Informe

# Predicciones de amenazas para 2012

McAfee® Labs™

# Índice





Cuando una empresa de investigación sobre seguridad hace predicciones sobre amenazas en el futuro, nunca tiene la certeza de que vayan a cumplirse. Efectivamente, puede ser interesante coger la bola de cristal y hacer pronósticos sobre lo que puede pasar o no pasar en los próximos meses, pero ¿en qué medida cambian las amenazas cada año? Este último año ha estado marcado por importantes transformaciones. Pero esas transformaciones, ¿suponen una revolución o una evolución? Hemos asistido a grandes cambios en las amenazas dirigidas a dispositivos móviles, el hacktivismo, y los ataques del lado del cliente, contra medios sociales y selectivos. Muchos de estos cambios y tendencias seguirán afectando al panorama de las amenazas durante los próximos años.

¿Cuáles son los cambios en las amenazas que prevé McAfee Labs para el año que viene? Entrarán en juego nuevos escenarios y veremos igualmente una importante evolución incluso en los vectores de amenaza más establecidos:

- Las amenazas industriales se consolidarán y se segmentarán.
- Los ataques al hardware incrustado serán más amplios y profundos.
- El hacktivismo y Anonymous se reinventarán y evolucionarán.
- Los sistemas de monedas virtuales sufrirán ataques a mayor escala y con más frecuencia.
- Este será el "el año *para* (no "de") la ciberguerra".
- La tecnología DNSSEC, de protección de DNS, dará lugar a nuevos vectores de amenazas a redes.
- El spam tradicional se va a "legalizar", el phishing dirigido o spearphishing evolucionará hacia un tipo de ataque selectivo a través de mensajes.
- Las redes de bots y los rootkits para dispositivos móviles evolucionarán y convergerán.
- Los certificados falsos y las autoridades de certificados falsas debilitarán la confianza de los usuarios.
- Las mejoras en los sistemas operativos y en la seguridad contribuirán a la aparición de redes de bots y rootkits de próxima generación.

Hechas las presentaciones, pasemos a los detalles.

## Amenazas dirigidas a sistemas industriales

Las amenazas a las redes de infraestructuras industriales y nacionales han recibido recientemente gran atención, y no sin razón. Se trata de una de las pocas áreas en las que las ciberamenazas suponen un verdadero riesgo para la pérdida de vidas y de propiedades. Los sistemas industriales de registro de datos y control de supervisión (SCADA, Supervisory Control And Data Acquisition) son tan vulnerables como cualquier otro sistema conectado a la red; la gran diferencia es que muchos de ellos no fueron diseñados para el entorno de red que se sigue adoptando de manera global. El aumento de la interconectividad de sistemas y dispositivos no diseñados para este tipo de acceso es terreno abonado de problemas, debido a la falta de prácticas de protección de la información en muchos de los entornos en los que se despliegan los sistemas SCADA. Conectar sistemas de infraestructuras críticas a Internet para después administrarlos mediante software de uso extendido parece haberse convertido en una práctica habitual. No existe ninguna aplicación de software que no presente alguna vulnerabilidad, pero los sistemas de TI industriales requieren una mayor solvencia en arquitectura, diseño e implementación. Los agresores aprovecharán esta falta de preparación con mayor frecuencia y éxito en 2012, aunque solo sea para practicar el chantaje y la extorsión. Si analizamos los objetivos de muchos grupos hacktivistas, la posibilidad de que se combinen los objetivos e intereses políticos con vulnerabilidades en los sistemas de control industrial (industrial controller systems, ICS) debe tomarse *muy* en serio.

Stuxnet demuestra que el código malicioso puede crear una respuesta física en el mundo real[1]. Los recientes ataques dirigidos contra servicios de abastecimiento de agua en Estados Unidos demuestran que estas instalaciones despiertan cada vez más el interés de los agresores. Cuanto mayor es la atención que reciben los sistemas SCADA y de infraestructuras críticas, mayor parece ser la inseguridad que se advierte. Pensamos que esta inseguridad dará paso a amenazas de mayor envergadura a través de plataformas y toolkits de ataque, así como a un aumento de las acciones dirigidas a servicios públicos y sistemas ICS de abastecimiento de energía. Una vez que se descubra el punto débil de un grupo, los agresores no dudarán en aprovecharlo.

Los agresores tienden a dirigir sus ataques a sistemas que ofrecen altas probabilidades de éxito y los sistemas ICS han demostrado ser un entorno ideal. Sus administradores deberían tomar nota de los eventos recientes. Ha llegado la hora de realizar pruebas de penetración exhaustivas y configurar planes de respuesta ante emergencias que incluyan cibercomponentes y la colaboración con las fuerzas de seguridad a todos los niveles. Deben hacerse la siguiente pregunta: ¿Qué ocurre cuándo son atacados?

