Tendencias en Seguridad informática 2016:

Guía sobre las estadísticas más importantes en seguridad

Microsoft

Durante diez años, Microsoft ha estudiado y analizado el panorama de las amenazas informáticas, que incluyen vulnerabilidades de seguridad y malware. Utilizamos datos recopilados en más de 600 millones de equipos de todo el mundo para desarrollar uno de los conjuntos de datos de seguridad más completos que existen. La investigación que se realiza durante todo el año luego se recopila y publica en el Informe de inteligencia sobre seguridad de Microsoft, un informe de 160 páginas acreditado en todo el mundo que describe de forma integral el panorama de la seguridad.

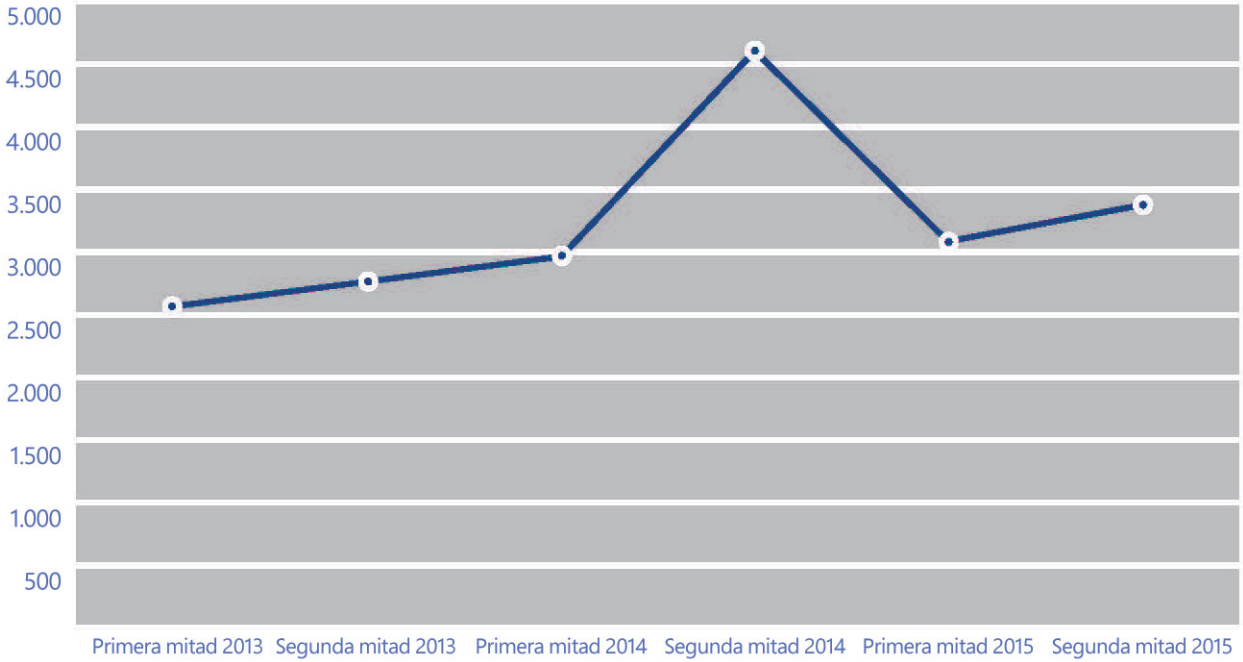
Este año, con el objetivo de generar conciencia sobre las estadísticas y tendencias más importantes, también creamos una Guía sobre las estadísticas más importantes en seguridad, un resumen preciso que los lectores pueden consultar para conocer los factores clave de la compleja matriz de la seguridad informática.

En este e-book, hemos reunido nuestros 10 hallazgos más importantes. Siga leyendo para obtener más información esencial sobre tasas de vulnerabilidades, ubicaciones con los porcentajes más altos de infección, vulnerabilidades de seguridad de programas claves de software y mucho más. Debido a que todos los años se divulgan más de 6.000 vulnerabilidades en la industria, es fundamental garantizar que se evalúen y actualicen todos los software de su entorno de TI. A continuación, encontrará nuestros 10 hallazgos más importantes para ayudar a mejorar su nivel de seguridad.

Tendencias

El 41,8% de todas las divulgaciones de vulnerabilidades se califican como muy graves, la cifra más alta en tres años.

