamente "porque ahí es donde está el dinero"[3]. Las bandas de ciberdelincuentes del siglo 21 pondrán el punto de mira en las aplicaciones y repositorios de datos basados en la nube, porque ahí es donde están los datos, o lo estarán más pronto que tarde. Esto podría ocurrir a través de aplicaciones empresariales que no han sido evaluadas por el departamento de TI respecto a las directivas de seguridad empresariales. Según un reciente informe, más del 80 % de los usuarios empresariales utilizan aplicaciones en la nube sin el conocimiento o la asistencia del departamento de TI de la empresa[4].

Aunque las aplicaciones basadas en la nube aportan atractivos beneficios funcionales y económicos, también ponen a disposición de los agresores una familia de superficies de ataque completamente nueva, como los omnipresentes hipervisores existentes en todos los centros de datos, la infraestructura de comunicaciones múltiple implícita en los servicios en la nube y la infraestructura de administración que se utiliza para aprovisionar y supervisar servicios en la nube de gran envergadura. El problema para los responsables de la seguridad de las empresas estriba en el hecho de que cuando una aplicación se traslada a la nube, las empresas pierden visibilidad y control sobre el perfil de seguridad.

Esta pérdida de control directo del perímetro de seguridad de la empresa ejerce una tremenda presión sobre los profesionales de la seguridad y administradores a la hora de asegurarse de que el acuerdo de usuario y los procedimientos operativos del proveedor de los servicios en la nube, que garantizan las medidas de seguridad, se aplican y se actualizan de manera constante con el fin de hacer frente al panorama de amenazas, en constante evolución. Es posible que las grandes empresas tengan la suficiente influencia como para exigir a los proveedores de los servicios en la nube que pongan en práctica medidas de seguridad acordes con el enfoque de seguridad de la empresa, Sin embargo, los pequeños consumidores de servicios basados en la nube no tendrán esa ventaja, por lo que deberán examinar cuidadosamente los a menudo ambiguos acuerdos de usuario de los proveedores en lo que se refiere a seguridad y propiedad de los datos. Los nuevos servicios basados en la nube pueden también ofrecer nuevas superficies de ataque hasta que alcancen un nivel de madurez que incluya la instrumentación y las contramedidas necesarias para garantizar la seguridad de los datos que deben proteger.

Acerca de los autores

Este informe ha sido preparado y redactado por Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky y Chong Xu.

Acerca de los laboratorios McAfee Labs

McAfee Labs es la referencia mundial en investigación sobre amenazas, información sobre amenazas y liderazgo de pensamiento sobre ciberseguridad. Un equipo compuesto por 500 investigadores recopila datos sobre amenazas de millones de sensores sobre los principales vectores de amenazas: los archivos, la Web, la mensajería y las redes. A partir de ahí realiza un análisis de correlación de amenazas entre vectores y proporciona información sobre amenazas en tiempo real a los productos de seguridad de redes y endpoints de McAfee, perfectamente integrados, a través de su servicio McAfee Global Threat Intelligence basado en la nube. McAfee Labs desarrolla asimismo tecnologías de detección de amenazas fundamentales, como DeepSAFE, generación de perfiles de aplicaciones y administración de listas grises, que se incorporan al más amplio portfolio de productos de seguridad del sector.

Acerca de McAfee

McAfee, empresa subsidiaria de propiedad total de Intel Corporation (NASDAQ:INTC), permite a las empresas, el sector público y los usuarios particulares disfrutar con seguridad de las ventajas de Internet. La empresa ofrece soluciones y servicios de seguridad proactivos y de eficacia probada para sistemas, redes y dispositivos móviles en todo el mundo. Con su estrategia Security Connected, su innovador enfoque de la seguridad ampliada mediante hardware y su exclusiva red Global Threat Intelligence, McAfee dedica todos sus esfuerzos a la protección de sus clientes. www.mcafee.com/mx.

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, "*The Hidden Truth Behind Shadow IT.*" (La verdad oculta tras las TI en la sombra), noviembre de 2013. http://www.mcafee.com/mx/resources/reports/rp-six-trends-security.pdf

[3] El propio Sutton admitió que nunca dijo la famosa frase que se le atribuía y que robaba bancos simplemente porque "le divertía".

[4] Stratecast, "*The Hidden Truth Behind Shadow IT.*" (La verdad oculta tras las TI en la sombra), noviembre de 2013. http://www.mcafee.com/mx/resources/reports/rp-six-trends-security.pdf

McAfee, Inc.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.mcafee.com/mx

60756rpt_threats-predictions_1213_fnl_ETMG