Informe

Informe de McAfee sobre amenazas: Segundo trimestre de 2011

Laboratorios McAfee® Labs™

El panorama de amenazas de 2011 ha estado marcado por el caos y los cambios. Los grandes retos que plantean los grupos de hacktivistas como LulzSec y Anonymous han sido los responsables de sembrar el caos, mientras que los cambios han ido de la mano de los nuevos tipos de malware y de dispositivos que tienen por objetivo.

Este trimestre, los laboratorios McAfee Labs han observado una considerable actividad de los hacktivistas, pero de una forma muy distinta. El grupo Lulz Security, conocido como LulzSec, se diferencia de otros grupos hacktivistas en que no tiene objetivos específicos. Según ellos, su razón de ser es la pura diversión (de ahí "lulz", el equivalente al acrónimo inglés LOL en los mensajes de texto, que viene a decir "carcajadas"). Sin embargo, demostraron una tremenda agilidad a la hora de poner en peligro redes y servidores, y de robar nombres de usuario, contraseñas y otra información. El grupo LulzSec se introdujo ilegalmente en múltiples empresas, atacó a diferentes cuerpos de policía y organizaciones de inteligencia, y fue responsable de otras muchas amenazas a la seguridad. Aunque muchos de los resultados y usos de estos ataques aún siguen en juego (por lo que ofrecemos un valioso resumen de la actividad del trimestre), una cosa es evidente: muchas empresas, tanto grandes como pequeñas, son más vulnerables de lo que podían sospechar. Además, el sector de la seguridad puede tener que replantearse algunos de los supuestos básicos, como si realmente estamos protegiendo a los usuarios y a las empresas. Aunque LulzSec parece no haber actuado este trimestre, este y otros grupos hacktivistas han planteado cuestiones que estarán sobre la mesa durante mucho tiempo.

Un cambio significativo que se produjo en el primer trimestre de 2011 fue que Android se convirtió en la tercera plataforma objetivo del malware para móviles. Este trimestre, el recuento de malware nuevo específico para Android han situado este tipo de amenazas en el puesto número uno, seguido de J2ME (Java Micro Edition), que se sitúa en segundo lugar con sólo un tercio del malware. El aumento de las amenazas para esta plataforma tan popular debería hacer que nos planteemos cómo usamos los dispositivos móviles y si el sector de la seguridad está preparado para combatir este crecimiento.

También observamos un aumento del malware para móviles con fines lucrativos, como los simples troyanos que envían SMS y los troyanos más complejos que se aprovechan de las vulnerabilidades para poner en riesgo los smartphones. En este informe ofrecemos una actualización de la "lista de precios" de la ciberdelincuencia, así como los cambios en los precios de las herramientas y los servicios. Las "herramientas delictivas como servicio" y el floreciente "hacktivismo como servicio" siguen evolucionando a medida que los intereses y los objetivos cambian. Afortunadamente, este trimestre ha habido algunas victorias importantes en la lucha contra los ciberdelincuentes.

Siguiendo con el tema de los cambios que se han producido, hemos observado una considerable reducción de AutoRun y Koobface, que se compensa con el gran aumento de los antivirus falsos dirigidos a los Mac. Durante años, los creadores de malware han ignorado el sistema operativo Mac OS X de Apple, por lo que esto supone un gran cambio en los objetivos de los ciberdelincuentes.

El malware se ha mantenido con un crecimiento continuado durante el trimestre, así como los rootkits, que se utilizan principalmente para garantizar un acceso sigiloso y sólido y permitir que el malware sea más eficaz y persistente. La popularidad de los rootkits está subiendo como la espuma, y algunos como Koutodoor y TDSS aparecen cada vez con mayor frecuencia. Por otra parte, el malware dirigido a atacar las vulnerabilidades de los productos de Adobe sigue superando en número al dirigido a los productos de Microsoft.

Los botnets y las amenazas de la mensajería, aunque siguen en mínimos históricos, han empezado a aumentar de nuevo. Era una recuperación que esperábamos después de que recientemente se desactivaran algunos botnets. Los usuarios y las empresas deben planificar medidas para afrontar este crecimiento y, por consiguiente, prever defensas y respuestas. Más adelante volveremos a examinar los temas de ingeniería social tanto por localización geográfica como por tema, y analizaremos los botnets por localización geográfica y tipo.

Este trimestre hemos podido presenciar varios momentos álgidos en la actividad de los sitios web maliciosos, así como un gran crecimiento de los blogs y wikis con mala reputación. También han aumentado los sitios web que distribuyen malware y programas potencialmente no deseados, y los sitios web de phishing.

El segundo trimestre del año ha sido claramente un período de caos, cambios y nuevos desafíos.

Índice

Hacktivismo

Al parecer, a principios de este trimestre el grupo Anonymous se peleó y se separó. El 9 de mayo, el grupo Anonymous, a través de un comunicado de prensa, comunicaba que la red Anonops se había disuelto después de que Ryan, coadministrador del sitio web, intentara dar un "golpe de estado". Como represalia, sus datos de contacto se distribuyeron inmediatamente en Internet.

Sobre el 7 de mayo apareció una nueva cuenta de Twitter con el nombre de usuario @LulzSec, lo que dio a luz a Lulz Security. Sus primeras hazañas no lograron captar la atención de los medios de comunicación. Sin embargo, los ataques al sector del entretenimiento lograron lanzarlo al estrellato.

Después de 50 días en activo, las aventuras de LulzSec llegaron a su fin debido a las peleas entre grupos. Estos acontecimientos dejan traslucir la inmadurez de ciertos grupos clasificados como hacktivistas políticos y que dicen ser parte de Anonymous. Jester (th3j35t3r, un rival de Anonymous conocido por luchar contra los jihadistas y los sitios web detractores de los Estados Unidos) y otros grupos (Team Web Ninjas, Backtrace, The A-Team, Teamp0ison, etc.) se ocuparon de denunciar a sus antiguos colegas. Las peleas internas ayudaron a las autoridades a identificar a algunos de estos hackers.

Otro de los incidentes más destacados fue un "grave" ataque contra la Comisión Europea justo antes de la cumbre para debatir la futura estructura de la Unión Europea, la estrategia económica y la guerra de Libia[1]. El Ministerio de Economía francés sufrió un ataque similar. La Australian Security Intelligence Organisation (la agencia de inteligencia australiana) reveló que estaba investigando un ataque que puso en peligro los equipos de al menos 10 ministros, incluido el Primer Ministro, el Ministro de Asuntos Exteriores y el Ministro de Defensa. El gobierno alemán, por su parte, informó de que observa un promedio de cinco ataques diarios dirigidos contra usuarios de las redes del gobierno[2].

Algunas cuentas publicadas detallan una relación de las operaciones de algunos hacktivistas, como #antisec, #OpNewBlood, #OpLibya, #OpBrazil, con más de 4.000 en total, aunque esta cifra es difícil de comprobar. Estas operaciones se han traducido en sitios web que han acabado offline, grandes cantidades de nombres de usuario y contraseñas robados, y numerosos documentos confidenciales sustraídos y publicados. Muchas empresas han sufrido ataques muy eficaces con motivaciones políticas. Numerosos observadores han calificado estos ataques de simples, incluso de incompetentes, pero los expertos se olvidan de algo: en el hacktivismo es el mensaje lo que cuenta, no el método.

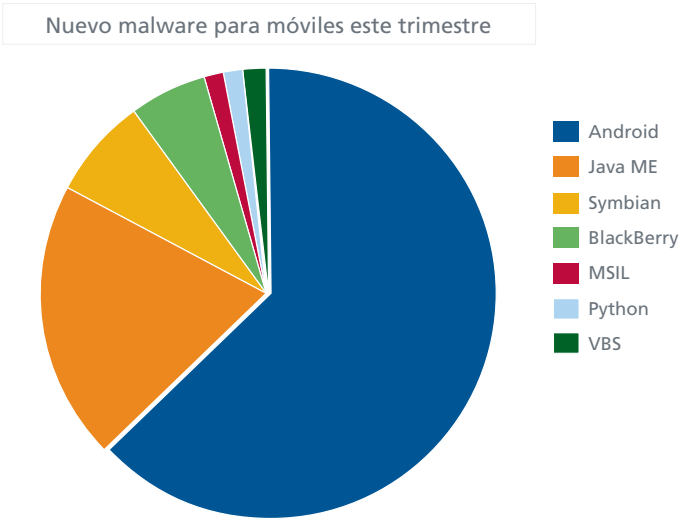
Dos intrusiones de un hacker rumano también llamaron nuestra atención debido a sus ambiciosos objetivos: las agencias espaciales de Estados Unidos y Europa.

