

Informe de inteligencia de seguridad de Microsoft

Volumen 11

*Una revisión exhaustiva
de las vulnerabilidades de seguridad del software,
de la amenaza del código malintencionado y
del software potencialmente no deseado
en la primera mitad del año 2011*

PRINCIPALES CONCLUSIONES

Microsoft®

Informe de inteligencia de seguridad de Microsoft

Este documento se publica exclusivamente a título informativo. MICROSOFT NO GARANTIZA, NI EXPLÍCITA, NI IMPLÍCITA NI LEGALMENTE, LA INFORMACIÓN CONTENIDA EN EL PRESENTE DOCUMENTO.

Este documento se presenta “tal cual”. La información y las opiniones contenidas en el mismo, incluyendo las direcciones URL y otras referencias a sitios web de Internet, pueden cambiar sin previo aviso. El lector asume el riesgo de utilizarlo.

Copyright © 2011 Microsoft Corporation. Reservados todos los derechos.

Los nombres de las empresas y productos reales aquí mencionados pueden ser marcas comerciales de sus respectivos titulares.

Contenido

| | |
|---|----|
| Informe de inteligencia de seguridad de Microsoft, volumen 11 | 3 |
| Concentración en los métodos de propagación de malware..... | 4 |
| Seguimiento de amenazas universales | 8 |
| Divulgación de vulnerabilidades | 8 |
| Vulnerabilidades de seguridad | 9 |
| Vulnerabilidades de seguridad en documentos..... | 10 |
| Malware y software potencialmente no deseado | 12 |
| Índices de infección de sistemas operativos | 12 |
| Familias de amenazas y sus categorías..... | 13 |
| Amenazas de empresa..... | 14 |
| Amenazas de correo electrónico | 14 |
| Sitios web malintencionados | 15 |

Informe de inteligencia de seguridad de Microsoft, volumen 11

El volumen 11 del *Informe de inteligencia de seguridad de Microsoft® (SIRv11)* proporciona una revisión exhaustiva de las vulnerabilidades de seguridad del software, las amenazas del código malintencionado y el software potencialmente no deseado en Microsoft y software de terceros. Microsoft se ha basado en análisis detallados de las tendencias de los últimos años, especialmente de la primera mitad del año 2011, para desarrollar estas revisiones.

Este documento resume las principales conclusiones del informe. El informe completo incluye también un análisis profundo de las tendencias descubiertas en más de 100 países/regiones de todo el mundo, y propone distintas formas para gestionar los riesgos a los que se expone su organización, su software y su personal.

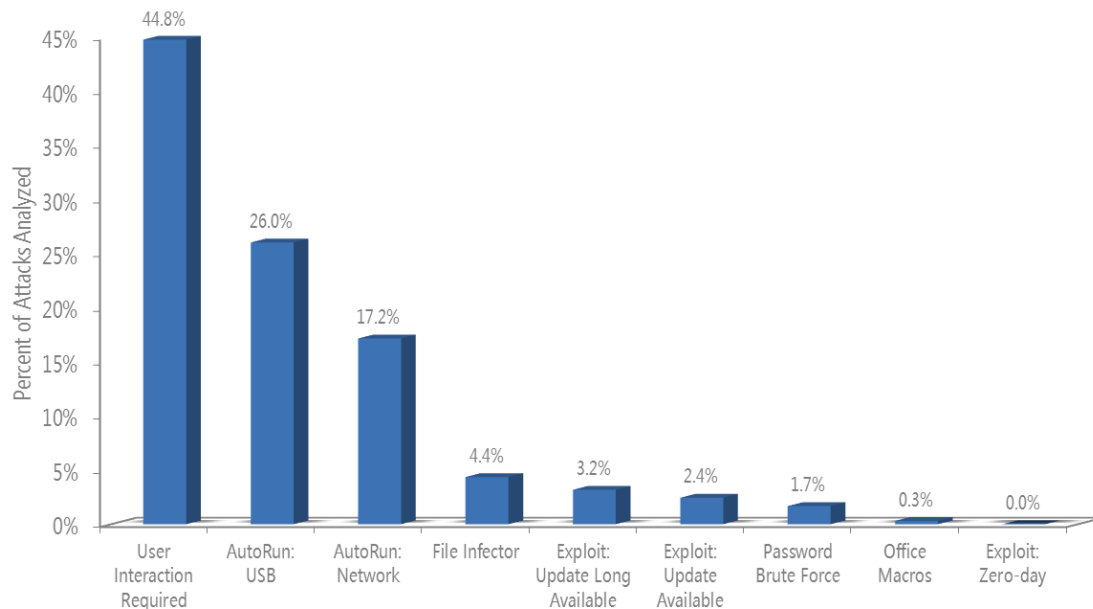
El informe completo, al igual que los volúmenes anteriores y los vídeos relacionados, se puede descargar en www.microsoft.com/sir.