## La amenaza desde el interior: hardware incrustado

Los sistemas incrustados han crecido en popularidad e importancia durante los últimos años. En general, están diseñados para llevar a cabo una función de control específica dentro de un sistema mayor, a menudo con necesidades de computación en tiempo real. En ocasiones residen en un dispositivo completo que incluye hardware y otros componentes mecánicos. Esta arquitectura se ha utilizado tradicionalmente en sectores como la industria aeroespacial, el transporte, la energía y los dispositivos médicos, y se está introduciendo cada vez con más fuerza en el mundo empresarial y de consumo. GPS, enrutadores, puentes de red y, últimamente, una gran cantidad de dispositivos electrónicos utilizan funciones y diseños incrustados.

En el caso de los sistemas incrustados es preciso que el malware lance su ataque a nivel de hardware y el nivel de competencia requerido para este tipo de ataques presagia consecuencias que van más allá de las plataformas incrustadas.

Cada vez más, los desarrolladores crean malware que ataca los componentes inferiores del sistema operativo. En muchas ocasiones, los agresores intentarán obtener acceso raíz a un sistema en su nivel más bajo; por ejemplo, en el registro de arranque maestro en la BIOS. Si los agresores consiguen insertar código que altere el orden de arranque o de carga del sistema operativo, tendrán un mayor control y acceso a largo plazo al sistema y a sus datos. El control del hardware es la tierra prometida para los agresores más sofisticados.

Como consecuencia de esta tendencia, otros sistemas que utilizan hardware incrustado podrán convertirse en víctimas de estos tipos de ataques. Ya hemos visto código de concepto que ataca el hardware incrustado de los sistemas de automoción, médicos y de servicios públicos. Pensamos que este código de prueba de concepto será más eficaz en 2012 y en adelante.

## Hacktivismo

Aunque el hacktivismo no es una novedad, la presencia constante en los medios de la saga WikiLeaks durante 2010 lo ensalzó hasta cuotas inéditas de publicidad, aceptación y práctica. En general, 2011 ha sido un año un tanto confuso para los activistas online, con enfrentamientos frecuentes entre ellos y sin objetivos claramente definidos. En ocasiones, era difícil distinguir las campañas con motivaciones políticas de los meros juegos de jóvenes hackers, pero una cosa ha quedado clara: cuando los activistas escogen un objetivo, consiguen comprometerlo, ya sea a través de una fuga de datos o de un ataque de denegación de servicio. No se debe subestimar su fortaleza. Se esté de acuerdo o no con sus objetivos, Anonymous y otros grupos hacktivistas han demostrado dedicación, ingenio e incluso agilidad a la hora de elegir algunos de sus objetivos y operaciones.

El año próximo será decisivo para el hacktivismo y los casos de Anonymous representan únicamente un aspecto del problema.

- El "verdadero" Anonymous (es decir, el ala histórica) se reinventará a sí mismo y al escenario en el que actúa, o desaparecerá. Si los círculos de influencia de Anonymous son incapaces de organizarse, convocando a sus integrantes a actuar de manera clara y asumiendo responsabilidades, los activistas que se declaran parte de Anonymous corren el riesgo de acabar siendo marginalizados. Sea como fuere, estos ataques aumentarán de manera importante. Los ataques de denegación de servicio distribuido (DDoS) y la revelación de datos personales con un objetivo político seguirán aumentando.
- Los líderes de las protestas digitales se aproximarán a los responsables de las manifestaciones físicas. Veremos más casos de unión entre el hacktivismo basado en medios sociales y el hacktivismo coordinado a través de medios sociales. Pensamos que en el futuro, muchas operaciones incluirán tanto componentes físicos como digitales. Las acciones conjuntas y coordinadas, a pie de calle y a través de Internet, se planificarán de forma simultánea. No es difícil predecir que Occupy y otros grupos de indignados evolucionarán hacia una acción digital más directa. Como ya comentamos en otras predicciones, existe la posibilidad real de que se conjuguen objetivos hacktivistas con la disponibilidad de sistemas de control industrial o SCADA. Pensamos que los hacktivistas de la línea dura que apoyan los movimientos de indignados Occupy en todo el mundo dejarán de identificarse como Anonymous y pasarán a operar como "Ciberocupas".
- En nombre de objetivos políticos e ideológicos, la vida privada de personajes públicos (políticos, líderes empresariales, jueces y responsables de las fuerzas de seguridad) será revelada con mayor frecuencia que en años anteriores. Los manifestantes no van a escatimar esfuerzos para obtener de redes sociales o servidores web datos que faciliten sus operaciones.



- Algunos hacktivistas actuarán en la línea de los "ciberejércitos" que florecieron fundamentalmente en estados no democráticos o no seculares (Ciberejército iraní, Ciberejército paquistaní, grupo ChinaHonker, etc.). Aunque en la mayoría de los casos estos ejércitos se dedicaron básicamente a la desfiguración de sitios web, prevemos que el año próximo sus acciones sean más perjudiciales. Algunos de estos grupos entrarán en conflicto, lo que podría producir daños colaterales impredecibles (palestinos contra israelíes, indios contra paquistaníes, coreanos del sur contra coreanos del norte, etc.). En 2011, se rumoreaba que los ciberejércitos eran manipulados o financiados por sus respectivos gobiernos. Los estados totalitarios irán un paso más allá el próximo año, hasta el punto de reconocer las acciones de los ciberejércitos locales.

