Microsoft Security Intelligence Report

Volumen 13

ENERO-JUNIO 2012

PRINCIPALES CONCLUSIONES

www.microsoft.com/sir

Microsoft Security Intelligence Report

Este documento tiene fines exclusivamente informativos. MICROSOFT NO OTORGA NINGUNA GARANTÍA, YA SEA EXPRESA, IMPLÍCITA O PREVISTA POR LEY, CON RESPECTO A LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO.

Este documento se proporciona “tal cual”. Tanto la información como las opiniones expresadas en este, incluidas las direcciones URL y otras referencias a sitios web de Internet, pueden cambiar sin previo aviso. Usted acepta el riesgo de utilizarlo.

Copyright © 2012 Microsoft Corporation. Todos los derechos reservados.

Los nombres de los productos y las compañías reales aquí mencionados pueden ser marcas comerciales de sus respectivos propietarios.

Microsoft Security Intelligence Report, Volumen 13

El volumen 13 del *Microsoft® Security Intelligence Report* (*SIRv13*) presenta en detalle perspectivas acerca de las vulnerabilidades de software, amenazas de código malicioso y software posiblemente no deseado en programas de software de Microsoft y de terceros. Microsoft ha elaborado estas perspectivas basándose en detallados análisis de tendencias realizados en los últimos años, haciendo hincapié en el primer semestre de 2012.

Este documento resume las principales conclusiones del informe. El informecompleto incluye también un análisis a fondo de las tendencias observadas en más de 100 países/regiones del mundo, y presenta sugerencias que contribuirán a gestionar los riesgos para su organización, sus programas de software y su personal.

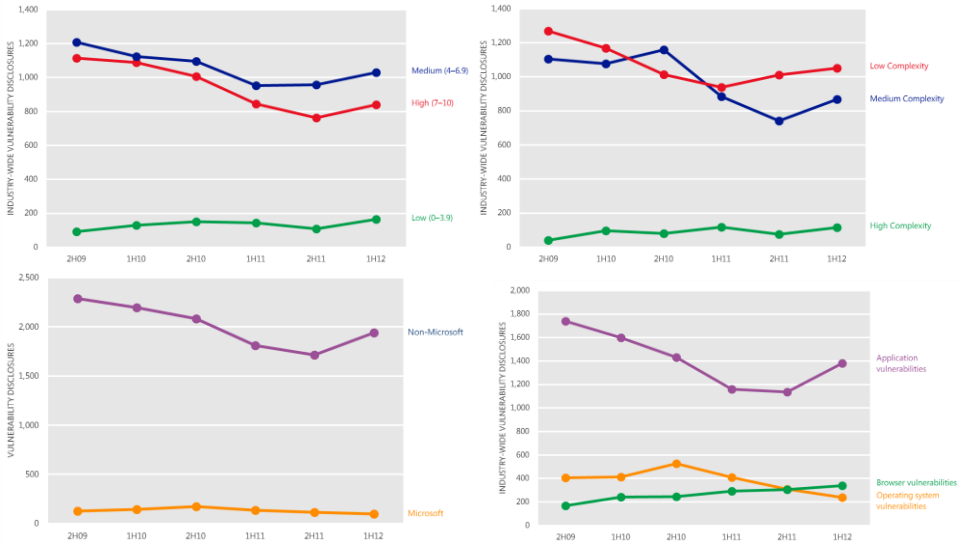
Puede descargar el informe completo desde www.microsoft.com/sir.

Evaluación de la amenaza mundial

Vulnerabilidades

Las *vulnerabilidades* son los puntos débiles de un programa de software que permiten a un atacante comprometer la integridad, disponibilidad o confidencialidad del software o de los datos que procesa. Algunas de las peores vulnerabilidades permiten a los atacantes aprovecharse del sistema comprometido haciéndolo ejecutar códigos maliciosos sin conocimiento del usuario.

Figura 1. Tendencias de severidad (CVE) y complejidad de la vulnerabilidad, denuncias por proveedor y por tipo, en todo el sector del software, 2S09-1S12[1]



[1] La nomenclatura utilizada en el documento para hacer referencia a los diferentes períodos de informes es nSAA, siendo la S el primer (1) o el segundo (2) semestre del año, y AA el año. Por ejemplo, 2S09 denota el segundo semestre del año 2009 (del 1 de julio hasta el 31 de diciembre), en tanto que 1S12 representa el período que cubre el primer semestre de 2012 (desde el 1 de enero hasta el 30 de junio).