Concentración en los métodos de propagación de malware

Microsoft ha realizado un análisis para comprender mejor la frecuencia de los ataques de vulnerabilidad de día cero y los riesgos a los que se exponen los clientes por su causa. Este análisis se inició para poder proporcionar información a los profesionales de la seguridad que les permita establecer prioridades entre sus preocupaciones y gestionar los riesgos de forma efectiva. Como todos, los departamentos de TI se enfrentan a restricciones de tiempo, presupuesto, personal y recursos durante la planificación y ejecución de su trabajo. Disponer de una información precisa y actualizada sobre el panorama de amenazas permitiría a los profesionales de la seguridad establecer prioridades en sus mecanismos de defensa y, por lo tanto, mantener a salvo sus redes, software y personal.

Para el análisis, las amenazas detectadas por la Herramienta de eliminación de software malintencionado (MSRT) durante la primera mitad del año 2011 (1H11) se clasificaron según los medios de propagación programados para cada familia de amenazas para infectar a sus víctimas. Si se informaba de que la amenaza usaba varios vectores para infectar a los usuarios, entonces el número de infecciones notificadas por la herramienta MSRT para esa familia se dividía y se atribuían las infecciones a cada vector de manera equitativa. La Figura muestra los resultados de ese análisis.

Figura . Malware detectado por MSRT en la primera mitad de 2011, según los métodos de propagación programados



- Los distintos métodos de propagación de amenazas de malware citados en la Figura se describen a continuación:
 - **Interacción con el usuario requerida.** Cuando el usuario realiza alguna acción que pone en peligro el PC. En este caso, “acción” significa una acción intencionada, en contraposición al uso habitual del PC.
 - **Ejecución automática: USB.** La amenaza aprovecha la función de ejecución automática de Windows para infectar dispositivos de almacenamiento USB y otros volúmenes extraíbles.
 - **Ejecución automática: Redes.** La amenaza aprovecha la función de ejecución automática para infectar volúmenes de red asignados a letras de unidad.
 - **Virus de archivo.** La amenaza modifica los archivos, normalmente con extensión .exe o .scr, volviendo a escribir o sobrescribiendo algunos segmentos de código para propagarse.
 - **Vulnerabilidad de seguridad: Actualización disponible desde hace mucho tiempo.** El proveedor lanzó una actualización de seguridad para

