Tendencias de 2016 en ciberseguridad:

Guía rápida del conocimiento más importante sobre la seguridad

Microsoft

Microsoft lleva 10 años estudiando y analizando el panorama de las amenazas que suponen los ataques, las vulnerabilidades y el malware. Hemos utilizado datos recopilados de más de 600 millones de ordenadores de todo el mundo para elaborar uno de los conjuntos de datos sobre seguridad más completos. La investigación realizada se ha reunido y publicado en el documento The Microsoft Security Intelligence Report, un informe de 160 páginas reconocido mundialmente que aborda de forma integral el panorama de la seguridad.

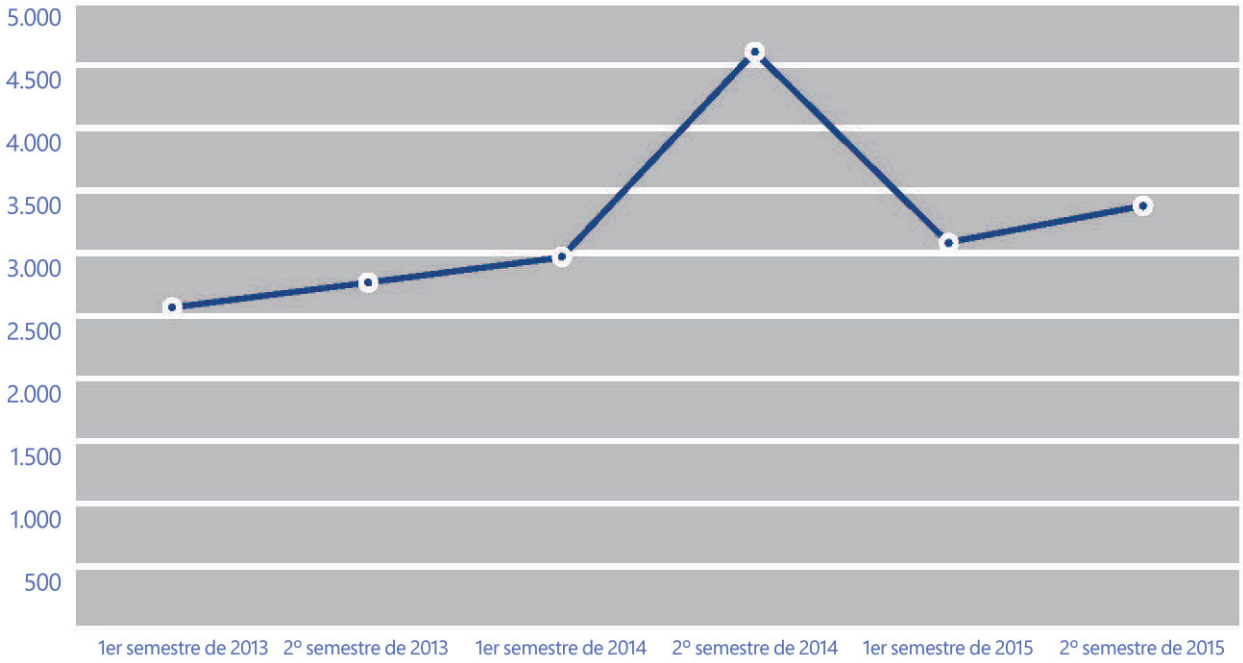
Este año, en un esfuerzo por dar a conocer las tendencias y el conocimiento clave, hemos elaborado también una Guía rápida del conocimiento más importante sobre la seguridad, un documento muy resumido y conciso en el que se exponen los factores más importantes de la ciberseguridad, que es muy compleja.

En este libro electrónico, hemos plasmado nuestras 10 conclusiones principales. Siga leyendo para obtener información importante sobre las tasas de vulnerabilidad, ataques en los principales programas informáticos, los lugares que presentan las tasas de infección más altas y mucho más. Cada año se comunican más de 6.000 vulnerabilidades en el sector, por lo que es sumamente importante evaluar y actualizar todo el software de su entorno de TI. A continuación ofrecemos nuestras 10 conclusiones principales para ayudarle a aumentar su nivel de seguridad.

Las tendencias

El 41,8 % de todas las vulnerabilidades declaradas se califican como muy graves, el valor máximo de los últimos tres años.

