

Informe de McAfee sobre amenazas: Cuarto trimestre de 2011

McAfee Labs™

Índice

Amenazas para los dispositivos móviles	4
Malware	5
Amenazas que se propagan a través de mensajería	10
Distribución de las redes de bots	11
La ingeniería social en el mundo	15
Fugas de datos y ataques a redes	16
Amenazas Web	17
Ciberdelincuencia	20
Herramientas de crimeware	20
Principales acontecimientos	20
Acciones contra los ciberdelincuentes	20
Hactivismo	21
Ciberescaramuzas	22
Acerca de los autores	23
Acerca de los laboratorios McAfee Labs	23
McAfee, Inc.	23

El panorama mundial de amenazas ha sufrido algunas fluctuaciones importantes durante el último trimestre de 2011. En cierta forma, constituye un microcosmos representativo de un año marcado por algunos de los eventos más notables que hemos observado hasta la fecha. Con ataques de gran repercusión, como el de Duqu¹, y el aumento del hacktivismo, encarnado por Anonymous, 2011 ha sido un año realmente activo para el sector de la seguridad informática. La creciente atención recibida por los sistemas de control industrial, junto al aumento de actividades hacktivistas, pueden presagiar un año 2012 agitado.

Cuando examinamos el trimestre, destacan algunos hechos notables. Excepto el malware para móviles, casi todas las categorías de malware y de spam han experimentado descensos en su crecimiento. El malware para móviles, sin embargo, ha aumentado durante el último trimestre y ha marcado el año de más actividad hasta la fecha. Una vez más, los desarrolladores de malware han elegido Android como objetivo principal. Y, aunque la producción de nuevo malware se ha ralentizado, el malware total que hemos capturado ha conseguido batir el récord de 75 millones, confirmando las previsiones de McAfee Labs a finales de 2010.

A pesar de que las cifras de spam caen en todo el mundo (en algunas regiones se registran los niveles más bajos en varios años), seguimos observando una gran diversidad y especificidad en las líneas del asunto. Los timadores son expertos en descubrir qué cebos y asuntos funcionan tanto a nivel global como local. Esta táctica no ha cambiado. Paradójicamente, el crecimiento de las redes de bots ha continuado este trimestre. (Normalmente las redes de bots envían spam; por lo tanto, un crecimiento de las redes de bots indicaría un incremento del spam. Pero este no ha sido el caso). Hemos observado un salto considerable en detecciones de redes de bots en todo el mundo, con Grum a la cabeza.

Este trimestre, Estados Unidos ha sido de nuevo el país que ha albergado más contenido web malicioso y los sitios web con mala reputación registran un aumento generalizado. El número de URL maliciosas activas ha aumentado y el número de sitios web de malware nuevo casi se ha duplicado en los tres últimos meses de 2011. La Web continúa siendo un lugar peligroso para los internautas mal informados e insuficientemente protegidos.

En este informe sobre amenazas hemos incluido un análisis de dos nuevos dominios: fugas de datos y de información de bases de datos, por un lado, y ataques basados en la red, por otro. El número de fugas de datos comunicadas ha aumentado durante el trimestre y las llamadas a procedimientos remotos, inyección SQL y secuencias de comandos entre sitios siguen contándose entre los métodos más utilizados para los asaltos a la red.

Algunas de las acciones hacktivistas y ciberdelitos más peligrosos del año han ocurrido durante este trimestre, lo que podría ser un augurio para el 2012. Igualmente, cabe destacar los progresos llevados a cabo por los ciberdelincuentes en sus toolkits, así como el aumento de sucesos en los que se sospecha la participación de gobiernos nacionales. Un dato positivo en el panorama de las amenazas, sin embargo, ha sido el número de arrestos y acciones judiciales contra los ciberdelincuentes.

Como siempre, las amenazas siguen evolucionando y los agresores siguen superando los límites. Por lo tanto, no debemos bajar la guardia.

Amenazas para los dispositivos móviles

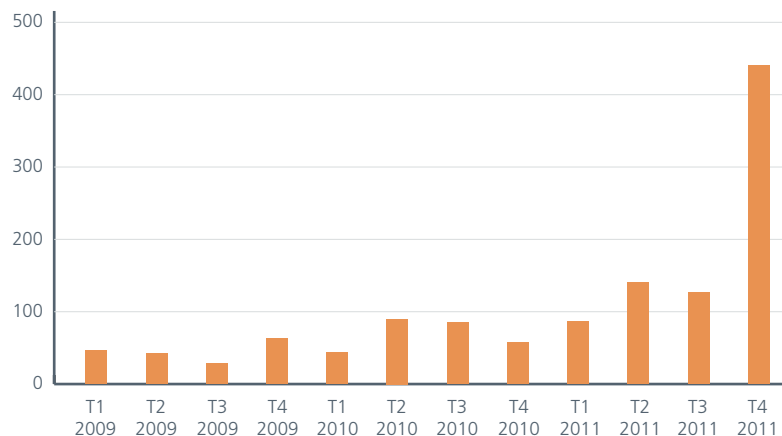
Este trimestre hemos asistido a la confirmación de Android como objetivo principal de los creadores de malware para dispositivos móviles. Al igual que los PC, las plataformas móviles son víctimas del spyware y del adware comercial. En total, el año 2011 en general y el cuarto trimestre en particular han batido todos los récords en lo que a producción de malware para dispositivos móviles se refiere. Pensamos que esta tendencia continuará durante algún tiempo.

Buena parte del malware para Android observado fueron troyanos que envían SMS con fines lucrativos. Los ciberdelincuentes utilizan estos troyanos para piratear los teléfonos y enviar mensajes que cuestan dinero a sus propietarios. Hemos identificado una interesante variante, Android/Arspam, que utiliza esta técnica con fines hacktivistas. En lugar de enviar la aplicación a Android Market o a otra tienda de aplicaciones online, los autores cargaban el malware en una serie de foros de discusión en árabe. (El troyano es una versión modificada de una aplicación de calendario de oraciones musulmán). Esta variante envía mensajes SMS relacionados con una figura clave cuya muerte desencadenó el inicio de la revolución en Túnez. Los miembros de los foros de discusión, en lugar de reformatear sus teléfonos para eliminar el malware, reenviaban el troyano a otros individuos de ideas afines y propagaban el mensaje.

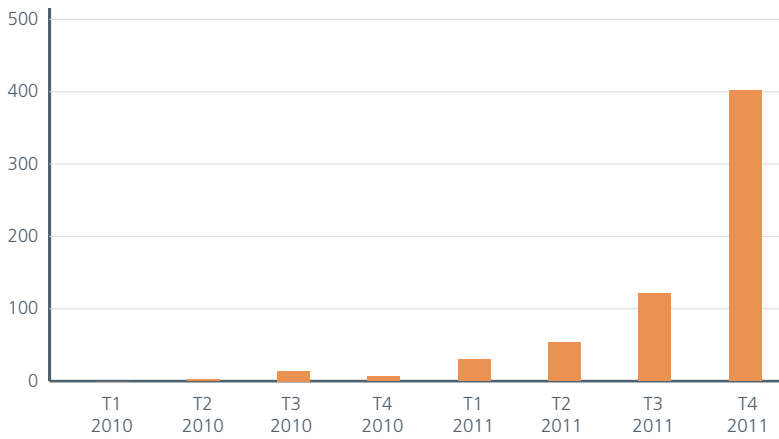
Piraterar dispositivos Android se ha convertido en una operación más sencilla gracias a la disponibilidad de aplicaciones que combinan varios exploits. Los usuarios pueden instalar una aplicación, hacer clic en un botón y desbloquear sus teléfonos. Esto significa que los agresores también pueden hacer lo mismo, incluyendo estos exploits de desbloqueo en el malware (en dispositivos Android al desbloqueo se le conoce en inglés como *rooting*, ya que se trata de desbloquear el teléfono para obtener acceso raíz, o *root*). Esta técnica se utiliza desde hace mucho tiempo en el mundo del malware para PC y constituye un ejemplo perfecto de cómo trasladar lo que funciona de una plataforma a otra. Esta es la razón por la que McAfee ha incluido reglas de detección para una serie de aplicaciones de desbloqueo fáciles de conseguir y sus exploits.

Los ciberdelincuentes no son los únicos que utilizan los exploits. Los profesionales encargados de las pruebas de penetración para comprobar la seguridad informática han descubierto la utilidad de los dispositivos móviles para llevar a cabo su trabajo. Hemos identificado una aplicación Android comercial que permite, durante una prueba de penetración, atacar un ordenador con Windows desde un teléfono o un tablet. Hasta ahora, los probadores siempre han necesitado llevar un portátil o netbook para su trabajo; ahora pueden utilizar dispositivos más discretos para acceder a la red de un cliente y llevar a cabo ataques. Puesto que los agresores también pueden utilizar esta herramienta, la hemos clasificado como programa potencialmente no deseado con el nombre Android/AnitTool.