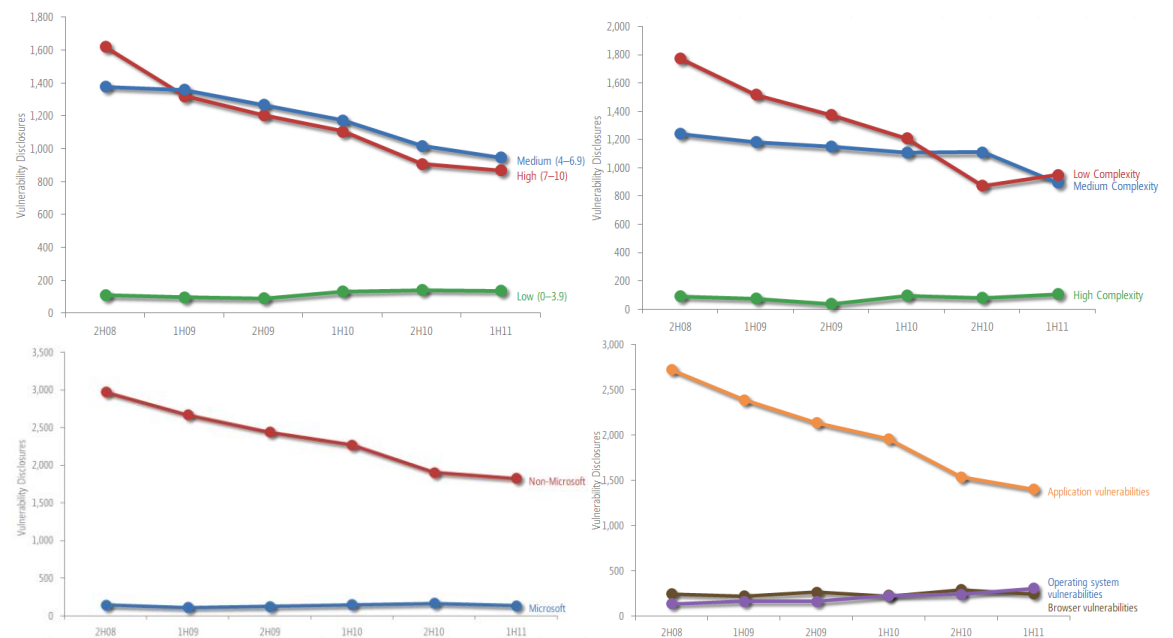
- tratar la vulnerabilidad cuya fecha es por lo menos un año anterior al ataque.
- **Vulnerabilidad de seguridad: Actualización disponible.** El proveedor lanzó una actualización de seguridad para tratar la vulnerabilidad menos de un año antes del ataque.
 - **Vulnerabilidad de seguridad: Día cero.** El proveedor no lanzó una actualización de seguridad para tratar la vulnerabilidad en el momento del ataque.
 - **Ataque a contraseña por fuerza bruta.** La amenaza se propaga mediante ataques a contraseña por fuerza bruta en volúmenes disponibles, como con el comando `net use`.
 - **Macros de Office.** La amenaza se propaga mediante la infección de documentos de Microsoft Office con macros malintencionadas de Visual Basic® para Aplicaciones (VBA).
 - **Vulnerabilidad de seguridad de día cero.** El proveedor no lanzó una actualización de seguridad para tratar la vulnerabilidad en el momento del ataque.
- Más de una tercera parte de las detecciones de malware analizadas fueron atribuidas a software malintencionado que realizó un uso indebido de la función de ejecución automática de Windows®.
 - Las amenazas que aprovecharon la ejecución automática se dividieron entre las que se propagan a través de volúmenes extraíbles (26 por ciento del total) y las que se propagan a través de volúmenes de red (17 por ciento).
 - Para combatir estas amenazas y ayudar a proteger a los clientes, Microsoft siguió varios pasos, incluido el lanzamiento de una actualización automática, en febrero de 2011, para hacer más segura la función de ejecución automática en las plataformas Windows XP y Windows Vista®, como ya lo es en Windows 7.
 - Cerca del seis por ciento de las detecciones de la herramienta MSRT que se analizaron fueron atribuidas a las *vulnerabilidades de seguridad*: código malintencionado que aprovecha las vulnerabilidades de las aplicaciones o los sistemas operativos.

- No se registró el uso de vulnerabilidades de seguridad de día cero por parte de ninguna de las principales familias detectadas por la herramienta MSRT en la primera mitad del año 2011.
- De todas las explotaciones de vulnerabilidades detectadas por el MMPC, las vulnerabilidades de seguridad de día cero constituyen menos del uno por ciento.

Seguimiento de amenazas universales

Divulgación de vulnerabilidades

Figura . Tendencias de la vulnerabilidad (CVE) por gravedad, complejidad, divulgaciones por proveedor y divulgaciones por tipo