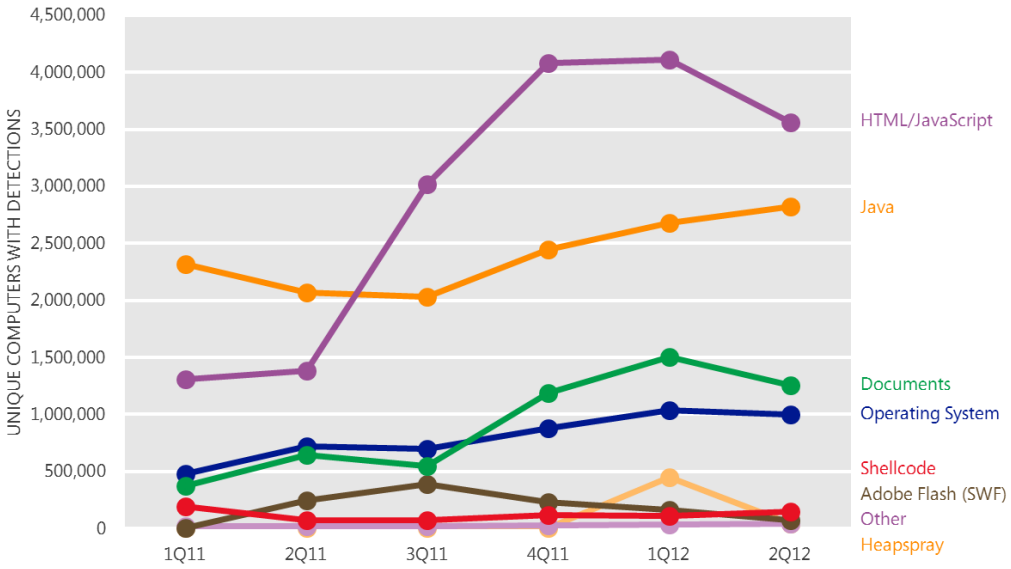
- En el 1S12, las denuncias de vulnerabilidad del sector crecieron el 11,3% con respecto al 2S11 y el 4,8% desde el 1S11.
- Este aumento invierte una tendencia de pequeños descensos en cada período de seis meses comprendido entre el 2S09 y el 2S11, y proviene en su mayor parte de las vulnerabilidades de las aplicaciones, ya que las vulnerabilidades de los sistemas operativos prosiguen una tendencia a la baja.

Manipulaciones

Una *manipulación* es un código malicioso que se aprovecha de las vulnerabilidades de un programa de software para infectar, trastornar o controlar un equipo informático sin autorización del usuario y, por lo general, sin su conocimiento. Las manipulaciones van dirigidas a vulnerabilidades de los sistemas operativos, exploradores web, aplicaciones o componentes de software instalados en los equipos. Para obtener más información, descargue el informe *SIRv13* completo desde www.microsoft.com/sir.

La figura 2 muestra la prevalencia de distintos tipos de manipulaciones detectadas por los productos antimalware de Microsoft en cada trimestre del 1T11 al 2T12, por número de equipos únicos afectados.

Figura 2. Equipos únicos que informan de distintos tipos de manipulaciones, 1T11-2T12



- El número de equipos que informaron de manipulaciones ejecutadas a través de HTML o de JavaScript se mantuvo alto durante el primer semestre de 2012, impulsado principalmente por la prevalencia continuada de Blacole, la familia de manipulaciones más detectada en el 1S12.
- Las manipulaciones de Java, el segundo tipo de manipulación más detectado en el 1S12, aumentaron a lo largo de dicho período, impulsadas por la detección incrementada de manipulaciones para CVE-2012-0507 y CVE-2011-3544.
- Las manipulaciones dirigidas a vulnerabilidades de lectores y editores de texto fueron el tercer tipo más habitual detectado durante el 1S12, principalmente por las detecciones de manipulaciones dirigidas a versiones anteriores de Adobe Reader.

Familias de manipulaciones

La figura 3 enumera las familias relacionadas con las manipulaciones más detectadas durante el primer semestre de 2012.

