

Volumen 6 del informe de inteligencia sobre seguridad de Microsoft (de julio a diciembre de 2008)

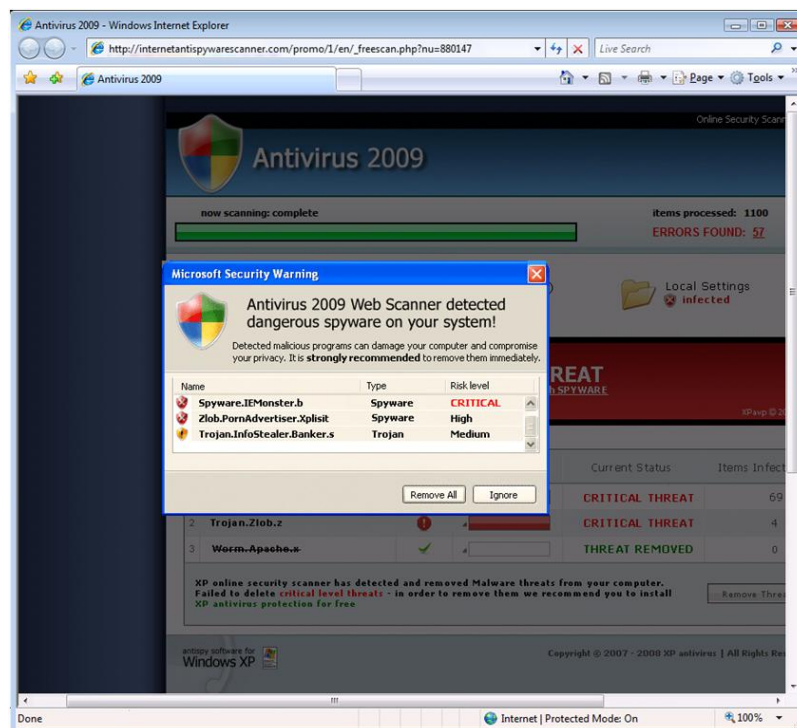
Resumen de resultados clave

El volumen 6 del informe de inteligencia sobre seguridad de Microsoft® ofrece una perspectiva detallada acerca de las diferentes vulnerabilidades de software (tanto en software de Microsoft como en software de terceros), así como de las tendencias del software malintencionado y el software potencialmente no deseado, que Microsoft ha observado en los últimos años, con un enfoque especial en la segunda mitad de 2008 (2M08)¹. El informe también contiene nueva información acerca del software de seguridad falso, junto con las vulnerabilidades de seguridad de los exploradores y los formatos de documentos más habituales, además de información actualizada acerca de las infracciones de seguridad y privacidad.

Este documento es un resumen de los resultados clave de dicho informe. El informe completo de inteligencia sobre seguridad, que también ofrece estrategias, métodos para minimizar el impacto de estos problemas y otras contramedidas, puede descargarse de <http://www.microsoft.com/sir>.

Software de seguridad falso

La presencia del software de seguridad falso se ha incrementado significativamente a lo largo de los tres últimos periodos (consulte la categoría de Troyanos varios en la Ilustración 16 que figura más adelante). El software de seguridad falso emplea técnicas basadas en el miedo y la insistencia para convencer a las víctimas de pagar por “versiones completas” del software para evitar y eliminar el malware, detener las alertas y advertencias continuas, o ambas cosas. En el informe completo de inteligencia sobre seguridad pueden encontrarse ejemplos de técnicas de ingeniería social del software de seguridad falso, incluidas capturas de pantalla. El informe también cuenta con una sección dedicada a las acciones legales emprendidas contra los distribuidores de software de seguridad falso.



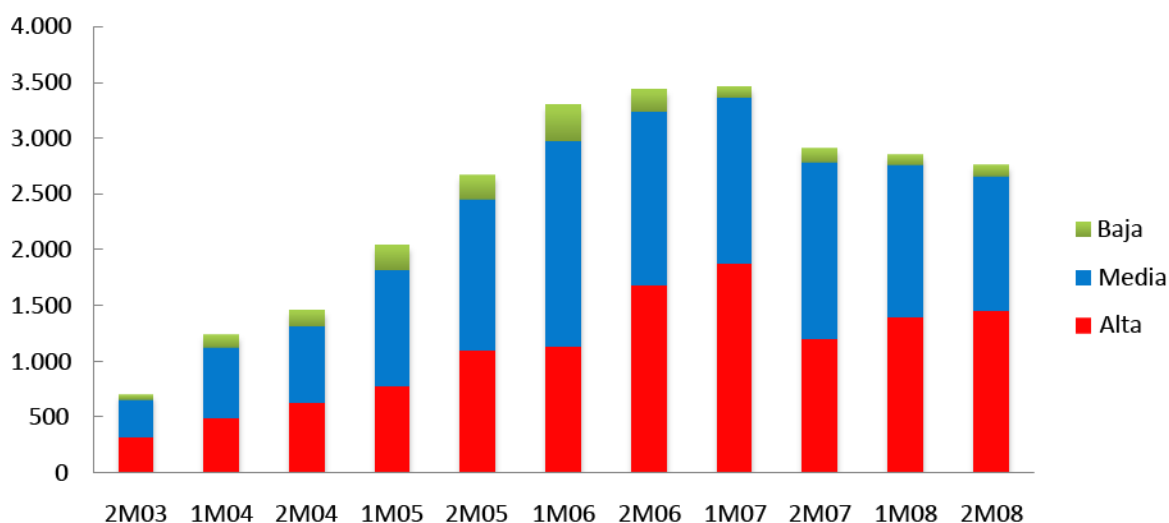
¹ En el informe se usa una nomenclatura específica para hacer referencia a diferentes periodos: en nMAA, nM se refiere a la primera mitad del año (1) o a la segunda (2), y AA indica el año. Por ejemplo, 2M08 representa el periodo que cubre la segunda mitad de 2008 (del 1 de julio al 31 de diciembre), mientras que 1M08 representa el periodo que cubre la primera mitad de 2008 (del 1 de enero al 30 de junio).