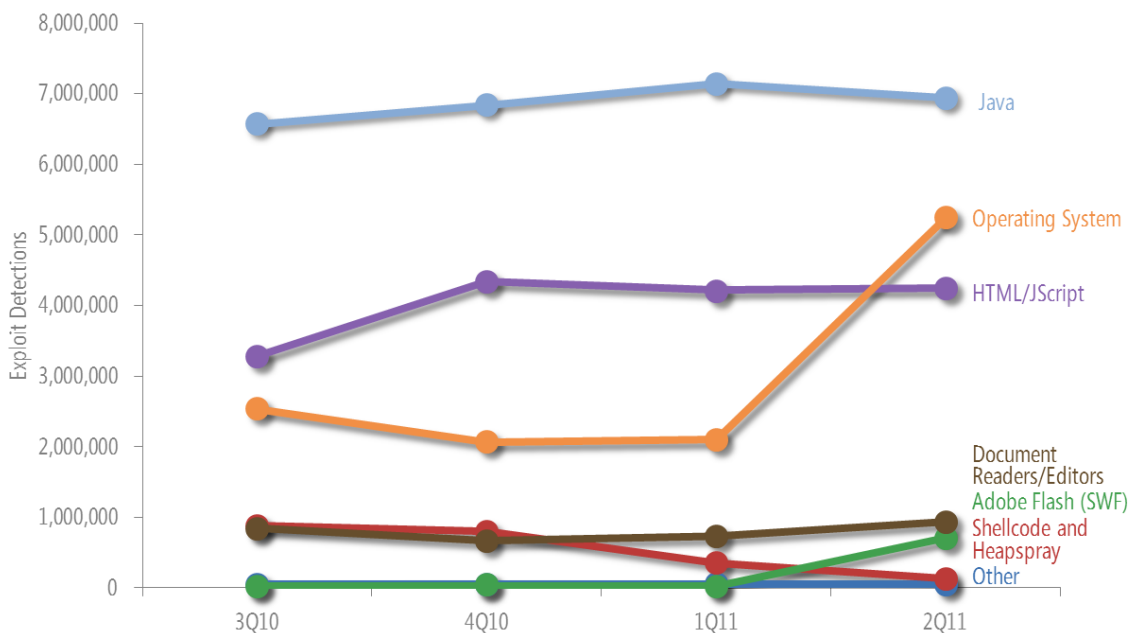
- La tendencia general de la gravedad de vulnerabilidad (en base al número de Exposiciones y vulnerabilidades comunes o CVE) ha sido positiva. Las vulnerabilidades de gravedad media y alta reveladas en la primera mitad del año 2011 disminuyeron un 6,8 por ciento y 4,4 por ciento respectivamente con respecto a la segunda mitad de 2010.
- Las vulnerabilidades de baja complejidad (aquellos que se pueden explotar con mayor facilidad) disminuyeron un 41,2 por ciento respecto al año anterior.

- La vulnerabilidad de los sistemas operativos y los exploradores han sido especialmente estables durante varios años, con una media del 12,7 y el 15,7 por ciento de todas las vulnerabilidades reveladas en la primera mitad de 2011 respectivamente.
- Las vulnerabilidades en productos de Microsoft representaron un 6,9 por ciento del total revelado en la primera mitad de 2011, frente al 8,2 por ciento en la segunda mitad de 2010.

Vulnerabilidades de seguridad

Figura muestra la prevalencia de diferentes tipos de vulnerabilidades de seguridad en cada trimestre entre el 3T10 y el 2T11.

Figura . Vulnerabilidades de seguridad detectadas y bloqueadas por los productos antimalware de Microsoft, del 3T10 al 2T11, por plataforma o tecnología de destino