Divulgación de vulnerabilidades de seguridad para toda la industria dos veces al año hasta la segunda mitad de 2015

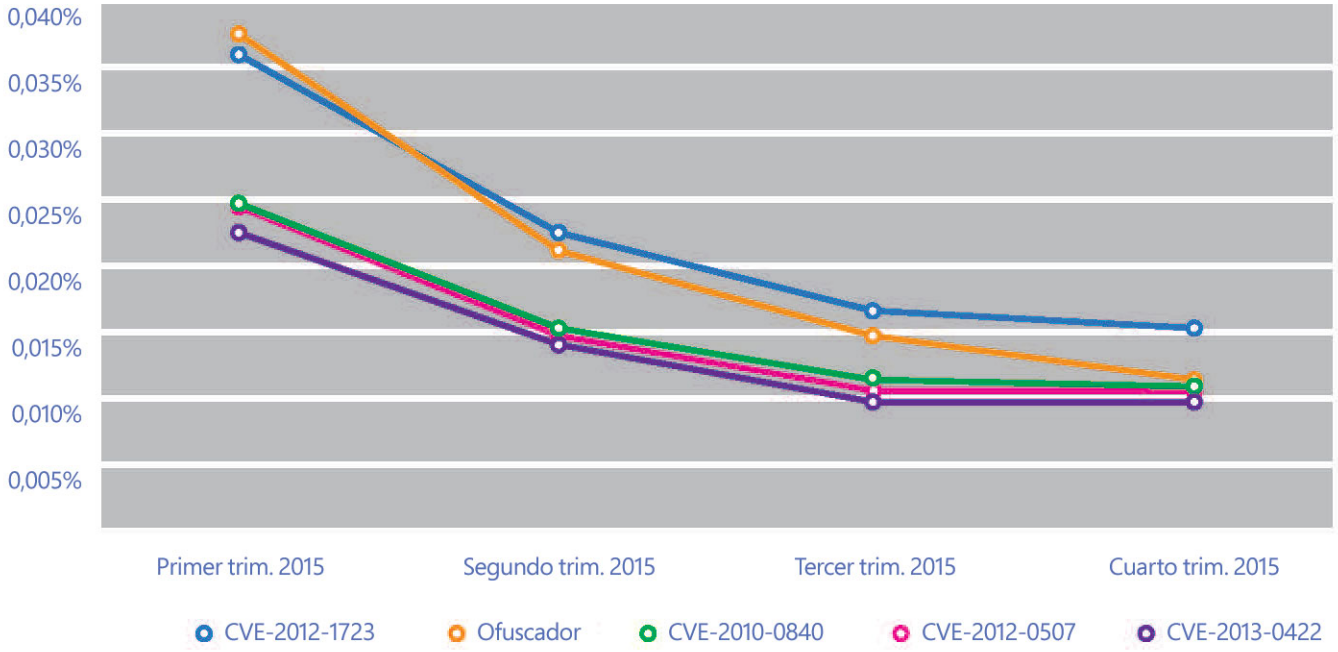


Por qué es importante

Las divulgaciones de vulnerabilidades son revelaciones de vulnerabilidades de software para el público en general. Diversas fuentes pueden realizar las divulgaciones, como editores del software afectado, proveedores de software de seguridad, investigadores independientes de seguridad e incluso creadores de malware. Los atacantes y los malware intentan constantemente usar las vulnerabilidades sin revisiones para comprometer y victimizar a las organizaciones. Las divulgaciones de vulnerabilidades en la industria aumentaron un 9,4% entre la primera y la segunda mitad de 2015 hasta superar las 3.300. Estas son las vulnerabilidades de gravedad alta que temen los equipos de seguridad porque podrían posibilitar ataques remotos. Debido a que todos los años se divulgan públicamente más de 6.000 vulnerabilidades en la industria, es fundamental que se evalúen y actualicen de forma periódica todos los software de su entorno de TI. Instale las revisiones de software sin demora, supervise que no exista actividad sospechosa en las redes y envíe a la cuarentena los dispositivos que tengan un comportamiento inusual.

La detección de vulnerabilidades de seguridad de Java están disminuyendo.

Tendencia de las principales vulnerabilidades de seguridad de Java que los productos antimalware en tiempo real de Microsoft detectaron y bloquearon en la segunda mitad de 2015