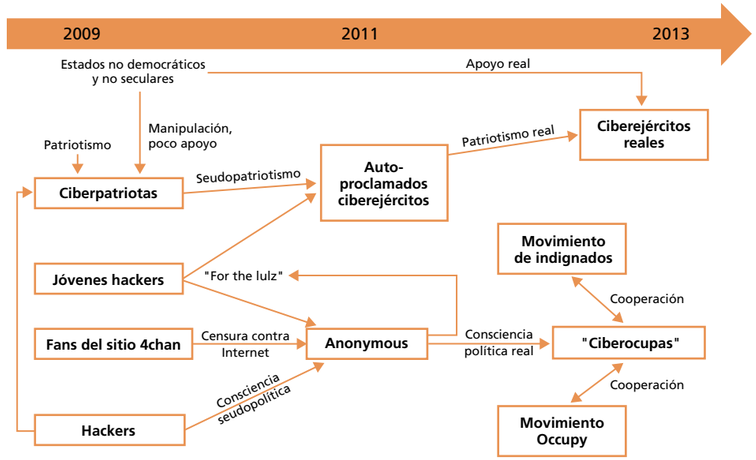


Figura 1: Las numerosas conexiones y motivaciones del hacktivismo.

## Moneda virtual

La moneda virtual, en ocasiones llamada cibermoneda, se han convertido en una popular forma de intercambio de dinero online. Aunque no necesariamente respaldados por activo fijo material o bienes tangibles, servicios como Bitcoin permiten a los usuarios realizar transacciones a través de redes descentralizadas, peer-to-peer. Básicamente se trata de dinero electrónico que permite realizar pagos directos, online. Lo único que el cliente necesita es un software y un servicio de monedero online para recibir las "monedas", que se almacenan en el monedero y pueden transferirse a otros como pago por bienes y servicios. Para que los usuarios puedan recibir estas monedas, solamente necesitan la dirección del monedero. No es difícil ver los problemas y las oportunidades que plantea este servicio.

El malware en forma de troyano encaja fácilmente en esta arquitectura. Los monederos no están cifrados y las transacciones son públicas. Esto convierte a este sistema en un objetivo atractivo para los ciberdelincuentes. En 2011 se produjeron varios sucesos importantes relacionados con las monedas virtuales:

- La base de datos de intercambio de dinero digital Mt. Gox fue atacada por ciberdelincuentes, que consiguieron apoderarse de miles de Bitcoins.
- Se distribuyó spam que publicitaba herramientas de recolección de Bitcoins falsas. En realidad, estas herramientas contenían malware diseñado para enviar los archivos del monedero de las víctimas a una ubicación central. Además, permitía a otros recolectores utilizar el ordenador infectado para obtener más Bitcoins.
- Se localizaron redes de bots de recolectores de Bitcoins en circulación. Valiéndose de un gran número de ordenadores infectados, estas redes de bots eran capaces de acelerar la recopilación y el proceso de Bitcoins, así como lanzar ataques de denegación de servicio distribuido (DDoS).

La naturaleza de las monedas y tecnologías virtuales como Bitcoin las convierten en un objetivo demasiado irresistible para que los ciberdelincuentes lo pasen por alto. En 2011 hemos observado un importante aumento del malware que ataca estas tecnologías. Veamos un ejemplo de malware diseñado específicamente para Bitcoin:

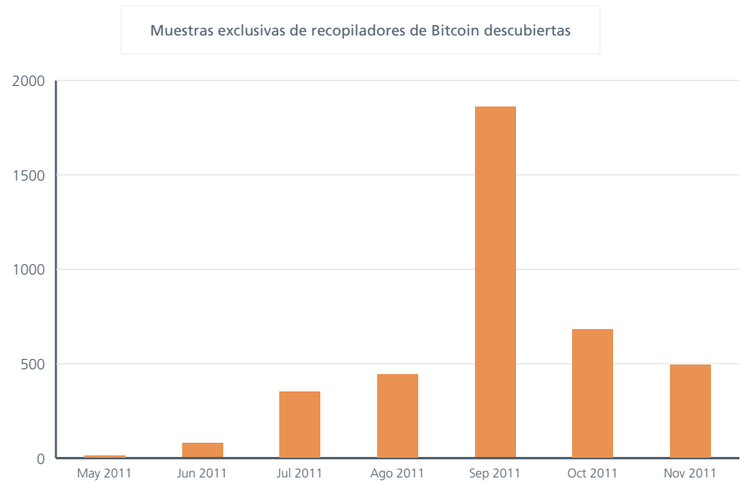


Figura 2: El robo (denominado "recopilación") de moneda virtual Bitcoin alcanzó su punto álgido en septiembre. Creemos que los timos aumentarán en 2012.

Pensamos que esta amenaza va a transformase en una industria distribuida de la ciberdelincuencia el año que viene, con spam, robo de datos, herramientas y redes de apoyo, así como otros servicios asociados dedicados exclusivamente a explotar las monedas virtuales. Está claro que los ciberdelincuentes han encontrado un sistema de pagos que se ajusta a sus necesidades.