Total de muestras de malware para dispositivos móviles



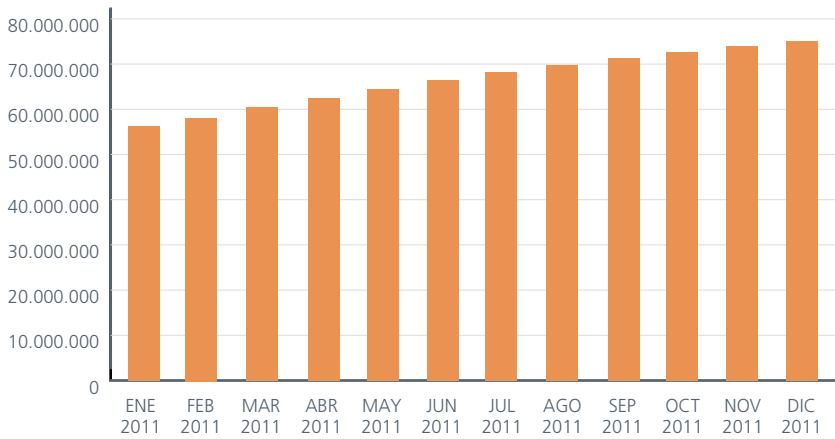
Malware para Android por trimestre

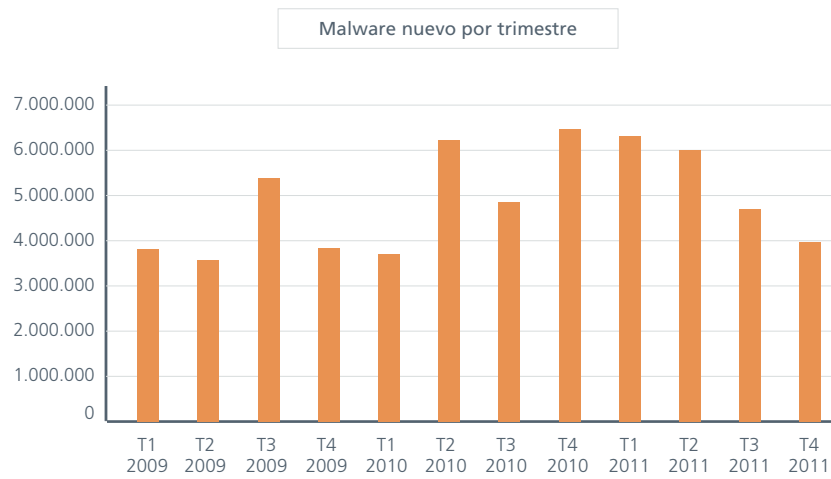


Malware

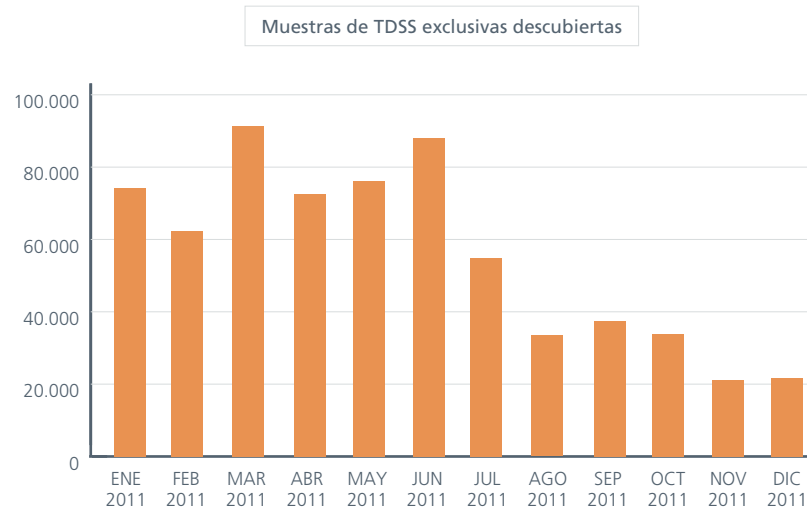
El crecimiento total del malware basado en PC siguió descendiendo durante el trimestre y ha alcanzado un nivel significativamente inferior respecto al mismo período del año anterior. Pero no lance las campanas al vuelo. El número acumulado de muestras de malware exclusivas de nuestra colección todavía supera la barrera de los 75 millones, tal y como pronosticábamos en el último informe. ¿Ha alcanzado el malware masivo una masa crítica? Es difícil responder con exactitud, pero, a medida que aumenta la adopción de la informática móvil, podemos asumir sin temor a equivocarnos que las amenazas también realizarán esta transición.

Total de muestras de malware en la base de datos

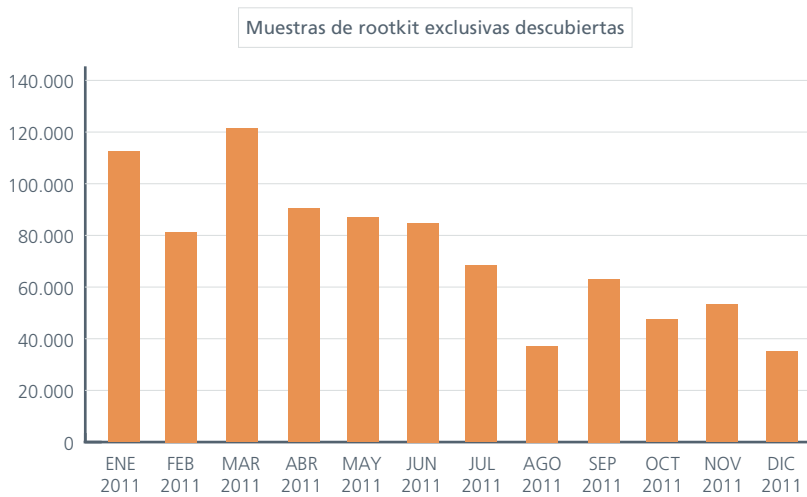
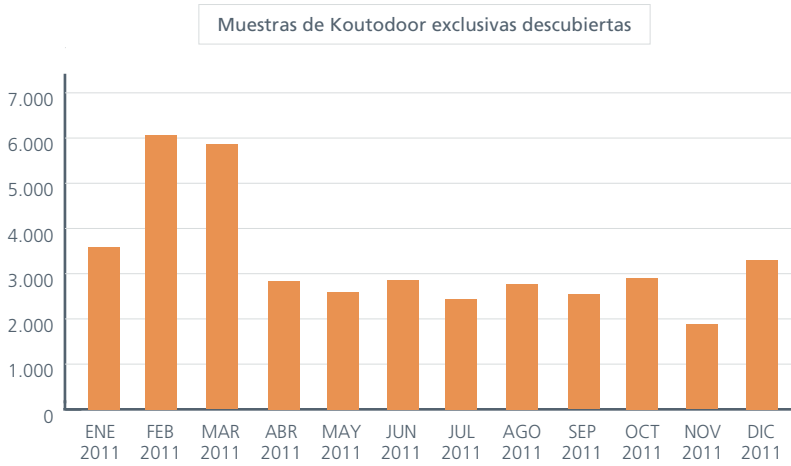




A pesar de haber tenido una incidencia menor este trimestre, la familia de rootkits TDSS sigue representando más de la mitad de todos los rootkits. Los rootkits, o malware invisible, constituyen una de las categorías de malware más virulentas. Tienen una enorme influencia en prácticamente todas las otras categorías de malware. Están diseñados para eludir la detección y "vivir" en un sistema durante períodos prolongados. Como observamos en el siguiente gráfico, el número de rootkits TDSS sigue en aumento.

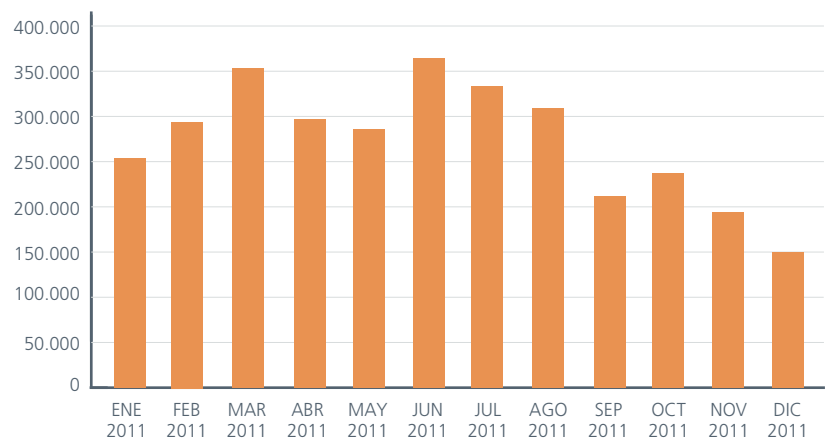


En otros casos las cifras se estancan, como en el caso de Koutodoor. Además, hemos constatado una disminución de la frecuencia de aparición de rootkits. Sin embargo, no baje la guardia.

