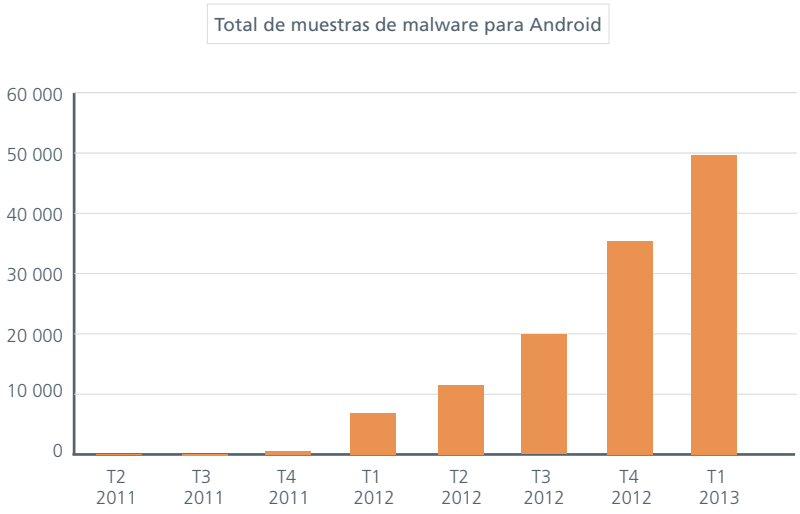
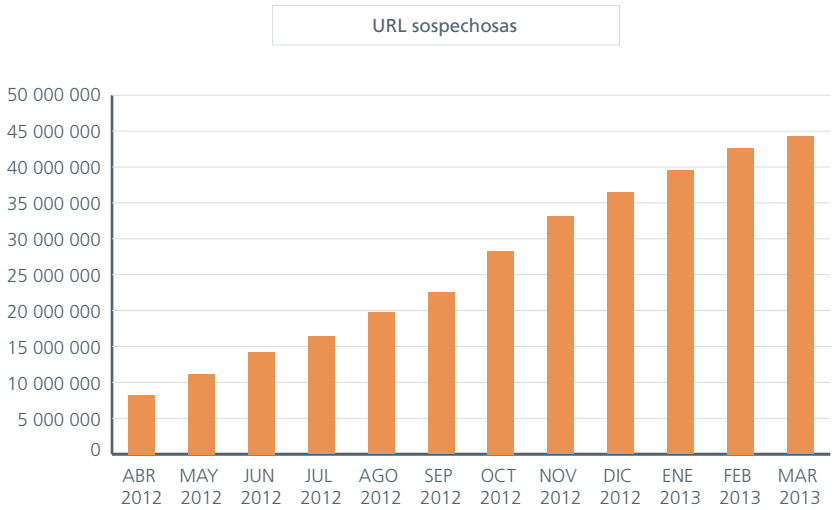
Durante el primer trimestre de 2013, la ciberdelincuencia global vivió un "Regreso al futuro" en su interminable búsqueda de víctimas y beneficios. Buena parte de las tendencias más significativas observadas por McAfee Labs en los tres trimestres anteriores remitieron en su actividad, mientras que algunos tipos de ataques antiguos, lo que podríamos denominar "retromalware", experimentaron un crecimiento importante.

A continuación se incluyen ejemplos de importantes tendencias observadas anteriormente que se ralentizaron durante el primer trimestre de 2013:

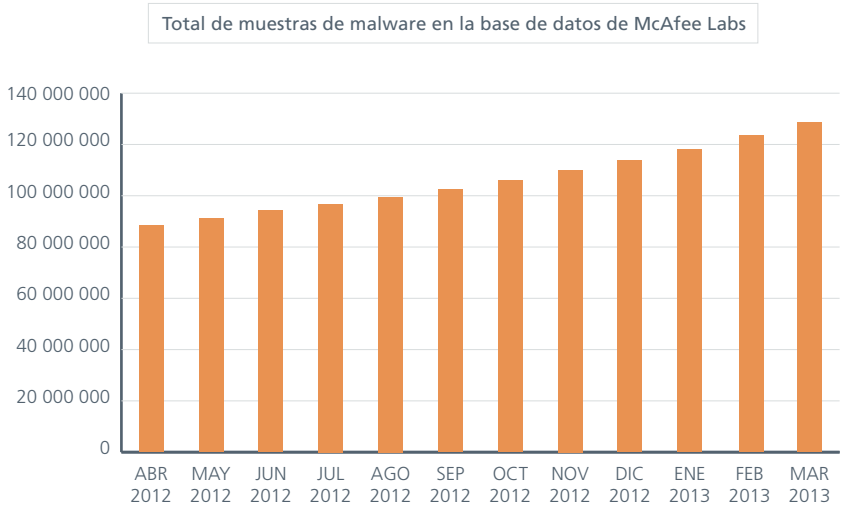
Descenso en la aparición de nuevo malware para dispositivos móviles (Android). A pesar de que el número total de nuevas muestras para Android aumentó un 40 %, esto representa una disminución del 10 % en la tasa de crecimiento respecto al cuarto trimestre de 2012.