Divulgaciones de vulnerabilidades del sector

Las vulnerabilidades se definen como puntos débiles del software que permiten a los atacantes comprometer la integridad, disponibilidad o confidencialidad de dicho software. Algunas de las vulnerabilidades más peligrosas permiten a los atacantes ejecutar código arbitrario en sistemas en peligro. Los datos acerca de vulnerabilidades de esta sección se recopilaron a partir de fuentes de terceros, informes publicados y los propios datos de Microsoft.

- El número total de divulgaciones exclusivas de vulnerabilidades de todo el sector disminuyó en 2M08 un 3% respecto a 1M08. Considerando 2008 en su conjunto, las divulgaciones totales se redujeron en un 12% respecto a 2007.
- Por el contrario, las vulnerabilidades calificadas como graves según el sistema de clasificación común de vulnerabilidades (CVSS)² aumentaron un 4% durante 1M08 y, aproximadamente, el 52% de todas las vulnerabilidades se clasificaron como graves. Considerando 2008 en su conjunto, el número total de vulnerabilidades graves se redujo en un 16% respecto a 2007.

Ilustración 1. Divulgaciones de vulnerabilidades en todo el sector de gravedad CVSSv2, divididas por semestre, de 1M03 a 2M08

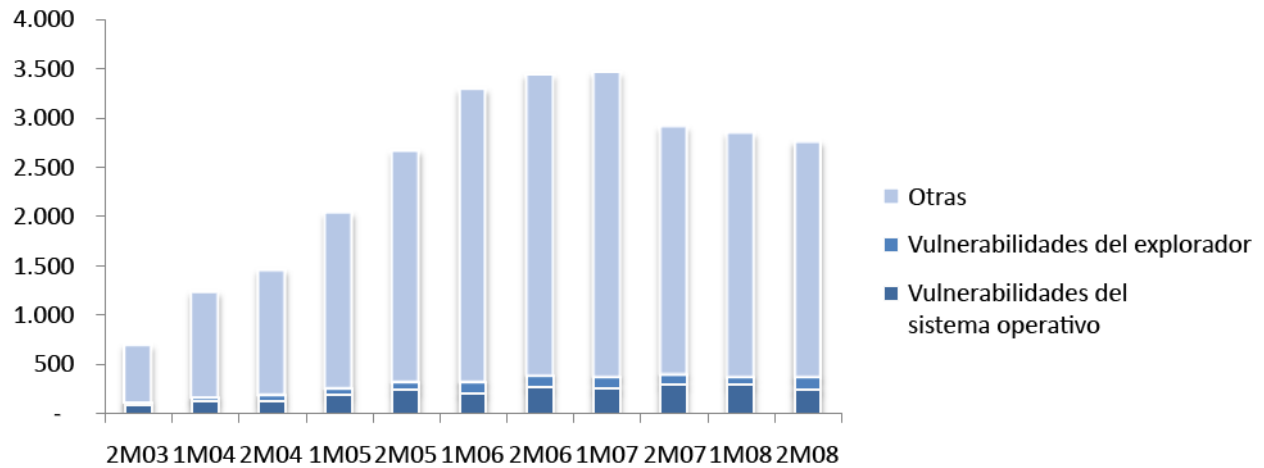


- Además de la seriedad de las vulnerabilidades graves, el porcentaje de vulnerabilidades divulgadas que se consideran las más fáciles de aprovechar también aumentó, con un 56% que sólo precisan un nivel de complejidad bajo para poder aprovecharlas³.
- La proporción de vulnerabilidades divulgadas en los sistemas operativos de todo el sector continúa disminuyendo. De hecho, más del 90% de las vulnerabilidades divulgadas afectaban a aplicaciones o exploradores.

² CVSS es un estándar del sector para clasificar la gravedad de las vulnerabilidades de software. Consulte <http://www.first.org/cvss/> para obtener más documentación e información al respecto.

³ Definición de: Mell, Peter, Karen Scarfone y Sasha Romanosky. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", (<http://www.first.org/cvss/cvss-guide.html>), sección 2.1.2.