En abril, este hacker publicó en su blog información procedente del servidor de la Agencia Espacial Europea, que incluía los nombres, nombres de usuario y correos electrónicos de más de 150 usuarios. En mayo, el mismo hacker declaró que se había introducido en un servidor del Goddard Space Flight Center de la NASA y que había accedido a los datos confidenciales de los satélites. Incluso llegó a colgar en su blog una captura de pantalla de lo que afirmaba ser uno de los principales servidores de FTP de la NASA.

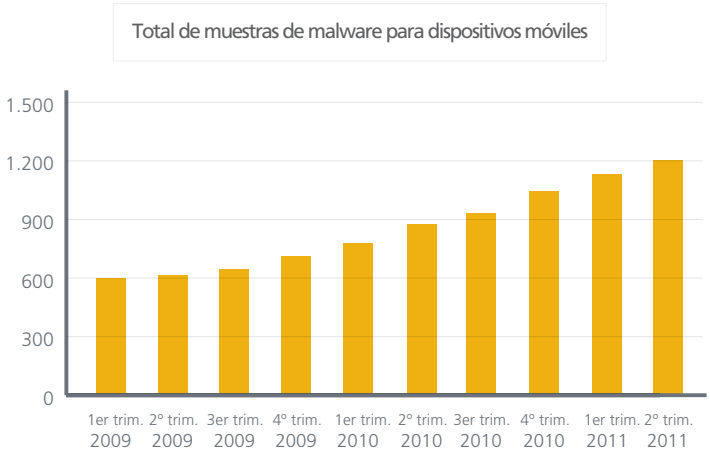
1. http://www.bbc.co.uk/news/world-europe-12840941
2. http://www.bundestag.de/presse/hib/2011_05/2011_201/08.html

Amenazas para los dispositivos móviles

Este trimestre, el sistema operativo Android se convirtió en el blanco favorito de los desarrolladores de malware para móviles. Los ataques contra Android han experimentado un rápido aumento, y han conseguido triplicar y dejar en segundo lugar los ataques contra Java Micro Edition.



Si observamos el crecimiento continuado y significativo del panorama de amenazas de malware para móviles, podemos comprobar que el código base se nutre de muchas de las funciones y características que ya poseen las amenazas para PCs. Las amenazas para móviles ya aprovechan vulnerabilidades, utilizan botnets e incluso utilizan funcionalidades del rootkit para introducirse furtivamente y garantizar su permanencia.



Las aplicaciones modificadas con fines maliciosos todavía son un vector muy utilizado para infectar este tipo de dispositivos. Estas aplicaciones corrompen aplicaciones o juegos legítimos, de modo que los usuarios acaben instalando por sí mismos el malware en sus smartphones al descargarlas.

Este trimestre, las aplicaciones modificadas más populares fueron Android/Jmsonez.A, Android/Smsmecap.A y Android/DroidKungFu, así como las familias Android/DrdDreamLite. Pero veamos más detenidamente algunos de los programas maliciosos para móviles más recientes.

Android/Jmsonez.A es una versión de una aplicación de calendario que no hace lo que debe[3]. Siempre que se inicia el programa, muestra el calendario de enero de 2011. Si el usuario intenta cambiar el mes a una fecha futura, el malware empieza a enviar mensajes SMS a un número de tarifa elevada. Además, Android/Jmsonez.A también supervisa los mensajes de confirmación de la bandeja de entrada procedentes del servicio de tarifa alta para evitar que lo detecten.

Android/Smsmecap.A es una versión modificada de una aplicación legítima de entretenimiento[4]. El malware envía mensajes SMS graciosos, irreverentes, a todos los contactos de la libreta de direcciones del usuario. De hecho, lleva enviando mensajes en tono de burla desde el 21 de mayo, la fecha en la que supuestamente empezó el "arrebato" jocoso.

La familia Android/DroidKungFu es similar a Android/DrdDream. También utiliza dos ataques a la raíz para permanecer en el dispositivo[5]. Las amenazas son en realidad idénticas a las que utiliza Android/DrdDream, excepto que se han cifrado con AES. Estas variantes también pueden cargar URLs e instalar software y actualizaciones adicionales.

La familia Android/DrdDreamLite es una variante con un potencial menor que la Android/DrdDream original[6]. La versión Lite utiliza DES para cifrar los datos que envía al atacante. Android/DrdDreamLite no incluye ningún ataque a la raíz para permanecer en los dispositivos infectados.

Otros troyanos complejos son Android/Tcent.A, la familia Android/Crusewin.A, Android/J.SMSHider.A y Android/Toplank.A.

Android/Tcent.A es otro troyano que envía SMS de tarifa alta, similar a Android/Jmsonez.A, pero incluye una interesante función para autoprotegerse[7]. El objetivo del malware es el servicio QQ de mensajería instantánea, muy utilizado en China. El malware trata de desinstalar el antivirus y otro software de seguridad incluidos en los clientes móviles de QQ.

La familia Android/Crusewin.A incluye algunos troyanos que envían mensajes de tarifa alta[8]. A diferencia del malware más simple, la familia Android/Crusewin.A incorpora algunas funciones típicas de los botnets, como la ejecución de órdenes procedentes del servidor de comandos del atacante. Esto permite al atacante enviar mensajes de SMS desde un dispositivo infectado, lo que es útil para abonar a la víctima a servicios de suscripción de tarifa alta e intentar desinstalar determinado software. Esta última función es similar a la de Android/Tcent.A, aunque tiene un pequeño inconveniente. Android/Crusewin.A utiliza un código de desinstalación que sólo funciona en los smartphones con Symbian y no funciona correctamente en Android. Esto apunta a que el desarrollador del malware puede estar migrando el código del troyano o botnet de Symbian a la plataforma Android.

Android/J.SMSHider.A es un malware que envía mensajes de tarifa alta[9]. Su creador modificó un "analizador de amor SMS" legítimo para añadir funciones de puerta trasera y la capacidad de borrar mensajes SMS entrantes. Android/J.SMSHider.A utiliza cifrado DES para encubrir sus comunicaciones con el atacante.

Android/Toplank.A se hace pasar por una actualización multiusuario del famoso juego Angry Birds. El malware envía información confidencial al atacante (la identidad internacional de abonado móvil, la lista de permisos del malware, etc.) para posteriormente poder descargar una aplicación Android en el dispositivo infectado. La nueva aplicación proporciona una puerta trasera al atacante, quien después puede agregar y eliminar los marcadores, el historial del navegador y los accesos directos, además de descargar software adicional.

Los autores de programas delictivos siguen desplegando sus trucos con SymbOS/Zitmo.C y BlackBerry/Zitmo.D, que simplemente reenvían mensajes SMS. Los autores ya han puesto en peligro los PCs de las víctimas con malware avanzado, así que los ataques a las plataformas móviles parecen exigirles un esfuerzo mínimo.

3. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501748
4. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=509500
5. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=522281
6. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=518925
7. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501599
8. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=501639
9. http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=527859

Ciberdelincuencia

Se vende listín de direcciones de correo electrónico

Los que se dedican al spam, ya sea a través de sus botnets o de servicios de alquiler, necesitan listas de direcciones de correo electrónico para colapsar el mundo. Los precios de estos listines varían, a menudo en función de la localización geográfica.

País	Precios del listín de direcciones (en dólares estadounidenses)
Rusia	400.000 direcciones en San Petersburgo: 25 $ 1.000.000 (en todo el país): 25 $ 3.000.000: 50 $ 5.000.000: 100 $ 8.000.000: 200 $
Estados Unidos	1.000.000: 25 $ 3.000.000: 50 $ 5.000.000: 100 $ 10.000.000: 300 $
Ucrania	2.000.000: 40 $
Alemania	1.000.000: 25 $ 3.000.000: 50 $ 5.000.000: 100 $ 8.000.000: 200 $
Turquía	1.000.000: 50 $
Portugal	150.000: 25 $
Australia	1.000.000: 25 $ 3.000.000: 50 $ 5.000.000: 100 $
Inglaterra	1.500.000: 100 $

Herramientas delictivas

Este trimestre hemos vuelto a ver productos nuevos y actualizaciones de los kits de exploits. Lo más destacado ha sido la versión 1.6.5 de Eleonore, con dos exploits de 2011, y Best Pack, con un exploit de 2011.