Figura 3 [TopExploitFamilies] Familias de manipulaciones más importantes detectadas por los productos antimalware de Microsoft en el 1S12, por número de equipos únicos con detecciones, sombreadas según la prevalencia relativa

Familia de manipulaciones	Plataforma o tecnología	3T11	4T11	1T12	2T12
Blacole	HTML/JavaScript	1.054.045	2.535.171	3.154.826	2.793.451
CVE-2012-0507*	Java	–	–	205.613	1.494.074
Win32/Pdfjsc	Documentos	491.036	921.325	1.430.448	1.217.348
IFrame malintencionado	HTML/JavaScript	1.610.177	1.191.316	950.347	812.470
CVE-2010-0840*	Java	1.527.000	1.446.271	1.254.553	810.254
CVE-2011-3544	Java	–	331.231	1.358.266	803.053
CVE-2010-2568 (MS10-046)	Sistema operativo	517.322	656.922	726.797	783.013
JS/Phoex	Java	–	–	274.811	232.773
CVE-2008-5353	Java	335.259	537.807	295.515	215.593
Código shell	Código shell	71.729	112.399	105.479	145.352

* Esta vulnerabilidad también la usa el kit Blacole; los totales aquí proporcionados para esta vulnerabilidad excluyen las detecciones de Blacole.

- Blacole, una familia de manipulaciones empleadas por el así llamado kit "Blackhole", que carga software malicioso a través de páginas web infectadas, fue la familia de manipulaciones más detectada en el primer semestre de 2012. Los posibles atacantes compran o alquilan el kit Blacole en foros de hackers y a través de otros puntos de venta ilegítimos. Se compone de una colección de páginas web malintencionadas que contienen manipulaciones para vulnerabilidades en versiones de Adobe Flash Player, Adobe Reader, Microsoft Data Access Components (MDAC), el entorno de tiempo de ejecución de Java (JRE) para Oracle, así como en otros productos y componentes populares. Cuando el atacante instala el kit Blacole en un servidor web malintencionado o vulnerado, los visitantes que no tengan instaladas las actualizaciones de seguridad adecuadas correrán el riesgo de infección mediante un ataque de descarga drive-by.

Malware y software potencialmente no deseado

Salvo en los casos en que se especifica, la información de esta sección fue compilada a través de datos de telemetría generados a partir de más de 600 millones de equipos en todo el mundo y de algunos de los servicios en línea más utilizados de Internet. Las tasas de infección se presentan como equipos limpiados por millares (CCM, por sus siglas en inglés), y representan el número de equipos que se limpiaron durante el trimestre por cada 1000 ejecuciones de la Herramienta de eliminación de software malintencionado de Windows®, disponible a través de Microsoft Update y del sitio web Centro de seguridad y protección de Microsoft.

Desde una perspectiva de patrones de infección en todo el mundo, la Figura 4 muestra las tasas de infección en distintos lugares utilizando el parámetro CCM. Las detecciones y eliminaciones en los distintos países/regiones pueden variar significativamente entre un trimestre y otro.