Divulgación de vulnerabilidades en todo el sector cada semestre en la segunda mitad de 2015

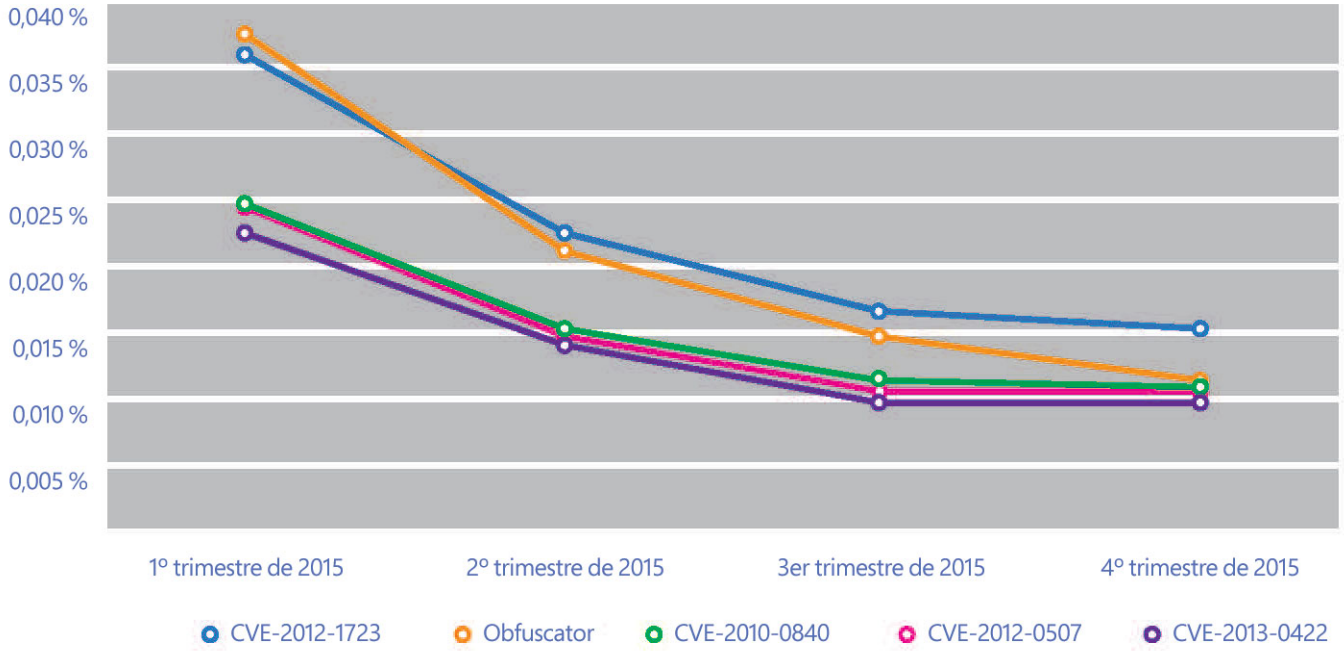


Por qué es importante

Las divulgaciones de vulnerabilidades son revelaciones de vulnerabilidades de software al público en general. Estas revelaciones pueden proceder de diversas fuentes, incluidos editores de software afectado, proveedores de software de seguridad, investigadores de seguridad independientes e incluso creadores de malware. Los atacantes y el malware intentan utilizar de manera sistemática vulnerabilidades sin parches para poner en peligro y cobrarse víctimas entre las organizaciones. Las divulgaciones de vulnerabilidades en el sector aumentaron un 9,4 % entre el primer y el segundo semestre de 2015, hasta situarse por encima de las 3.300. Estas son las vulnerabilidades graves que los equipos de seguridad tanto temen porque facilitan la actuación de atacantes remotos. Cada año se comunican públicamente más de 6.000 vulnerabilidades en el sector, por lo que es sumamente importante evaluar y actualizar periódicamente todo el software de su entorno de TI. Instale parches de software puntualmente, supervise las redes en busca de actividades sospechosas y ponga en cuarentena aquellos dispositivos que presenten un comportamiento inusual.

La presencia de ataques de Java están disminuyendo.

Tendencias de los principales ataques de Java detectados y bloqueados por productos antimalware en tiempo real de Microsoft en el segundo semestre de 2015