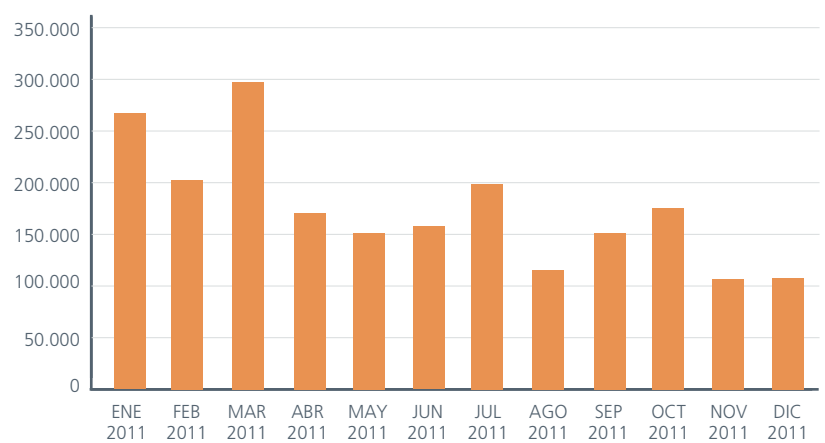


Cada trimestre vigilamos también la aparición de soluciones antivirus falsas (también llamadas alertas falsas o software de seguridad falso), así como de software autoejecutable y troyanos ladrones de contraseñas. Las soluciones antivirus falsas descendieron considerablemente respecto al trimestre anterior, pero siguen siendo una de las formas de malware más populares. Los autoejecutables y los troyanos bancarios ladrones de contraseñas experimentaron un ligero descenso.

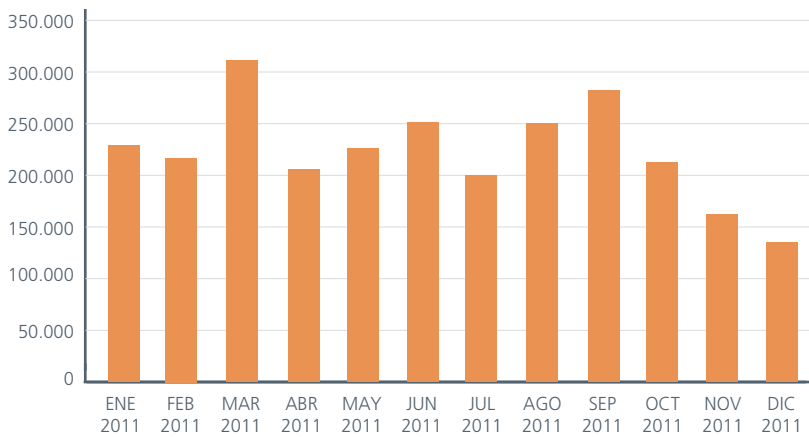
Muestras de soluciones antivirus falsas exclusivas descubiertas



Muestras de autoejecutables exclusivas descubiertas

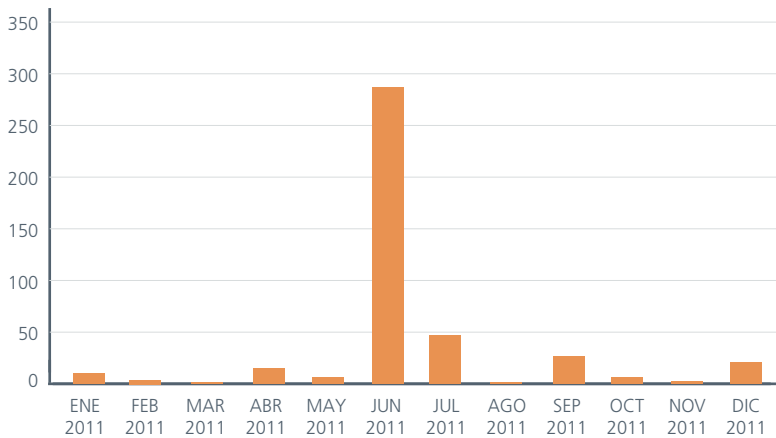


Muestras de ladrones de contraseñas exclusivas descubiertas

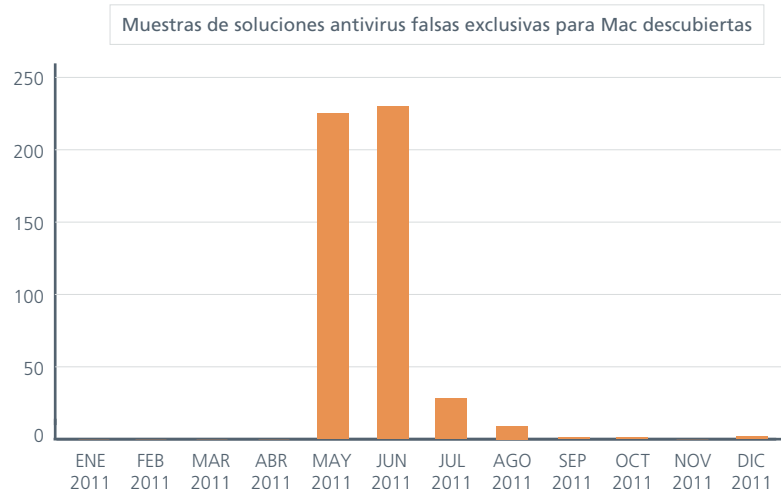


El malware para Mac experimentó un pronunciado repunte durante el segundo trimestre, pero ha permanecido estable desde entonces. Como siempre, si comparamos el crecimiento global del malware para Mac con las cifras para PC, la amenaza para los sistemas Mac parece inofensiva, pero siempre es conveniente proteger su sistema, incluso si se trata de un MacBook Air.

Muestras para Mac OS exclusivas descubiertas



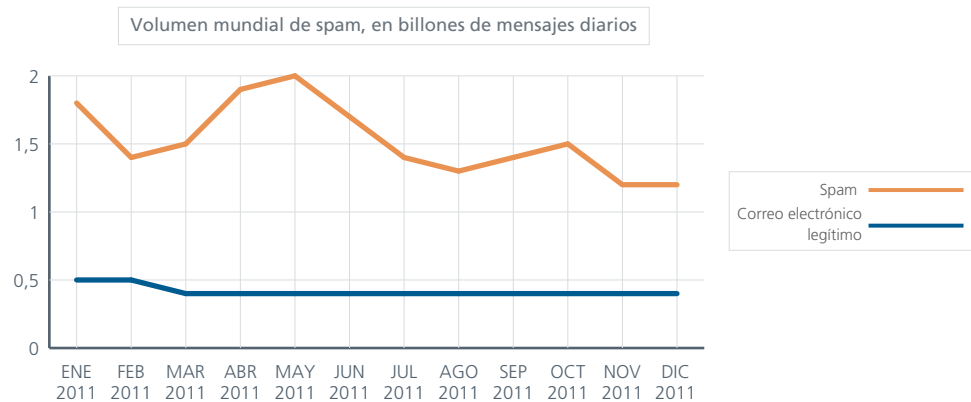
A diferencia del repunte del segundo trimestre, este trimestre las soluciones antivirus falsas para Mac son una vez más prácticamente inexistentes.



Aunque hemos observado muy poca actividad contra los Mac, cualquier sistema operativo puede convertirse en objetivo.

Amenazas que se propagan a través de mensajería

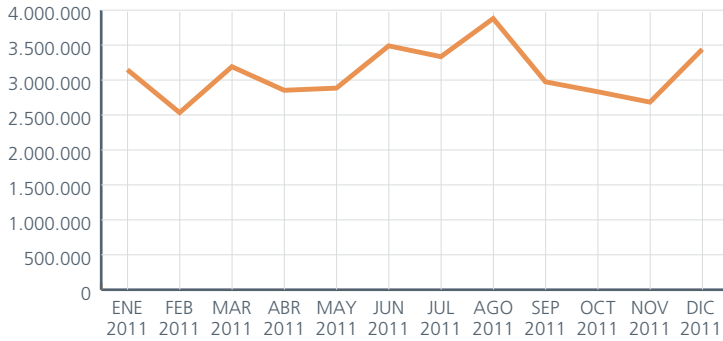
A finales de 2011, las cifras del spam a nivel mundial alcanzaron su nivel más bajo en años. Este fenómeno se observa en países como Brasil, Argentina, el Reino Unido, Turquía y Corea del Sur, todos a su nivel más bajo desde 2007. Durante este periodo, Estados Unidos y Alemania, por citar dos ejemplos, experimentaron un ligero aumento. A pesar del descenso en los niveles globales, el phishing dirigido (o *spearphishing*) y el spam son tan peligrosos como siempre. No olvide que, aunque la incidencia es menor, el nivel y la sofisticación de las amenazas siguen siendo altos. Hace algunos años, los remitentes de spam enviaban mensajes a numerosas direcciones generadas de forma aleatoria, pero en la actualidad, las listas de direcciones son mucho más precisas.



Distribución de las redes de bots

El crecimiento global de las redes de bots ha repuntado en noviembre y diciembre tras la bajada registrada desde el mes de agosto. Brasil, Colombia, la India, España y Estados Unidos han experimentado fuertes aumentos. Por el contrario, en Alemania, Indonesia y Rusia la tendencia ha sido a la baja.