Nombre	Precios (en dólares estadounidenses)	Descripción
Weyland-Yutani BOT versión 1.0	1.000 $	Se movió en el mercado clandestino. El vendedor cerró la oferta rápidamente tras afirmar que había encontrado un comprador.
BlackHole Exploit Kit versión 1.1.0	Licencia anual: 1.500 $ Semestral: 1.000 $ Trimestral: 700 $	El primer kit apareció en septiembre de 2010. Actualizado en abril, contiene nueve exploits, seis de los cuales ya estaban presentes en 2010.
Best Pack		Anunciado por ScriptKiddieSec y Kahu Security como el posible sucesor de Dragon Pack, este kit de exploits contiene siete exploits anteriores y uno de 2011[10]: • CVE-2011-0611 (afecta a las versiones de Adobe Flash Player anteriores a la 10.2.159)
Phoenix Exploit Kit versión 2.7	2.200 $	Esta versión sustituye a la versión 2.5, cuyo código se filtró en abril. La versión actual contiene al menos 15 exploits, de los cuales 6 ya estaban presentes en 2010.
Eleonore versión 1.6.5	2.000 $	10 exploits, de los cuales 2 están dirigidos contra Flash Player desde 2011: • CVE-2011-0558 (Flash anterior a la versión 10.2) • CVE-2011-0611 (Flash anterior a la versión 10.2.159)
YES Exploit Kit 4.0	400 $	Desde abril de 2010 reemplaza a la versión 3.0RC. Esta versión contiene casi 20 exploits, de los cuales 7 son de 2010.

10. http://www.kahusecurity.com/2011/best-pack/

Acciones contra los ciberdelincuentes

No todo fueron desgracias este trimestre. Los tribunales y las fuerzas de seguridad siguen haciendo progresos contra los ciberdelincuentes en todo el mundo.

País y fecha	Descripción
Reino Unido Abril	La Police Central e-Crime Unit (Unidad Central de la Policía contra la Delincuencia Electrónica) detiene a tres hombres (de origen lituano, letón y de nacionalidad desconocida) relacionados con el uso del malware SpyEye para robar información de bancos en Internet[11].
Estados Unidos Abril	En la operación Adeona, el Departamento de Justicia de los Estados Unidos y el F.B.I. cierran el botnet Coreflood, que había infectado cientos de miles de PCs desde 2002. Desde marzo de 2009 y durante 11 meses, Coreflood había desviado 190 GB de contraseñas bancarias y otra información confidencial de más de 413.000 sistemas infectados mientras los usuarios navegaban en Internet[12].
Finlandia Mayo	A principios de este año la policía arresta a 17 personas sospechosas de participar en fraudes bancarios online, cuyo objetivo eran los titulares de cuentas de Nordea. Los autores del delito intentaron robar casi 1,2 millones de euros con una serie de más de 100 transacciones falsas[13]. Se cree que la mayoría de sospechosos eran traficantes de phishing. Los dos cerebros de la operación eran de Estonia.
Reino Unido Mayo	Un estudiante de la Universidad de Salford es condenado por una estafa en la que utilizaba malware para irrumpir en los ordenadores y las cuentas de correo de unas 100 víctimas. La policía solicitó a McAfee que analizara el malware y reconoció su contribución a la hora de recoger las pruebas que permitieron el arresto inmediato[14].
Estados Unidos, Ucrania y Letonia Junio	El Departamento de Justicia de los Estados Unidos y el F.B.I. anuncian la operación Trident Tribunal, una acción coordinada e internacional de las fuerzas de seguridad, que interrumpió las actividades de dos organizaciones internacionales de ciberdelincuentes que vendían software antivirus de alertas falsas (scareware)[15]. Realizada en cooperación con los servicios de seguridad ucranianos, parece que fue la primera vez que el objetivo era una banda que utilizaba Conficker[16]. Posteriormente, la policía se centró en la detención de ciudadanos letones acusados de crear una agencia de publicidad fraudulenta.
Rusia Junio	Uno de los personajes más polémicos del mundo de Internet en Rusia, Pavel Vrublevsky, cofundador y Presidente Ejecutivo de ChronoPay, es arrestado bajo la sospecha de haber ordenado un ataque de denegación de servicio distribuido (DDoS) contra una empresa rival. Vrublevsky, de 32 años, probablemente sea más conocido por ser copropietario de Rx-Promotion, un programa farmacéutico online poco fiable. Su empresa también ha participado en el procesamiento de tarjetas de crédito para, en muchos casos, constituir empresas en nombre de otros, distribuir antivirus falsos o realizar estafas de scareware que utilizan alertas de seguridad engañosas en un intento de asustar a la gente para que compre programas de seguridad inservibles[17].

Unas líneas sobre la ciberguerra

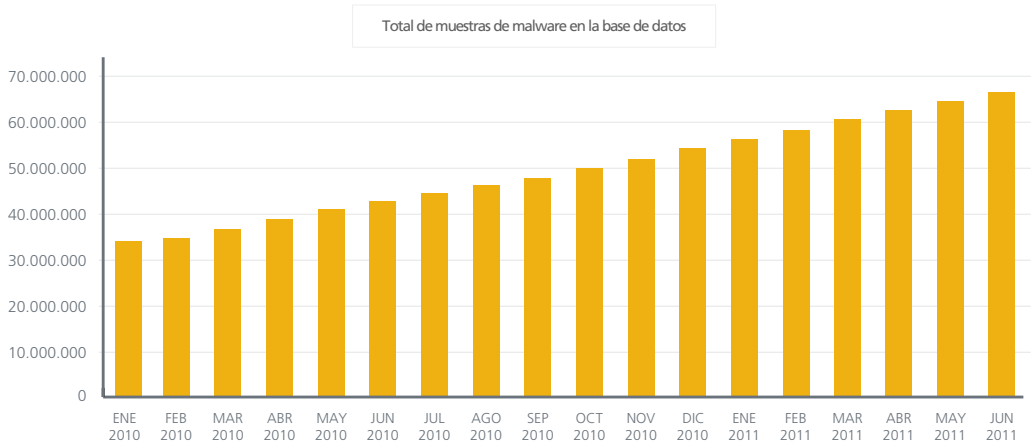
Sólo el hecho de intentar definir lo que es la "ciberguerra" puede dar lugar a un acalorado debate. Paralelamente, son cada vez más los países que intentan clasificar este conflicto creciente. El debate puede complicarse aún más si consideramos que el hacktivismo es cada vez más frecuente.

País y fecha	Descripción
Rusia Marzo/abril	Entre el 24 de marzo y el 4 de abril se lanzan varios ataques de DDoS contra algunos blogueros de LiveJournal, que aloja a más de 4,7 millones de blogueros rusos (incluido el Presidente Dmitry Medvedev) que intercambian información y a menudo comparten puntos de vista críticos que no pueden expresarse en los medios de comunicación habituales[18].
Estados Unidos Abril	El laboratorio Oak Ridge National, que posee uno de los superordenadores más potentes del mundo, es víctima de un ciberataque complejo con correos electrónicos de phishing enviados a unos 573 empleados del laboratorio. Al parecer, algunos hicieron clic en un vínculo del correo y descargaron malware que robaba información[19].
Corea del Sur Mayo	Las autoridades de Corea del Sur alegan que los servicios secretos de Corea del Norte han atacado el sistema informático de la Federación Nacional de Cooperativas Agrícolas, que proporciona servicios de suministro, procesamiento, marketing y bancarios a más de 4.000 sucursales[20].
Noruega Mayo	El ejército noruego admite haber sido víctima de un ciberataque potencialmente grave el mes de marzo. El ataque se produjo cuando 100 militares de alta graduación recibieron un correo electrónico con un archivo adjunto que parecía proceder de otro departamento oficial[21].

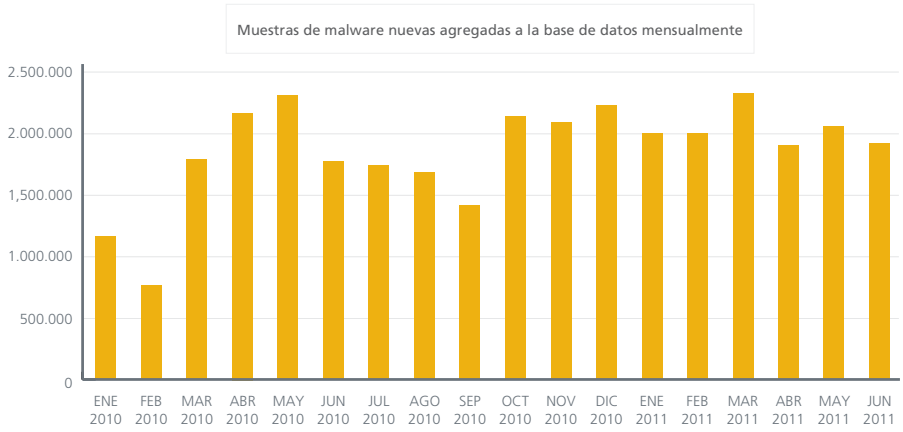
11. http://www.networkworld.com/news/2011/041111-uk-police-arrest-three-men.html
12. http://www.theregister.co.uk/2011/04/13/coreflood_botnet_takedown/
13. http://www.theregister.co.uk/2011/05/10/finnish_banking_trojan_investigation/
14. http://www.zdnet.co.uk/news/security-management/2011/05/18/gamer-sentenced-for-stealing-steam-passwords-40092802/
15. http://www.fbi.gov/news/stories/2011/june/cyber_062211/cyber_062211
16. http://www.zdnet.co.uk/news/security-management/2011/06/24/ukrainian-sting-targets-conficker-fraudsters-40093222/
17. http://krebsonsecurity.com/tag/pavel-vrublevsky/
18. http://uk.reuters.com/article/2011/04/06/oukin-uk-russia-medvedev-cyberattack-idUKTRE7354OV20110406
29. http://www.computerworlduk.com/news/security/3275613/us-government-energy-research-lab-shuts-down-email-and-internet-access-after-phishing-attack/
20. http://www.koreaittimes.com/story/14507/north-korea-behind-cyber-attack-south-korea-bank
21. http://www.cio.com.au/article/387581/norwegian_military_admits_march_cyberattack