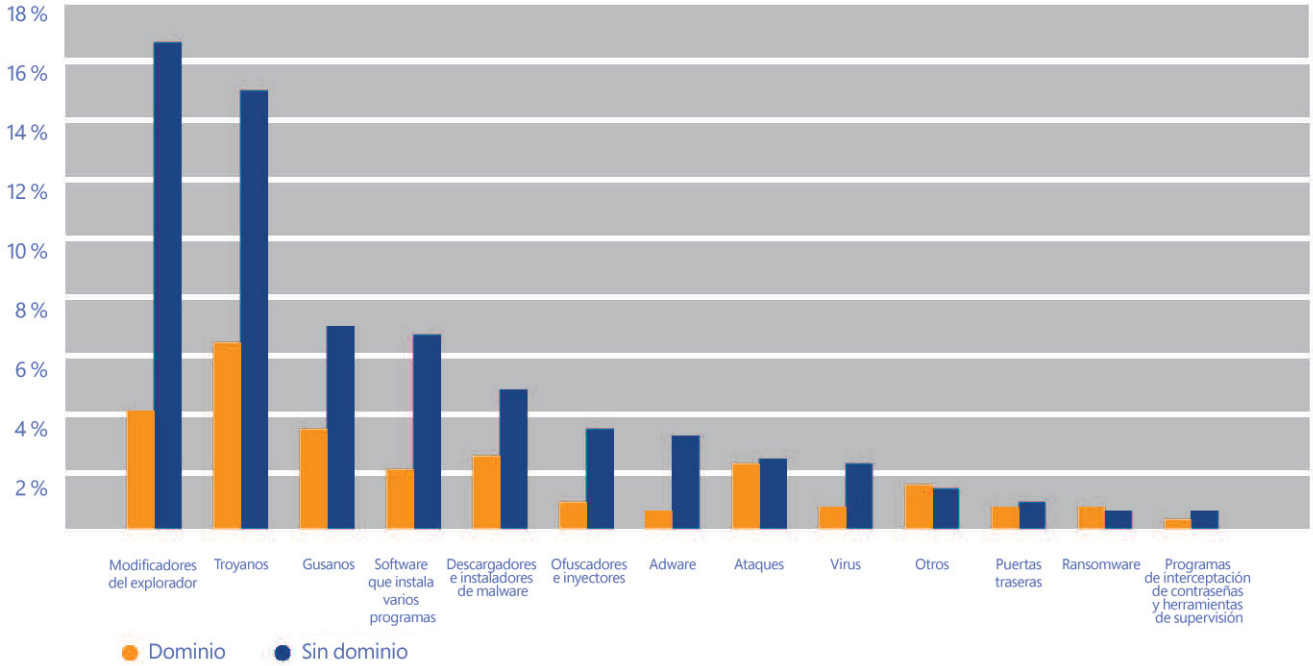


Por qué es importante

Los atacantes solían preferir los ataques de Java, pero eso ya es cosa del pasado. Esta disminución probablemente sea resultado de varios cambios importantes en la manera en que los exploradores web evalúan y ejecutan los applets Java. Ahora, los equipos de seguridad pueden establecer prioridades de sus esfuerzos y atender riesgos de mayor prioridad. Los usuarios de Java deben seguir instalando los parches de seguridad a medida que estén disponibles para seguir luchando contra posibles ataques futuros.

Los ordenadores de consumo presentan el doble de amenazas en comparación con los de empresa.

Tasa de presencia de malware y software no deseado en equipos basados en dominio y que no están unidos a un dominio.