Figura 4. Tasas de infección por país/región el 2T12, por CCM

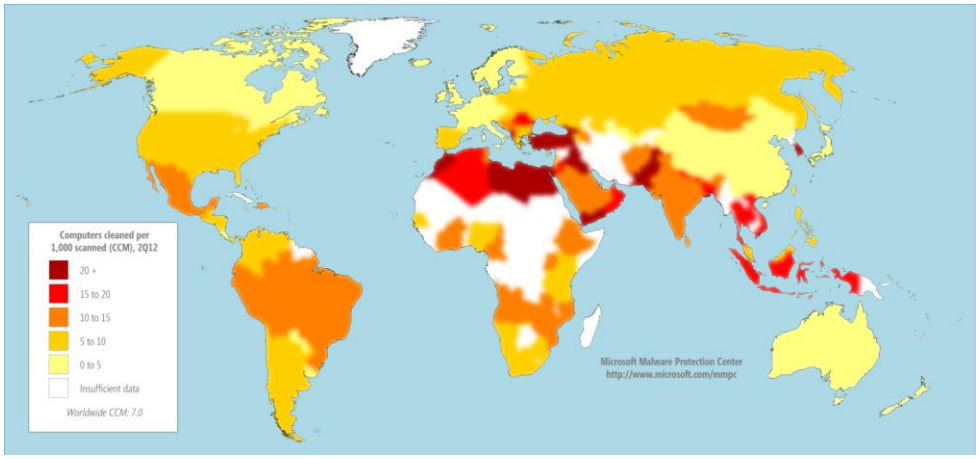
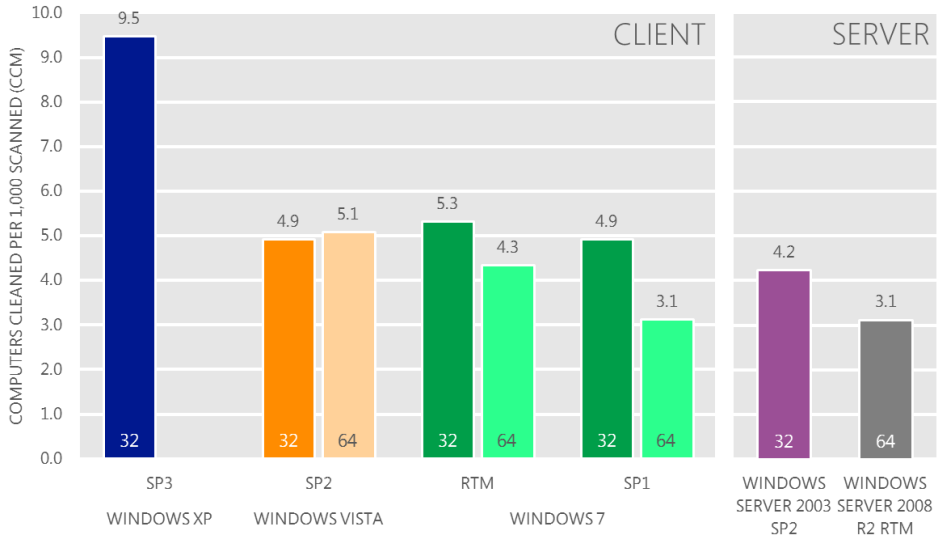


Figura 5. Tasas de infección (CCM) por sistema operativo y Service Pack el 2T12

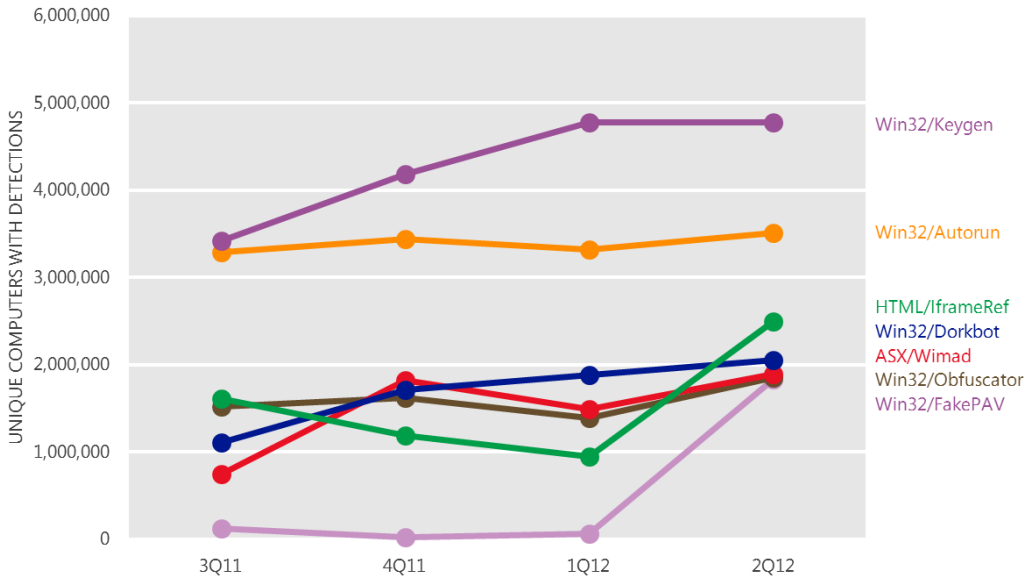


"32"= edición de 32 bits; "64" = edición de 64 bits. SP = Service Pack. RTM = enviado a producción. Se indican los sistemas operativos con al menos un 0,1% de ejecuciones totales de la MSRT en el 2T12.

- Estos datos han sido normalizados: la tasa de infecciones por cada versión de Windows se calcula comparando un número equivalente de equipos por versión (por ejemplo, 1000 equipos con sistema operativo Windows XP SP3 comparados con 1000 equipos con Windows 7 RTM).