Infecciones globales por redes de bots detectadas mensualmente

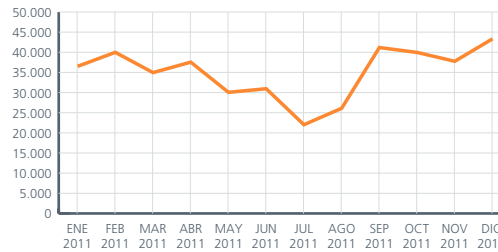


Nuevos remitentes de redes de bots por país

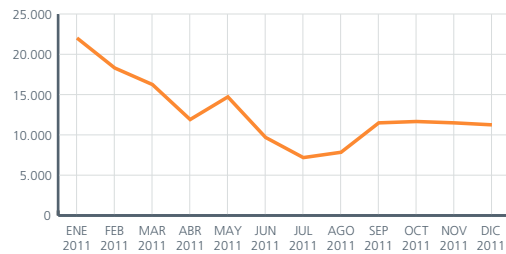
Alemania



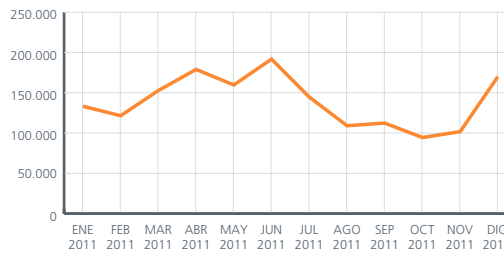
Argentina



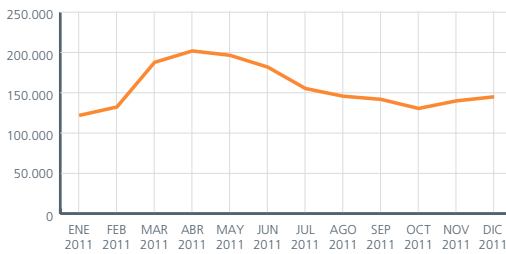
Australia



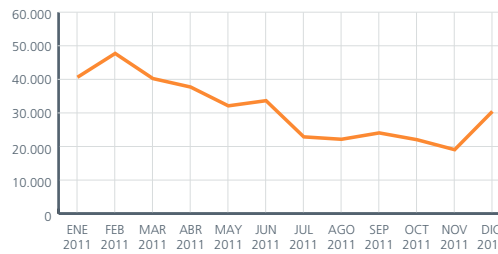
Brasil



China

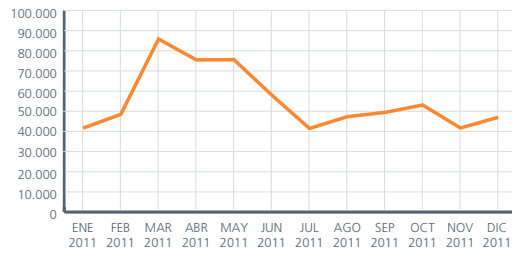


Colombia

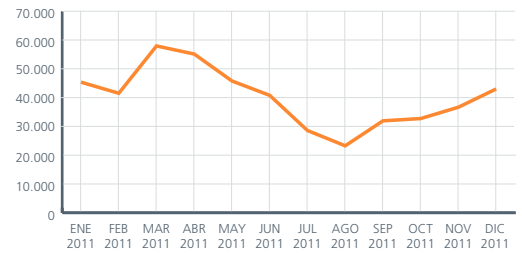


Nuevos remitentes de redes de bots por país

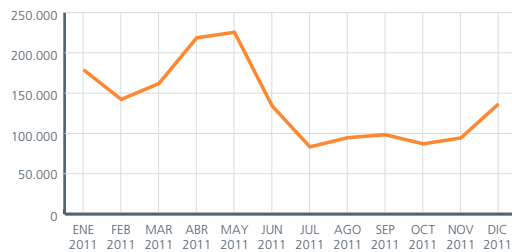
Corea del Sur



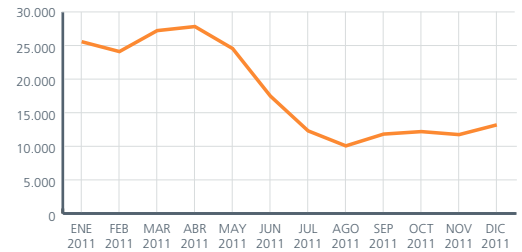
España



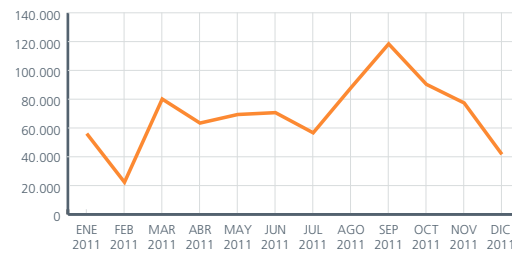
Estados Unidos



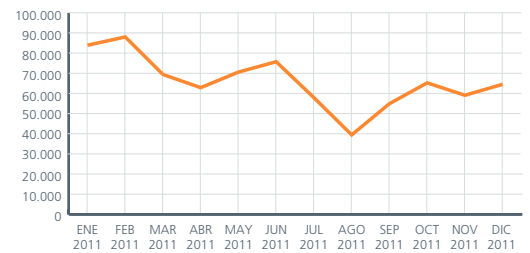
Francia



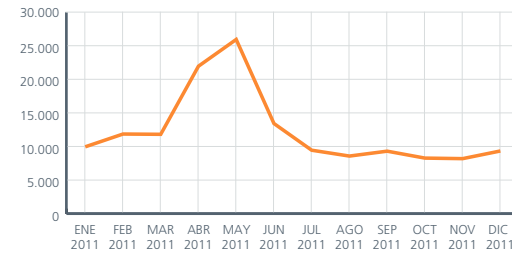
Indonesia



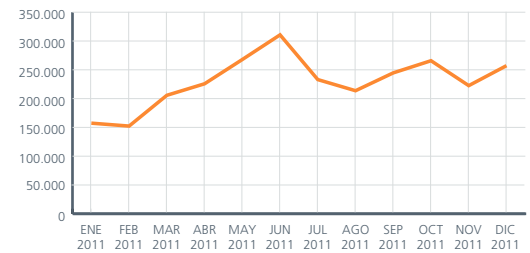
Italia



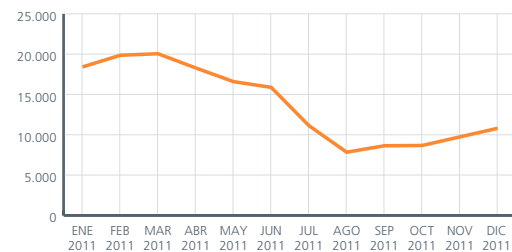
Japón



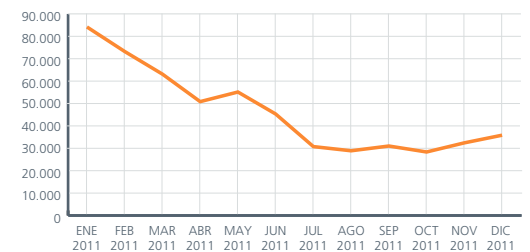
La India



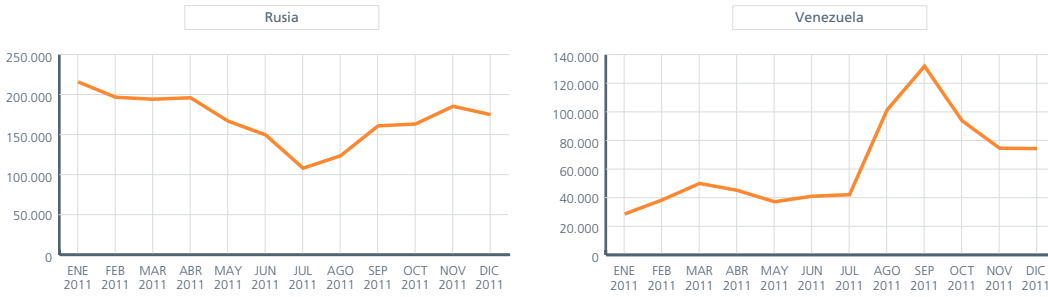
Portugal



Reino Unido

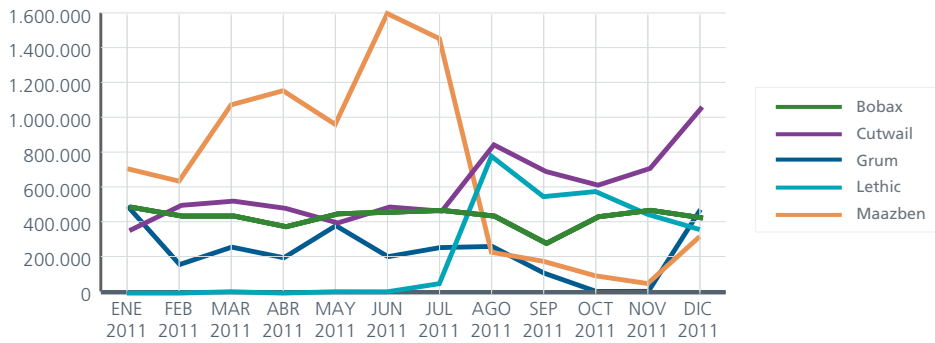


Nuevos remitentes de redes de bots por país



En el mundo de las redes de bots, los protagonistas no han cambiado mucho. Bobax aumentó en octubre y noviembre antes de caer en diciembre. Lethic continuó su regresión tras el repunte experimentado en el último trimestre. Cutwail y Maazben registraron un importante aumento en diciembre, pero el cambio más espectacular del trimestre hay que atribuirlo a Grum que, tras un largo declive, ha recuperado su nivel de hace un año.