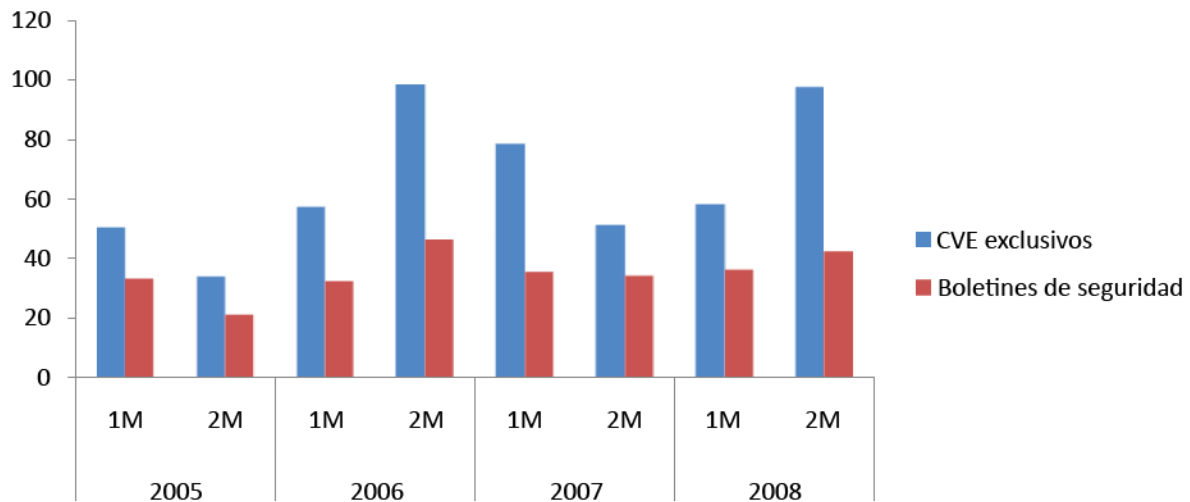
Ilustración 2. Vulnerabilidades en los sistemas operativos, exploradores y otros elementos de todo el sector, de 2M03 a 2M08



Detalles de vulnerabilidades de Microsoft de 2M08

En 2M08, Microsoft publicó 42 boletines de seguridad acerca de 97 vulnerabilidades individuales identificadas por CVE, lo que supone un incremento del 67,2% respecto al número de vulnerabilidades tratadas en 1M08. En todo el año 2008, Microsoft publicó 78 boletines de seguridad acerca de 155 vulnerabilidades, lo que supone un incremento del 16,8% respecto a 2007.

Ilustración 3. Boletines de seguridad publicados y vulnerabilidades de CVE tratadas por semestre, de 1M05 a 2M08

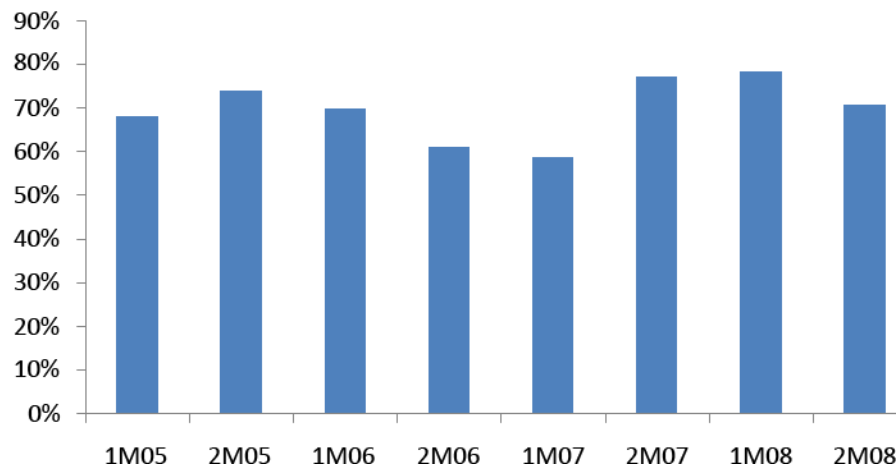


Divulgación para responsables

La *divulgación para responsables* es la divulgación privada de vulnerabilidades para un proveedor afectado, con el fin de que éste pueda desarrollar una actualización de seguridad completa para tratar la vulnerabilidad antes de que sus detalles se hagan públicos. De esta forma, los usuarios están más seguros, ya que se evita que los atacantes potenciales conozcan las nuevas vulnerabilidades antes de que las actualizaciones de seguridad estén disponibles.

- En 2M08, el 70,6% de las divulgaciones de vulnerabilidades de Microsoft correspondió a divulgaciones para responsables, lo que supone una disminución respecto al 78,2% de 1M08. El porcentaje de divulgaciones para responsables de todo el 2008 fue significativamente superior al del año anterior.
- La relación directa con la comunidad del ámbito de la seguridad, junto con el tratamiento proactivo de los problemas de seguridad, da como resultado que los responsables informen acerca de la mayoría de los problemas.

Ilustración 4. Porcentaje de divulgaciones de vulnerabilidades para responsables respecto al total de divulgaciones, de 1M05 a 2M08



Vulnerabilidades basadas en exploradores

Para evaluar la frecuencia relativa de las vulnerabilidades de los exploradores durante 2M08, Microsoft analizó una muestra de datos obtenidos a partir de incidentes que denunciaron los clientes, envíos de código malintencionado e informes de errores de Microsoft Windows®. Los datos abarcan diversos sistemas operativos y versiones de exploradores, desde Windows XP a Windows Vista®. Asimismo, incluye datos de exploradores de terceros que hospedan el motor de representación de Internet Explorer, denominado Trident.⁴

- La configuración regional más habitual de las víctimas de vulnerabilidades de exploradores fue la del inglés de EE.UU., que constituyó el 32,4% de los incidentes, seguida del chino (simplificado) con un 25,6% de los incidentes.
- El número de vulnerabilidades de Microsoft relacionadas con ataques a exploradores de equipos con Windows XP supuso un 40,9% del total, una disminución con respecto al 42,0% de 1M08. Sin embargo, en equipos con Windows Vista, la proporción de vulnerabilidades de Microsoft fue mucho menor; tan sólo un 5,5% del total, disminuyendo con respecto al 6,0% de 1M08.