Igualmente, el número de URL web maliciosas detectadas aumentó un 12 % en el primer trimestre, pero la tasa de crecimiento, que se situó por encima del 80 % en el cuarto trimestre de 2012, cayó casi 40 puntos porcentuales.



Incluso el crecimiento de muestras de malware conocido experimentó un ligero descenso durante el primer trimestre (28 %), en comparación con el cuarto trimestre de 2012 (38 %). McAfee Labs incorporó más de 14 millones de muestras de malware nuevas a su "zoológico" durante el pasado trimestre.



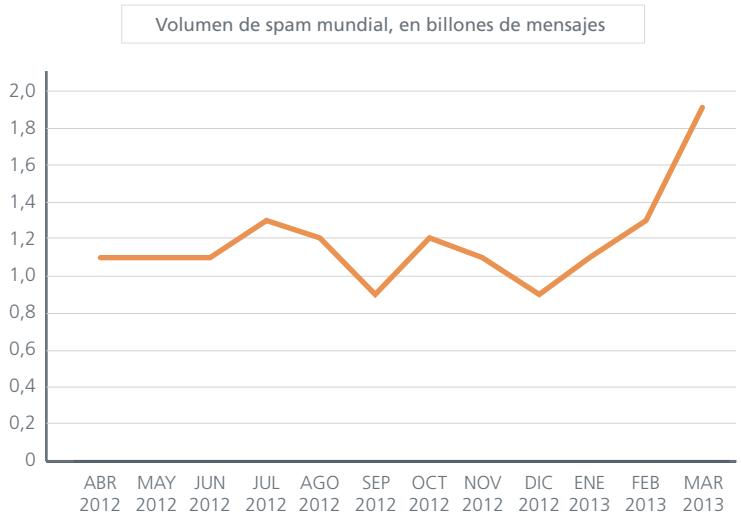
Por último, la tasa de crecimiento en el volumen de ladrones de contraseñas, ransomware, antivirus falso y rootkits descubiertos se mantuvo relativamente estable durante el primer trimestre. Aunque sus tasas de crecimiento hayan descendido ligeramente, todas estas amenazas siguen creciendo en cifras absolutas.

Sin embargo, esta ralentización en las tasas de crecimiento no significa que el ciberespacio sea cada vez más seguro. Muy al contrario, si combinamos este hecho con otras tendencias observadas durante el primer trimestre, daría la impresión de que los ciberdelincuentes son más inteligentes y disciplinados, ya que se inclinan claramente por ataques selectivos dirigidos contra comunidades o territorios específicos. Al igual que las empresas, los sindicatos de la ciberdelincuencia buscan optimizar su eficacia y sus beneficios. La tendencia observada hacia los ataques selectivos parecería indicar que el panorama de amenazas mundial se mueve en una dirección nueva y más peligrosa.

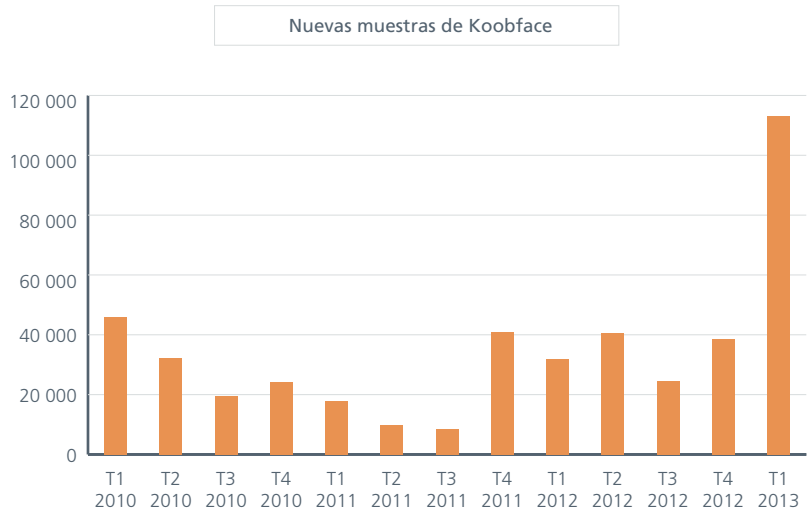
Un ejemplo clave de esta tendencia hacia los ataques selectivos es el troyano Citadel. Diseñado originalmente para robar dinero de determinados bancos, Citadel se ha "actualizado" ahora y puede utilizarse para apoderarse de información personal de las víctimas elegidas por los delincuentes.