Amenazas de malware

El panorama del malware nos ha dado varias sorpresas este trimestre. Aunque numéricamente no ha sido el período de mayor actividad de la historia (ha sido algo inferior al año pasado), si lo combinamos con el primer trimestre, observamos el primer semestre del año más activo jamás visto en lo referente a este vector. El aumento con respecto a 2010 es de un asombroso 22%. Los laboratorios McAfee Labs identificaron casi seis millones de muestras de malware únicas durante este trimestre, lo que hará que la colección acumulada en nuestro "zoológico de malware" llegue a 75 millones de muestras a finales de año.

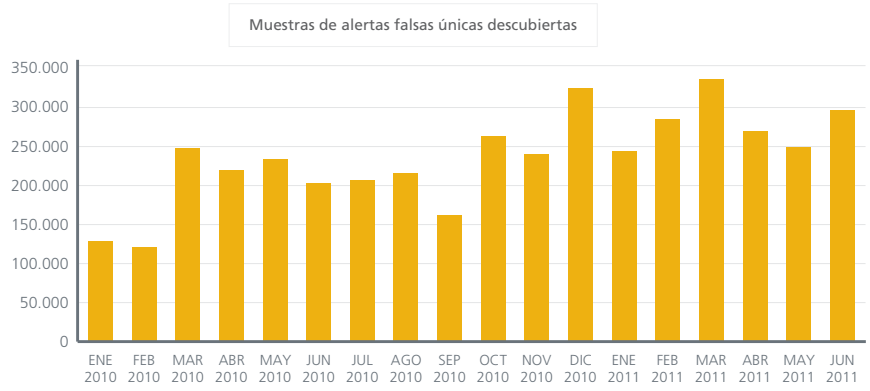


Sólo para constatar lo significativo que ha sido el crecimiento en los últimos años, echemos un vistazo al incremento del crecimiento mensual de archivos binarios de malware únicos:

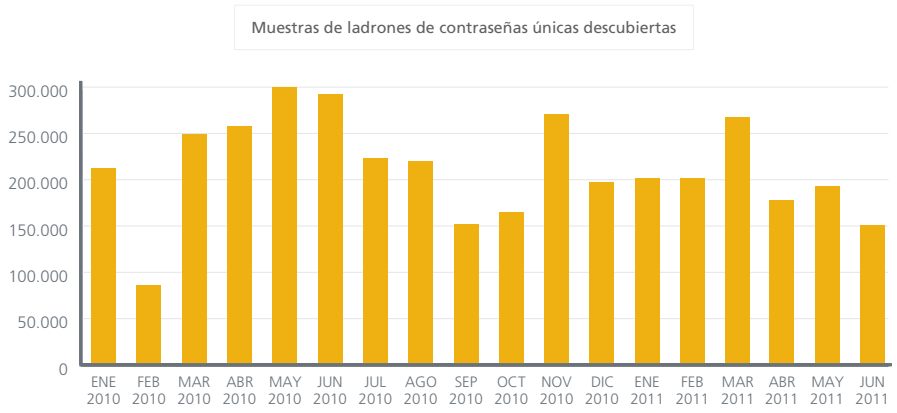


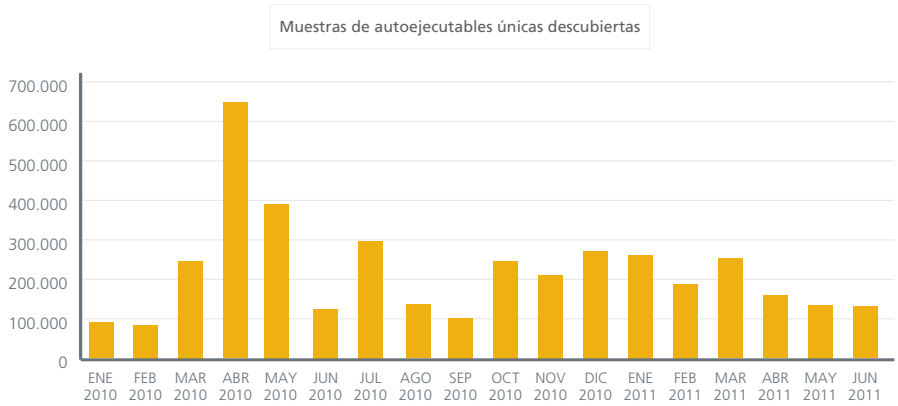
Actualmente recogemos una media de casi dos millones de muestras nuevas al mes. Esta cifra no es una buena noticia, ciertamente, pero es coherente y predecible si se tiene en cuenta cómo las empresas y nuestra vida privada están ligadas ahora a la tecnología.

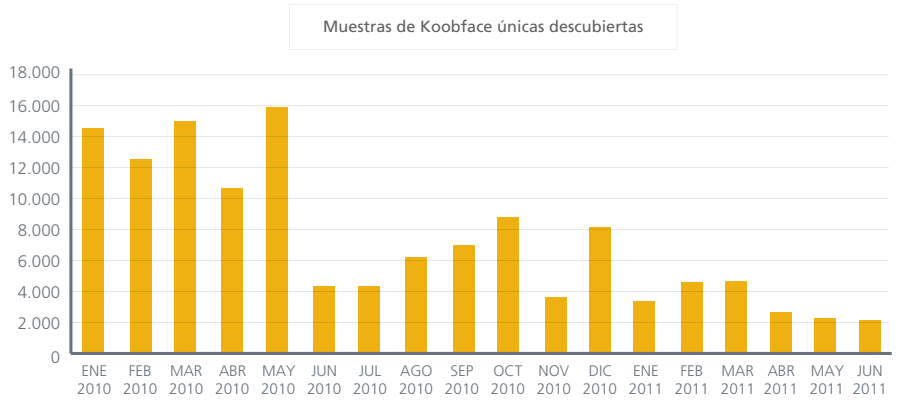
Entre las familias específicas que sometemos a seguimiento, el software antivirus falso (también llamado falsas alertas o software antivirus no fiable) sigue mostrando un crecimiento constante e incluso ha empezado a subir a bordo de una nueva plataforma: el Mac. Ha leído bien, los antivirus falsos para la plataforma Apple son ya una realidad. Para los laboratorios McAfee Labs esto no es ninguna sorpresa, puesto que hay más usuarios de Mac que nunca y las empresas están adoptan esta plataforma de forma constante. Ello coloca a las plataformas Apple directamente en el punto de mira de los autores de malware. Será interesante ver si este tipo de malware también consigue abrirse camino entre los iPhone y los iPad, aunque la pregunta debería ser más bien cuándo lo conseguirá.



Los troyanos genéricos de robo de contraseñas descendieron ligeramente este trimestre, mientras que el malware AutoRun se redujo considerablemente. Por su parte, las amenazas Koobface disminuyeron a niveles mínimos históricos.

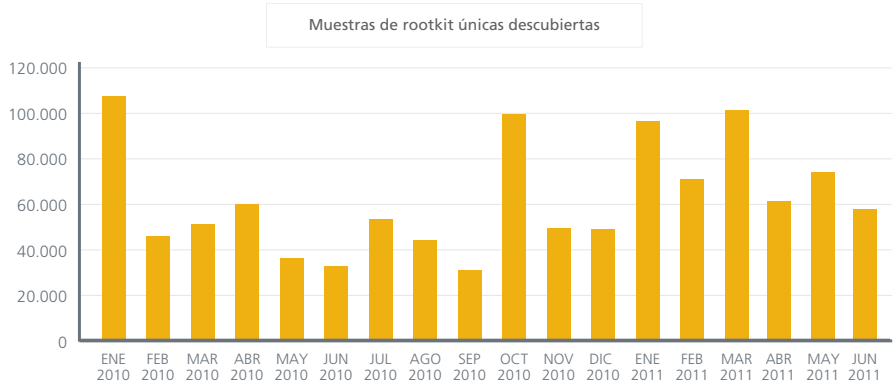






Rootkits y malware invisible

Otra categoría de malware que recientemente ha mostrado un crecimiento constante son los rootkits. Un rootkit (a veces llamado malware invisible) es un código que oculta sus elementos al sistema operativo y al software de seguridad. Los ciberdelincuentes utilizan rootkits para que el malware sea aún más sigiloso y persistente. Cuanto más oculto esté, más tiempo permanecerá en el sistema y podrá realizar actividades maliciosas. Como puede verse en los siguientes gráficos, en general los rootkits están aumentando. En la primera mitad de 2011 eran equivalentes al total del malware: los rootkits han tenido el primer semestre más activo, con un crecimiento de casi el 38% con respecto a 2010. Dos de los rootkits más activos que hemos encontrado son Koutodoor y TDSS, que se ocultan para robar datos.