## Ciberguerra

¿Será 2012 el año de la ciberguerra o simplemente el de la exhibición de las ciberarmas y su potencial? Aunque sin duda esperamos acertar con la segunda opción, el desarrollo de esta situación durante los últimos años hace pensar que una ciberguerra es prácticamente inevitable. Hemos observado el uso frecuente de "cibertécnicas" para complementar los métodos tradicionales de operaciones de inteligencia o espionaje, con acusaciones cruzadas de amigos y enemigos por igual. Resulta una forma muy barata de espiar, siempre deja un resquicio para una negación verosímil, no pone en riesgo vidas humanas y, lo más importante, parece muy efectiva. Lo que no hemos observado mucho es el uso de cibertécnicas como parte del arsenal de un conflicto armado. Hasta el momento, únicamente se ha visto a pequeña escala y con un nivel de sofisticación limitado, por ejemplo, en los ataques que se produjeron durante el conflicto de Georgia.

Pero ahora la situación ha cambiado. Muchos países se han dado cuenta del potencial devastador de los ciberataques contra infraestructuras críticas y de lo difícil que es defenderse contra ellos. Su potencial abre oportunidades para que pequeños países u organizaciones lancen ataques, en particular si esos países u organizaciones disponen de pocos objetivos que puedan ser contraatacados. El ataque de Stuxnet fue un suceso decisivo en muchos aspectos; uno de ellos fue dejar absolutamente claro para todos que la amenaza es real y revelar la magnitud de este tipo de ataques.

Estados Unidos sabe que probablemente sea el país más vulnerable, sobre todo debido a su enorme dependencia de la informática y de una ciberdefensa que básicamente protege únicamente las redes militares y de la Administración. Imagínese un ejército que únicamente se preocupara de proteger las bases militares y se olvidara del resto del país. Tras recibir numerosas críticas por la ausencia de una doctrina formal, el país ha acabado reaccionando.



En julio, se publicó "Department of Defense Strategy for Operating in Cyberspace" (Estrategia del Departamento de Defensa para operar en el ciberespacio)[2]. En el informe se incluye la "Iniciativa estratégica 1: El Departamento de Defensa declara oficialmente el ciberespacio como campo de operaciones tácticas para organizarse, formarse y equiparse de manera que pueda aprovechar todo el potencial del ciberespacio" (N. d. T.: traducción libre). Sin embargo, no encontrará en este documento un tema que de los abordados anteriormente: que los ciberataques podrían provocar contraataques si tienen un impacto suficiente. Por el contrario, el Departamento de Defensa está preparando una nueva doctrina para complementar la ciberestrategia que ofrece directrices concretas al equipo encargado de la ciberguerra. Aunque esa doctrina describe en qué circunstancias se podría considerar la posibilidad de una ciberrepresalia, esto aun queda muy lejos de la doctrina de "amenaza de aniquilación total" que ayudó al mundo a sobrevivir a la guerra fría.

En realidad no va a disuadir a nadie de lanzar un ataque, ya que se desconoce la posible respuesta por estar clasificada.

Según los informes, en la revolución de Libia se pensó en el uso de ciberarmas, sin embargo la idea no llegó a materializarse; nadie se atrevió a ser el primero en abrir la caja de Pandora. O tal vez no fuera un entorno con muchos objetivos que atacar. Por ahora, sin embargo, no hemos visto ninguna demostración pública de la capacidad de la ciberguerra ofensiva que tenga el potencial de disuadir a nadie. Cada vez se oyen más voces a favor de la desclasificación de esa información, por lo que esperamos ver algún tipo de demostración al respecto (más allá de mostrar a ministros de asuntos exteriores vídeos alarmantes de máquinas que dejan de funcionar). Una demostración eficaz tiene el potencial de crear una reacción en cadena, de forma que otros países demuestren que ellos también pueden utilizar los mismos recursos.

Esperamos que el próximo año se caracterice únicamente por las demostraciones y no por los efectos de una ciberguerra real.

## DNSSEC

DNSSEC (Domain Name System Security Extensions, Extensiones de seguridad del sistema de nombres de dominio) es una tecnología diseñada para proteger los servicios de resolución de nombres contra la falsificación y el envenenamiento de la caché mediante el uso de una "web de confianza" basada en criptografía de clave pública. El objetivo es impedir que un ordenador cliente se comunique de forma inadvertida con un host como consecuencia de un ataque de intermediario, que redirige el tráfico del servidor deseado (página web, correo electrónico, etc.) a otro servidor. Cuando se trata de proteger a los usuarios online y dificultar el trabajo a los hackers, se trata de una etapa extremadamente importante en la evolución de Internet.

Desafortunadamente, la tecnología DNSSEC también podría impedir a las autoridades falsificar y redirigir el tráfico de Internet destinado a los sitios web que trafican con software o imágenes ilegales. Para que un gobierno pudiera redirigir el tráfico, tendría que ser considerado una autoridad en los dominios de nivel raíz y éste es un nivel de confianza que otros órganos de gobierno dudarían en otorgar si supieran que el resultado iba a ser la supresión de contenido de Internet motivado por opiniones privadas de gobiernos extranjeros.