Infecciones globales por redes de bots detectadas mensualmente

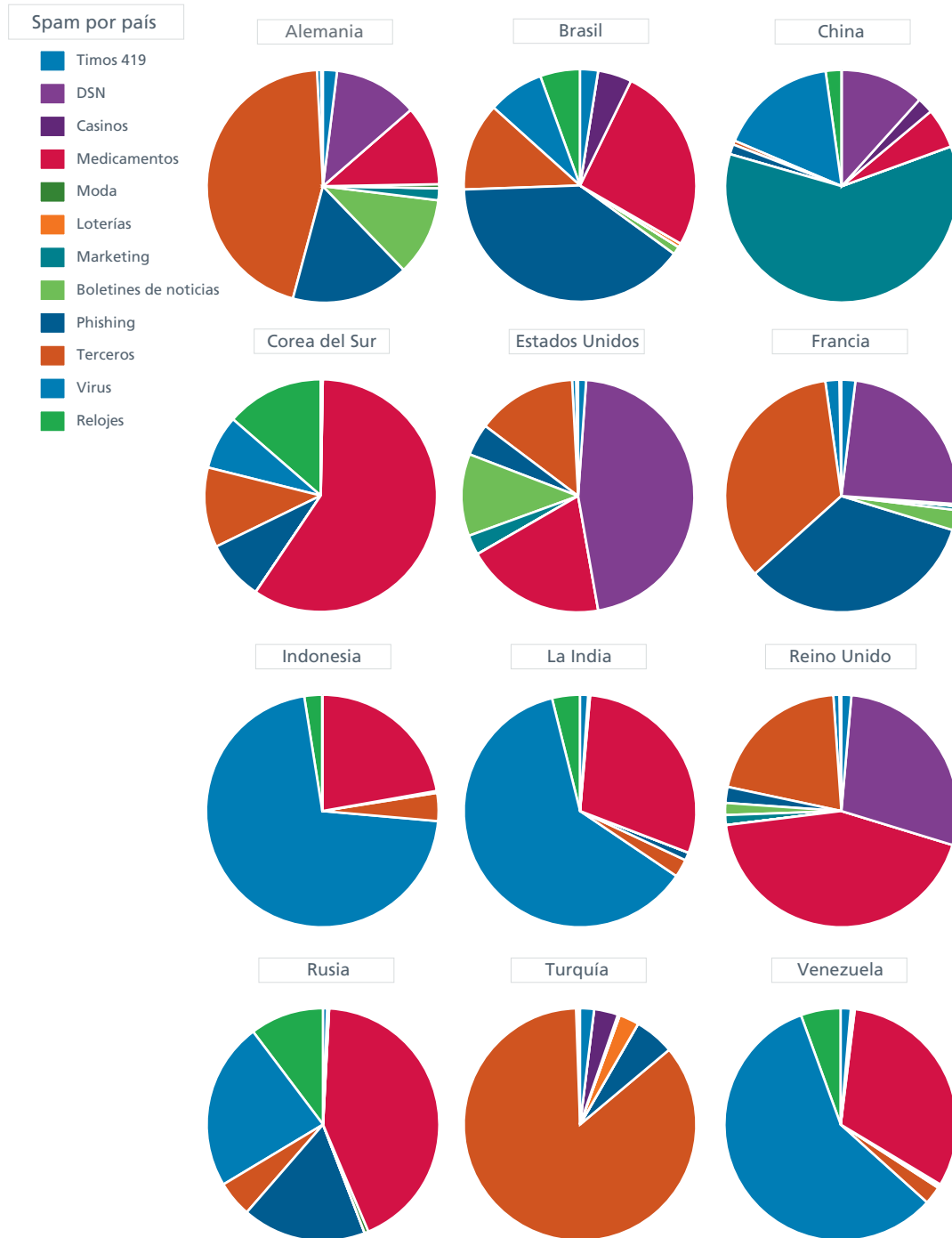


Una bajada de los índices de nuevas infecciones no significa que una red de bots haya perdido ímpetu. Tal y como se refleja en nuestra distribución por país, muchas de estas redes de bots mantienen un importante nivel de actividad. Cada sector representa el porcentaje de actividad de esa red de bots en el país concreto. No deben compararse los sectores de un país con los de otro, ya que el número total de detecciones por país varía considerablemente.



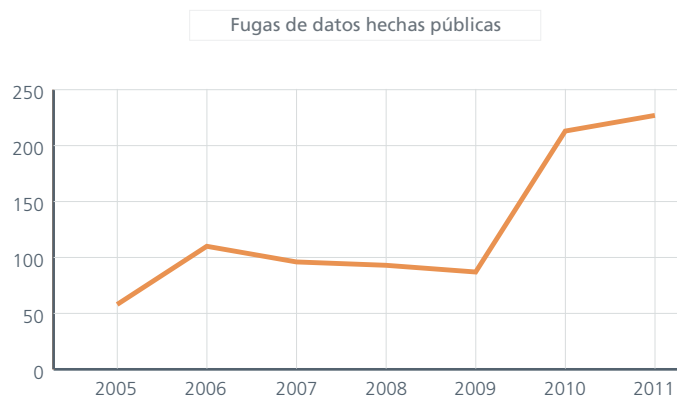
La ingeniería social en el mundo

Como siempre, los cebos de la ingeniería social y las líneas de asunto del spam varían considerablemente en función de la región geográfica. Los asuntos de los mensajes se siguen caracterizando por una gran diversidad y especificidad. Los cebos varían según el mes o la estación y, a menudo, aprovechan los períodos vacacionales o los eventos deportivos. En Brasil, el phishing es la forma de spam más popular, mientras que el spam de marketing es el más utilizado en China. En Alemania, el spam enviado por cuenta de terceros es el más extendido, al igual que en Francia, donde el phishing mantiene su popularidad. Por contraste, el spam para la venta de medicamentos se sitúa en primer lugar en el Reino Unido, mientras que en la India e Indonesia predominan las alertas de virus. Los cebos son diferentes según la cultura del país.



Fugas de datos y ataques a redes

En lo que se refiere a ataques a bases de datos, hemos observado varias tendencias durante este trimestre y el año pasado. Por un lado, parece claro que la ola de fugas de datos comunicadas que comenzaron hace algunos años se ha acentuado rápidamente durante los dos últimos años. El número de casos de fugas de datos a través de piratería, malware, fraude o imputables a personal interno se ha doblado desde 2009, según privacyrights.org.



Solo en este trimestre, se hicieron públicas más de 40 fugas. Aunque el número de fugas de datos detectadas en los tres últimos meses no supone un récord, los casos siguen en aumento.

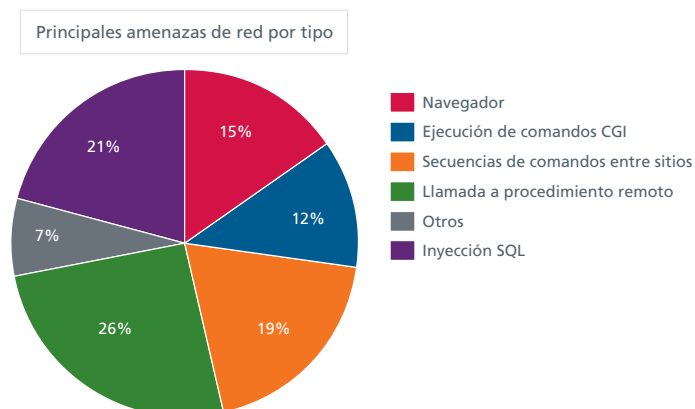
La segunda tendencia es consecuencia de la primera. Los equipos de TI y de seguridad son en la actualidad más conscientes de las intrusiones en bases de datos. Dado el aumento en el volumen de fugas, una mayor sensibilización es siempre algo positivo.

Un estudio reciente realizado por usuarios de Oracle demuestra este nivel de concienciación:

"Más del 25% de los encuestados contestaron que en los próximos 12 meses serán 'inevitables' o 'más que probables'. Más de un tercio de los encuestados responsables de la seguridad de las bases de datos de sus empresas habían tomado medidas para impedir ataques de inyección SQL y afirmaban disponer de sistemas de supervisión de las bases de datos de producción. Las estadísticas son muy halagüeñas, sobre todo si tenemos en cuenta que las soluciones de seguridad de bases de datos han sido históricamente un producto de seguridad raramente utilizado en las empresas²".

Aunque la situación dista mucho ser ideal, la sensibilización sobre el problema de seguridad de las bases de datos ha mejorado bastante. Es una pena que haya hecho falta una ola de fugas de datos sin precedentes para que se llegue a esta situación.

Los datos y el análisis de nuestro segundo dominio de estudio, los ataques basados en la red, provienen del servicio de información global sobre amenazas McAfee Global Threat Intelligence™.