Clasificación de equipos infectados en todo el mundo

A escala mundial y por localización geográfica, gran parte del malware que recopilamos este trimestre coincidió con los mismos tipos que pudimos observar durante el primer trimestre. Observamos también algunas diferencias entre los diferentes continentes, pero en general son más las similitudes que las diferencias.

Clasificación	5 tipos de malware más detectados a nivel mundial
1	Malware autoejecutable
2	Adware OpenCandy
3	Adware HotBar
4	Troyanos genéricos
5	Adware HotBar vF

Clasificación	Norteamérica
1	Malware autoejecutable
2	Adware HotBar
3	Adware OpenCandy
4	Malware de descargas
5	Adware HotBar vF

Clasificación	América del Sur
1	Malware autoejecutable
2	Ataque a Java Runtime
3	Malware autoejecutable Conficker
4	Troyanos de acceso remoto
5	Malware de descargas

Clasificación	Europa y Oriente Próximo
1	Adware HotBar vF
2	Malware autoejecutable
3	Adware HotBar
4	Adware OpenCandy
5	Malware autoejecutable Conficker

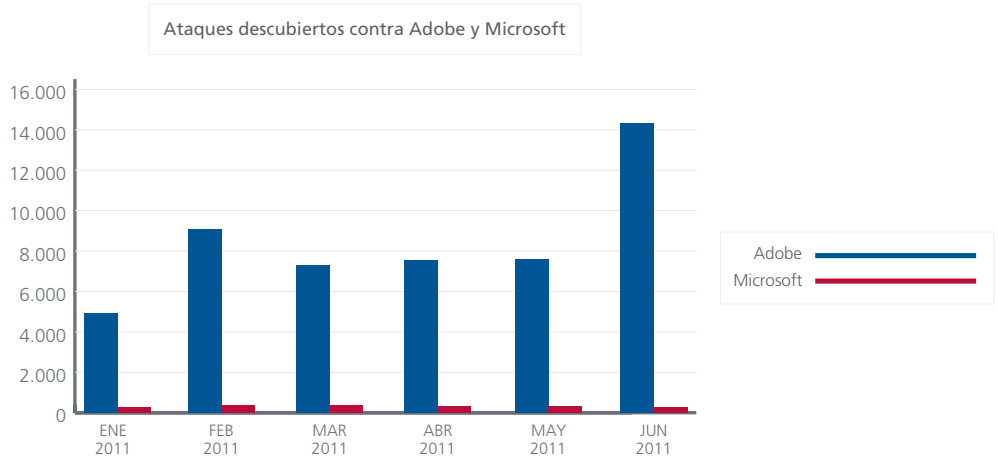
Clasificación	África
1	Malware autoejecutable
2	Malware de descargas
3	Malware de descargas
4	Malware de Yahoo Messenger
5	Virus Sality

Clasificación	Asia
1	Malware autoejecutable
2	Malware de descargas
3	Malware autoejecutable Conficker
4	Malware de descargas
5	Ataques a navegadores

Clasificación	Australia
1	Adware OpenCandy
2	Malware de descargas
3	Adware Hotbar
4	Malware de descargas
5	Malware autoejecutable

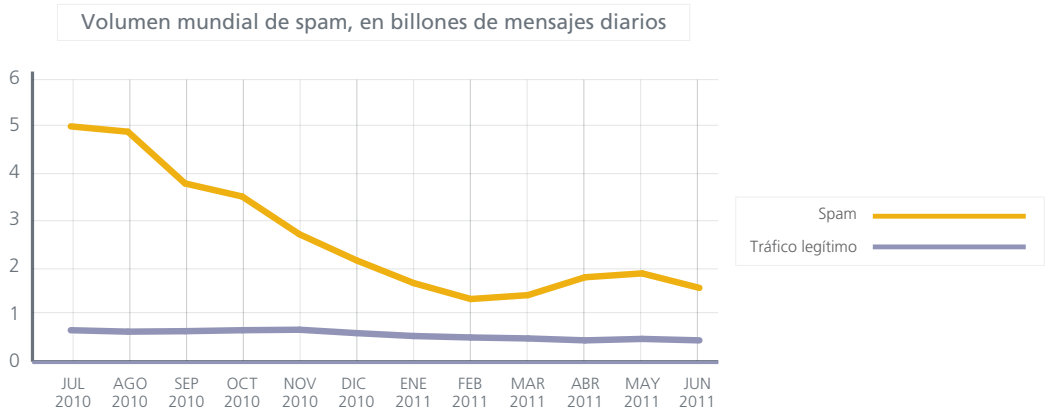
Los ataques a Adobe superan a los de Microsoft

Durante varios trimestres, una de las principales tendencias que hemos observado es que los autores de malware prefieren desarrollar ataques dirigidos a aprovechar las vulnerabilidades de los productos de Adobe, y no a los productos de Microsoft. Esta tendencia no demuestra que las tecnologías de Adobe sean más vulnerables o tengan más errores que las de Microsoft, sino más bien que Adobe es uno de los principales líderes mundiales en el sector de las aplicaciones cliente, un liderazgo que mueve a los creadores de malware y a los ciberdelincuentes: buscan lo que es muy conocido y de uso generalizado. El siguiente gráfico muestra el malware que los laboratorios McAfee Labs han observado este trimestre y que intenta explotar las vulnerabilidades de los productos de Adobe y de Microsoft.



