

Informe sobre amenazas

McAfee Labs

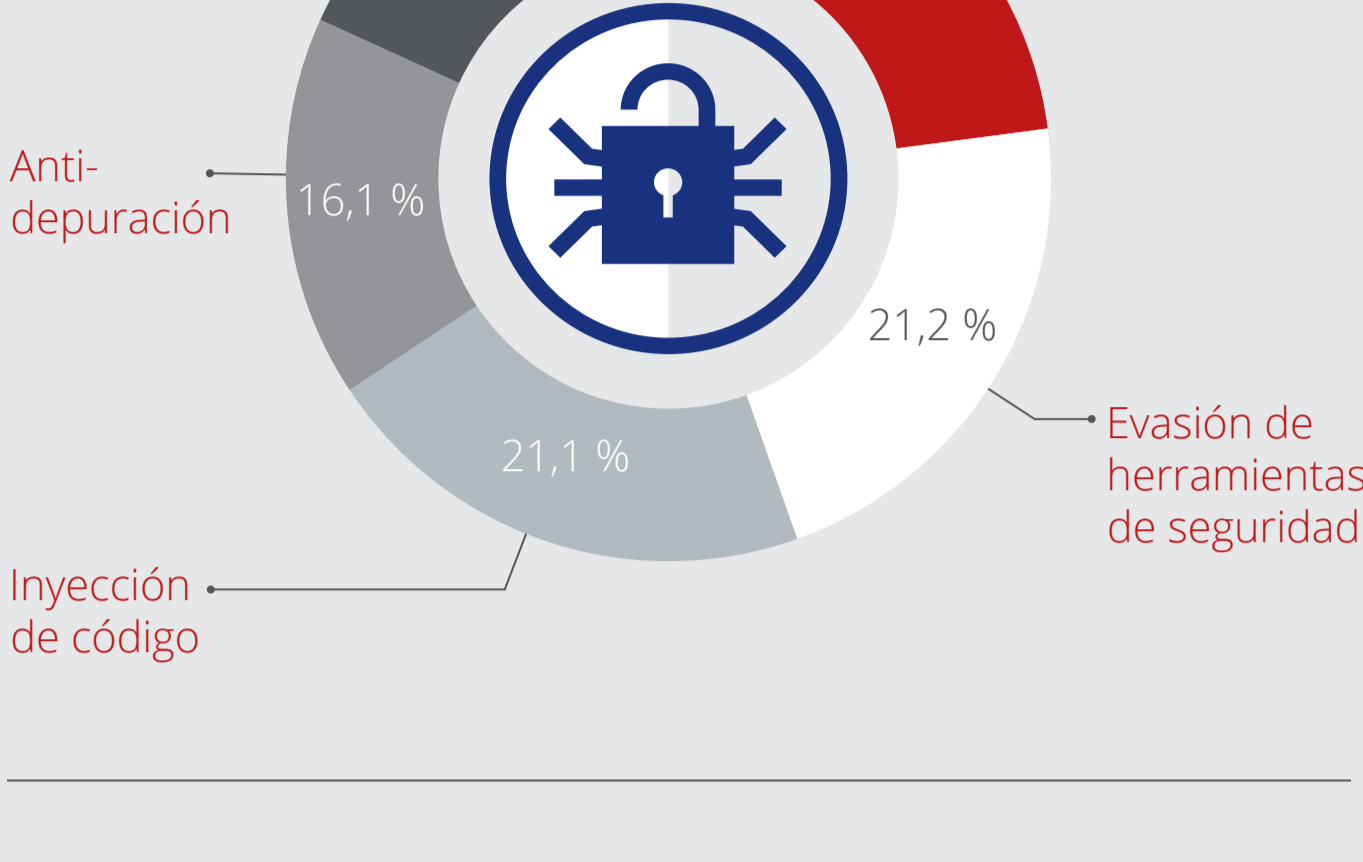
Técnicas de evasión de malware y tendencias

Las técnicas de evasión que emplea el malware son fáciles de conseguir y cada vez más potentes.

Historia de las técnicas de evasión



Técnicas de evasión empleadas por el malware



Evasión
El código de técnicas de evasión puede comprarse en el mercado, en ocasiones gratis.