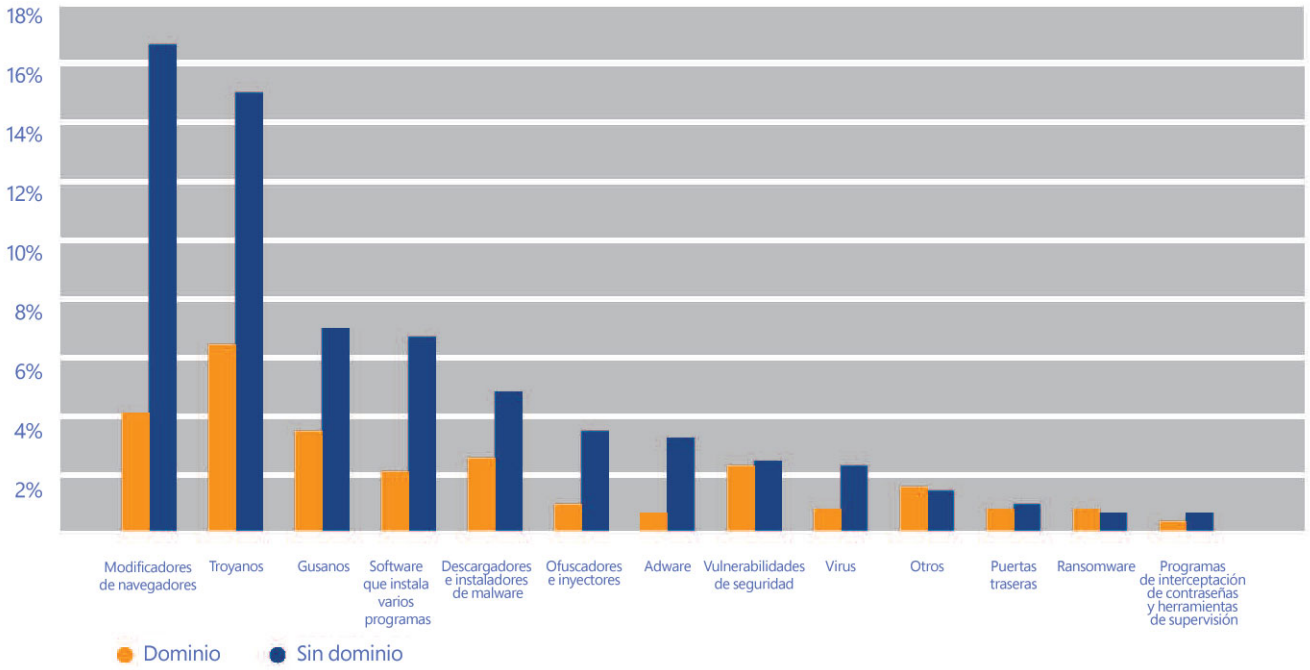
Por qué es importante

Los atacantes solían preferir las vulnerabilidades de seguridad de Java, pero eso ya no es así. Es probable que esta disminución sea resultado de varios cambios importantes en la forma en la que los navegadores web evalúan y ejecutan applets Java.

Los equipos de seguridad ahora pueden centrar sus esfuerzos en riesgos de mayor gravedad. Los usuarios de Java deben seguir instalando las revisiones de seguridad a medida que estén disponibles para continuar evitando posibles ataques futuros.

Los equipos de consumidores encuentran el doble de amenazas en comparación con los equipos empresariales.

Tasas de detección de software no deseado y malware para equipos basados en dominios y equipos que no son de dominios