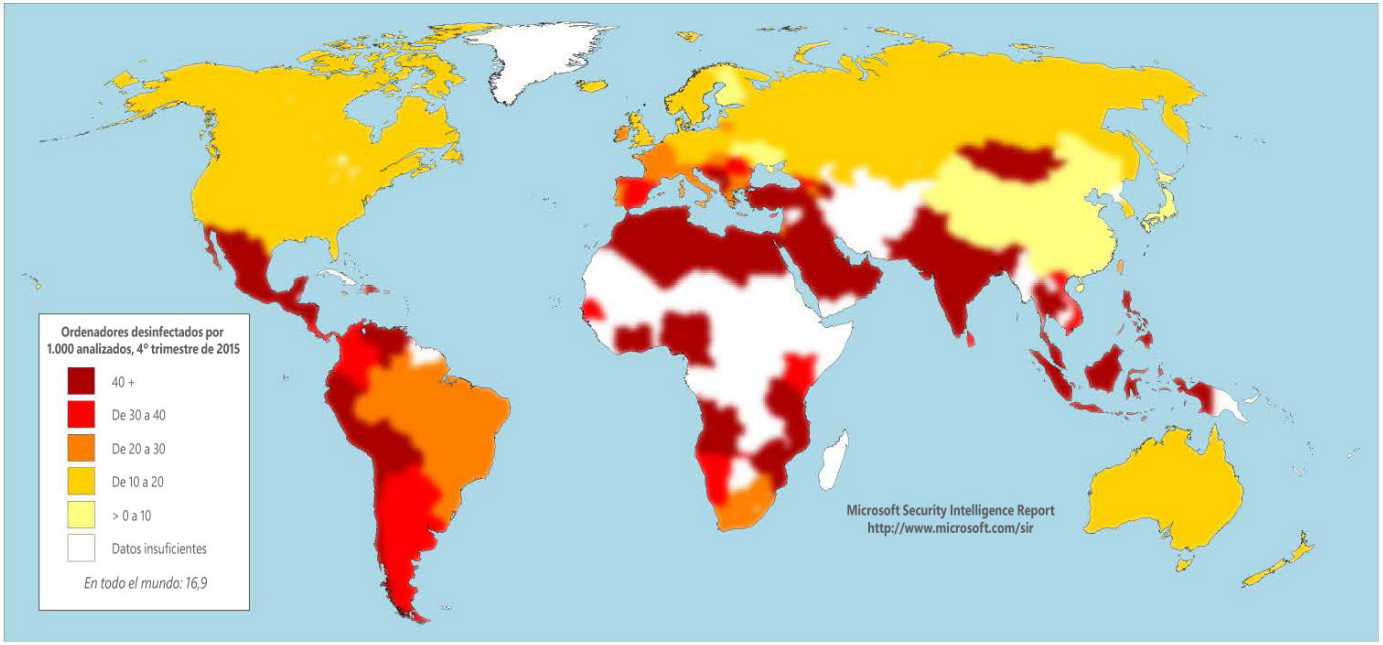


Por qué es importante

Los entornos empresariales suelen implementar medidas de defensa en profundidad, como firewalls empresariales, que impiden la llegada de cierta cantidad de malware a los ordenadores de los usuarios. Por tanto, los ordenadores de empresa suelen tener un índice de malware inferior al de los ordenadores de consumo. La tasa de presencia en los ordenadores de consumo era unas 2,2 veces superior a la de los ordenadores de empresa. Mientras tanto, los ordenadores de empresa (basados en un dominio) sufrieron ataques casi con la misma frecuencia que los ordenadores de consumo (sin dominio), a pesar de padecer menos de la mitad de malware que los ordenadores sin dominio en general. Esto indica a los responsables centrales de seguridad informática (CISO) que los ataques representan un problema para las organizaciones y que su mejor defensa consiste en mantenerse actualizadas con las actualizaciones de seguridad y las versiones más recientes del software. Pese a esas tendencias, puede proteger los activos de su compañía si comprende el panorama de amenazas y concibe una estrategia de seguridad en todos los frentes, incluidos: credenciales de identidad y acceso, aplicaciones y datos, dispositivos de red e infraestructura. La adopción de una actitud proactiva en cuanto a la seguridad y el uso de las últimas tecnologías de autenticación multifactor, aprendizaje automático y análisis le permiten reforzar las defensas de su empresa contra los ciberataques, y estar preparado para responder en caso de que se produzca alguna infracción.

Los lugares que presentaban las tasas de infección por malware más altas eran Mongolia, Libia, los Territorios Palestinos, Irak y Pakistán.

Tasas de infección por país o región



Por qué es importante

El malware está distribuido de manera desigual en todo el mundo y cada lugar cuenta con su propia combinación de amenazas. Estudiando las áreas del mundo que se ven muy afectadas por malware y comparándolas con las menos infectadas, podemos intentar descubrir los factores técnicos, económicos, sociales y políticos que influyen en las tasas de infección regionales por malware. Esta información podría facilitar la adopción de futuras políticas públicas fundamentadas lo que, a su vez, podría provocar una reducción de las tasas de infección por malware en partes muy infectadas del mundo.

También hay disponible un estudio anterior

Los kits de ataques representan el 40 % de los ataques más comunes.

Tendencias en la tasa de presencia trimestral para las familias de ataques detectados y bloqueados con más frecuencia por productos antimalware en tiempo real de Microsoft en el segundo semestre de 2015, de acuerdo con la prevalencia relativa

Ataque	Tipo	1º trimestre de 2015	2º trimestre de 2015	3er trimestre de 2015	4º trimestre de 2015
Axpergle	Kit de ataques	0,86 %	0,66 %	0,71 %	0,92 %
CVE-2010-2568 (cplLnk)	Sistema operativo	0,30 %	0,23 %	0,18 %	0,24 %
HTML/Meadgive	Kit de ataques	0,06 %	0,05 %	0,07 %	0,17 %
JS/NeutrinoEK	Kit de ataques	0,06 %	0,03 %	0,01 %	0,11 %
HTML/IframeRef	Genérico	0,07 %	0,05 %	0,04 %	0,05 %
JS/Neclu	Kit de ataques	0,03 %	0,15 %	0,05 %	0,01 %
ShellCode	Otro	0,01 %	0,02 %	0,01 %	0,03 %
Win32/Sdbby	Otro	0,00 %	0,09 %	0,02 %	0,01 %
CVE-2012-1723	Java	0,04 %	0,02 %	0,02 %	0,02 %
Java/Obfuskator	Java	0,04 %	0,05 %	0,02 %	0,01 %