La principal amenaza del trimestre hay que imputarla a las vulnerabilidades en las llamadas a procedimientos remotos de Microsoft Windows. El segundo lugar se lo disputan los ataques de inyección SQL y los ataques de secuencias de comandos entre sitios. Se trata de ataques a distancia, es decir, que pueden lanzarse contra objetivos selectivos en todo el mundo. Los ataques basados en el navegador, por el contrario, constituyen generalmente una amenaza del lado del cliente. Si el elevado número de ataques remotos que dan lugar a fugas de datos refleja un aumento de las acciones de hacktivismo o actividades relacionadas se trata de una cuestión que examinaremos de cerca el año que viene.

Amenazas Web

Los sitios web pueden tener buena o mala reputación por distintas razones. Las reputaciones pueden basarse en dominios completos, en cualquier cantidad de subdominios, así como en direcciones IP o URL específicas. Los sitios web de phishing o los que alojan malware y programas potencialmente no deseados serán catalogados como sitios web maliciosos. A menudo observamos combinaciones de código y funcionalidades dudosas. Hay varios factores que contribuyen a nuestra calificación de la reputación de un sitio web.

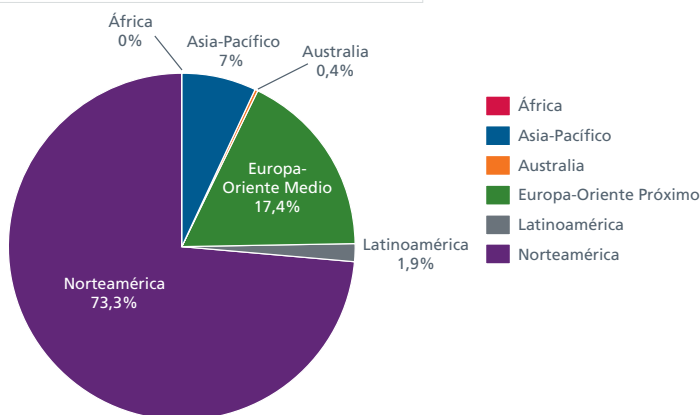
En el tercer trimestre, McAfee Labs registró una media de 6.500 nuevos sitios web maliciosos al día; el último trimestre esta cifra llegó a 9.300. Además, hemos observado que casi una de cada 400 URL que hemos intentado cargar era maliciosa; algunos días la proporción llegó a ser de una de cada 200. Con las fiestas de fin de año en pleno apogeo, circunstancia que los ciberdelincuentes no dejan escapar, los resultados no son una sorpresa.

URL nuevas de mala reputación al día



La gran mayoría de los sitios web maliciosos nuevos se encuentran en Estados Unidos, seguido por los Países Bajos, Canadá, Alemania, Corea del Sur, Alemania, el Reino Unido, Rusia y China. En el trimestre anterior, los ocho primeros países coincidieron, aunque no exactamente en el mismo orden. Nuestro gráfico de distribución geográfica revela la ubicación de la mayoría de los servidores maliciosos.

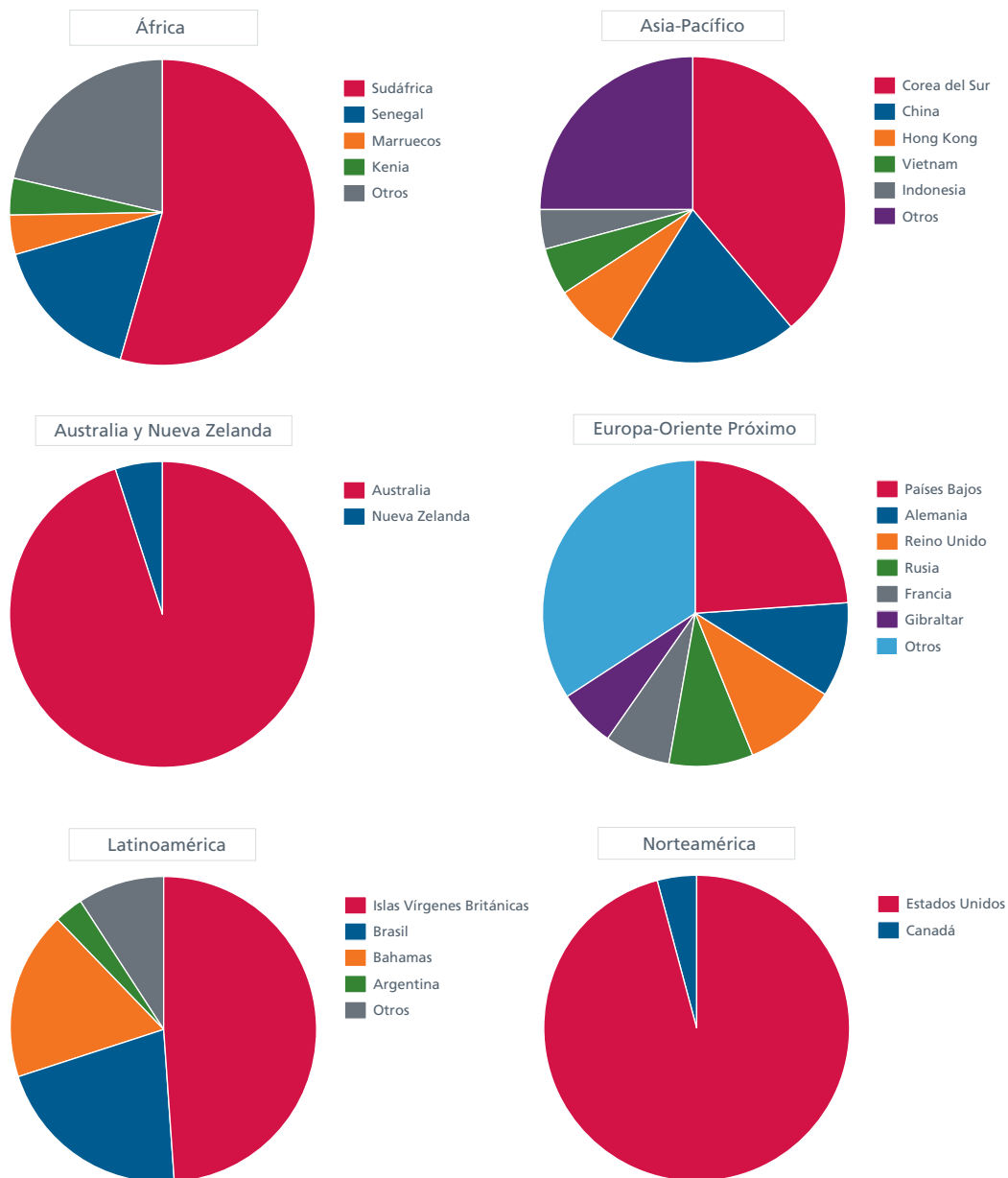
Ubicación de servidores que alojan contenido malicioso



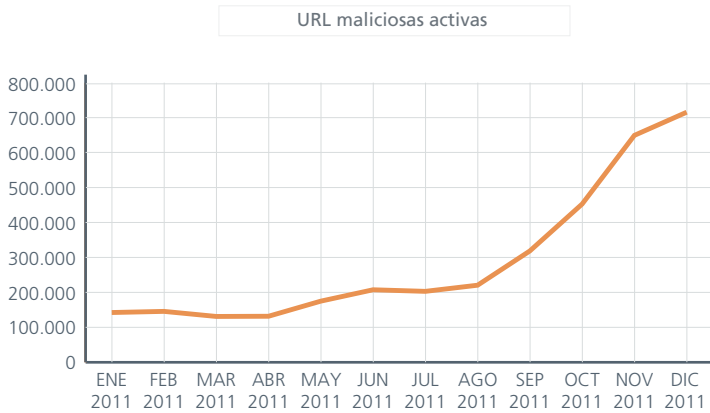
En la página anterior, hemos visto que Estados Unidos es líder indiscutible y alcanza su porcentaje más alto del año (su nivel más bajo era del 60% en el segundo trimestre). Europa y Oriente Medio siguen en segundo lugar (del 18 al 25% durante los otros tres trimestres).

Si examinamos más detenidamente la clasificación por región, observamos que no hay ninguna área de Internet en el mundo sin ningún riesgo.

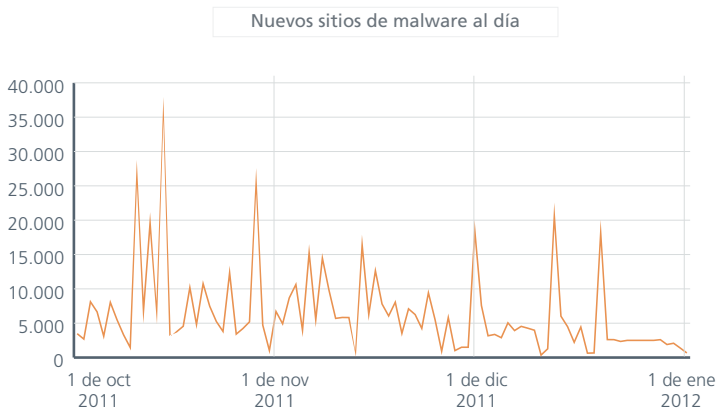
Ubicación de servidores que alojan contenido malicioso, por país



El número de sitios web que albergan URL maliciosas, una combinación de descargas maliciosas y exploits del navegador, continúa su progresión.