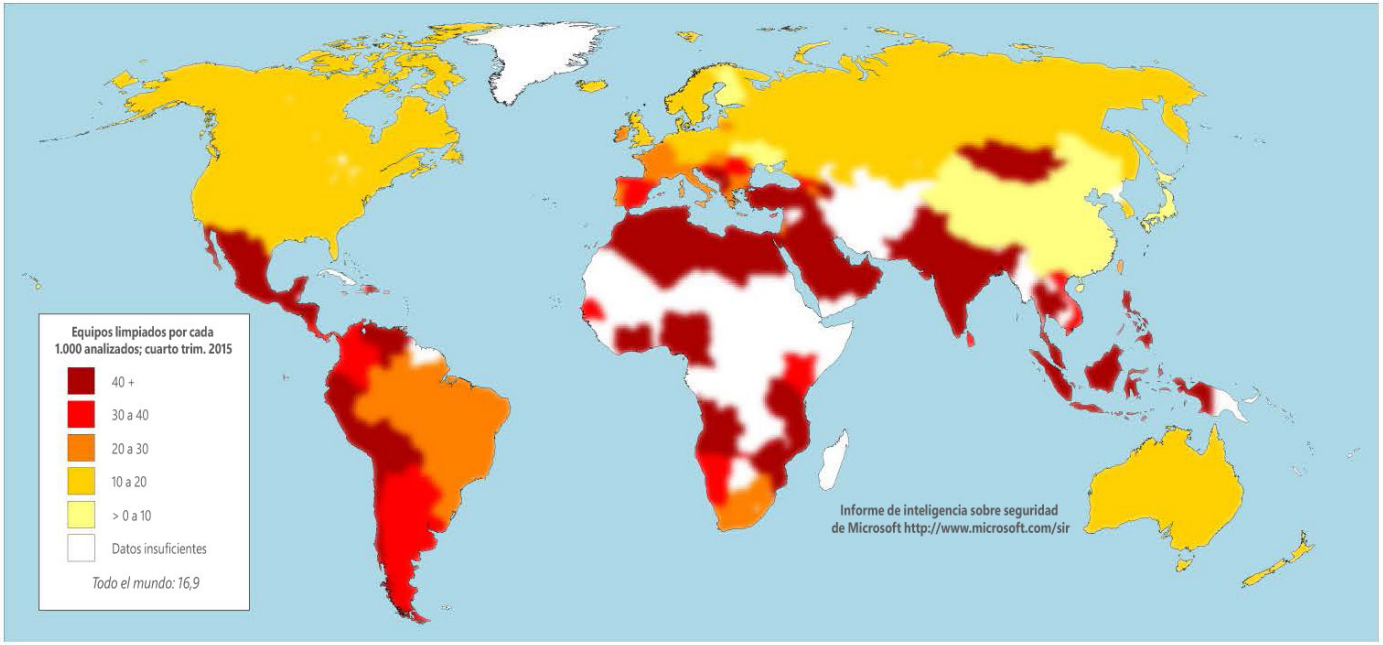
Por qué es importante

Normalmente, los entornos empresariales implementan medidas de defensa en profundidad, como firewalls empresariales, que evitan que una cantidad determinada de malware llegue a los equipos de los usuarios. En consecuencia, los equipos empresariales suelen encontrar malware en menor cantidad que los equipos de consumidores. La tasa de detección en los equipos de consumidores fue alrededor de 2,2 veces más alta que la tasa en los equipos empresariales. Mientras tanto, los equipos empresariales (basados en dominio) encontraron vulnerabilidades de seguridad casi tan seguido como los equipos de consumidores (no basados en dominio), a pesar de encontrar menos de la mitad de malware que encuentran los equipos que no se basan en dominios en general. Debido a esto, los responsables centrales de la seguridad informática han concluido que las vulnerabilidades de seguridad son un problema para las organizaciones y que la mejor manera de defenderse es mantenerse al día con las actualizaciones de seguridad y los software más recientes. A pesar de estas tendencias, para asegurar los activos de su empresa, debe comprender el panorama de amenazas y trazar una estrategia de seguridad para resguardar todos los frentes, incluidas credenciales de acceso e identidad, aplicaciones y datos, infraestructura y dispositivos de red.

Si adopta una actitud proactiva frente a la seguridad y aprovecha las tecnologías más recientes de análisis, "machine learning" y autenticación multifactor, puede fortalecer las defensas de su empresa contra los ataques cibernéticos y contar con el equipamiento necesario para responder en caso de una infracción de seguridad.

Las ubicaciones con los porcentajes de infección de malware más altos fueron Mongolia, Libia, los Territorios Palestinos, Iraq y Pakistán.

Porcentajes de infección por país/región



Por qué es importante

El malware se distribuye de forma dispareja en el mundo, y cada ubicación tiene su propia combinación de amenazas. Si estudiamos las zonas del mundo donde el malware tiene mayor impacto y las comparamos con las áreas menos infectadas del mundo, podemos intentar descubrir los factores técnicos, económicos, sociales y políticos que influyen en los porcentajes regionales de infección de malware. Estos datos podrían ayudar a conformar la próxima política pública que, a cambio, podría disminuir los porcentajes de infección de malware en las zonas más afectadas del mundo.

Estudio anterior disponible

Los kits de vulnerabilidades de seguridad representan casi el 40% de las vulnerabilidades de seguridad detectadas con más frecuencia.

Tendencias trimestrales de la tasa de detección de las familias de vulnerabilidades de seguridad que los productos antimalware en tiempo real de Microsoft detectaron y bloquearon con más frecuencia en la segunda mitad de 2015, sombreadas según el predominio relativo

Vulnerabilidad de seguridad	Tipo	Primer trim. 2015	Segundo trim. 2015	Tercer trim. 2015	Cuarto trim. 2015
Axpergle	Kit de vulnerabilidad de seguridad	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 vulnerabilidad de seguridad	0,06%	0,05%	0,07%	0,17%
JS/NeutrinoEK	Kit de vulnerabilidad de seguridad	0,06%	0,03%	0,01%	0,11%
HTML/IframeRef	Genérico	0,07%	0,05%	0,04%	0,05%
JS/Neclu	Kit de vulnerabilidad de seguridad	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/Ofuscador	Java	0,04%	0,05%	0,02%	0,01%