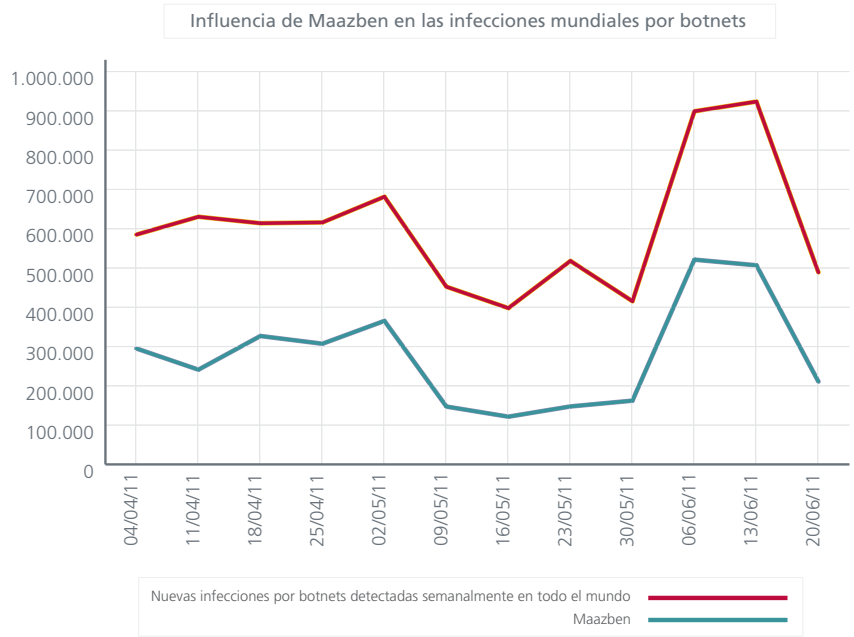
Amenazas de la mensajería

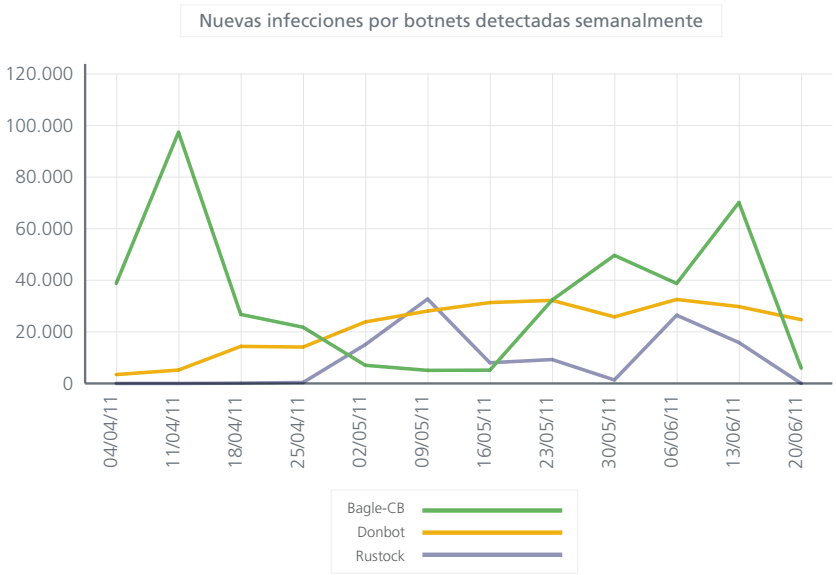
Las amenazas de la mensajería siguen en ligero descenso desde el último trimestre, aunque la disminución no es significativa. Durante el último trimestre, una acción coordinada de varios proveedores de seguridad, fuerzas de seguridad e incluso del CERT (equipo de respuesta de emergencias informáticas) ha logrado desactivar cantidades importantes de botnets, así como su estructura de mando. Es posible que esta victoria reciente tenga todavía un efecto positivo. Prevemos que volveremos a ver un aumento considerable del spam. Entretanto, seguiremos vigilando de cerca esta área. Aunque el volumen de spam se mantiene en mínimos históricos, el spearphishing (un tipo de spam) que podemos ver hoy en día tiene objetivos más claros y es más eficaz que nunca. Así pues, este vector sigue evolucionando.

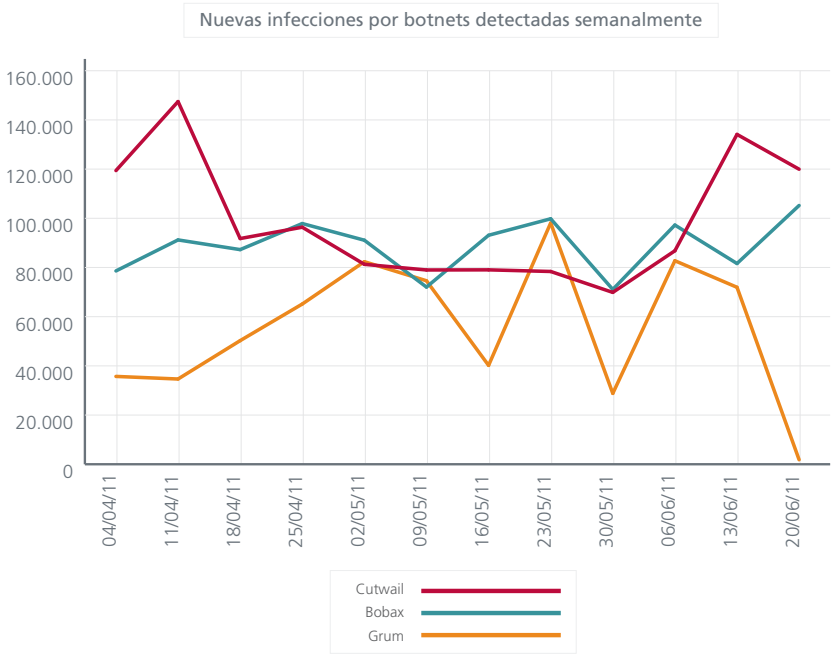



Volumen de spam por países
Italia
250.000.000
200.000.000
150.000.000
100.000.000
50.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Japón
50.000.000
40.000.000
30.000.000
20.000.000
10.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Polonia
200.000.000
150.000.000
100.000.000
50.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Portugal
100.000.000
80.000.000
60.000.000
40.000.000
20.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Rusia
350.000.000
300.000.000
250.000.000
200.000.000
150.000.000
100.000.000
50.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Corea del Sur
200.000.000
150.000.000
100.000.000
50.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
España
200.000.000
150.000.000
100.000.000
50.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Reino Unido
500.000.000
400.000.000
300.000.000
200.000.000
100.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Estados Unidos
1.500.000.000
1.200.000.000
900.000.000
600.000.000
300.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011
Venezuela
500.000.000
400.000.000
300.000.000
200.000.000
100.000.000
0
JUL 2010 AGO 2010 SEP 2010 OCT 2010 NOV 2010 DIC 2010 ENE 2011 FEB 2011 MAR 2011 ABR 2011 MAY 2011 JUN 2011

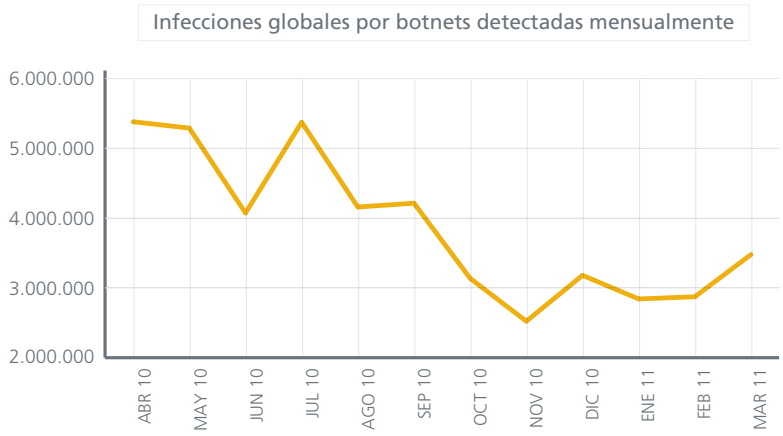
Este trimestre, los laboratorios McAfee Labs han observado una disminución de Rustock, aunque en los próximos meses los ciberdelincuentes podrían resucitarlo de nuevo. Entretanto, los dueños de los botnets Maazben, Cutwail y Bobax han intensificado su actividad. De estos tres botnets dominantes, el uso y la influencia de Maazben supera con creces a los de los otros en todo el mundo.



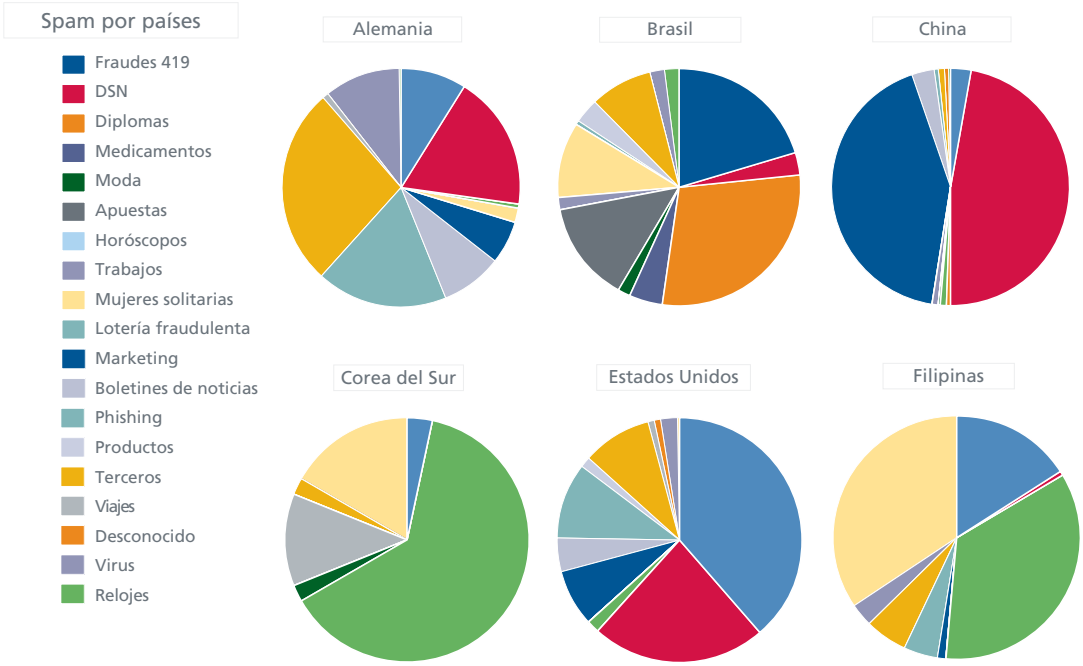

Nuevas infecciones por botnets detectadas semanalmente
120.000
100.000
80.000
60.000
40.000
20.000
0
04/04/11
11/04/11
18/04/11
25/04/11
02/05/11
09/05/11
16/05/11
23/05/11
30/05/11
06/06/11
13/06/11
20/06/11
Bagle-CB
Donbot
Rustock