Las tentativas recientes de aprobar leyes para impedir el pago de propiedad intelectual se basan en el entendimiento actual de cómo funcionan los DNS hoy día y no en el funcionamiento de la tecnología DNSSEC en el futuro. Esta laguna puede generar nuevos requisitos legales a la hora de administrar la infraestructura de DNS actual, que puede no ser compatible con la infraestructura de DNSSEC. Si se implementan dichos requisitos, el proceso de actualización de la seguridad en nuestra infraestructura de DNS puede estancarse hasta que los comités encuentren un punto técnico intermedio entre la ley y la tecnología DNSSEC.

En un entorno en el que crece el interés de los órganos de gobierno en todo el mundo por establecer "un código de conducta" para el tráfico de Internet, pensamos que cada vez serán más los casos en los que las soluciones de futuro se vean dificultadas por las disputas legislativas sobre los problemas del pasado. El resultado es que probablemente la Internet del futuro se parecerá a la Internet del pasado durante más tiempo del que nosotros, los expertos en seguridad, desearíamos.

## El spam se "legaliza"

Durante los últimos cuatro años, hemos observado una mayor concienciación y colaboración internacional en la lucha contra el spam asociado a las redes de bots. Esta cooperación se ha traducido en el desmantelamiento de varias infraestructuras de primera línea, esenciales para el control de las redes de bots (como el caso del proveedor de servicios de Internet McColo), el alojamiento de dominios de spam (Glavmed) o el procesamiento de tarjetas de crédito relacionado con medicamentos falsos. Incluso se han producido demandas contra grandes corporaciones de Internet que ofrecían medios publicitarios para empresas ilegales. Estas acciones han dado como resultado un enorme descenso en los volúmenes de spam a nivel mundial desde su momento álgido a mediados de 2009, así como un importante aumento del coste en el mercado negro de venta de spam a través de redes de bots.

Aunque estas medidas no representan en absoluto el fin de todo el spam (tal y como auguraban algunos profetas tecnológicos), sin duda han cambiado el panorama. Si echamos un vistazo al panorama actual, observamos que cada vez se envía más spam no solicitado no ya desde hosts infectados por redes de bots, sino desde las propias agencias de publicidad "legítimas" reales, que utilizan técnicas muy criticadas por la comunidad antispam. Esas agencias han conseguido que las direcciones de correo electrónico de los usuarios entren en listas publicitarias sin su conocimiento o consentimiento. Entre estas técnicas se pueden citar la compra descarada de listas de correo electrónico que, según la publicidad, ofrecen usuarios que ya han dado su consentimiento para recibir publicidad (una afirmación que resulta difícilmente creíble), el proceso de "e-pending" (recopilación de direcciones de correo electrónico a través de algoritmos que determinan que el usuario aceptaría la publicidad si se le ofreciera la opción de decidir, olvidando preguntar y añadiéndole a la lista sin más), la adquisición de bases de datos de clientes a empresas que cierran, ignorando cualquier política de privacidad en vigor, o la "asociación" con otras agencias de publicidad o proveedores de listas de correo para bombardear a los miembros de dichas listas con publicidad.

Las agencias de publicidad que hacen esto saben que están enviando spam y emplean las mismas técnicas que los operadores de redes de bots para evitar ser detectadas. Todos los días se registran miles de dominios de correo electrónico nuevos valiéndose de la privacidad que concede whois para impedir la identificación del propietario, y se activan miles de direcciones IP en las subredes de proveedores de alojamiento para que un cañón de spam inunde durante algunas horas los buzones de entrada con mensajes de correo mal formateados, llenos de errores de ortografía y con una gramática desastrosa. La mayoría de estos mensajes contienen un vínculo para eliminar la dirección de la lista, sin embargo, para lo único que sirve es para informar a los creadores de spam de que su dirección de correo electrónico está activa y que ha leído el mensaje que le han enviado. Además, suele haber una dirección de correo ordinario para solicitar que le eliminen de la lista. Sin embargo, una simple búsqueda en Internet revela que se trata de una choza en medio de alguna región deshabitada de Canadá o en una árida región en medio del desierto de Arizona. Ha habido algunos casos en los que una sola dirección de correo electrónico ha recibido más de 9.000 mensajes de spam prácticamente idénticos en un día, ensalzando los beneficios para la salud del uso de una conocida pulsera magnética.

Estas prácticas publicitarias corruptas cuentan con el respaldo de la ley. La ley antispam de EE. UU. (CAN-SPAM Act) está tan edulcorada que no se exige a los anunciantes recibir el consentimiento para enviar la publicidad. Visto que la publicidad es un negocio tan rentable, y tan influenciado por los lobbies, resulta extremadamente improbable que se produzcan cambios significativos en las prácticas de administración de listas de correo o que vayan a aplicarse a corto plazo importantes sanciones por comportamientos indebidos.