Familias de amenazas

Figura 6. Tendencias de detección de determinada cantidad de familias destacadas, 3T11-2T12



- Un par de detecciones genéricas, Win32/Keygen y Win32/Autorun, fueron la primera y la segunda familia más detectadas en el 1S12. Keygen es una detección genérica de herramientas que generan claves para versiones obtenidas ilícitamente de diversos productos de software.

  Autorun es una detección genérica de gusanos que se propagan entre los volúmenes montados mediante la característica de ejecución automática de Windows. Los cambios recientes aplicados a esta característica en Windows XP y Windows Vista han hecho que esta técnica sea menos eficaz, si bien los atacantes continúan distribuyendo malware dirigido a esta.

- Las detecciones de la familia de genéricos JS/IframeRef aumentaron más del doble entre el 1T12 y el 2T12 tras varios trimestres de pequeños descensos. IframeRef es una detección genérica de etiquetas de marco flotante (IFrame) HTML con formato especial que apuntan a sitios web remotos con contenido malintencionado.

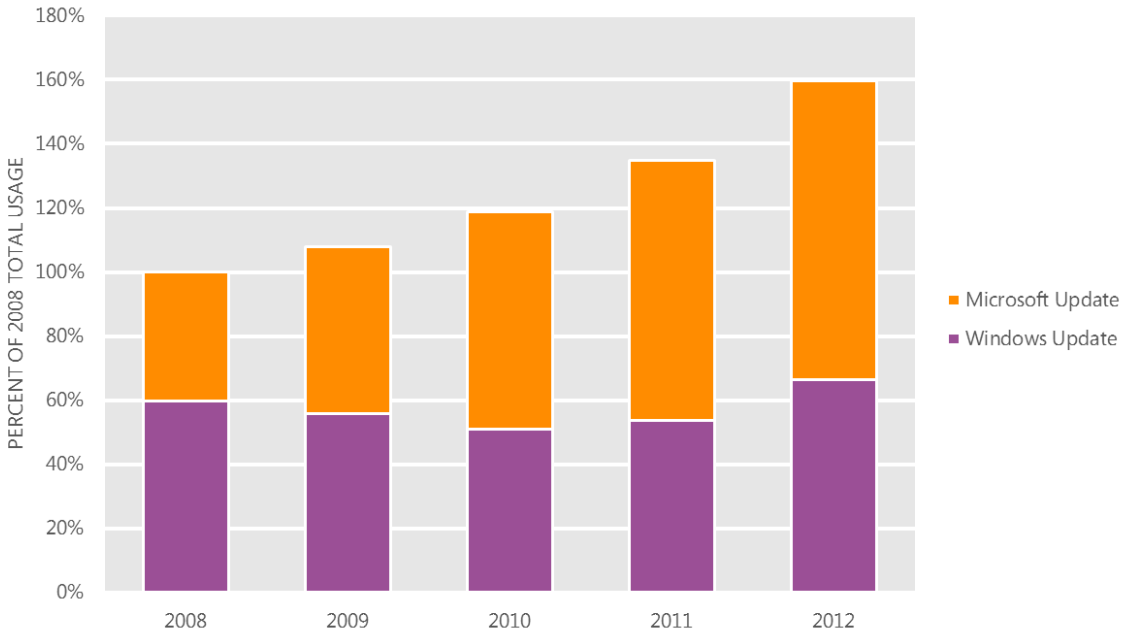
Amenazas para particulares y empresas

La comparación de las amenazas detectadas por equipos unidos y no unidos a un dominio puede facilitar información sobre los diversos métodos que emplean los atacantes para dirigirse a usuarios de empresas y particulares, y también cuáles son las amenazas con mayores probabilidades de éxito en cada entorno.

- Cinco familias son comunes en ambas listas, notablemente las familias de genéricos Win32/Keygen y Win32/Autorun, y la familia de manipulaciones Blacole.
- Entre las familias significativamente mas prevalentes en equipos pertenecientes a un dominio durante al menos un trimestre se incluyen la familia de genéricos JS/IframeRef y la familia de gusanos Win32/Conficker.
- Entre las familias significativamente mas prevalentes en equipos no pertenecientes a un dominio se incluyen Keygen y las familias de publicidad no deseada JS/Pornpop y Win32/Hotbar.