Otras tendencias del primer trimestre que, aunque rememoran tiempos pasados, se emplean ahora en ataques selectivos y más peligrosos, son las siguientes:

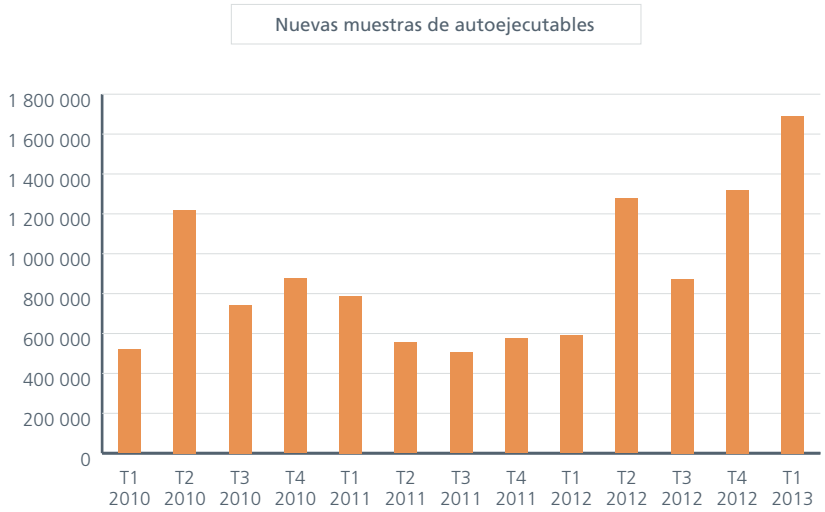
McAfee Labs detectó el primer aumento en el volumen mundial de spam en más de tres años. Y no se trata de un hecho sin importancia, ya que el volumen se multiplicó casi por dos en el primer trimestre de 2013. Sin embargo, a nivel mundial este dato puede llevar a confusión, ya que McAfee Labs observó diferencias muy significativas en el crecimiento del spam por regiones. Una vez más, los agresores parecen inclinarse por regiones y timos concretos con la esperanza de embaucar a nuevas víctimas. Entre los timos más populares detectados durante el primer trimestre se encuentran las manipulaciones bursátiles (operaciones especulativas "pump-and-dump") y las ofertas de supuestos medicamentos relacionados con la hormona del crecimiento.



Los casos de Koobface, un gusano descubierto por primera vez en 2008, habían sido relativamente escasos durante el último año, pero se *triplicaron* durante el primer trimestre de 2013, alcanzado niveles nunca vistos hasta la fecha. Como no podía ser de otra manera, los ciberdelincuentes están convencidos de que los usuarios de medios sociales son una mina de víctimas potenciales.



La otra "amenaza retro" que experimentó un importante repunte en el primer trimestre fueron las muestras de malware autoejecutable. Tradicionalmente, los gusanos autoejecutables se distribuían a través de unidades USB o CD. Los ciberdelincuentes los encuentran especialmente útiles, ya que pueden utilizarse para instalar puertas traseras o ladrones de contraseñas en las máquinas infectadas. Es posible que este repunte en las detecciones de autoejecutables pueda atribuirse a la popularidad de los servicios para compartir archivos basados en la nube.



Además de estos ataques "del pasado", McAfee Labs observó un importante crecimiento en una técnica relativamente nueva de ataques a la "pila de almacenamiento". Conocidos habitualmente como ataques contra el registro de arranque maestro (MBR), su objetivo es infectar el sistema de almacenamiento de la máquina y desde ahí hacerse con el control de todo el dispositivo. El número de muestras de ataques MBR aumentó más del 30 % durante el primer trimestre.

¿Cuáles son las implicaciones de estas tendencias en un momento en que las empresas intentan optimizar su nivel de seguridad? En lo relativo a la protección de endpoints, esta evolución del panorama de amenazas exige el uso de defensas por capas que incluyan no solo una solución antivirus básica, sino también prevención de intrusiones y filtrado web. Con el aumento continuado del uso de sitios web infectados para distribuir malware, estas dos funciones son más importantes que nunca. En determinados entornos, es posible que también se requiera la incorporación de herramientas de seguridad de dispositivos y de control de aplicaciones para garantizar la protección de la información esencial almacenada en los dispositivos de los usuarios finales.

Además de la protección de endpoints por capas, los administradores de seguridad deberían contar con herramientas de informes y respuestas más funcionales. Esta evolución en la que podríamos llamar "cabina de mando de la seguridad" será cada vez más esencial para que los profesionales puedan responder con rapidez y efectividad a los nuevos ataques selectivos que están surgiendo.

La protección de la infraestructura también precisará la adopción de un enfoque por capas para hacer frente a las amenazas que proceden de la Web, el correo electrónico y la red. La mejor manera de protegerse contra las nuevas amenazas es neutralizarlas antes de que se introduzcan en la infraestructura de la empresa. Sin embargo, además de las estrategias estándar de protección del perímetro, el aumento del uso de servicios basados en la nube hace que la seguridad de la empresa deba ampliarse a la nube e implementarse de forma coherente, con independencia de dónde se encuentren los datos confidenciales y las aplicaciones esenciales.

Puede encontrar el informe completo en http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2013.pdf.

McAfee
An Intel Company

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