Junio de 2017

McAfee Together is power.

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

1980
Virus Cascade
Primer virus que utiliza cifrado para codificar su contenido.

1990
Familia de virus Chameleon
Primeros virus polimórficos

1998
Malware metamórfico
Regswap utiliza el metamorfismo a través de distintos registros para las mismas funciones.

1990s
Packers (Compresores)
Los compresores que cifran o comprimen se hacen muy populares debido al menor tamaño de la RAM y los discos.

1999-2003
Rootkits
En 1999, apareció el primer rootkit Windows —NTRootkit—, seguido por HackerDefender en 2003.

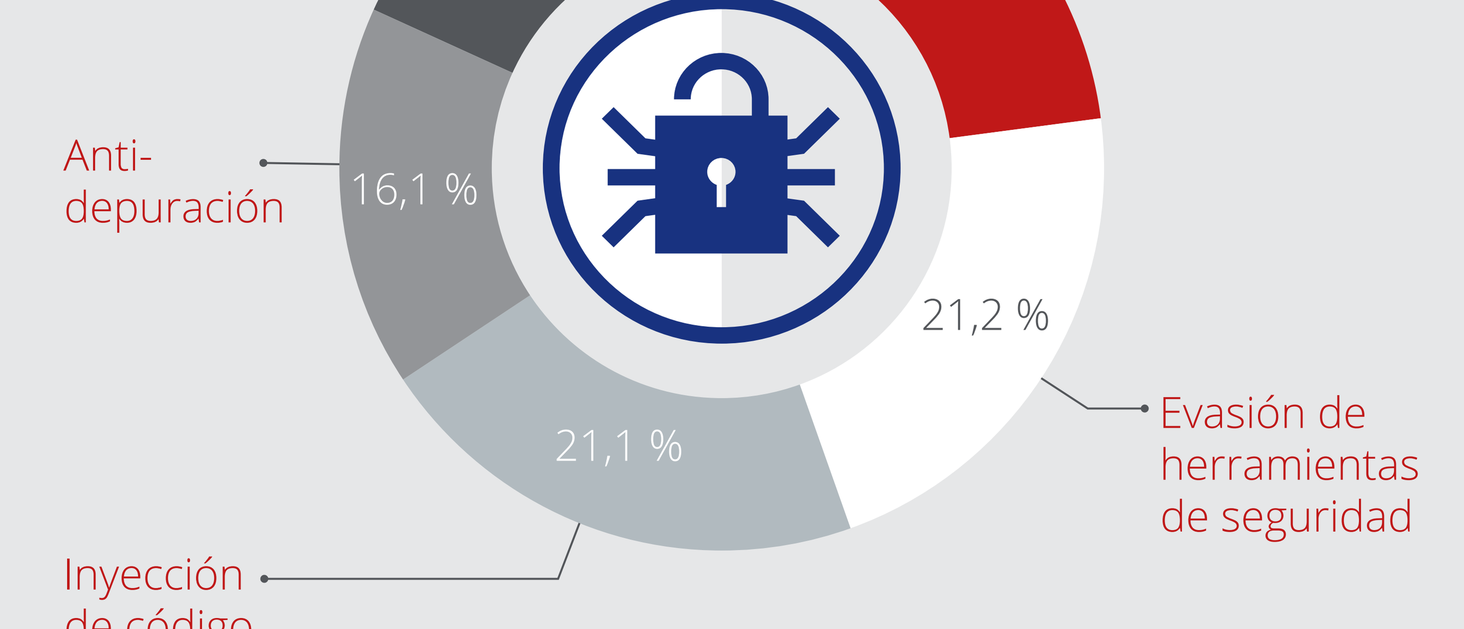
2008
Algoritmos de generación de dominios
El gusano Conficker utiliza un algoritmo de generación de dominios para sortear la detección de la red.