Uso de Windows Update y Microsoft Update

Figura 7. [WU-MU] Equipos con Windows actualizados mediante Windows Update y Microsoft Update en todo el mundo, 2008-2012



- La figura 7 muestra el aumento del número de equipos actualizados mediante Windows Update y Microsoft Update en todo el mundo durante los últimos cuatro años, indizado respecto al uso total de ambos servicios en 2008.
- Desde 2008, el uso de Windows Update y Microsoft Update en todo el mundo se ha incrementado en un 60%. Casi todo este crecimiento se debe al uso cada vez mayor de Microsoft Update, que experimentó un incremento de 53 puntos porcentuales entre 2008 y 2012, frente a los 6 puntos porcentuales de Windows Update.
- **Windows Update** ofrece actualizaciones de los componentes de Windows y de los controladores de dispositivos que facilitan Microsoft y otros vendedores de hardware. Asimismo, también distribuye actualizaciones de firma de los productos antimalware de Microsoft y la versión mensual de la MSRT. De forma predeterminada, siempre que un usuario habilita la actualización automática, el cliente de actualización se conecta al servicio Windows Update por si hubiera actualizaciones.

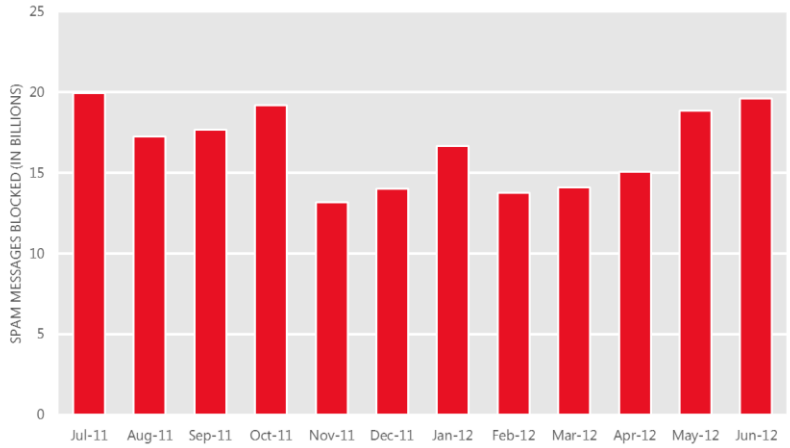
- **Microsoft Update** proporciona todas las actualizaciones ofrecidas a través de Windows Update, así como actualizaciones para otro software de Microsoft, como Microsoft Office System, Microsoft SQL Server y Microsoft Exchange Server. Los usuarios pueden optar al servicio al instalar software que se ofrece a través de Microsoft Update o en el sitio web de Microsoft Update (update.microsoft.com/microsoftupdate). Microsoft recomienda que los usuarios configuren los equipos para usar Microsoft Update en lugar de Windows Update para ayudar a garantizar que estos reciban las actualizaciones de seguridad de los productos de Microsoft a su debido tiempo.

Amenazas de correo electrónico

Mensajes de correo no deseado bloqueados

La información de esta sección del *Microsoft Security Intelligence Report* se compila a partir de datos de telemetría facilitados por el servicio de protección en línea de Microsoft Exchange (FOPE), que presta servicios de filtrado de correo no deseado, de suplantaciones de identidad y de software malicioso a miles de clientes empresariales de Microsoft que procesan decenas de miles de millones de mensajes cada mes.

Figura 8. Mensajes bloqueados por el servicio de protección en línea de Exchange, julio de 2011 a junio de 2012



- Los volúmenes de correo bloqueado en el 1S12 estuvieron en concordancia con los correspondientes al 2S11 y se mantienen en niveles muy inferiores a los obtenidos antes de finales de 2010. El espectacular descenso de correo no deseado observado en el último año y medio se ha producido tras las medidas adoptadas satisfactoriamente contra una serie de robots emisores de correo no deseado a gran escala, en particular Cutwail (agosto de 2010) y Rustock (marzo de 2011).