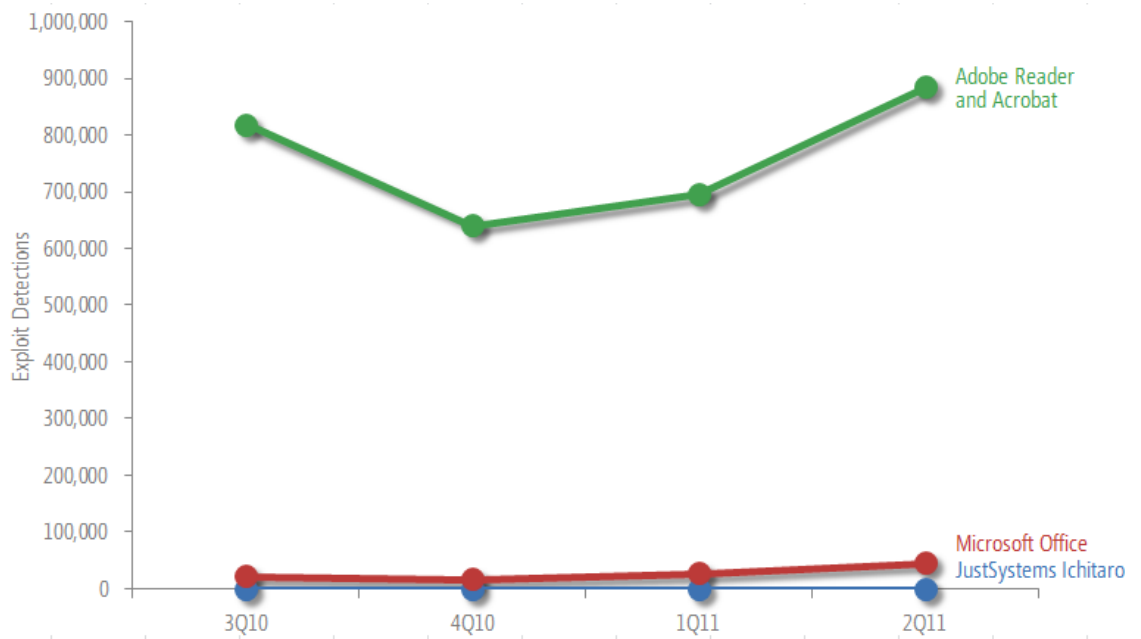


- Los tipos de vulnerabilidad de seguridad que más se observaron en la primera mitad de 2011 fueron los dirigidos al entorno de ejecución Java Runtime Environment (JRE) de Oracle (previamente Sun), Java Virtual Machine (JVM) y Java SE en el kit de desarrollo Java Development Kit (JDK). Las vulnerabilidades de Java fueron las culpables de entre una tercera parte y la mitad de todas las vulnerabilidades observadas durante trimestres más recientes.

- En el segundo trimestre de 2011 aumentaron drásticamente las detecciones de vulnerabilidades de seguridad en sistemas operativos, debido al aumento de explotación de la vulnerabilidad CVE-2010-2568.
- Las detecciones de vulnerabilidades de seguridad dirigidas a Adobe Flash, aunque poco habituales en comparación con otros tipos de vulnerabilidades, aumentaron en el segundo trimestre de 2011 en más de 40 veces el volumen detectado durante el primer trimestre, debido a la explotación de un par de nuevas vulnerabilidades descubiertas.
- Las vulnerabilidades de seguridad cuyo objetivo es CVE-2010-2568, una vulnerabilidad de Windows Shell, aumentaron de manera significativa en el segundo trimestre de 2011 y fueron las causantes del aumento general de vulnerabilidades de seguridad en sistemas operativos en ese trimestre. La vulnerabilidad se descubrió por primera vez a mediados de 2010, cuando la usaba la familia Win32/Stuxnet.

Vulnerabilidades de seguridad en documentos

Figura . Tipos de vulnerabilidades analizadoras de documentos detectadas y bloqueadas por los productos antimalware de Microsoft, del 3T10 al 2T11



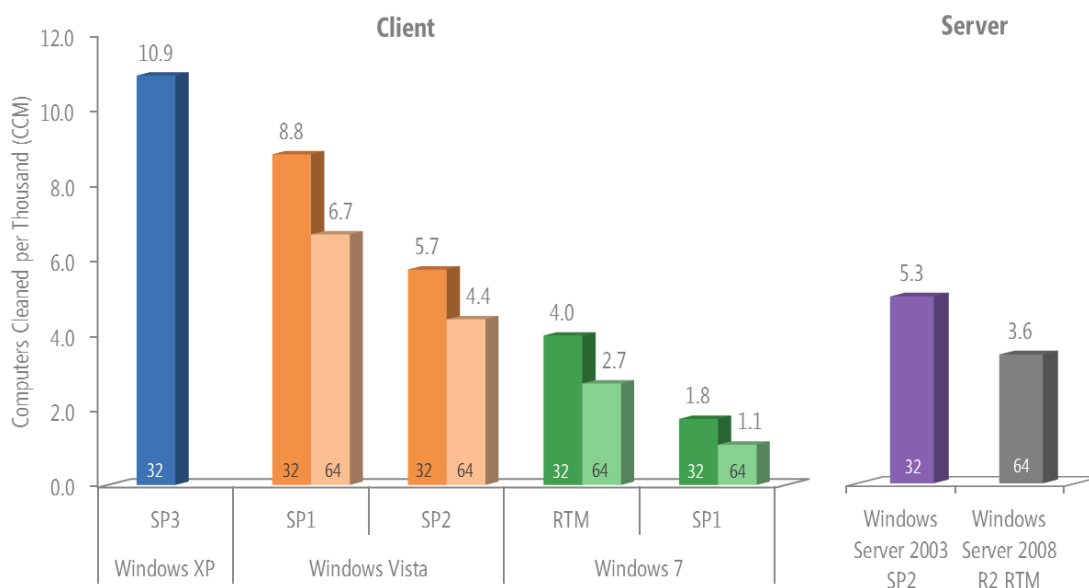
- En la primera mitad de 2011, la mayoría de vulnerabilidades de seguridad detectadas afectaban a documentos con formato de Adobe Acrobat y Adobe Reader. En la mayor parte de ellas estaba implicada la familia genérica de vulnerabilidades de seguridad [Win32/Pdfjsc](#).
- En más de la mitad de las vulnerabilidades de seguridad de Microsoft Office estaba implicada la vulnerabilidad [CVE-2010-3333](#), que afecta al analizador de Formato de texto enriquecido (RTF) en versiones de Microsoft Word.