Con este panorama, pensamos que el spam "legal" seguirá creciendo a un ritmo alarmante. Resulta más barato y menos arriesgado enviar spam a particulares a través de empresas de publicidad que hacerlo mediante hosts infectados por redes de bots. Este tipo de actividad, conocida como snowshoe spamming (literalmente "spam de raqueta de nieve"), ha crecido tanto que en el momento de redactar este documento los 10 principales asuntos de correo electrónico incluyen un spam de notificación de estado de entrega, un spam de Rolex falsos relacionados con redes de bots, un timo de abuso de confianza y siete mensajes de spam de tipo snowshoe. Este tipo de tráfico continuará creciendo a mayor ritmo que el phishing y que los timos de abuso de confianza, mientras que el spam relacionado con redes de bots seguirá disminuyendo debido a que los dueños de bots encontrarán formas mejores y más seguras de enriquecerse a través de sus ejércitos de ordenadores infectados. Es solo cuestión de tiempo que la mayor parte del volumen mundial de spam provenga de entidades con comportamientos discutibles pero "legales".



## Amenazas para los dispositivos móviles

Durante los últimos dos años, hemos observado un aumento de los ataques dirigidos a smartphones y a dispositivos móviles. Nos hemos encontrado con rootkits, redes de bots y otros tipos de malware. Los agresores han pasado del uso de malware destructivo básico al empleo de spyware y malware que les reporta dinero. Les hemos visto aprovechar vulnerabilidades para eludir las protecciones de los sistemas y conseguir mayor control sobre los dispositivos móviles. En 2012 estamos convencidos de que los agresores seguirán con su actividad y mejorarán sus ataques. También prevemos que los ataques se centren más en las operaciones bancarias que se realizan mediante dispositivos móviles.

### Redes de bots + rootkits = problemas de bajo nivel

En los ordenadores, los rootkits y las redes de bots distribuyen publicidad y generan dinero a cuenta de sus víctimas. En los dispositivos móviles, hemos observado un uso similar de estos tipos de malware. Los rootkits permiten la instalación de software o spyware adicional, y las redes de bots pueden provocar clics en anuncios o enviar mensajes de texto con tarifa premium.

Hemos encontrado variantes para dispositivos móviles de familias de malware conocidas, como Android/DrdDream, Android/DrdDreamLite y Android/Geinimi, así como Android/Toplank y Android/DroidKungFu. Algunos de estos tipos de malware han utilizado ataques a la raíz (desarrollados originalmente para que los clientes desbloqueen sus teléfonos) para conseguir acceso y hacerse con el control de los teléfonos de las víctimas. El año que viene, los desarrolladores e investigadores crearán nuevos métodos para desbloquear los teléfonos (lo que se conoce como rooting) y veremos cómo los creadores de malware adaptan las lecciones aprendidas en el desarrollo de malware para PC, con el fin de lanzar ataques que saquen mayor provecho del hardware de los dispositivos móviles. El malware basado en PC se mueve a niveles "más bajos" del sistema operativo para aprovechar mejor el hardware y, en nuestra opinión, el malware para dispositivos móviles seguirá el mismo camino.

Los bootkits, o malware que sustituye o ignora el inicio del sistema, también amenaza a los dispositivos móviles. Aunque el desbloqueo del teléfono o del lector electrónico le ofrece al usuario el acceso a un mayor número de funciones, o incluso la sustitución del sistema operativo, también puede permitir a los agresores cargar sus propios sistemas operativos modificados. Mientras que un rootkit para móviles únicamente modificaría el sistema operativo existente para evitar ser detectado, un bootkit puede facilitar al agresor un control mucho mayor de un dispositivo.

Por ejemplo, el toolkit de pruebas de penetración para móviles "Weapon of Mass Destruction" (literalmente, armas de destrucción masiva) se ejecuta en teléfonos antiguos con Windows Mobile. Este toolkit se instala de forma autónoma mediante herramientas desarrolladas para cargar Linux en teléfonos con Windows Mobile y permite a los usuarios arrancar con el sistema operativo original. Los agresores ya han utilizado rootkits antiguos para ocultarse; a medida que se desarrollen nuevos exploits, los agresores acabarán siendo capaces de instalar su propio firmware personalizado.

### Ataques contra servicios bancarios con dispositivos móviles

Los usuarios de PC han sufrido ataques de ciberdelincuentes que utilizaban los kits Zeus y SpyEye para robar dinero de cuentas bancarias online. Tanto Zeus como SpyEye han comenzado a utilizar aplicaciones para dispositivos móviles como ayuda para sortear la autenticación de dos factores y obtener acceso al dinero de las víctimas.

Zitmo (Zeus-in-the-mobile, o Zeus para móviles) y Spitmo (SpyEye-in-the-mobile, o SpyEye para móviles) son dos familias de spyware para móviles que reenvían mensajes SMS a los agresores. El uso de este spyware obligaba a los agresores a iniciar una sesión manualmente para robar el dinero de los usuarios.