⁴ Para obtener más información acerca de Trident, consulte <http://msdn.microsoft.com/en-us/library/aa939274.aspx>.

Ilustración 5. Vulnerabilidades de seguridad en exploradores de Microsoft y de terceros en equipos con Windows XP, 2M08

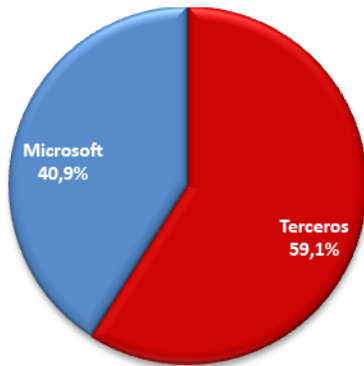
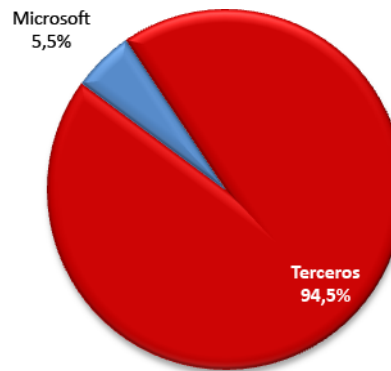


Ilustración 6. Vulnerabilidades de seguridad en exploradores de Microsoft y de terceros en equipos con Windows Vista, 2M08



- El software de Microsoft presentó 6 de las 10 principales vulnerabilidades de exploradores que afectaron a los equipos con Windows XP en 2M08, en comparación con las cero vulnerabilidades en equipos con Windows Vista, de forma similar al patrón observado en 1M08. Las siguientes ilustraciones muestran las 10 principales vulnerabilidades de exploradores que afectaron a equipos con Windows XP y Windows Vista. Se hace referencia a cada vulnerabilidad en función del número del boletín de CVSS o del boletín sobre seguridad de Microsoft, según corresponda.

Ilustración 7. Las 10 principales vulnerabilidades de exploradores en equipos con Windows XP, 2M08

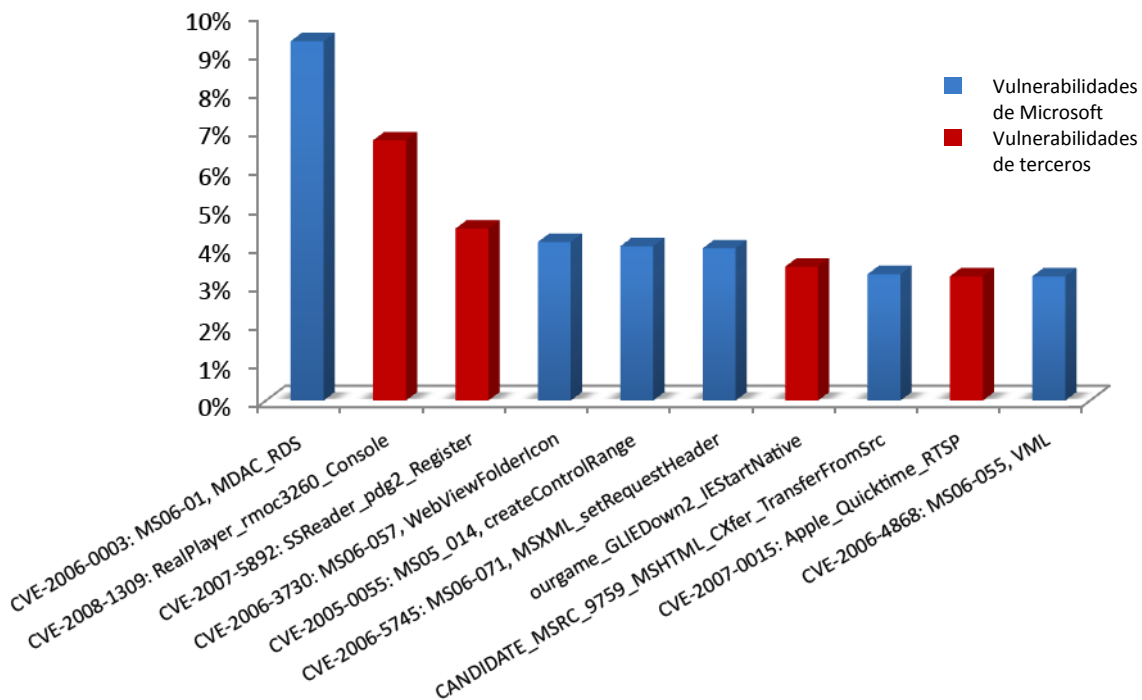
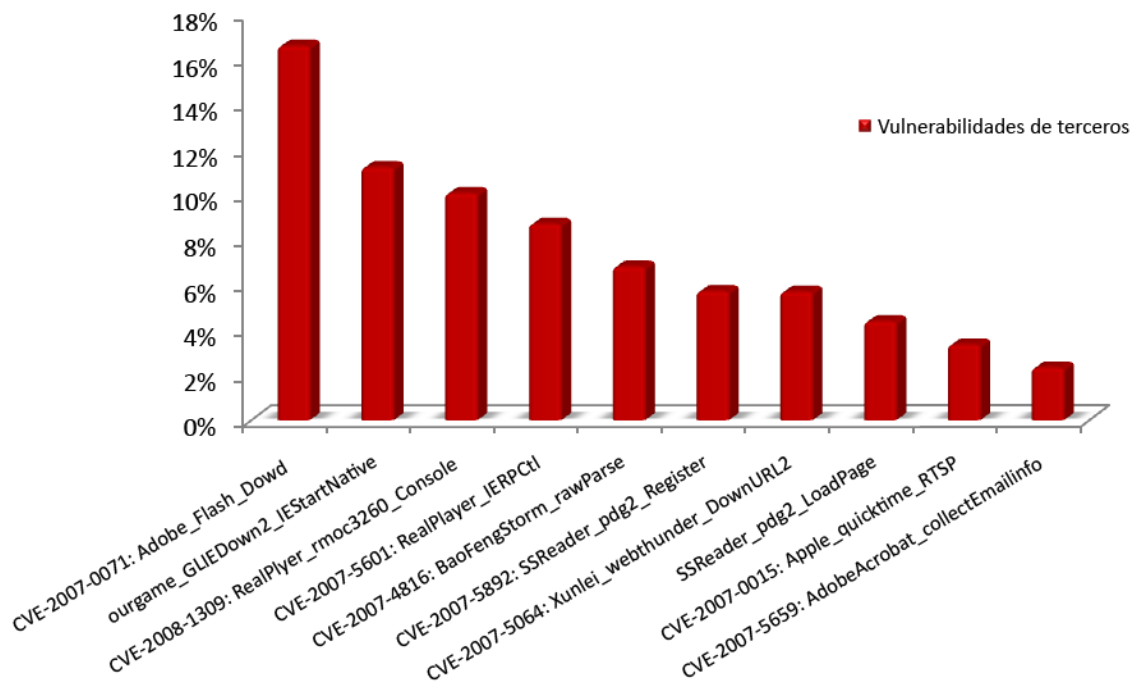