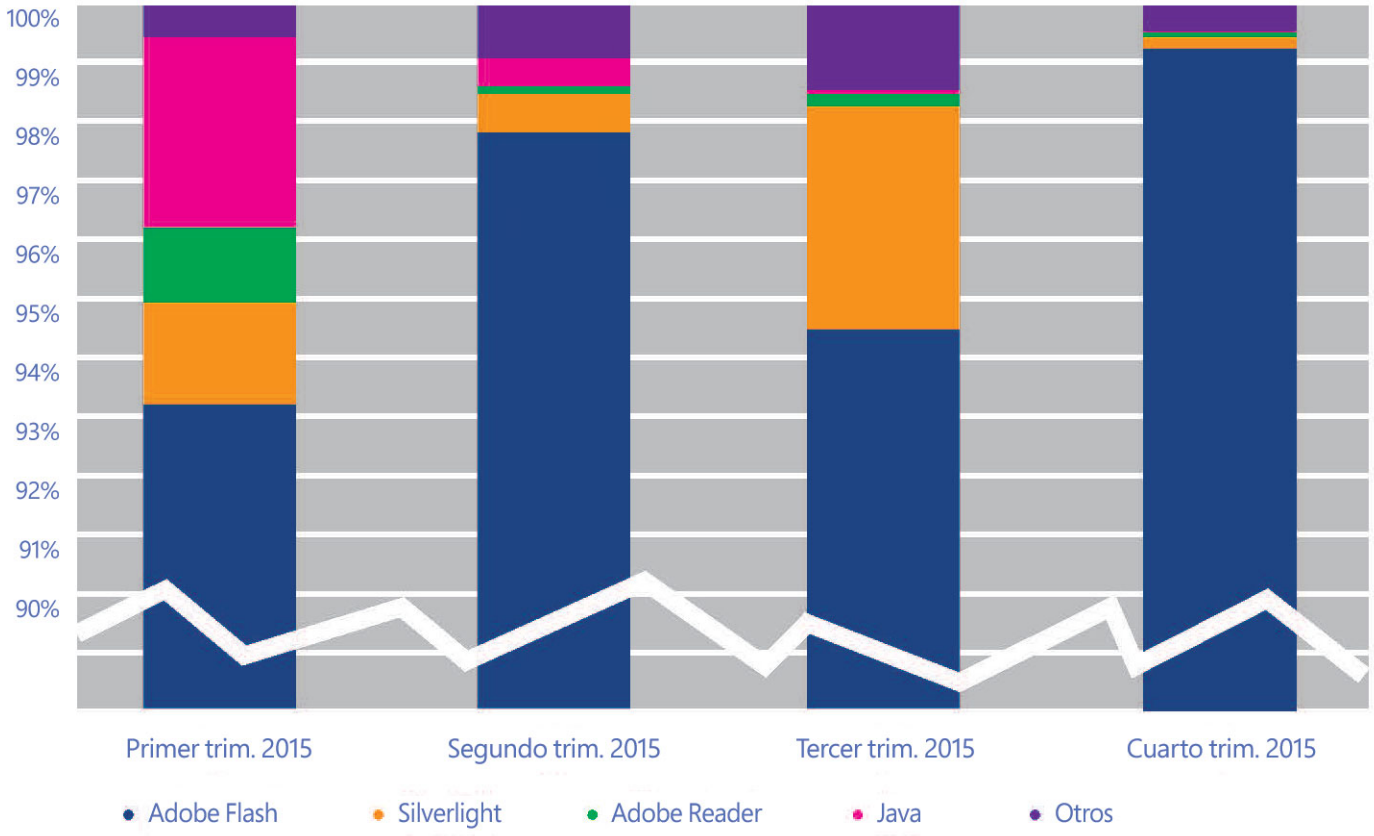
Por qué es importante

Los kits de vulnerabilidades de seguridad son recopilaciones de vulnerabilidades de seguridad que se venden como un software comercial o como un servicio. Los atacantes potenciales compran o alquilan kits de vulnerabilidades de seguridad en foros malintencionados de hackers y a través de otras tiendas ilegítimas. Un kit típico incluye una recopilación de páginas web que contienen diversas vulnerabilidades de seguridad en navegadores web populares y complementos de navegadores. Cuando el atacante instala el kit en un servidor web comprometido o malintencionado, los visitantes que no tienen instaladas las actualizaciones adecuadas de seguridad están en riesgo de comprometer sus equipos mediante ataques mediante descargas ocultas. Los kits de vulnerabilidades de seguridad les permiten a los atacantes menos hábiles llevar a cabo ataques más sofisticados.

Comprender qué vulnerabilidades de seguridad y kits de vulnerabilidades de seguridad usan los atacantes les ayuda a los equipos de seguridad a proteger sus organizaciones.

El tipo de objeto que se detectó con mayor frecuencia fueron los objetos de Adobe Flash Player, que aparecieron en más del 90% de las páginas malintencionadas durante un período de un año.