Malware y software potencialmente no deseado

Excepto en los lugares donde se indique lo contrario, la información de esta sección se recopiló a partir de datos de telemetría de más de 600 millones de PCs de todo el mundo y de algunos de los servicios en línea con más tráfico de Internet. El índice de infecciones se muestra en *PCs desinfectados por millares (CCM)* y representa el número de PCs desinfectados en un trimestre por cada 1.000 ejecuciones de la Herramienta de eliminación de software malintencionado. Para obtener más información sobre la métrica CCM consulte la sección “Malware” del sitio web del *Informe de inteligencia de seguridad de Microsoft*.

Índices de infección de sistemas operativos

Figura . Índice de infección (CCM) por sistema operativo y service pack en el 2T11



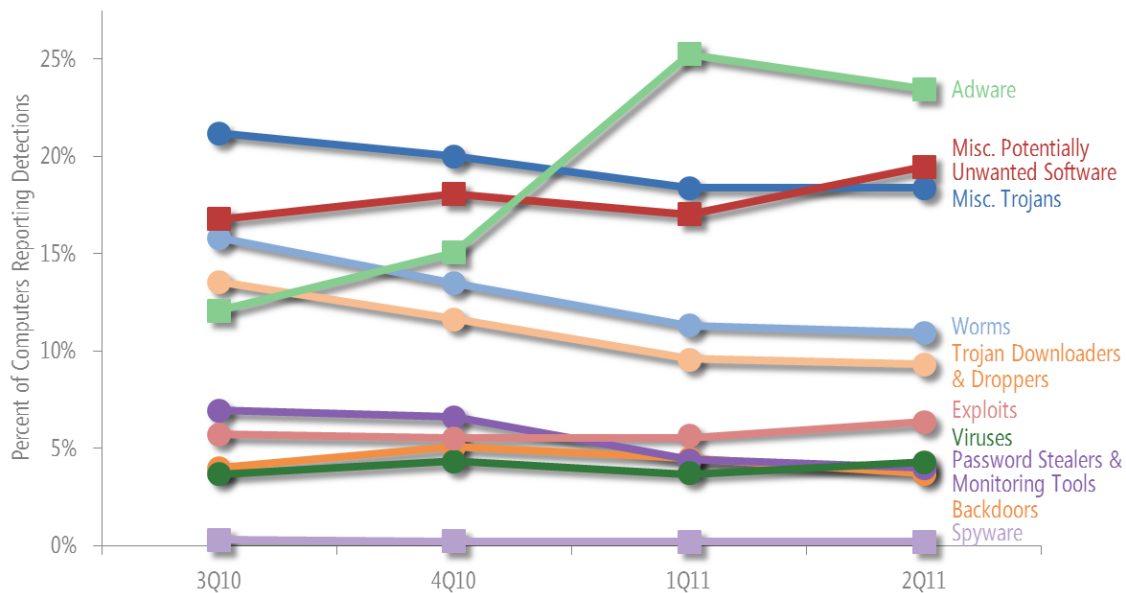
“32” = edición de 32 bits; “64” = edición de 64 bits. SP = Service Pack. Se muestran los sistemas operativos admitidos con al menos el 0,1 por ciento del total de ejecuciones en el 2T11...

- Como en periodos anteriores, los índices de infección de los sistemas operativos y service packs de Microsoft lanzados recientemente son sistemáticamente más bajos que los más antiguos, tanto para la plataforma de cliente como la de servidor. Windows 7 y Windows Server® 2008 R2, las versiones más recientes de cliente y servidor de Windows respectivamente, tienen el índice de infección más bajo, tal como se muestra en Figura .

- Los índices de infección de Windows XP SP3 y Windows Vista descendieron tras el lanzamiento en febrero de 2011 de una actualización automática, que modificaba la función de ejecución automática en esas plataformas para igualar su funcionalidad en Windows 7. El impacto de este cambio se puede ver en las estadísticas de infección por Win32/Rimecud, la novena familia de amenazas más común a nivel mundial durante la primera mitad de 2011 y uno de los principales infractores de la función de ejecución automática.