Ilustración 8. Las 10 principales vulnerabilidades de exploradores en equipos con Windows Vista, 2M08



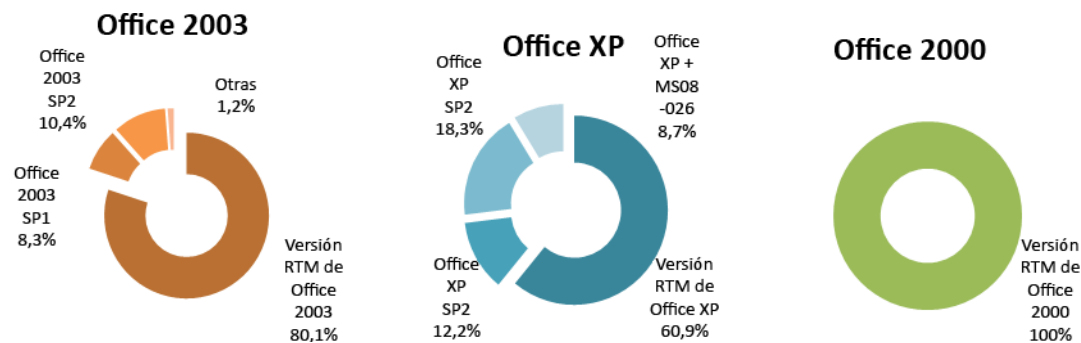
Vulnerabilidades de seguridad en los formatos de archivo de documentos

Los atacantes están usando cada vez con mayor frecuencia formatos de archivo comunes como instrumentos de transmisión de sus ataques. La mayoría de los programas actuales de correo electrónico y mensajería instantánea están configurados para bloquear la transmisión de archivos potencialmente peligrosos según su extensión. Sin embargo, estos programas permiten habitualmente la transmisión de los formatos de archivo habituales como Microsoft Office y Adobe Portable Document Format (.pdf). Estos formatos son usados diariamente de manera legítima por multitud de usuarios, por lo que no se han bloqueado. Sin embargo, esto los ha convertido en un objetivo atractivo para los atacantes de las vulnerabilidades de seguridad.

Archivos con formato de Microsoft Office

- Las vulnerabilidades atacadas con más frecuencia en el software de Microsoft Office son también algunas de las más antiguas. El 91,3% de los ataques examinados se sirvieron de una vulnerabilidad específica para la que existía una corrección de seguridad disponible desde hace más de 2 años (CVE-2006-2492).
- La configuración regional más habitual de las víctimas fue el inglés de EE.UU., que constituyó el 32,5% de los incidentes, seguida del chino (tradicional) con un 15,7% de los incidentes.
- En la mayoría de los casos, las versiones de las aplicaciones atacadas no disponían de los Service Packs actualizados. La gran mayoría de los ataques afectó a la versión de lanzamiento (RTM) de la aplicación, en la que no se había aplicado ningún Service Pack. En el caso de Office 2000, por ejemplo, el 100% de los ataques afectó a la versión RTM del conjunto de aplicaciones lanzado en 1999, a pesar de los numerosos Service Packs y otras actualizaciones de seguridad que se han publicado para el sistema a partir de 2000.