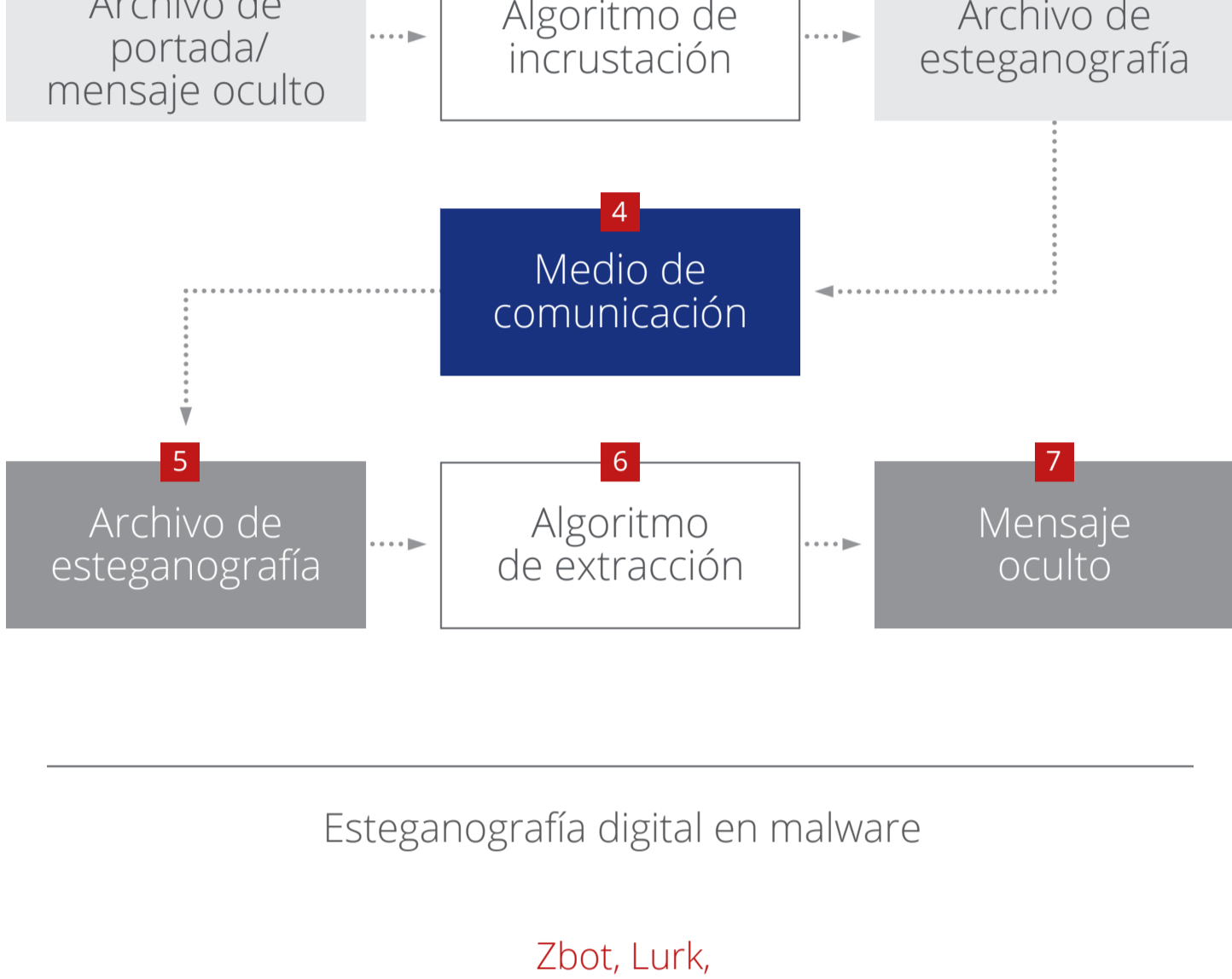
Firmware
La infección del firmware es un método en auge para evitar la detección.

Aprendizaje automático
Los ciberdelincuentes desarrollan técnicas para evadir la seguridad mediante aprendizaje automático.

Ocultos a plena vista: la amenaza oculta de la esteganografía

La esteganografía: el arte y la ciencia de ocultar información secreta.

El proceso de esteganografía digital



Esteganografía digital en malware



Mensaje secreto
La esteganografía oculta un mensaje secreto dentro de un mensaje aparentemente legítimo.

440 a.C.
La esteganografía se ha venido utilizando de distintas maneras al menos desde el año 440 a.C.