El número de sitios web que distribuyen malware y programas potencialmente no deseados creció considerablemente durante el último trimestre, con una media aproximada de 6.500 sitios web nuevos al día, comparados con los 3.500 al día del tercer trimestre.



Los sitios web de phishing han experimentado un leve descenso; hemos identificado, aproximadamente, 2.200 nuevas URL de phishing al día, comparadas con las 2.700 del trimestre anterior.



Ciberdelincuencia

Herramientas de crimeware

En octubre, se anunció una nueva vulnerabilidad de Java que aprovechaba el motor de secuencias de comandos de Rhino. Esta vulnerabilidad permitía a un applet de Java sin firmar obtener mejores privilegios y ejecutar código Java arbitrario fuera del entorno aislado (o "sandbox"). Poco después del descubrimiento, se publicó un módulo de ataque como parte del proyecto Metasploit. Asimismo, se incorporó a varios kits de crimeware.

Nombre	Precios (en dólares estadounidenses)	
Phoenix Exploit Kit 3.0 (Diciembre)	2.200 dólares (un dominio) 2.700 dólares (dominio multiproceso)	En nuestro informe del segundo trimestre, incluimos la versión 2.7. Este trimestre hemos advertido tres actualizaciones. La versión 3.0 incluye el exploit Java Rhino (CVE-2011-3544).
BlackHole Exploit Kit 1.2.1 (Noviembre)	Licencia anual: 1.500 dólares Licencia semestral: 1.000 dólares Licencia trimestral: 700 dólares	Esta actualización incluye también Java Rhino.

Principales acontecimientos

Este trimestre ha estado marcado por una serie de ataques a sistemas industriales e infraestructuras nacionales. Dos de los ataques han tenido lugar en el sur de Estados Unidos.

- A principios de noviembre, un malware en Nueva Zelanda desactivó el sistema de respuesta automática de los centros de comunicación de ambulancias de St. John, que reciben más de un millón de llamadas al año. El incidente obligó al personal a suspender temporalmente los servicios automatizados y asignar las ambulancias de forma manual³.
- El 18 de noviembre, un agresor conocido como PrOf publicó capturas de pantalla que mostraban una interfaz de usuario empleada para supervisar y controlar los equipos del departamento de agua y saneamiento de la ciudad de South Houston, en Texas⁴.
- Del 7 al 10 de diciembre, un malware detectado en las redes de Lawrenceville y Duluth, en el estado de Georgia, obligó a un centro hospitalario regional a cerrar sus puertas y desviar a sus pacientes a otros hospitales⁵.

El 10 de noviembre, una nota del STIC (Statewide Terrorism & Intelligence Center) del estado de Illinois anunció que un sistema SCADA⁶ de una red de distribución de aguas había sufrido un ciberataque imputado a Rusia⁷. Seis días más tarde, el equipo de ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) informaba de que el incidente *no* podía atribuirse a un acto de piratería⁸. Resulta interesante constatar que hicieran falta varios días para determinar que no se trató de un ciberataque.

Acciones contra los ciberdelincuentes

Noviembre fue un buen mes en lo que se refiere a detenciones de ciberdelincuentes.

- El 9 de noviembre, el FBI anunció la detención, en Estonia, de seis ciberdelincuentes estonios que habían robado 14 millones de dólares estadounidenses tras piratear al menos cuatro millones de ordenadores en un timo de publicidad online. Las detenciones fueron el fruto de dos años de investigación en la llamada Operación Ghost Click⁹. Los sospechosos están a la espera de su extradición a Estados Unidos. Se les acusa de haber utilizado malware de la familia DNSChanger para redirigir a usuarios desprevenidos a servidores falsos controlados por ellos, en lugar de a los sitios web de comercios oficiales a los que pretendían acceder las víctimas. Se trata de uno de los desmantelamientos de redes de ciberdelincuencia más importantes de los últimos años.
- El 15 de noviembre, la división de lucha contra el terrorismo y el crimen organizado de Rumanía detuvo al rumano de 26 años conocido en la Web como "Iceman", sospechoso de haber accedido de manera ilegal a los servidores de la NASA en diciembre de 2010¹⁰.
- El 23 de noviembre, la policía de Filipinas y el FBI arrestaron a cuatro personas sospechosas de desviar fondos de cuentas bancarias tras piratear las líneas telefónicas de varias operadoras de telefonía, incluida AT&T. Los investigadores explicaron que los agresores posiblemente estaban relacionados con el grupo terrorista responsable de la financiación del sangriento ataque terrorista en la ciudad india de Bombay, en 2008¹¹.

- El 5 de diciembre un grupo de individuos y empresas tailandesas y nigerianas fueron condenados a pagar 610 millones de dólares en una sentencia en rebeldía. Se les acusaba del envío de spam, entre 2006 y 2009, a clientes de Yahoo sobre una lotería falsa¹².
- El 9 de diciembre, los investigadores del servicio PCeU (Police Central e-Crime Unit) del Reino Unido arrestaron a seis personas por su implicación en un sofisticado timo de phishing dirigido a cientos de estudiantes británicos en agosto de 2011. Los agresores consiguieron acceder a datos para robar más de 1 millón de libras esterlinas¹³.
- El 9 de diciembre, fue arrestado en Rumanía un general ucraniano condecorado, junto con otros dos individuos sospechosos de pertenecer a una banda de ciberdelincuencia organizada que blanqueó al menos 1,4 millones de dólares robados a empresas estadounidenses e italianas¹⁴. Los tres están acusados de robar los datos de acceso a las cuentas bancarias de sus víctimas y, posteriormente, transferir dinero desde dichas cuentas a sus propias empresas.
- El 9 de diciembre, la Comisión Federal de Comercio (FTC, Federal Trade Commission) de Estados Unidos anunció que había alcanzado un acuerdo con la empresa Innovative Marketing, con sede en Ucrania, para compensar a los 320.000 consumidores víctimas de un timo para adquirir programas de scareware de la empresa¹⁵. El importe de la compensación sería de unos 20 dólares. Entre 2003 y 2008, Innovative Marketing era líder en el sector del scareware. McAfee describe la saga de IMU en el informe "Cunde el pánico: el software de seguridad falso genera abundantes beneficios en todo el mundo", escrito por François Paget, investigador de McAfee Labs¹⁶.

Hacktivism

Las disensiones surgidas en las filas del grupo hacktivista Anonymous constituyen uno de los acontecimientos más destacados del trimestre.

- Como parte de su apoyo y financiación del movimiento Occupy Wall Street, Anonymous anunció la operación "Invade Wall Street". Había prometido que "el 10 de octubre, la Bolsa de Nueva York desaparecería de Internet", gracias a un ataque de denegación de servicio distribuido contra la plaza bursátil neoyorquina. El rechazo por parte de otras facciones del grupo pudo haber perturbado el ataque, cuyo impacto fue mínimo.
- Para el 7 de noviembre se anunció un ataque similar dirigido a la Bolsa de Toronto¹⁷. Sin embargo, una vez más, se produjeron discrepancias internas en el seno de Anonymous y no se observaron perturbaciones en las operaciones bursátiles ni en otras transacciones.
- Facebook sobrevivió al controvertido y discutido ataque programado para el 5 de noviembre.
- El 24 de diciembre, un grupo de personas que decían formar parte de Anonymous anunciaron haberse introducido en la red de Stratfor, una empresa estadounidense de servicios de consultoría de seguridad. Tras apoderarse de listas de clientes confidenciales y recopilar más de 4.000 números de tarjetas de crédito, contraseñas y direcciones postales, los ciberdelincuentes emplearon la información de las tarjetas de crédito para hacer donativos a organizaciones humanitarias como la Cruz Roja americana y CARE. La principal facción de Anonymous no tardó en desmentir su participación en el ataque y culpó a miembros de Sabu y de LulzSec¹⁸.
- El año terminó con la operación #lulzmas, descrita por Anonymous como una campaña de hacking de una semana contra sitios relacionados con finanzas, ejércitos y gobiernos en todo el mundo. Sus propósitos y objetivos aun están por descubrir.

Otra actividad hacktivista frecuente este trimestre ha sido la denominada "doxing", o publicación de fotos o información personal de miembros de la familia de las fuerzas del orden.

- El 26 de octubre se publicó en Internet información sobre oficiales de policía de Oakland, California, en respuesta al uso de la fuerza durante una manifestación de protesta por el desalojo del campamento del movimiento Occupy Oakland¹⁹.
- El 18 de noviembre, el Departamento de Justicia de California anunció que un agresor había conseguido acceder a la cuenta de Gmail/Google de un agente supervisor especial responsable de las investigaciones de delitos informáticos²⁰. Ese día, 38.000 mensajes de correo electrónico de dos cuentas y distinto material personal se publicaron en un sitio web oculto en la red Tor y se distribuyeron en sitios web para compartir archivos.
- Tras la aparición de fotos de un policía utilizando gas pimienta contra los manifestantes del movimiento Occupy en la Universidad de California, en el campus UC Davis el 18 de noviembre, se distribuyeron en Internet los datos de sus contactos personales²¹.