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



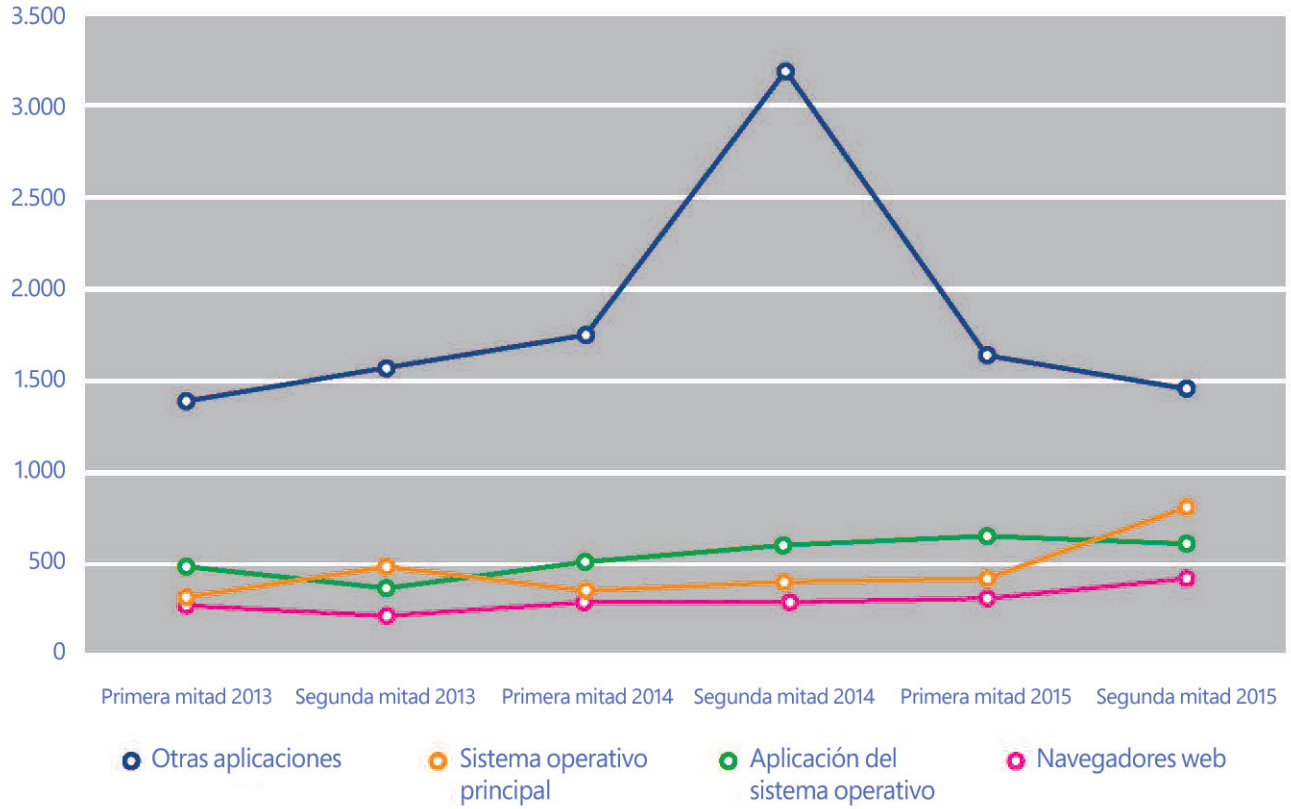
Por qué es importante

Con estos datos, los equipos de seguridad saben que los atacantes en vez de alojar sus ataques en páginas web malintencionadas de Java, ahora lo hacen en páginas web malintencionadas de Flash Player. Gracias a esto, se pueden planificar mitigaciones para páginas web malintencionadas más fácilmente.

Además, ilustra la importancia de mantener actualizado Adobe Flash Player. Los usuarios deberían dar prioridad a instalar actualizaciones de seguridad de Flash para protegerse contra esta amenaza que aumenta.

El 44,2% de todas las vulnerabilidades divulgadas se encuentran en aplicaciones que no son aplicaciones de navegadores web ni sistemas operativos.