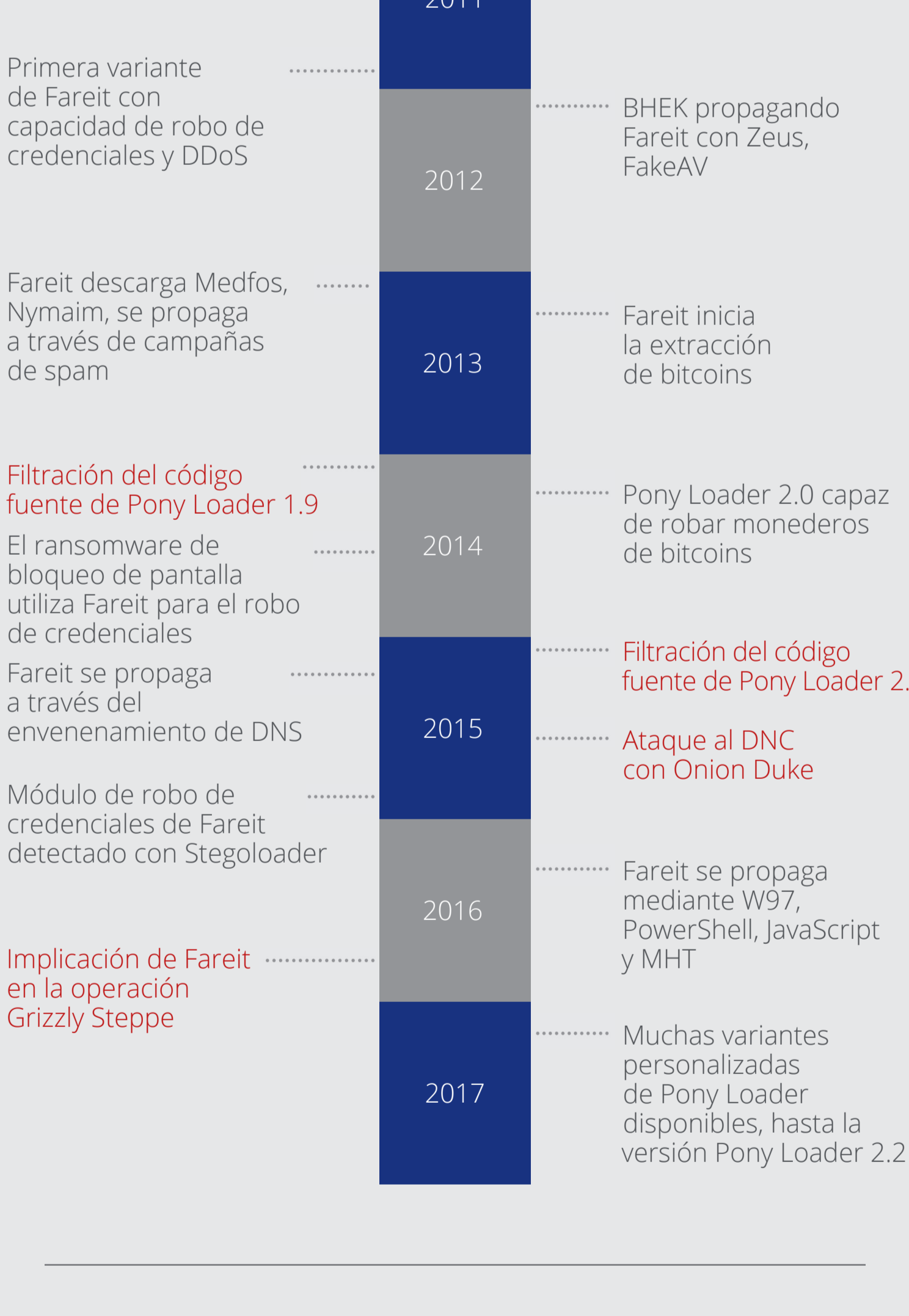
2011
El malware Duqu fue el primero en utilizar la esteganografía digital en 2011.

Red
La esteganografía de red es el último tipo de esteganografía digital utilizado por el malware.

El creciente peligro de Fareit, el ladrón de contraseñas

Casi todas las amenazas persistentes avanzadas utilizan ladrones de contraseñas en sus primeras fases. Probablemente Fareit se utilizó en el ataque de 2016 contra al Comité Nacional Demócrata de EE. UU.

Evolución de Fareit



5599
El malware Fareit fue descubierto en 2011. El año pasado se produjeron 5599 incidentes de clientes con Fareit.

Fareit tiene varias capacidades:

- Robar contraseñas
- Descargar y ejecutar malware arbitrario
- Lanzar ataques DDoS
- Robar monederos de criptomonedas
- Robar credenciales de FTP

Estadísticas sobre amenazas

En el primer trimestre aparecieron 244 amenazas nuevas cada minuto, o más de 4 cada segundo.

Incidentes

Contabilizamos 301 incidentes de seguridad hechos públicos en el primer trimestre, lo que supone un incremento del 53 % respecto al cuarto trimestre. Los servicios de salud, el sector público y el de la educación acumularon más del 50 % del total. El 78 % del total de incidentes de seguridad hechos públicos en el primer trimestre se produjeron en América.