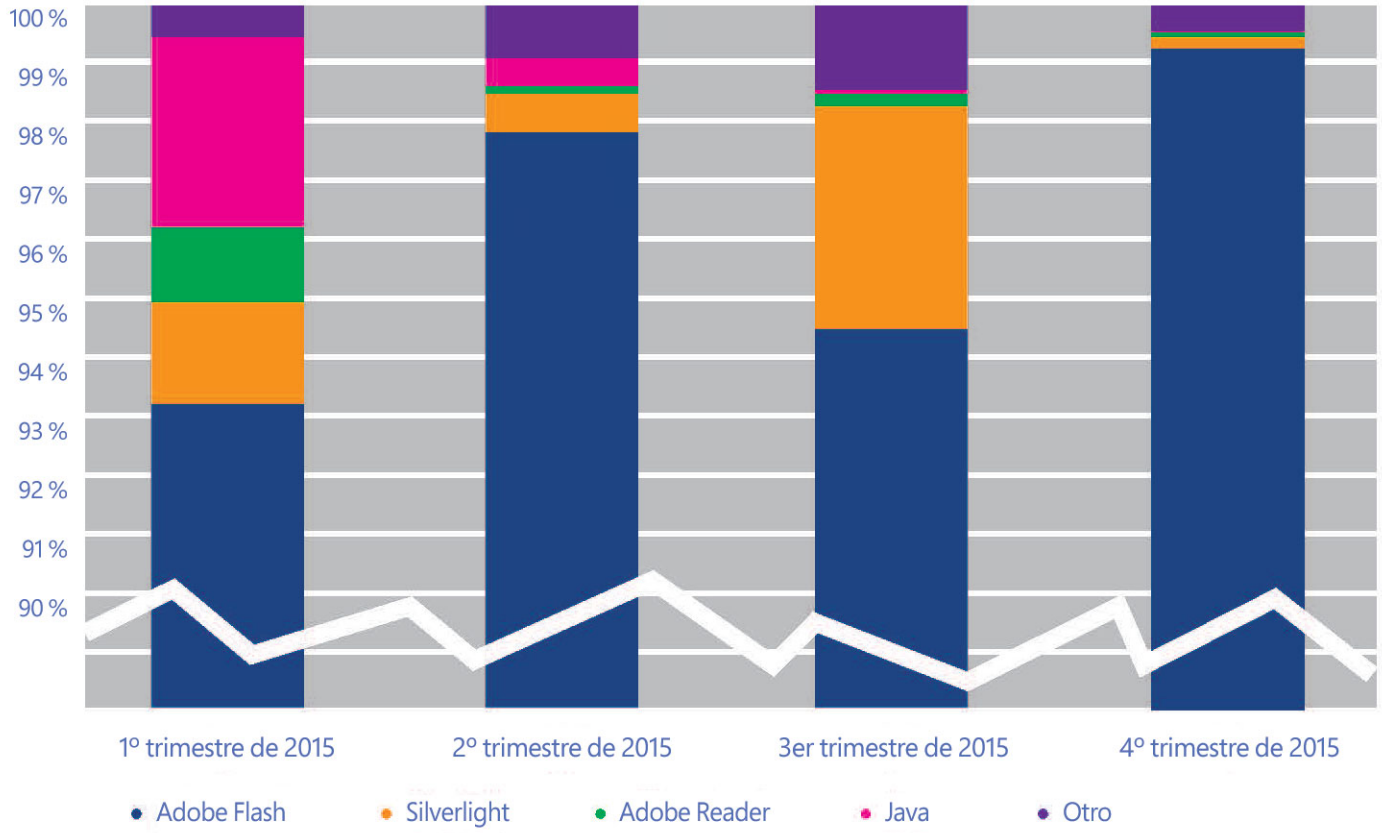
Por qué es importante

Los kits de ataques son recopilaciones de ataques agrupados que se venden como software comercial o como un servicio. Los posibles atacantes compran o alquilan kits de ataques en foros de hackers malintencionados y a través de otros puntos de venta ilegítimos. Un kit típico consta de una colección de páginas web que aprovechan varias vulnerabilidades de exploradores web y complementos de explorador populares.

Cuando el atacante instala el kit en un servidor web malintencionado o en peligro, los visitantes que no tienen instaladas las actualizaciones de seguridad adecuadas corren el riesgo de que sus ordenadores resulten infectados por ataques mediante descargas ocultas. Los kits de ataques permiten que atacantes poco cualificados lleven a cabo ataques más sofisticados.
Comprender los ataques y los kits de ataques usados por los atacantes ayuda a los equipos de seguridad a proteger sus organizaciones.

El tipo de objeto detectado con más frecuencia fue el de Adobe Flash Player, que aparecía en más del 90 % de las páginas malintencionadas durante un periodo de un año.

Controles ActiveX detectados en páginas web malintencionadas mediante IExtensionValidation en 2015, por tipo de control