Figura 9. [FOPEBlockedHistoric] Mensajes bloqueados por la protección en línea de Exchange cada semestre, 2S08-1S12

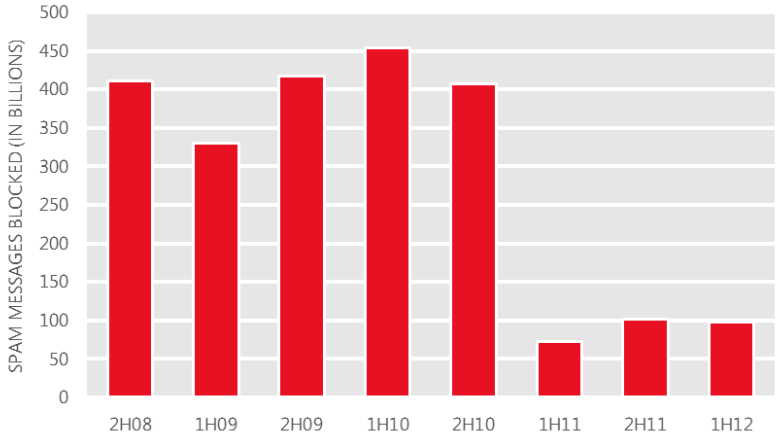
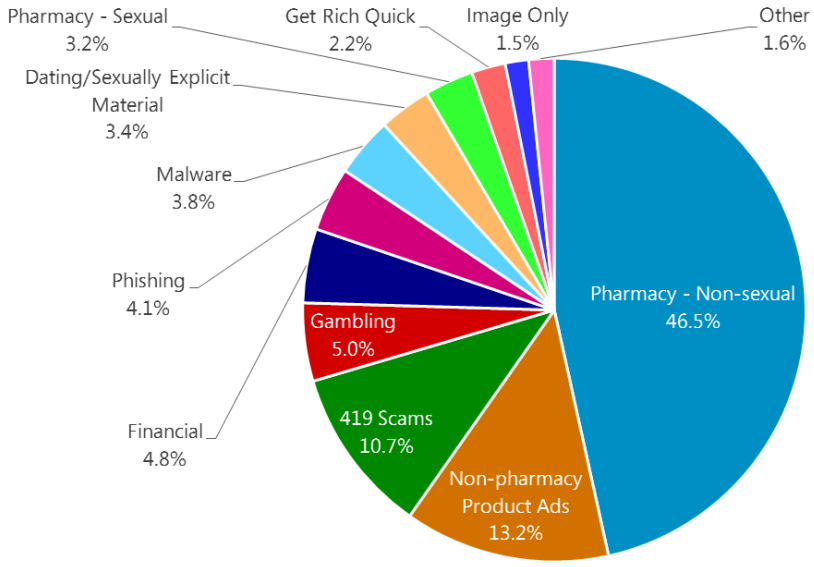


Figura 10. Mensajes entrantes bloqueados por los filtros de la protección en línea de Exchange el 1S12, por categoría

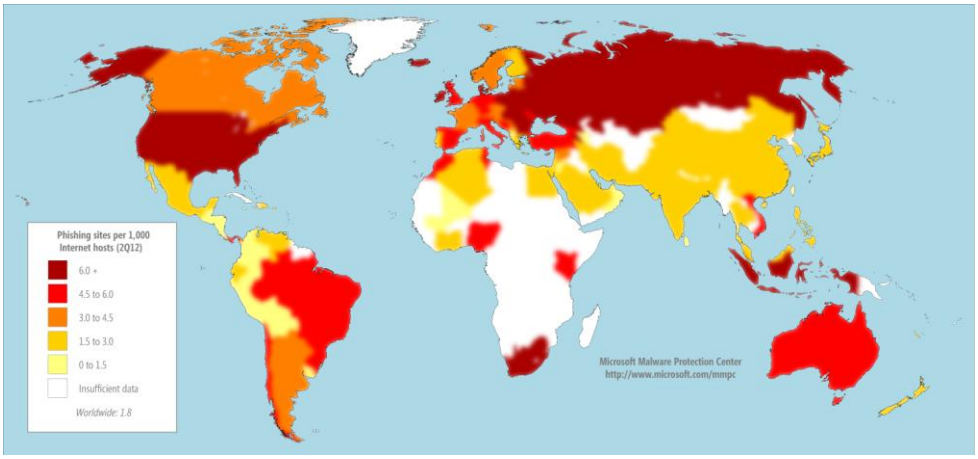


- Los filtros de contenidos de FOPE reconocen diversos tipos comunes de mensajes de correo no deseado. La figura 10 muestra la prevalencia relativa de los tipos de mensajes no deseados que se detectaron en el 1S12.