Vulnerabilidades de aplicaciones, navegadores y sistemas operativos de toda la industria, desde la primera mitad de 2013 hasta la segunda mitad de 2015

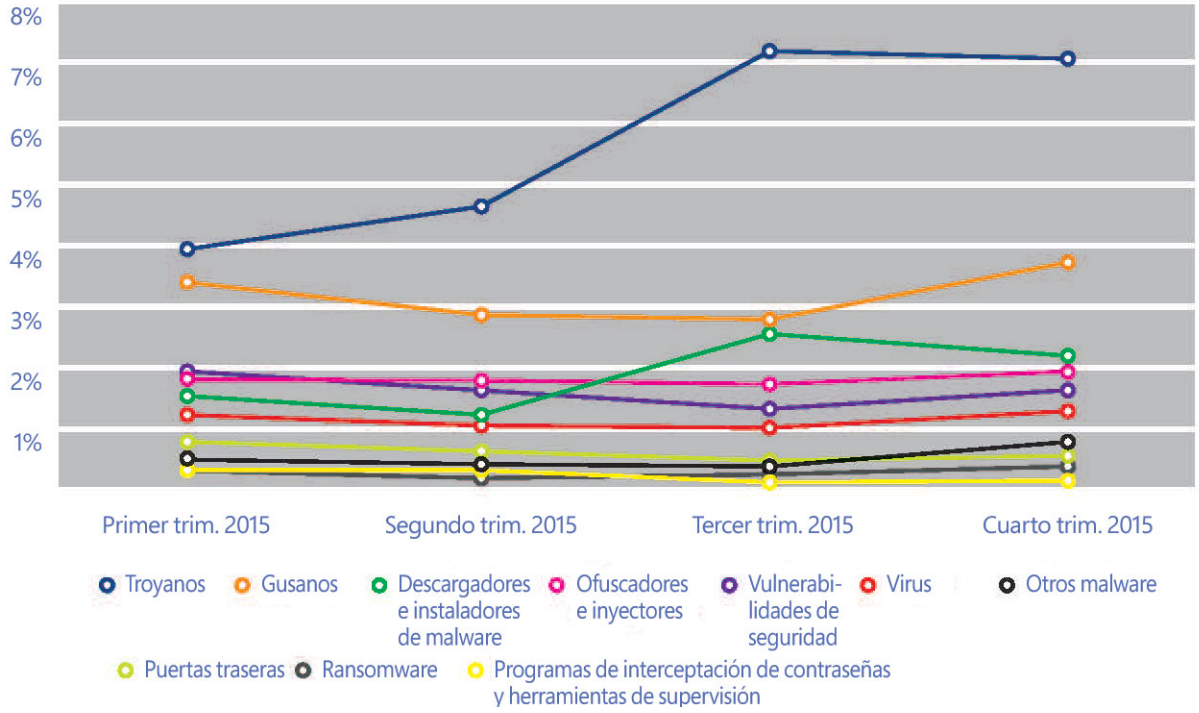


Por qué es importante

Muchos equipos de seguridad centran sus iniciativas en reparar los sistemas operativos y los navegadores web. Sin embargo, las vulnerabilidades en esos dos tipos de software suele representar un mínimo porcentaje de las vulnerabilidades que se divulgan públicamente. La gran mayoría de las vulnerabilidades se encuentran en las aplicaciones. Los equipos de seguridad deben invertir una cantidad de tiempo adecuada en evaluar y reparar estas vulnerabilidades. De lo contrario, podrían pasar por alto la mayor parte de las vulnerabilidades en sus entornos. Para aumentar la protección en la red, identifique las aplicaciones no autorizadas e implemente políticas corporativas con respecto a los recursos en la nube. Además, supervise la actividad para detectar cualquier movimiento inusual.

Los encuentros con troyanos, una categoría predominante de malware que usa la ingeniería social para engañar a los usuarios, aumentó un 57% y se mantuvo en niveles elevados.

Tasas de detección en las principales categorías de malware



Por qué es importante

El conocimiento es poder. Comprender qué tipos de amenazas es más probable que encuentren las personas de su organización permite dar prioridad a los planes de mitigación, incluidos los cursos de usuarios para identificar dichas amenazas.

Los troyanos se hacen pasar por una cosa, como un documento o video, pero realmente son una herramienta que usan los atacantes para engañar a las personas para que lleven a cabo una acción que no los beneficia, como instalar un malware en su sistema o reducir su configuración de seguridad. Debido a esto, los troyanos son una de las herramientas favoritas de los atacantes. Conocer esta información y observar cómo se comportan los troyanos más importantes en su zona lo ayudará a proteger mejor su organización.

Enseñe a sus trabajadores sobre los trucos más comunes de los troyanos, incluidos títulos web falsos con encabezados atractivos y correos electrónicos de suplantación de identidad (spoofing). Recomiéndeles usar dispositivos personales para acceder a medios sociales y navegar por la Web, en lugar de dispositivos conectados a su red corporativa.

El predominio de cualquier amenaza específica puede variar significativamente según el país y la naturaleza de la amenaza, el cual es uno de los motivos por el que no existe una fórmula mágica para lograr una seguridad "perfecta". Por ejemplo, para algunos tipos de amenazas, Rusia y Brasil presentaron una tasa de detección de casi tres veces las tasas de detección promedio del resto del mundo.