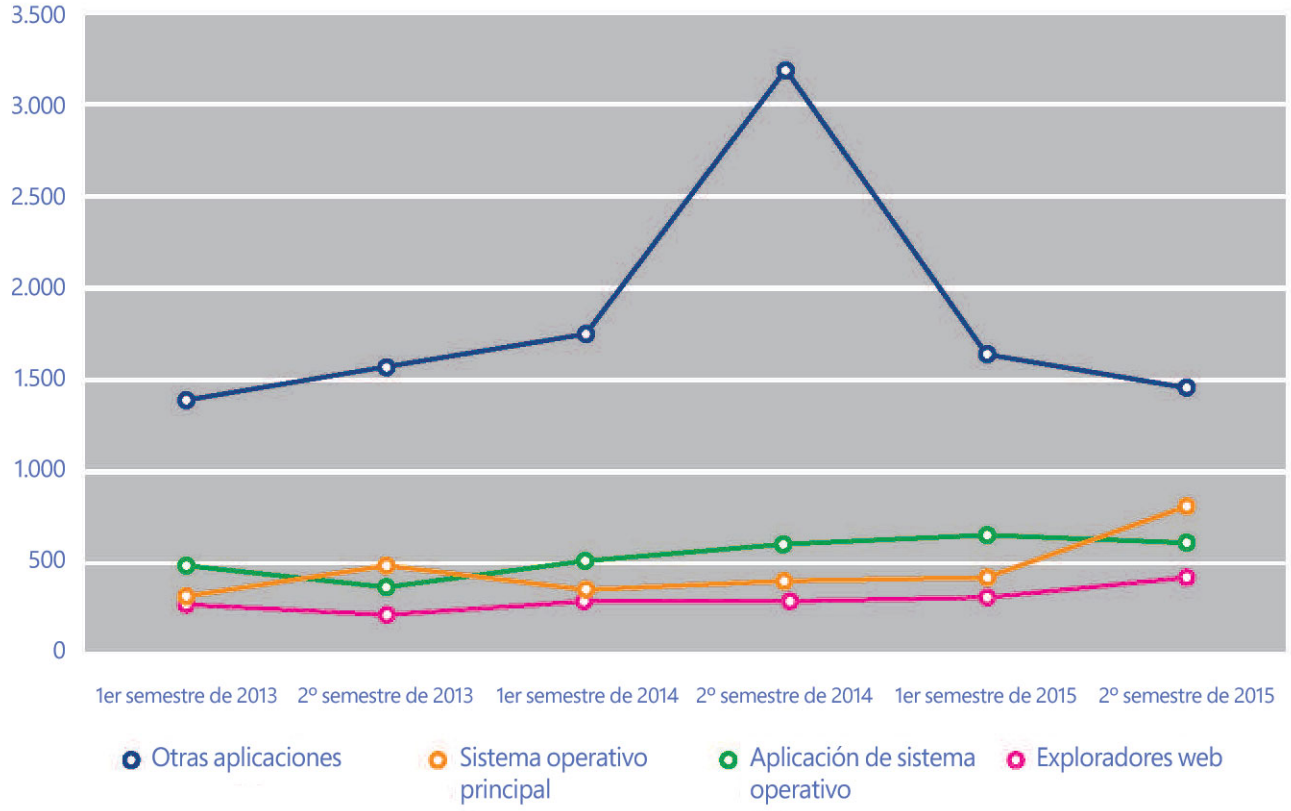
Por qué es importante

Estos datos indican a los equipos de seguridad que los atacantes han cambiado sus ataques hospedados en páginas web malintencionadas de Java a Flash Player. El hecho de saberlo facilita la planificación de mitigaciones para páginas web malintencionadas.

También pone de manifiesto la importancia de mantener Adobe Flash Player actualizado. Los usuarios deben dar prioridad a la instalación de actualizaciones de seguridad de Flash como ayuda para protegerse ante esta creciente amenaza.

El 44,2 % de todas las vulnerabilidades divulgadas se presentan en aplicaciones distintas de exploradores web y sistemas operativos.

Vulnerabilidades de sistemas operativos, exploradores y aplicaciones del sector, 1er semestre de 2013 a 2º semestre de 2015