En julio pasado, el investigador de seguridad Ryan Sherstobitoff explicaba cómo podrían rastrearse las transacciones realizadas por delincuentes mediante Zeus y SpyEye, a la vista de que se trataba de transacciones totalmente diferentes a las realizadas por los usuarios legítimos. El mes pasado mostró cómo se habían adaptado los delincuentes. Ahora pueden robar dinero a sus víctimas de forma programática mientras sus víctimas siguen conectadas. Esto contribuye a que las transacciones de los delincuentes parezcan proceder de usuarios legítimos. Además, al añadir un retraso, las hace parecer llevadas a cabo por una persona real. Los agresores se han adaptado rápidamente a todos los cambios realizados para proteger las operaciones bancarias en ordenadores. A medida que aumente la frecuencia de uso de dispositivos móviles para realizar operaciones bancarias, veremos a los agresores olvidarse de los PC y dirigir sus esfuerzos a las aplicaciones para la banca online en los móviles. Cada vez más usuarios gestionan sus finanzas a través de los móviles por lo que prevemos un aumento de prevalencia de los ataques que aprovechan este tipo de técnica programática.

## Certificados falsos

Tendemos a creer en los archivos y documentos cuando están firmados digitalmente debido a nuestra confianza en las firmas digitales y en las autoridades de certificados de las que proceden. Muchos sistemas de listas blancas y de control de aplicaciones dependen de firmas digitales válidas. Estas soluciones nos permiten aplicar directivas y controles a servicios, aplicaciones e incluso archivos que llevan una firma digital válida. La navegación web segura y las transacciones comerciales online seguras también se basan en firmas digitales de confianza. Las autoridades de certificación y sus certificados básicamente dicen al sistema operativo: "puede confiar en mí porque estoy validado y certificado".

Pero con tanta confianza, ¿qué pasa si nos encontramos con certificados digitales falsos o no fiables? O lo que es más, ¿cuáles son las implicaciones cuando una autoridad de certificación está en riesgo? Los certificados digitales nos conceden un cierto nivel de confianza en un archivo, proceso o transacción. Mediante la generación o puesta en circulación de certificados falsos o no fiables, los agresores pueden llevar a cabo ataques prácticamente indetectables. En el navegador, esto permitiría a un agresor ejecutar ataques de intermediario: tráfico que debería estar cifrado e invisible para el agresor puede ahora verse como texto puro, ya que éste dispone de la "clave". En el host, el software de seguridad ignorará un archivo firmado con una clave válida, ya que ahora aparece en la lista blanca: se autoriza su acceso gracias al certificado que presenta.

Amenazas recientes, como Stuxnet y Duqu, utilizaron certificados falsos para evitar ser detectadas, obteniendo óptimos resultados. Aunque no es la primera vez que hemos observado este comportamiento (ya lo vimos en antivirus falsos, en algunas variantes de Zeus, Conficker e incluso en algunos tipos de malware para Symbian antiguos), pensamos que esta tendencia aumentará en 2012 y en años sucesivos.

La mayor amenaza, que sería el ataque a autoridades de certificación para generar certificados falsos, también supone una preocupación para el futuro. Este tipo de ataque permitiría a un agresor crear varias claves, que podrían utilizarse en distintos escenarios basados en la Web y en el host, acabando con buena parte de la confianza generada en un sistema operativo. Estamos muy preocupados por las implicaciones del uso a gran escala de los certificados falsos en las tecnologías de listas blancas y de control de aplicaciones que utilizan estos certificados. DigiNotar, una autoridad de certificación holandesa, se declaró en bancarrota tras una brecha de seguridad que provocó la emisión de certificados fraudulentos. ¿Fue este ataque el desencadenante de la caída? Las investigaciones han demostrado que se emitieron un total de 531 certificados fraudulentos desde DigiNotar. Es probable que la caída de esta empresa sea únicamente la primera de las brechas que vamos a descubrir en este sector. Ahora debemos determinar el alcance de los daños y de la pérdida de confianza.

Un ataque a gran escala contra las autoridades de certificación y el uso generalizado de certificados fraudulentos, aunque válidos, tienen ramificaciones para la infraestructura de clave pública, la navegación segura, las transacciones, así como para las tecnologías basadas en hosts, como las listas blancas y el control de aplicaciones. Sacar provecho de nuestra confianza en este sistema ofrece una gran ventaja a los agresores, por lo que pensamos que se centrarán en esta área.

## Avances en los sistemas operativos

La protección de los datos es un continuo toma y daca, con medidas y contramedidas aplicadas en dosis similares. Los agresores crean código malicioso y nosotros contraatacamos. Los proveedores de sistemas operativos incorporan la seguridad en el núcleo de los sistemas operativos y los agresores encuentran la forma de eludirla. Esto es un componente intrínseco de la evolución de las amenazas y no va a cambiar. Pero, ¿provocarán los avances incorporados por el sector de la seguridad de la información y los proveedores de sistemas operativos el abandono de los sistemas operativos por parte de los agresores para centrarse directamente en el hardware?