Familias de amenazas y sus categorías

Figura . Detecciones por categorías de amenaza entre el 3T10 y el 2T11, por porcentaje de todos los PCs que generaron informes de detecciones



Los marcadores redondos representan las categorías de malware; los marcadores cuadrados representan categorías de software potencialmente no deseado.

- Win32/OpenCandy fue la familia de amenazas detectada con más frecuencia en la primera mitad de 2011 en general. OpenCandy es un programa de adware que puede estar incluido con algunos programas de instalación de software de terceros.
- JS/Pornpop, la segunda familia de amenazas detectada con más frecuencia en la primera mitad de 2011, es una detección de objetos con JavaScript habilitado que intentan desplegar anuncios emergentes en los exploradores web del usuario

- Win32/Hotbar, la familia de amenazas más común durante el segundo trimestre de 2011 y la tercera más común durante la primera mitad de 2011, es un adware que instala una barra de herramientas en el explorador que despliega anuncios emergentes basados en un seguimiento de la actividad de exploración por la web.
- Las detecciones de Win32/FakeRean aumentaron más de un 300 por ciento desde el 1T11 al 2T11, convirtiéndose en la familia de software de seguridad fraudulento más detectado en el segundo trimestre.

Amenazas de empresa

- Familias de gusanos registradas como las tres familias de malware más comunes detectadas en PCs unidos al dominio, que son más habituales en entornos empresariales que en entornos domésticos.
- Entre las familias de malware que prevalecen de forma considerable en PCs unidos al dominio se incluyen Win32/Conficker y el programa de software potencialmente no deseado Win32/RealVNC. RealVNC es un programa que permite controlar un PC de forma remota, similar a los Servicios de Escritorio Remoto. Tiene una serie de usos legítimos, pero los atacantes también lo han usado en ocasiones para controlar los PCs de usuario con fines malintencionados.
- La familia de Win32/Sality, que no se encontraba entre las 10 principales familias detectadas en PCs unidos al dominio en 2010, alcanza el décimo lugar en la primera mitad de 2011.

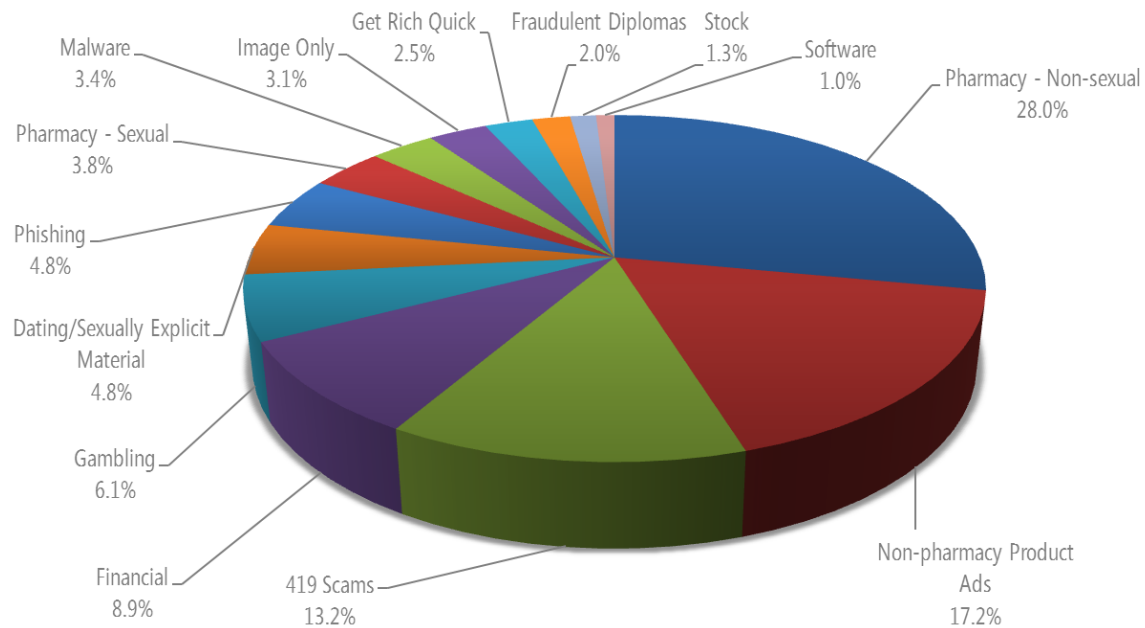
Amenazas de correo electrónico

- El volumen de correo no deseado bloqueado por Microsoft Forefront® Online Protection for Exchange (FOPE) descendió drásticamente en los últimos 12 meses, de 89.200 millones de mensajes en julio de 2010 a 25.000 millones en junio de 2011, en gran medida gracias a la desactivación de las dos principales redes de robots: Cutwail, que se apagó en agosto de 2010; y