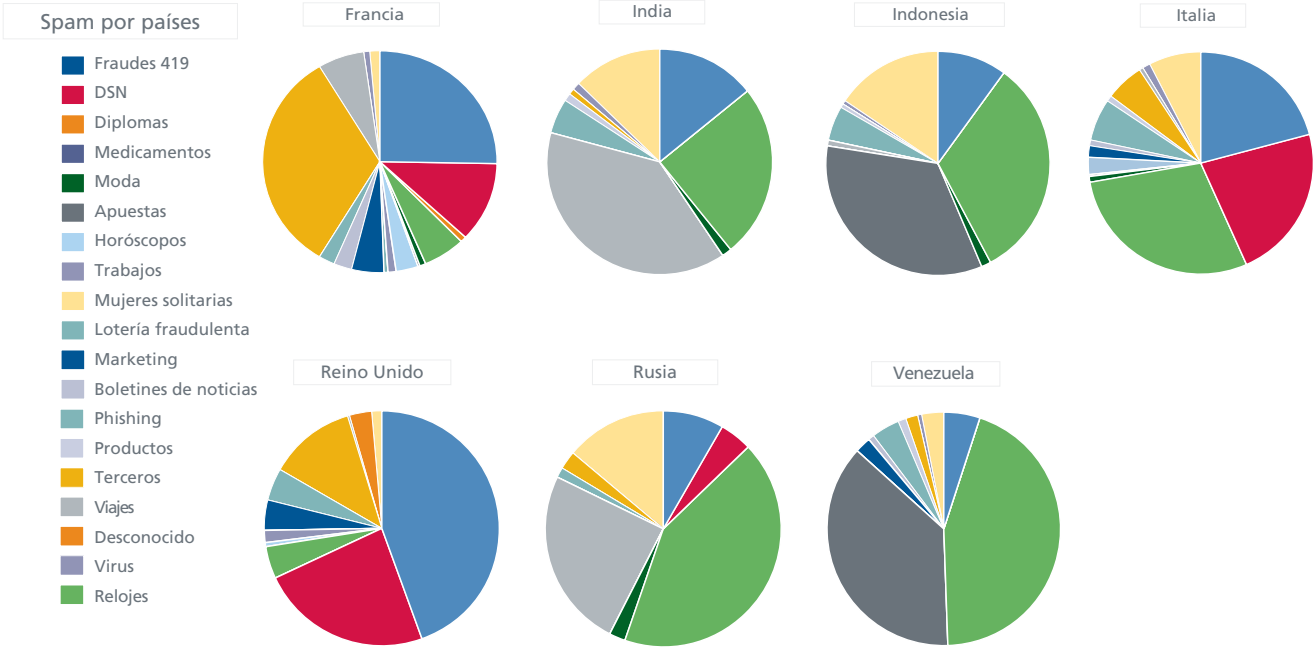

Nuevas infecciones por botnets detectadas semanalmente
160.000
140.000
120.000
100.000
80.000
60.000
40.000
20.000
0
04/04/11
11/04/11
18/04/11
25/04/11
02/05/11
09/05/11
16/05/11
23/05/11
30/05/11
06/06/11
13/06/11
20/06/11
Cutwail
Bobax
Grum

Las infecciones nuevas por botnets han seguido creciendo durante el trimestre, lo cual contrasta de forma interesante con la reducción global del spam. Es evidente que el uso de los botnets se encuentra en un momento de transición. Dado el crecimiento y los objetivos de los hacktivistas, seguramente presenciaremos grandes cambios en cómo se utilizan.



El spam es un señuelo y los asuntos (el gancho que utiliza la ingeniería social para que el mensaje sea atractivo) siguen siendo diversos. Las "estafas nigerianas 419" parecen un poco más extendidas este trimestre a escala mundial, mientras que la lotería fraudulenta también prevalece en muchas partes del mundo, junto con la antigua cuestión de los DSN falsos y los timos de apuestas. Con total seguridad, los señuelos seguirán diseñándose con técnicas de ingeniería social, ya que los estafadores conocen los intereses diversificados de su audiencia mundial.

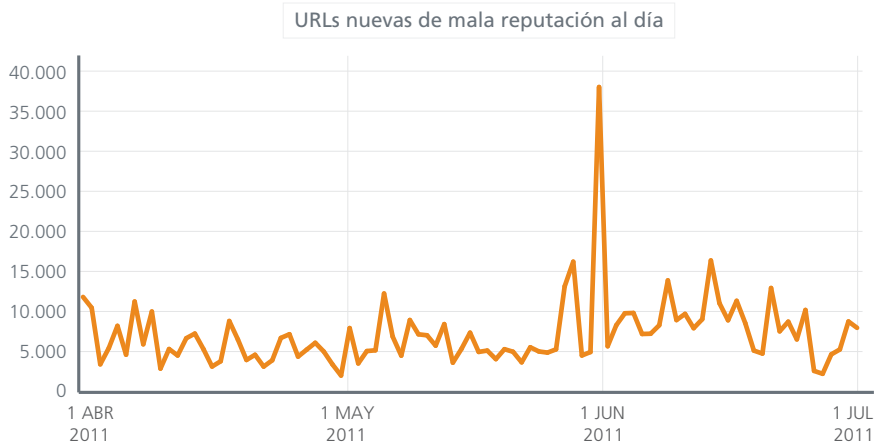




Amenazas de la Web

Los sitios web pueden tener 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 con mala reputación suelen alojar malware y programas potencialmente no deseados, o bien se trata de sitios web de phishing. A menudo se observa una combinación de código y funcionalidad dudosos. Son muchos los factores que influyen en la clasificación de la reputación de un sitio web.

El pasado trimestre, los laboratorios McAfee Labs registraron una media de 8.900 sitios web maliciosos nuevos al día, mientras que durante este período la cifra ha descendió ligeramente a 7.300, una cifra similar a la del mismo período el año pasado.

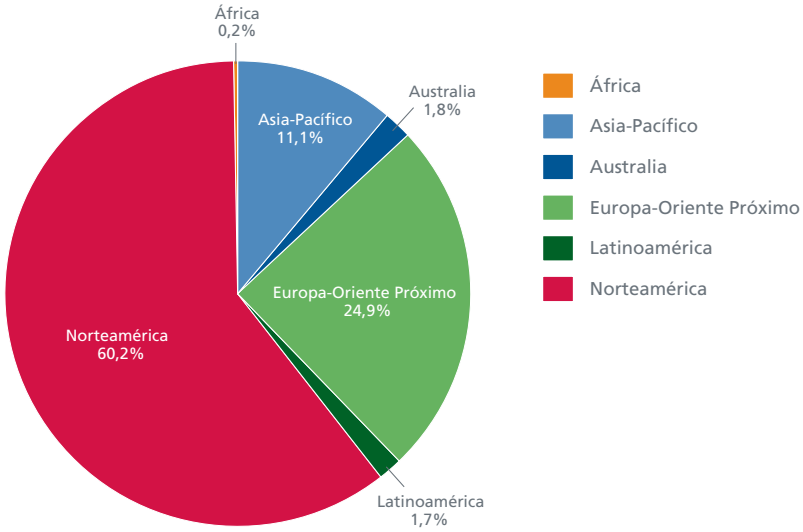


Este trimestre hemos visto algunos picos significativos en las páginas web de contenido malicioso, algunos de los cuales corresponden a intensas campañas con fines maliciosos.

El 31 de mayo, algunas campañas de spam, como una que ofrecía sitios web de contactos online con chats y vídeo y otra que informaba a los destinatarios que tenían pendientes facturas falsas, distribuyeron enlaces fraudulentos que contenían malware relacionado con Zeus (Generic FakeAlert.by y Generic PWS.y). Entre estos estos sitios web estaban undss-syria.org, baranava.com, emajic.net y sturtholdfastmarioncc.com.

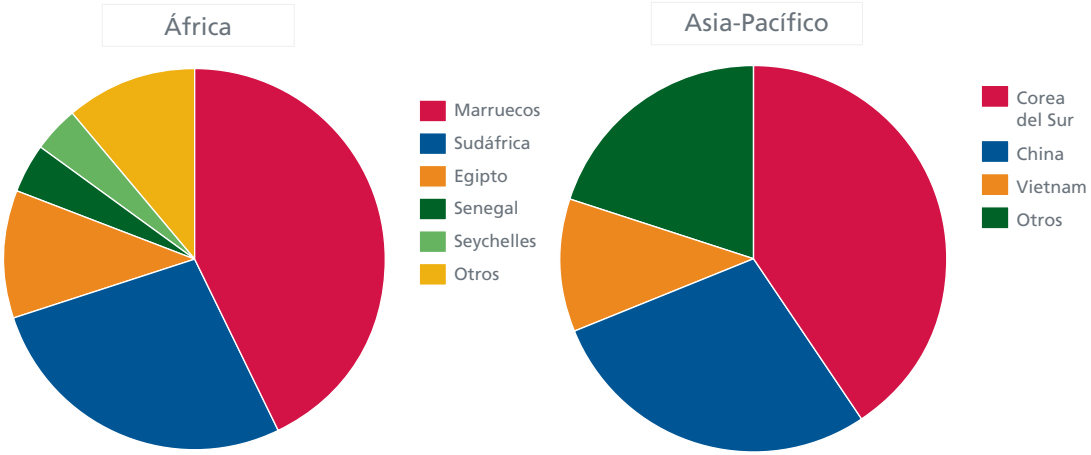
La gran mayoría de estos sitios web maliciosos nuevos se encuentran en Estados Unidos, seguidos por Corea del Sur, los Países Bajos, Canadá, el Reino Unido, China y Alemania.