Ilustración 9. Ataques por nivel de actualizaciones de Office 2003, Office XP y Office 2000 en el conjunto de muestra de equipos infectados, 2M08

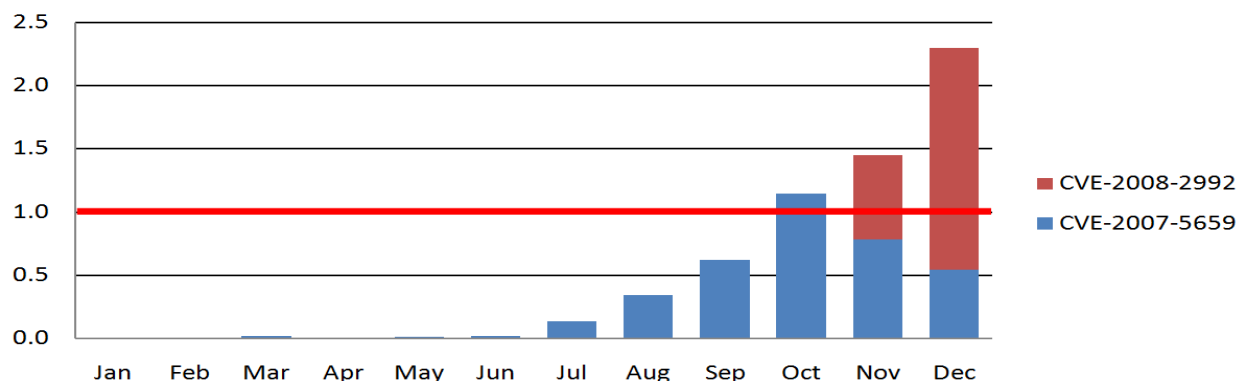


Archivos con formato Adobe PDF

El uso del formato PDF como vehículo para los ataques creció muy intensamente en 2M08, con un total de ataques en julio que suponía más del doble de todo 1M08 en conjunto, y siguió duplicándose o casi duplicándose durante el resto de meses del año.

- Hubo dos vulnerabilidades responsables de todos los ataques en los archivos de muestra examinados (CVE-2008-2992 y CVE-2007-5659). Ambas vulnerabilidades disponen de actualizaciones de seguridad de Adobe y ninguna de ellas existe en las versiones actuales de los productos afectados de Adobe.

Ilustración 10. Vulnerabilidades de seguridad de Adobe Reader por cada mes de 2008, según la media de 2M08



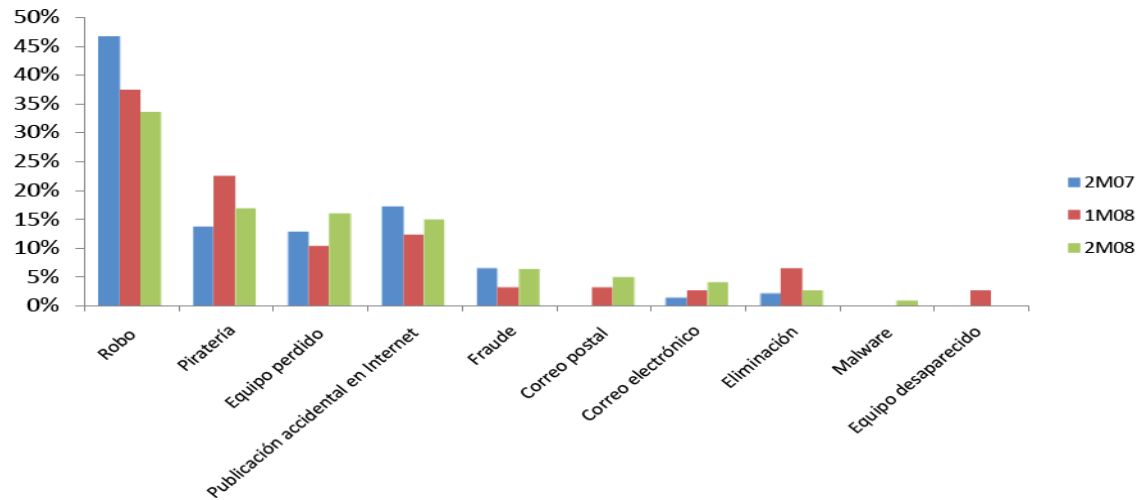
Tendencias de las infracciones de seguridad

En este apartado del informe se detallan los incidentes relacionados con infracciones de seguridad en todo el mundo, a partir de la información obtenida de la base de datos de Open Security Foundation relacionada con la pérdida de datos, disponible en <http://datalossdb.org>.

- La categoría principal de pérdida de datos a raíz de una infracción de seguridad durante 2M08 continuó siendo el robo de equipos, como por ejemplo portátiles (constituye el 33,5% de todos los incidentes registrados relacionados con la pérdida de datos). Junto con los equipos perdidos, estas dos categorías suponen el 50% de todos los incidentes registrados.
- Las infracciones de seguridad por incidentes de piratería o malware suponen menos de un 20% del total.
- Estos resultados refuerzan la necesidad de unas directivas y procedimientos apropiados para la administración de datos.⁵

⁵ Microsoft ofrece guías y recursos para la administración de datos en <http://www.microsoft.com/mscorp/twc/privacy/datagovernance/default.msp>

Ilustración 11. Incidentes relacionados con infracciones de seguridad, clasificados según el tipo y expresados como porcentajes del total, entre 2M07 y 2M08