Rustock, que se apagó en marzo de 2011, tras un periodo de letargo que comenzó en enero. ¹

- Como en periodos anteriores, la publicidad de productos farmacéuticos no sexuales (28 por ciento del total) y de productos no farmacéuticos (17,2 por ciento) constituyó la mayor parte del correo no deseado bloqueado por los filtros de contenido de FOPE en la primera mitad de 2011.
- El correo no deseado exclusivamente de imágenes descendió al 3,1 por ciento del total en la primera mitad de 2011, desde el 8,7 que constituía en 2010.

Figura . Mensajes entrantes bloqueados por los filtros de FOPE en la primera mitad de 2011, por categoría



Sitios web malintencionados

- Aunque los suplantadores de identidad se suelen dirigir a sitios financieros, el mayor número de impresiones de suplantación de identidad en la primera mitad de 2011 se produjo en sitios destinados a las redes sociales, alcanzando un 83,8 por ciento en abril. (Una impresión de suplantación de

¹ Para obtener más información sobre la desactivación de Cutwail, consulte el *Informe de inteligencia de seguridad de Microsoft, volumen 10 (julio a diciembre de 2010)*. Para obtener más información sobre la desactivación de Rustock, vea “La lucha contra la amenaza Rustock”, disponible en el Centro de descarga de Microsoft.

identidad es una instancia de un usuario que intenta visitar un sitio de suplantación de identidad conocido con Windows Internet Explorer® y es bloqueado por el filtro SmartScreen®. Para obtener más información consulte la sección “Sitios web malintencionados” del sitio web del Informe de inteligencia de seguridad de Microsoft). En general, las impresiones dirigidas a las redes sociales constituyeron el 47,8 por ciento de todas las impresiones de la primera mitad de 2011, seguidas de aquellas dirigidas a instituciones financieras, que constituyeron el 35 por ciento.

- Por el contrario, según el seguimiento realizado en los sitios de suplantación de identidad activos durante la primera mitad de 2011, la media de los sitios dirigidos a instituciones financieras fue del 78,3 por ciento, frente al 5,4 por ciento de aquellos dirigidos a las redes sociales. Las instituciones financieras objetivo de suplantadores de identidad pueden llegar a ser cientos y, para cada una de ellas, se necesita un enfoque personalizado de suplantación. El número de sitios de redes sociales populares es mucho menor, por lo que los suplantadores de identidad que se centran en las redes sociales pueden acceder de forma efectiva a muchas más personas por sitio. Además, la capacidad de acceso directo ilegal a las cuentas bancarias de las víctimas hace que las instituciones financieras continúen siendo los objetivos de suplantación de identidad más populares, ya que estos siguen recibiendo el mayor o segundo mayor número de impresiones por mes.
- Este fenómeno también se produce a menor escala con los servicios en línea y los sitios de juegos. La mayoría del tráfico hacia este tipo de sitios registra una cantidad muy pequeña de servicios en línea, por lo que los sitios de suplantación de identidad que se dirigieron a servicios en línea supusieron en total un 11 por ciento de impresiones en tan solo un 3,6 por ciento de sitios. El tráfico hacia juegos en línea tiende a dispersarse por un mayor número de sitios, por lo que los sitios de suplantación destinados a los juegos en línea se dirigieron a un 8,9 por ciento de los sitios activos, pero solo consiguieron llevar a cabo un 4,3 por ciento de las impresiones.

Los sitios de suplantación de identidad dirigidos al comercio electrónico solo fueron responsables del ataque al 3,8 por ciento de los sitios activos y del 1,9 de las impresiones, lo que indica que los sitios de comercio electrónico no resultan objetivos particularmente rentables.

Puede encontrar información sobre *cómo proteger su organización, su software y a su personal* en la sección “Gestión de riesgos” del sitio web del *Informe de inteligencia de seguridad de Microsoft*.
<http://www.microsoft.com/sir> (página en inglés)





Microsoft®

One Microsoft Way
Redmond, WA 98052-6399,
EE.UU.
microsoft.com/security