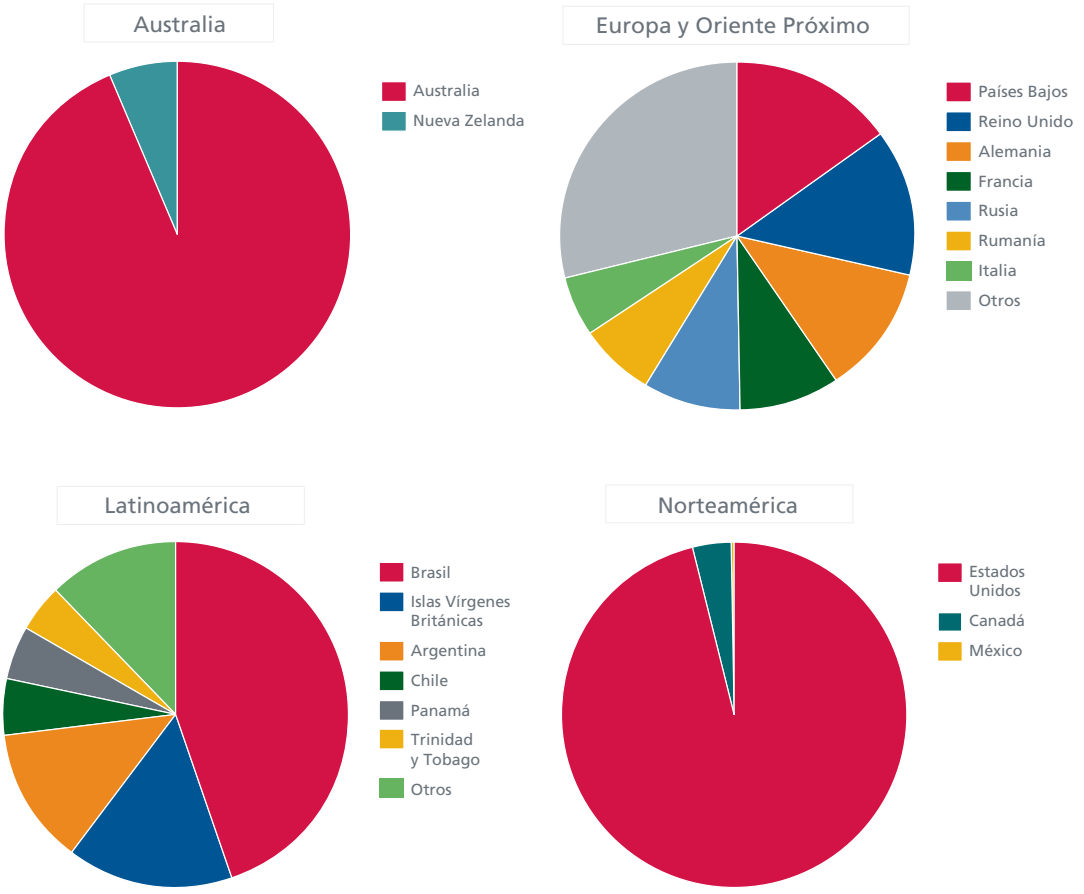
Durante el primer trimestre, los primeros países fueron Estados Unidos, Corea del Sur, Alemania y China. Este trimestre, sin embargo, es muy distinto. Nuestro análisis regional detallado revela dónde se encuentra la mayoría de los servidores maliciosos:



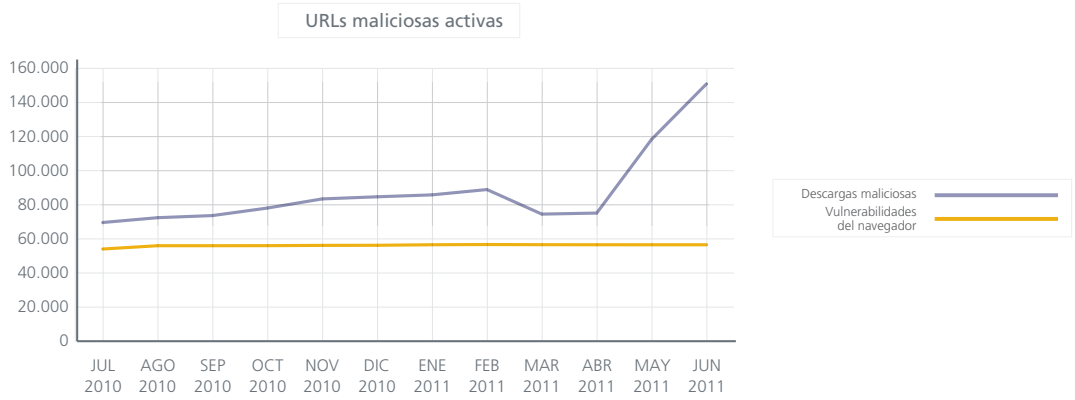
Norteamérica, principalmente Estados Unidos, sigue liderando la clasificación, pero la cifra combinada de Europa, Oriente Próximo y África ha crecido del 18% del primer trimestre hasta el 25%.

Echemos un vistazo más detallado a algunas regiones:





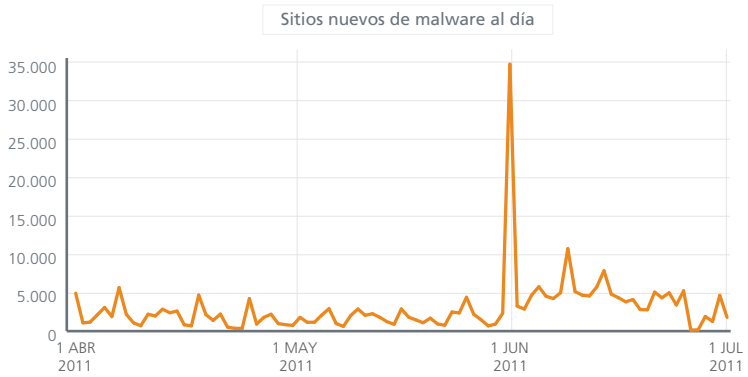
Este trimestre, la cantidad de sitios web que alojan descargas maliciosas ha aumentado de nuevo, y la cantidad de sitios web que atacan a los navegadores se mantiene invariable:



Este trimestre también observamos un aumento constante de los blogs y wikis con mala reputación.

Sitios web que distribuyen malware y programas potencialmente no deseados

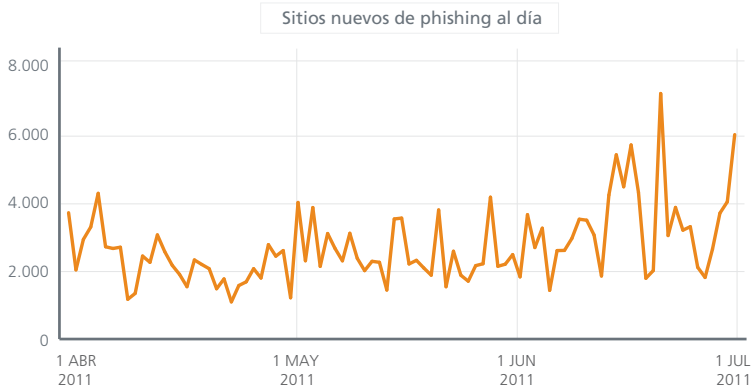
El siguiente gráfico ilustra a la perfección la cantidad de sitios web que distribuyen malware y programas potencialmente no deseados (PUPs) que los laboratorios McAfee Labs han detectado este trimestre.



Hemos observado un pequeño aumento este trimestre, con unos 3.000 sitios web nuevos al día en comparación con los 2.700 del primer trimestre.

Sitios web de phishing

Este trimestre hemos identificado aproximadamente 2.700 URLs de phishing al día, una cifra ligeramente superior a las 2.500 del trimestre anterior.



Acerca de los autores

Este informe ha sido preparado y redactado por Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, François Paget, Craig Schmugar, Jimmy Shah 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.

Acerca de McAfee

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 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. www.mcafee.com/es

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

32000rpt_quarterly-threat-q2_0711_ETMG