Malware

Las nuevas muestras de malware repuntaron hasta los 32 millones en el primer trimestre. El número total de muestras de malware aumentó un 22 % en los últimos cuatro trimestres hasta los 670 millones.

Malware para móviles

Las notificaciones de malware para móviles se duplicaron en Asia durante el primer trimestre, lo que contribuyó a aumentar las tasas generales de infección en un 57 %. El número total de muestras de malware para móviles aumentó un 79 % en los últimos cuatro trimestres hasta los 16,7 millones.

Ransomware

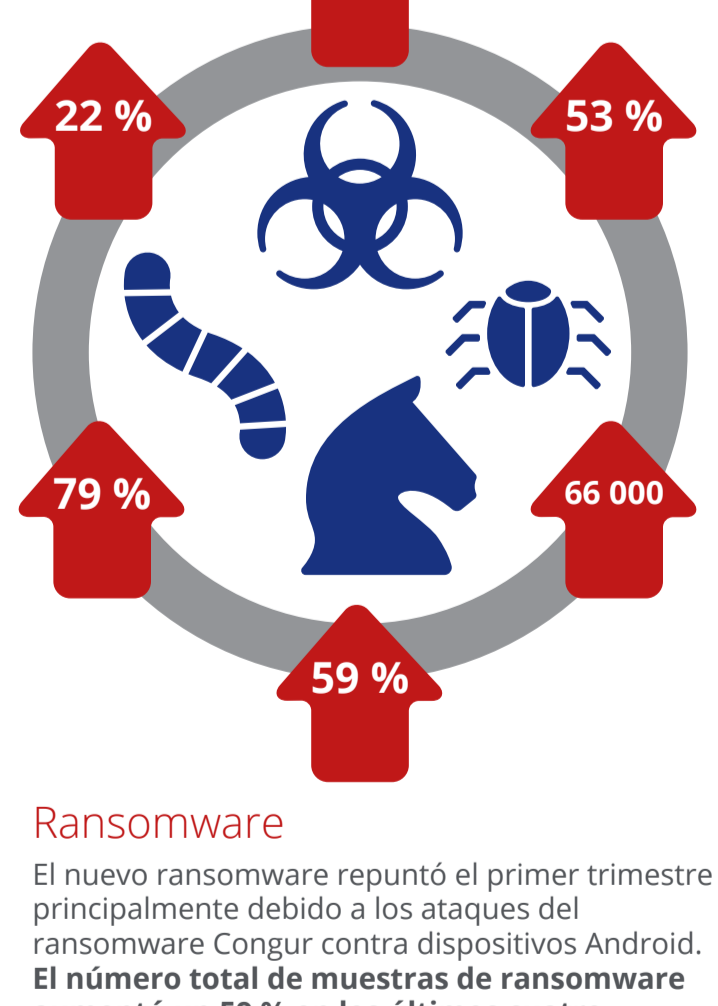
El nuevo ransomware repuntó el primer trimestre principalmente debido a los ataques del ransomware Congur contra dispositivos Android. El número total de muestras de ransomware aumentó un 59 % en los últimos cuatro trimestres hasta los 9,6 millones.

Malware para Mac OS

Durante los tres últimos trimestres, una plaga de adware ha hecho crecer el malware para Mac OS. Aunque aún es pequeño comparado con las amenazas que recibe Windows, el número total de muestras de malware para Mac OS ha aumentado un 53 % en el primer trimestre.

Malware basado en macros

El nuevo malware basado en macros remitió respecto a la media de los 3 últimos años. 66 000 nuevas muestras de malware para macros se detectaron en el primer trimestre.



McAfee Global Threat Intelligence

McAfee GTI recibió de media 55 000 millones de consultas al día en el primer trimestre.

95 millones
Las protecciones de McAfee GTI contra URL de riesgo **ascendieron hasta los 95 millones al día en el 1.º trimestre, desde los 107 millones del 4.º trimestre**, debido a una mejora de la precisión.

56 millones
Las protecciones de McAfee GTI contra programas potencialmente no deseados **aumentaron hasta los 56 millones al día en el 1.º trimestre, desde los 37 millones del 4.º trimestre**.

34 millones
Las protecciones de McAfee GTI contra archivos maliciosos **descendieron hasta los 34 millones al día en el 1.º trimestre, desde los 71 millones del 4.º trimestre**, debido a una detección más temprana y una mejor inteligencia local.

59 millones
Las protecciones de McAfee GTI contra URL peligrosas **descendieron hasta los 59 millones al día en el 1.º trimestre, desde los 88 millones del 4.º trimestre**, debido a una detección más temprana.

Informe de McAfee Labs sobre amenazas: Junio de 2017
Visite www.mcafee.com/June2017ThreatsReport para ver el informe completo.