- A finales de noviembre, LulzSec Portugal lanzó ataques DDoS contra servicios públicos, partidos políticos y sitios web de la policía nacional para denunciar las medidas de austeridad, las desigualdades sociales y los supuestos episodios de brutalidad policial contra manifestantes el 24 de noviembre. El grupo también distribuyó el nombre, rango, número de identificación, datos de contacto e historial profesional de más de 107 oficiales de policía de Lisboa²².
- Durante varios meses en Francia, el sitio web de Copwatch publicó datos personales de miembros de la policía acusados de brutalidad o ligados a ideales de la extrema derecha. Un mandamiento judicial del Tribunal Supremo exigió al principal proveedor de servicios de Internet francés que bloqueara el sitio web²³.

El objetivo del *doxing* como técnica no se limita a la policía, sino que también se dirige a personajes públicos, como políticos, en cuanto se percibe que adoptan una postura o acciones desfavorables o en contra de determinados ideales hacktivistas. El 15 de diciembre, Anonymous publicó varios volcados de información sobre senadores americanos que aprobaron la ley de autorización de defensa nacional (National Defense Authorization Act, NDAA). En Francia, hemos observado cómo se ha divulgado en Internet la información personal de políticos de derecha o de extrema derecha tras declaraciones o tomas de posición controvertidas.

Ciberescaramuzas

No fue hasta 2010 cuando el tema del hacktivismo alcanzó popularidad. En ese momento, nosotros habíamos citado ciberacciones en Estonia (2007) y en Georgia (2008) como ejemplos. De nuevo este trimestre, parece que varios sucesos han pasado de ser puro hacktivismo a contar con un respaldo oficial o político.

- El 1 de noviembre, el Ministro de Telecomunicaciones palestino, Mashur Abu Daqqa, culpó a hackers de todo el mundo de ser responsables del ataque a los servidores palestinos y de la interrupción de los servicios telefónicos y de Internet en Cisjordania y Gaza, así como de las comunicaciones de su ministerio. El incidente se produjo un día después de que los palestinos fueran admitidos en la UNESCO como miembros de pleno derecho, a pesar de las objeciones de Estados Unidos e Israel, y el ministro sugirió que Israel podría estar detrás del ataque²⁴.
- En Corea del Sur, el 3 de diciembre, el centro de respuesta contra ciberterrorismo (Cyber Terror Response Center) de la agencia de la policía nacional anunció que habían capturado y solicitado la orden de detención de cuatro individuos acusados de ordenar el ataque de denegación de servicio contra el sitio web de la Comisión Nacional Electoral en la mañana del 26 de octubre, día de elecciones. El ciberataque dejó inaccesible la información sobre los colegios electorales. Uno de los sospechosos era un asesor de un parlamentario del Gran Partido Nacional, en el poder. Se rumorea que, seis días antes de las elecciones municipales de Seúl, se transfirieron 10 millones de won (8.619 dólares) desde la cuenta bancaria de un secretario del portavoz de la Asamblea Nacional a la del sospechoso. Cinco días después, se detectaron varias transferencias de fondos a la cuenta de otro individuo que supuestamente llevó a cabo el ataque²⁵.
- Cuando Rusia se preparaba para celebrar elecciones a principios de diciembre, varios conocidos medios de comunicación liberales rusos y un organismo de control electoral quedaron fuera de servicio a causa de una serie de ataques de denegación de servicio coordinados. También resultaron afectados por ciberataques otros sitios de medios de comunicación independientes que habían cubierto las irregularidades en el proceso electoral²⁶.
- El grupo de agresores autodenominados Moroccan Deterrence Forces llevaron a cabo lo que denominaron la "venganza marroquí" mediante el ataque a varios sitios web oficiales de Qatar después de que el canal League and Cup mostrara imágenes de la delegación marroquí en los Juegos Panárabes (del 9 al 23 de diciembre) con un mapa de Marruecos que excluía el Sahara marroquí²⁷.

Los ciberataques financiados por los gobiernos son difíciles de identificar. Con toda seguridad, el año próximo veremos nuevos ejemplos de ataques y defensas contra ciberdelitos, hacktivismo y, posiblemente, ciberguerra.

Acerca de los autores

Este informe ha sido preparado y redactado por Zheng Bu, Toralv Dirro, Paula Greve, David Marcus, François Paget, Ryan Perme, Vadim Pogulievsky, Craig Schmugar, Jimmy Shah, Peter Szor 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 dedicada a investigar todos los vectores de amenazas (malware, web, correo electrónico, redes y vulnerabilidades), los laboratorios McAfee Labs recopilan información procedente de sus millones de sensores y de su servicio 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.

McAfee, Inc.

McAfee, empresa subsidiaria propiedad 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 las normativas, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar cualquier tipo de amenaza que pueda poner en peligro su seguridad. En McAfee centramos todos nuestros esfuerzos en la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes. www.mcafee.com/es

- ¹ <https://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-foes-of-the-stuxnet-files>
<https://blogs.mcafee.com/mcafee-labs/of-kernel-vulnerabilities-and-zero-day-a-duqu-update>
- ² "Databases are more at risk than ever: Oracle 2011 IOUG Data Security Survey" (El riesgo para las bases de datos es mayor que nunca: estudio sobre seguridad de datos de IOUG 2011 - Oracle)
- ³ <http://www.stuff.co.nz/waikato-times/news/5953497/Computer-virus-hits-ambulances>
- ⁴ http://news.cnet.com/8301-27080_3-57327968-245/hacker-says-he-broke-into-texas-water-plant-others/
- ⁵ <http://www.securitynewsdaily.com/computer-worm-shuts-down-atlanta-hospitals-1416/>
- ⁶ Supervisory Control and Data Acquisition (Registro de datos y control de supervisión)
- ⁷ <http://community.controlglobal.com/content/water-system-hack-system-broken>
- ⁸ http://us-cert.gov/control_systems/pdf/CSB-11-327-01.pdf
- ⁹ http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911
- ¹⁰ <http://news.softpedia.com/news/Romanian-NASA-Hacker-Graduates-From-University-of-Weed-235069.shtml>
- ¹¹ <http://www.reuters.com/article/2011/11/26/us-philippines-usa-idUSTRE7AP06320111126>
- ¹² [http://news.cnet.com/8301-27080_3-57338828-245/yahoo-awarded-\\$610-million-from-lottery-spammers/](http://news.cnet.com/8301-27080_3-57338828-245/yahoo-awarded-$610-million-from-lottery-spammers/)
- ¹³ <http://content.met.police.uk/News/Six-arrested-arrested-in-million-pound-phishing-scam/1400005228273/1257246745756>
- ¹⁴ <http://krebsonsecurity.com/2011/12/ukrainian-general-arrested-in-cyber-heists/>
- ¹⁵ <http://www.ftc.gov/opa/2011/12/rebates.shtml>
- ¹⁶ <http://www.mcafee.com/us/resources/white-papers/wp-running-scared-fake-security-software.pdf>
- ¹⁷ <http://www.nowtoronto.com/news/webjam.cfm?content=183319>
- ¹⁸ <http://www.talkleft.com/story/2011/12/25/124727/35>
- ¹⁹ <http://www.scmagazineus.com/anonymous-downs-oakland-police-site-after-violence/article/215433/>
- ²⁰ <http://arstechnica.com/tech-policy/news/2011/11/anonymous-exposes-cybercrime-investigators-gmail-voicemail.ars>
- ²¹ http://www.washingtonpost.com/blogs/blogpost/post/anonymous-targets-pepper-spraying-uc-davis-cop/2011/11/22/gIQA0Pr8IN_blog.html
- ²² http://tek.sapo.pt/noticias/internet/lulzsec_ataca_mai_e_divulga_dados_pessoais_de_1204169.html
- ²³ <http://blog.indexonensorship.org/2011/10/17/france-copwatch-site-blocked/>
- ²⁴ http://www.google.com/hostednews/afp/article/ALeqM5hsZ6qUDvnFlrGo9CyZ9u_NhGu-Og
- ²⁵ http://english.hani.co.kr/arti/english_edition/e_editorial/510303.html
- ²⁶ <http://www.euronews.net/2011/12/04/russian-election-hackers-attack-opposition-sites/>
- ²⁷ <http://morocccoworldnews.com/2011/12/moroccan-hackers-attack-media-websites-in-qatar/18702>



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

La información de este documento se proporciona únicamente con fines informativos y para la conveniencia de los clientes de McAfee. La información aquí contenida está sujeta a cambio sin previo aviso y se proporciona "tal cual" sin garantías respecto a su exactitud o a su relevancia para cualquier situación o circunstancia concreta.

McAfee, el logotipo de McAfee, McAfee Labs y McAfee Global Threat Intelligence son marcas comerciales registradas o marcas comerciales de McAfee, Inc. o de sus empresas filiales en EE. UU. o en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Los planes, especificaciones y descripciones de productos mencionados en este documento se proporcionan únicamente a título informativo y están sujetos a cambios sin aviso previo; y se ofrecen sin garantía de ningún tipo, ya sea explícita o implícita. Copyright © 2012 McAfee 41604rpt_quarterly-threat-q4_0112_fnl_ETMG