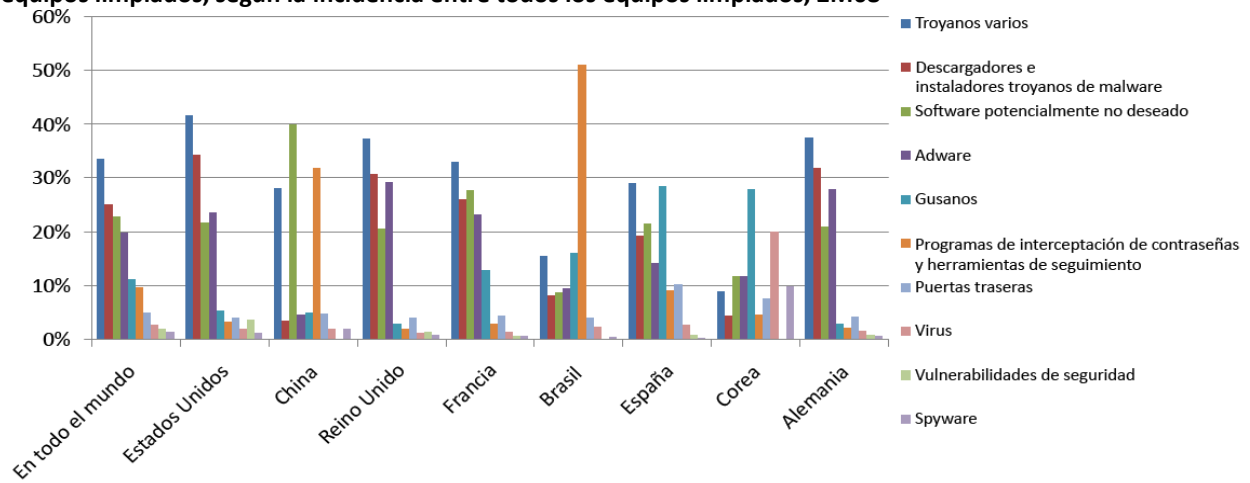
Software malintencionado y potencialmente no deseado

Tendencias globales

Los productos de seguridad de Microsoft recopilan, con el consentimiento del usuario, los datos de cientos de millones de sistemas informáticos en todo el mundo y de algunos de los servicios en línea con más tráfico de Internet. El análisis de estos datos da lugar a una perspectiva única y completa de la actividad del malware y del software potencialmente no deseado en todo el mundo.

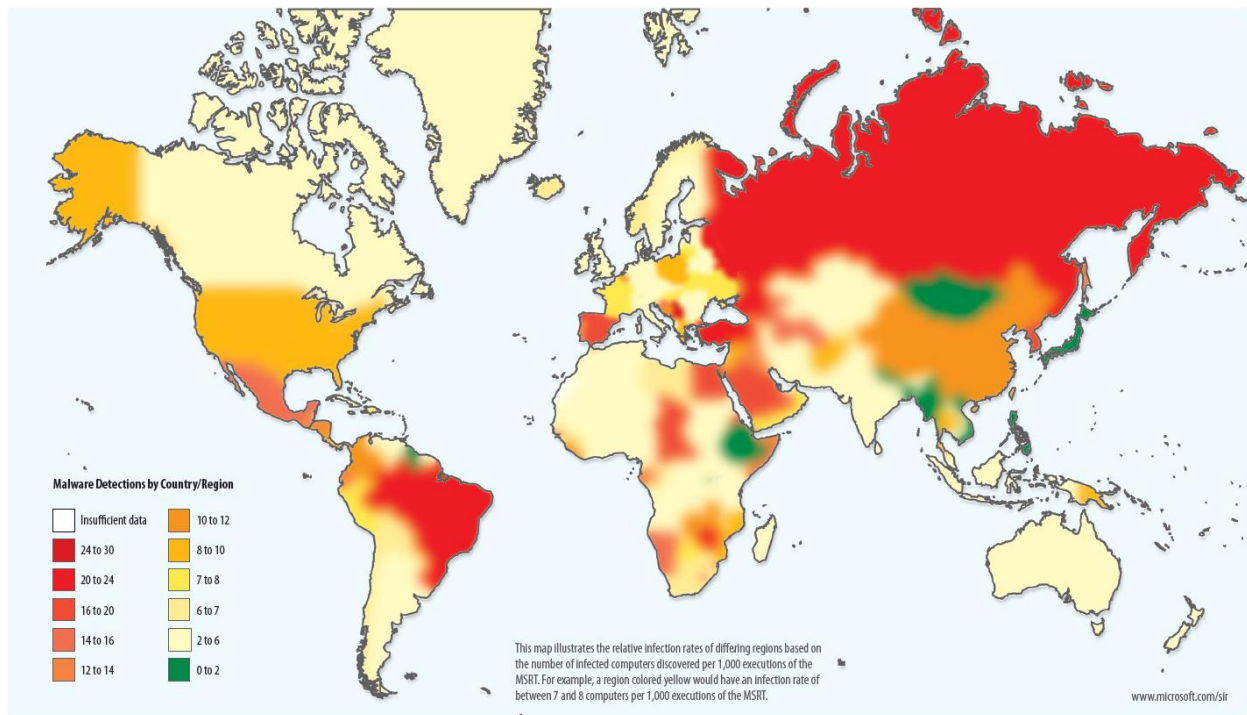
- A pesar de la naturaleza internacional de Internet, hay diferencias significativas en los tipos de amenazas que afectan a los usuarios en diferentes partes del mundo. Conforme el ecosistema del malware se vuelve más dependiente de la ingeniería social, las amenazas de todo el mundo se han vuelto más dependientes de los factores lingüísticos y culturales: así, en China, prevalecen varios modificadores maliciosos de los exploradores; en Brasil, está muy extendido el malware dirigido a los usuarios de la banca electrónica; y en Corea, son habituales los virus como Win32/Virut y Win32/Parite.

Ilustración 12. Categorías de amenazas en todo el mundo y en las ocho ubicaciones con el mayor número de equipos limpiados, según la incidencia entre todos los equipos limpiados, 2M08



- El siguiente mapa muestra las tasas de infección en diversas ubicaciones de todo el mundo, expresadas en CCM⁶.