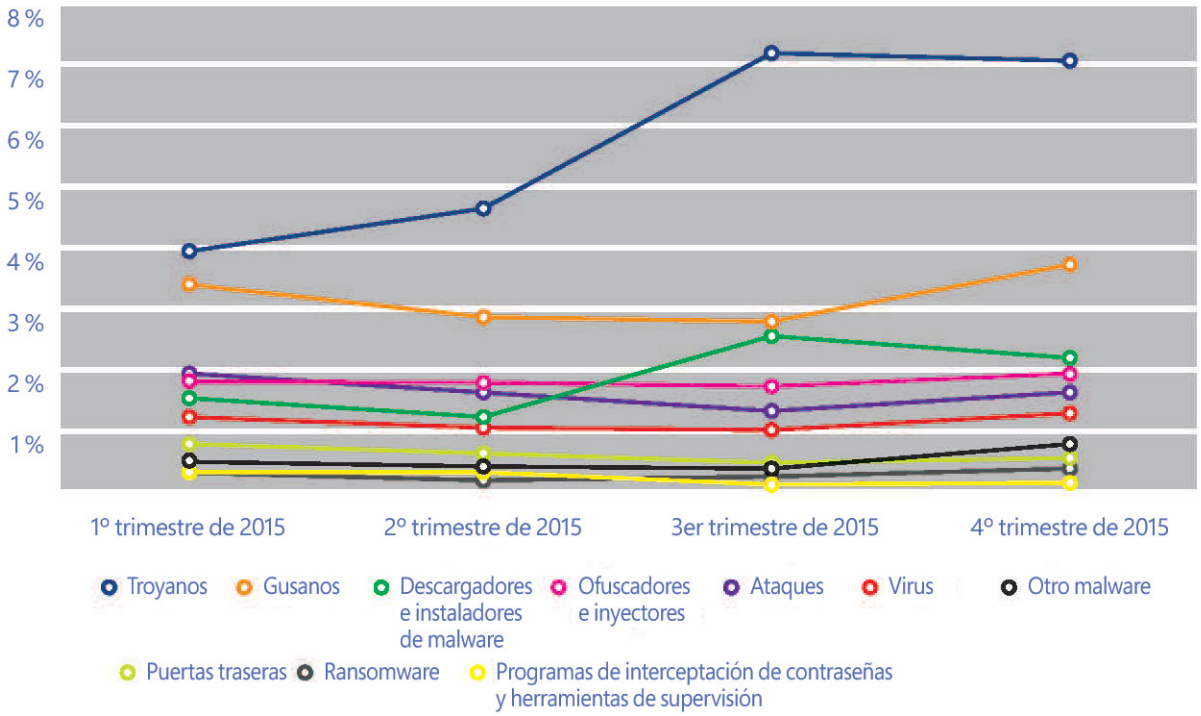
Por qué es importante

Muchos equipos de seguridad centran sus esfuerzos en aplicar parches a los sistemas operativos y exploradores web. Pero las vulnerabilidades de esos dos tipos de software suelen representar tan solo una minoría de las vulnerabilidades divulgadas públicamente. La mayoría de las vulnerabilidades se producen en las aplicaciones. Es necesario que los equipos de seguridad dediquen más tiempo a evaluar estas vulnerabilidades y aplicar parches para ellas. De lo contrario, pueden pasar por alto la mayor parte de las vulnerabilidades en sus entornos.

Para aumentar la protección en la red, identifique las aplicaciones no autorizadas y aplique las directivas de la empresa relativas a los recursos en la nube, y supervise la actividad para detectar cualquier anormalidad.

La presencia de troyanos, una categoría prevalente de malware que utiliza técnicas de ingeniería social para engañar a los usuarios, aumentó un 57 % y se mantuvo en niveles altos.

Tasas de presencia para las categorías de malware más importantes



Por qué es importante

¡El conocimiento es poder! Entender los tipos de amenazas que es más probable que se encuentren las personas de su organización ayuda a asignar prioridades a las mitigaciones, incluido formar al personal para que pueda identificar esas amenazas.

Los troyanos dicen ser una cosa, como un documento o un vídeo, pero en realidad son una herramienta que los atacantes utilizan para engañar a la gente para que realice alguna acción que no les conviene, como la instalación de malware en su sistema o la disminución de la configuración de seguridad. Esto es lo que hace de los troyanos una de las herramientas favoritas de los atacantes. El hecho de saberlo, y viendo cómo se comportan los principales troyanos de su área del mundo, le ayudará a proteger mejor su organización.

Forme a sus empleados sobre las artimañas más frecuentes que usan los troyanos, incluidos titulares web falsos con títulos provocativos y mensajes de correo electrónico falsificados.

Anime a los trabajadores a que utilicen sus dispositivos personales para las redes sociales y la navegación por Internet en lugar de usar dispositivos conectados a la red corporativa.

La prevalencia de cualquier amenaza concreta puede variar considerablemente, según el país y la naturaleza de la amenaza, y esta es una de las razones por las que no existen soluciones milagrosas para lograr una seguridad "perfecta". Por ejemplo, Rusia y Brasil tenían unas tasas de presencia que eran casi el triple que el promedio en todo el mundo para algunos tipos de amenazas.

Prevalencia de las categorías de amenazas en todo el mundo y los 10 lugares en los que hay más ordenadores que notifican la presencia de amenazas.