Sitios web malintencionados

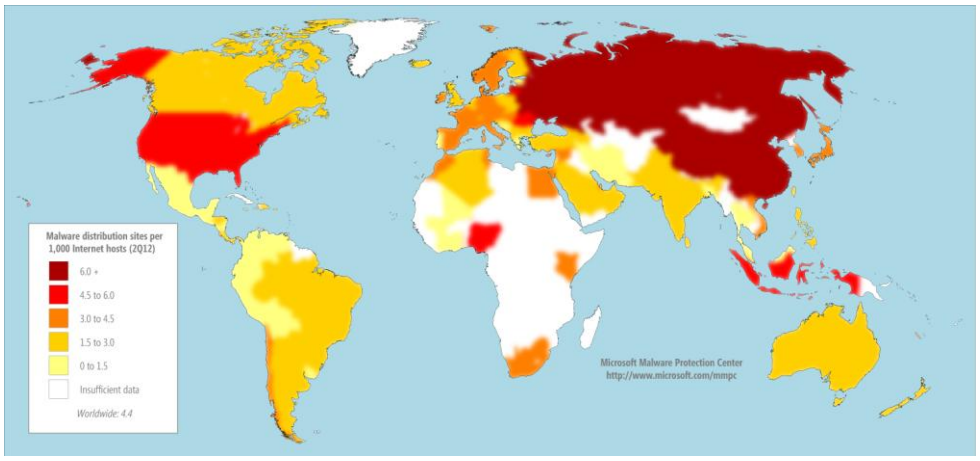
Los sitios de suplantación de identidad (phishing) están alojados en todo el mundo en sitios de alojamiento gratuito, en servidores web vulnerados y en muchos otros contextos.

Figura 11. Sitios de suplantación de identidad por cada 1000 hosts de Internet ubicados en todo el mundo durante el 2T12



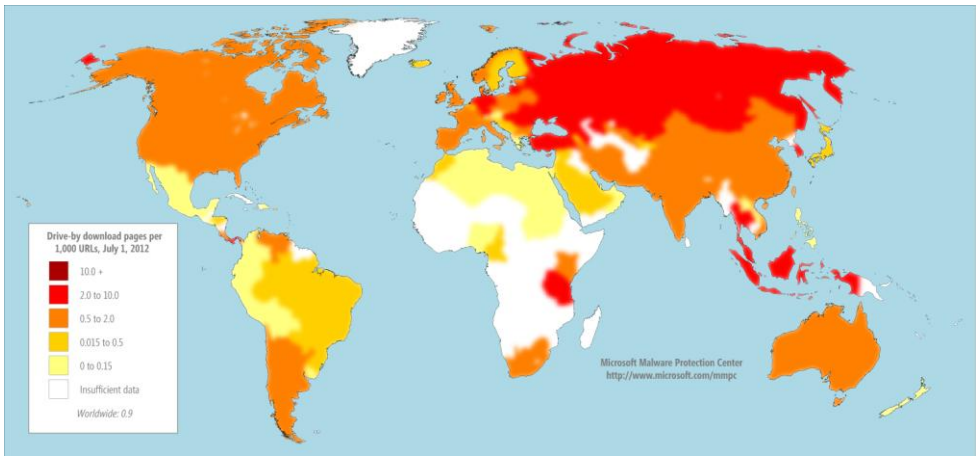
Los Estados Unidos, que tienen el mayor número de hosts, cuentan además con un gran número de sitios de suplantación de identidad (2,9 por cada 1000 hosts de Internet en el 2T12); China, que ocupa el segundo puesto en número de hosts, tiene una concentración mucho menor de estos (0,6 por cada 1000 hosts de Internet).

Figura 112. Sitios de distribución de software malintencionado por cada 1000 hosts de Internet en lugares de todo el mundo durante el 2T12



Un sitio de *descargas drive-by* es un sitio web que aloja una o más manipulaciones dirigidas a vulnerabilidades de exploradores web y complementos de exploradores. Los usuarios con equipos vulnerables pueden resultar afectados por software malintencionado por el solo hecho de visitar estos sitios, incluso sin intentar descargar nada.

Figura 13. Páginas de descargas drive-by indizadas por Bing.com a finales del 2T12, por cada 1000 direcciones URL de cada país/región



Este documento resume las principales conclusiones del informe. El informecompleto incluye también un análisis a fondo de las tendencias observadas en más de 100 países/regiones del mundo, y presenta sugerencias que contribuirán a gestionar los riesgos para su organización, sus programas de software y su personal.

Puede descargar el informe completo desde www.microsoft.com/sir.

Microsoft

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