Predominio de categorías de amenazas en todo el mundo y en las 10 ubicaciones donde más equipos registran detecciones.

Categoría	Todo el mundo	EE. UU.	Brasil	China	Rusia	Francia	Alemania	Reino Unido	Italia	Canadá	Japón
Modificadores de navegadores	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%
Vulnerabilidades de seguridad	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%

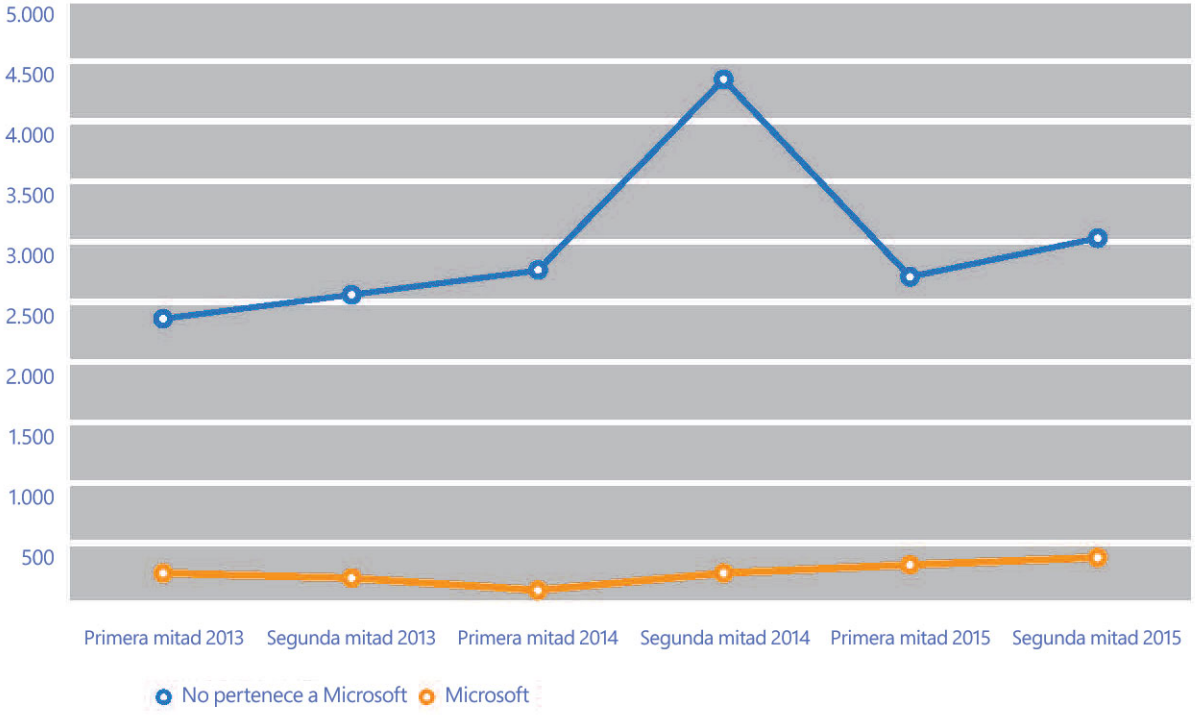
Por qué es importante

Comprender qué estrategias y tácticas usan los atacantes en los lugares del mundo donde opera su empresa le permitirá proteger mejor esas operaciones. Existen lugares del mundo donde ransomware se detecta mucho más que en otras ubicaciones.

Lo mismo sucede con los troyanos, las vulnerabilidades de seguridad y otros malwares. Utilice los datos del Informe de inteligencia sobre seguridad de Microsoft para entender las amenazas que es más probable que enfrente su organización y para conformar su plan de seguridad.

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

Divulgaciones de vulnerabilidades de productos de Microsoft y productos que no son de Microsoft, desde la primera mitad de 2013 hasta la segunda mitad de 2015



Por qué es importante

Si su organización solo se centra en reparar las vulnerabilidades en los software que más usa, es probable que no esté administrando todas las vulnerabilidades presentes en su entorno de TI. Es importante saber si necesita tomar alguna medida en cualquiera de las casi 3.000 otras vulnerabilidades que podrían existir en el entorno de su organización.

El cifrado de dispositivo y el cumplimiento constante de las normas de TI puede ayudar a disminuir las probabilidades de sufrir una infracción de seguridad. Si detecta comportamiento sospechoso, bloquee el dispositivo y envíelo a cuarentena fuera de la red hasta que se haya identificado y eliminado la amenaza.

Para obtener más información sobre estos y otros hallazgos, descargue el Informe de inteligencia sobre seguridad o visite: www.microsoft.com/security.

Microsoft