Las últimas versiones de Windows han incluido protección contra la ejecución de datos, así como la aleatorización del esquema del espacio de direcciones. Estos métodos de seguridad complican la tarea de los agresores a la hora de comprometer el ordenador de una víctima. Asimismo, en los últimos años las tecnologías de cifrado han contribuido a mejorar de forma importante la protección de los sistemas operativos. Como en la mayoría de las medidas internas de seguridad del sistema operativo, los agresores encuentran rápidamente formas de eludirlas. En el próximo lanzamiento de Windows 8, Microsoft incluirá un gran número de funciones de seguridad nuevas: almacenamiento de contraseñas seguras, funciones de inicio seguras, defensas antimalware e incluso funciones mejoradas de reputación. ¿Hacia dónde llevará a los agresores esta nueva arquitectura de seguridad?

La respuesta es "dentro y fuera": dentro del hardware y fuera del sistema operativo.



Durante los últimos siete años, los laboratorios McAfee Labs han sido testigos de grandes avances en rootkits y bootkis por parte de agresores y creadores de malware. Los rookits se utilizan para socavar tanto el sistema operativo como el software de seguridad, mientras que los bootkits atacan el cifrado y pueden sustituir cargadores de arranque legítimos. Se trata de técnicas avanzadas para interceptar las claves de cifrado y las contraseñas, e incluso socavar las defensas de firmas de controladores que emplean algunos sistemas operativos.

No resulta fácil atacar el hardware y el firmware, pero si se consigue con éxito, ofrece a los agresores la posibilidad de crear "imágenes" de malware persistente en tarjetas de red, en discos duros e incluso en la BIOS del sistema. Pensamos que en 2012 y en años sucesivos aumentarán los exploits para hardware y firmware, y sus ataques relacionados con el mundo real.

Aunque Windows 8 aún no ha salido al mercado, los investigadores ya han conseguido demostrar cómo usar la BIOS heredada para socavar las mejoras en la función de seguridad del cargador de arranque. Con los nuevos desarrollos en torno a las especificaciones de interfaz de firmware extensible unificado de Intel (diseñado como interfaz de software entre el sistema operativo y el firmware para favorecer un arranque seguro y sustituir la BIOS heredada), pensamos que cada vez más los agresores dedicarán su tiempo a investigar las posibilidades de eludirlas en los próximos años.

Observaremos con interés cómo utilizan los agresores estas funciones de bajo nivel para el control de las redes de bots, puede que migrando sus funciones de control a funciones de procesador gráfico, la BIOS o el registro de arranque maestro. Al mismo tiempo, a medida que las implementaciones de red avancen en la línea de los sistemas operativos, pensamos que los agresores aprovecharán los nuevos estándares de protocolos, como IPv6.

A pesar de nuestros esfuerzos por frustrar sus ambiciones, los agresores ven claramente las ventajas y el poder de atacar el hardware y de alejarse de los ataques tradicionales al sistema operativo.

## Acerca de los autores

Este informe ha sido preparado y redactado por Zheng Bu, Toralv Dirro, Paula Greve, David Marcus, François Paget, Ryan Permeh, Craig Schmugar, Jimmy Shah, Peter Szor, Guilherme Venere y Adam Wosotowsky, de los laboratorios McAfee Labs.

## Acerca de los laboratorios McAfee Labs

Los laboratorios McAfee Labs son el equipo de investigación a nivel mundial de McAfee, Inc. Con la única organización de investigación dedicada a todos los vectores de amenazas —malware, Web, correo electrónico, redes y vulnerabilidades—, McAfee Labs reúne información a través de millones de sensores y de su servicio basado en la Web, McAfee Global Threat Intelligence™. El equipo de 350 investigadores multidisciplinares de los laboratorios McAfee Labs, que trabajan en más de 30 países, sigue en tiempo real la gama completa de amenazas, identificando vulnerabilidades de aplicaciones, analizando y correlacionando riesgos, y activando soluciones instantáneas para proteger a las empresas y al público en general.

## Acerca de McAfee

McAfee, empresa subsidiaria de propiedad total de Intel Corporation (NASDAQ:INTC), es líder en tecnología de seguridad. McAfee tiene el firme compromiso de afrontar los más importantes retos de seguridad. La compañía proporciona servicios y soluciones probados y proactivos que ayudan a proteger redes, dispositivos móviles y sistemas en todo el mundo, permitiendo a los usuarios conectarse a Internet, navegar por la Web y realizar compras online de forma más segura. Gracias a la tecnología Global Threat Intelligence (Inteligencia Global de Amenazas), McAfee proporciona protección en tiempo real mediante sus soluciones de seguridad, permitiendo a las empresas, usuarios particulares, organismos públicos y proveedores de servicios cumplir con la normativa, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar cualquier tipo de amenaza que pueda poner en peligro su seguridad. En McAfee enfocamos todos nuestros esfuerzos en la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes. http://www.mcafee.com/es

[1] https://blogs.mcafee.com/mcafee-labs/stuxnet-update
[2] Lea la versión para el público en http://www.defense.gov/news/d20110714cyber.pdf

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es


40302rpt_threat-predictions_1211_fnl_ETMG