2011
Mercado de productos listos para utilizar
Silkroad es el primer mercado clandestino que vende productos y servicios de evasión para el malware.

2015-2017
Dridex, Locky
Primera ocultación a gran escala, uso de PowerShell y evasión de entorno aislado.

2015-2017
Malware de firmware
Las filtraciones de los grupos Equation Group y Hacking Team revelan el uso de malware de firmware para evitar ser detectados.

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

1. Archivo de portada/ mensaje oculto
2. Algoritmo de incrustación
3. Archivo de esteganografía
4. Medio de comunicación
5. Archivo de esteganografía
6. Algoritmo de extracción
7. Mensaje oculto

Esteganografía digital en malware

- 2010 – 2012: Duqu, Shady RAT, rootkit Alureon
- 2014: Zbot, Lurk, ZeusVM, MiniDuke, CosmicDuke
- 2016: Vawtrak, Stegoloader, Sundown, AdGholas, Magento CC, DNSChanger

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

440 a.C.
La esteganografía se ha venido utilizando de distantes 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

2011
- Primera variante de Fareit con capacidad de robo de credenciales y DDoS

2012
- BHEK propagando Fareit con Zeus, FakeAV

2013
- Fareit descarga Medfos, Nymaim, se propaga a través de campañas de spam
- Fareit inicia la extracción de bitcoins

2014
- Filtración del código fuente de Pony Loader 1.9
- El ransomware de bloqueo de pantalla utiliza Fareit para el robo de credenciales
- Pony Loader 2.0 capaz de robar monederos de bitcoins

2015
- Fareit se propaga a través del envenenamiento de DNS
- Filtración del código fuente de Pony Loader 2.0
- Ataque al DNC con Onion Duke
- Módulo de robo de credenciales de Fareit detectado con Stegoloader

2016
- Fareit se propaga mediante W97, PowerShell, JavaScript y MHT
- Implicación de Fareit en la operación Grizzly Steppe

2017
- Muchas variantes personalizadas de Pony Loader disponibles, hasta la versión Pony Loader 2.2

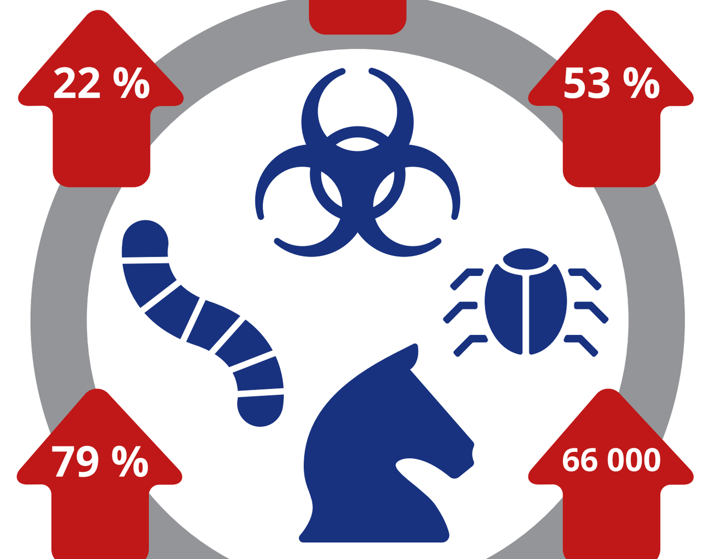
5599
El malware Fareit fue descubierto en 2011. El año pasado se produjeron 5599 incidentes de clientes con Fareit.

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 el 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 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 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.**

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.**

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.**

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 medio **descendieron hasta los 95 millones al día en el 1.er 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.er trimestre, desde los 37 millones del 4.º trimestre.**

McAfee GTI

34 millones
Las protecciones de McAfee GTI contra archivos maliciosos **descendieron hasta los 34 millones al día en el 1.er 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.er 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.

McAfee Together is power.

3181_0517_info-threat-report-malware-evasion