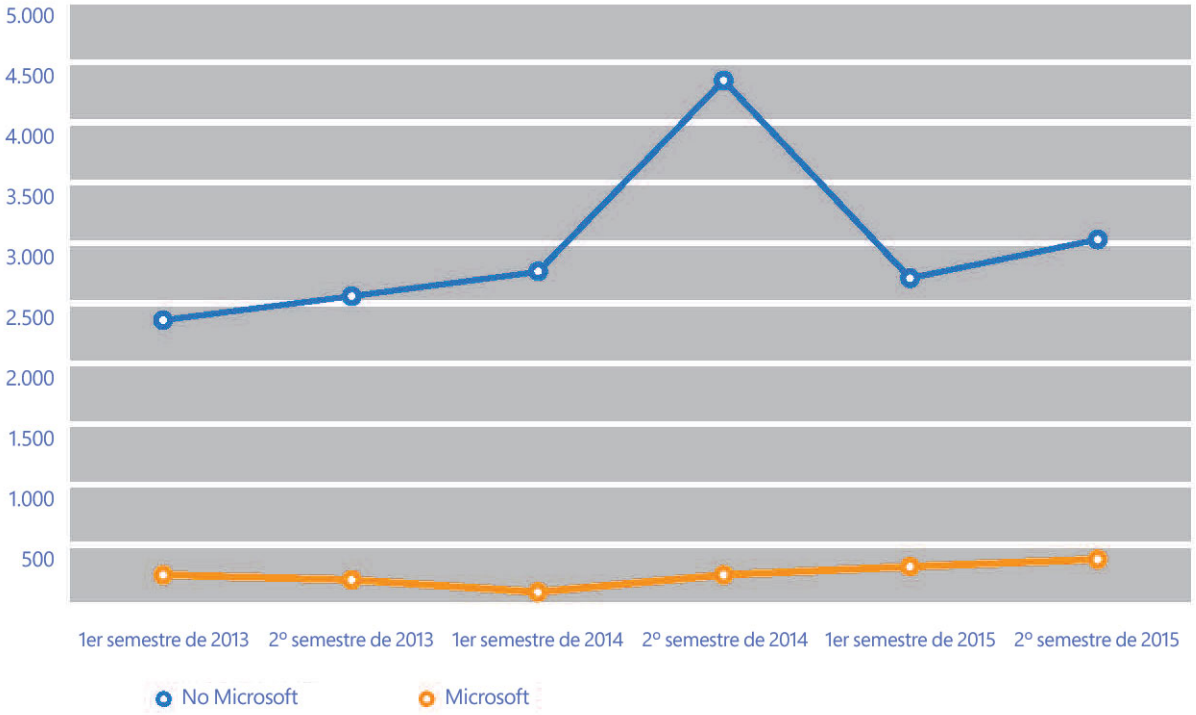
Categoría	En todo el mundo	EE. UU.	Brasil	China	Rusia	Francia	Alemania	Reino Unido	Italia	Canadá	Japón
Modificadores del explorador	7,6 %	9,1 %	11,8 %	0,6 %	7,0 %	14,3 %	8,7 %	10,9 %	15,3 %	11,3 %	4,2 %
Troyanos	7,1 %	4,2 %	12,7 %	10,2 %	20,8 %	5,7 %	4,3 %	4,4 %	7,0 %	5,1 %	1,5 %
Gusanos	3,3 %	0,6 %	8,9 %	5,6 %	4,6 %	1,9 %	1,1 %	0,8 %	3,9 %	0,6 %	0,7 %
Software que instala varios programas	3,1 %	1,7 %	1,5 %	0,2 %	0,5 %	2,2 %	0,9 %	2,3 %	2,5 %	2,5 %	0,5 %
Descargadores e instaladores de malware	2,2 %	2,3 %	6,5 %	3,2 %	6,6 %	2,8 %	1,5 %	3,2 %	3,1 %	3,3 %	0,4 %
Ofuscadores e inyectores	1,7 %	1,0 %	5,3 %	5,2 %	7,3 %	1,9 %	1,6 %	1,7 %	2,8 %	1,6 %	0,6 %
Adware	1,6 %	4,5 %	7,1 %	0,2 %	5,2 %	7,8 %	4,1 %	4,7 %	7,2 %	5,3 %	2,0 %
Ataques	1,4 %	3,4 %	2,4 %	1,7 %	1,3 %	2,5 %	3,2 %	4,4 %	4,3 %	5,7 %	3,2 %
Virus	1,1 %	0,4 %	2,2 %	7,4 %	1,5 %	0,4 %	0,3 %	0,3 %	0,8 %	0,4 %	0,2 %
Otros	0,6 %	0,9 %	0,3 %	1,2 %	0,3 %	0,5 %	0,5 %	0,6 %	0,7 %	1,5 %	0,2 %
Puertas traseras	0,5 %	0,7 %	1,4 %	1,8 %	2,0 %	0,9 %	0,6 %	0,9 %	1,0 %	0,7 %	0,3 %
Ransomware	0,3 %	0,6 %	0,5 %	0,0 %	0,6 %	0,7 %	0,6 %	0,4 %	1,4 %	0,7 %	0,4 %
Programas de interceptación de contraseñas y herramientas de supervisión	0,2 %	0,4 %	1,0 %	0,5 %	0,8 %	0,3 %	0,4 %	0,4 %	0,6 %	0,6 %	0,3 %

Por qué es importante

Entender las estrategias y tácticas que los atacantes emplean en aquellas partes del mundo donde tiene operaciones le permitirá proteger mejor esas operaciones. Hay lugares en el mundo donde el ransomware se encuentra mucho más que en otras partes; lo mismo ocurre con los troyanos, ataques y otro malware. Utilice los datos del informe de inteligencia sobre seguridad para entender las amenazas con las que es más probable que se encuentre su organización y para documentar su plan de seguridad.

En cualquier periodo de seis meses, menos del 10 % de las divulgaciones de vulnerabilidades se dan en software de Microsoft.

Divulgaciones de vulnerabilidades de productos Microsoft y que no son de Microsoft, 1er semestre de 2013 a 2º semestre de 2015



Por qué es importante

Si su organización se centra únicamente en aplicar parches para vulnerabilidades del software que usa con más frecuencia, es probable que no esté administrando todas las vulnerabilidades presentes en su entorno de TI. Es importante saber si necesitará tomar medidas sobre alguna de las otras casi 3.000 vulnerabilidades que podría haber en el entorno de su organización.

El cifrado de dispositivos y el cumplimiento coherente de las normas de TI pueden ayudar a reducir las probabilidades de una infracción. Si detecta algún comportamiento sospechoso, bloquee el dispositivo y póngalo en cuarentena fuera de la red hasta que se haya identificado y eliminado la amenaza.

Para obtener más información sobre estas y otras conclusiones, descargue el informe Security Intelligence Report, o visite: www.microsoft.com/security

Microsoft