Ilustración 13. Tasas de infección clasificadas por país/región, 2M08

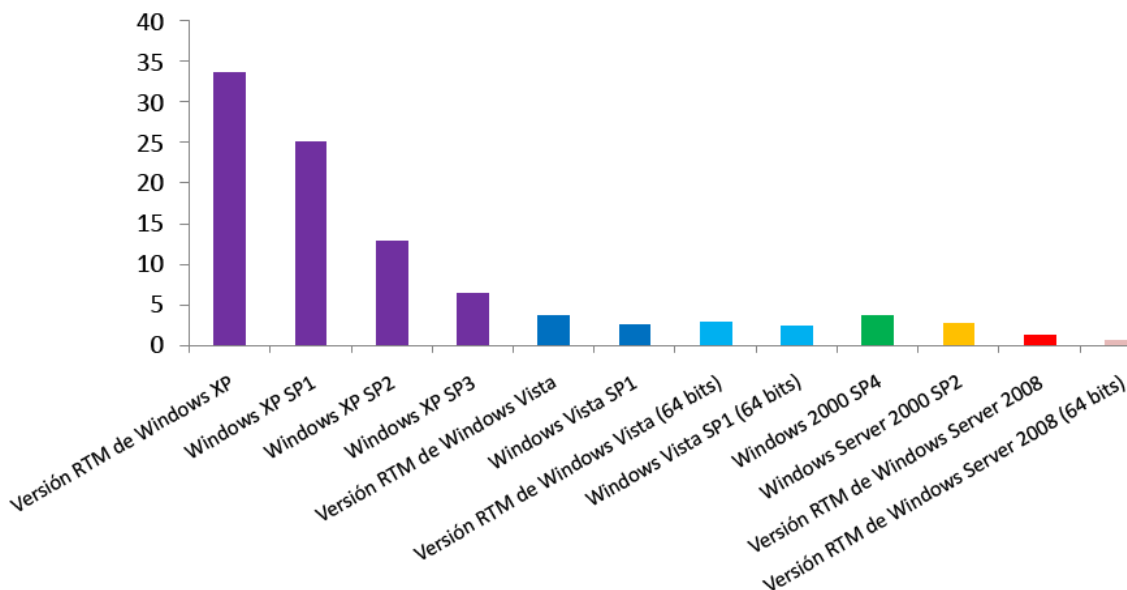


Tendencias de los sistemas operativos

- Las distintas versiones de los sistemas operativos de Microsoft Windows muestran diferentes tasas de infección debido a las diversas maneras en las que los usuarios y las organizaciones emplean cada versión, además de las distintas características y Service Packs disponibles para cada una.

⁶ Las tasas de infección en este informe se expresan a partir de un sistema métrico denominado Equipos limpiados por cada mil (CCM). Representa el número de equipos limpiados por cada mil ejecuciones de la herramienta MSRT.

Ilustración 14. Número de equipos limpiados por cada 1.000 ejecuciones de la MSRT, por sistema operativo, 2M08



- En todas sus configuraciones, la tasa de infección de Windows Vista es mucho menor que la de su predecesor, Windows XP.
 - Comparando los últimos Service Packs de cada versión, la tasa de infección de Windows Vista SP1 es un 60,6% inferior a la de Windows XP SP3.
 - Comparando las versiones RTM de estos sistemas operativos, la tasa de infección de la versión RTM de Windows Vista es un 89,1% inferior a la de la versión RTM de Windows XP.
- La tasa de infección de la RTM de Windows Server 2008 es un 52,6% menor que la de su predecesor, Windows Server 2003 SP2.
- Cuanto mayor es el nivel del Service Pack, menor es la tasa de infección. Esta tendencia se puede observar en todos los sistemas operativos cliente y de servidor. Esto se debe a dos razones:
 - Los Service Packs incluyen todas las actualizaciones de seguridad publicadas anteriormente. También pueden incluir características de seguridad adicionales, mitigación de riesgos o cambios en la configuración predeterminada para proteger a los usuarios.
 - Los usuarios que instalan los Service Packs generalmente mantienen sus equipos mejor que los usuarios que no los instalan; además, también pueden ser más precavidos al navegar por Internet, abrir archivos y realizar otras actividades que pueden exponer los equipos a los ataques.
- Las versiones de servidor de Windows normalmente muestran una tasa media de infección menor que las de las versiones cliente. Los servidores tienden a tener una superficie efectiva de ataque menor que la de los equipos con sistemas operativos cliente, ya que es más probable que se usen bajo condiciones controladas por administradores capacitados y estén protegidos por una o más capas de seguridad. En particular, Windows Server 2003 y sus sucesores están protegidos contra los ataques de diversas formas, lo que refleja esta diferencia de uso.

El panorama de amenazas domésticas y empresariales

- Los equipos con Forefront Client Security (que normalmente se encuentran en entornos corporativos) tienen muchas más probabilidades de encontrar gusanos que los equipos domésticos con Windows Live OneCare. Los equipos domésticos mostraron porcentajes mucho mayores de troyanos, descargadores troyanos, instaladores troyanos de malware, adware y vulnerabilidades de seguridad. En cambio, se detectaron porcentajes similares de puertas traseras y spyware en ambos productos.

Ilustración 15. Categorías de familias eliminadas por Windows Live OneCare y Forefront Client Security en 2M08, según el porcentaje del número total de equipos limpiados por cada programa

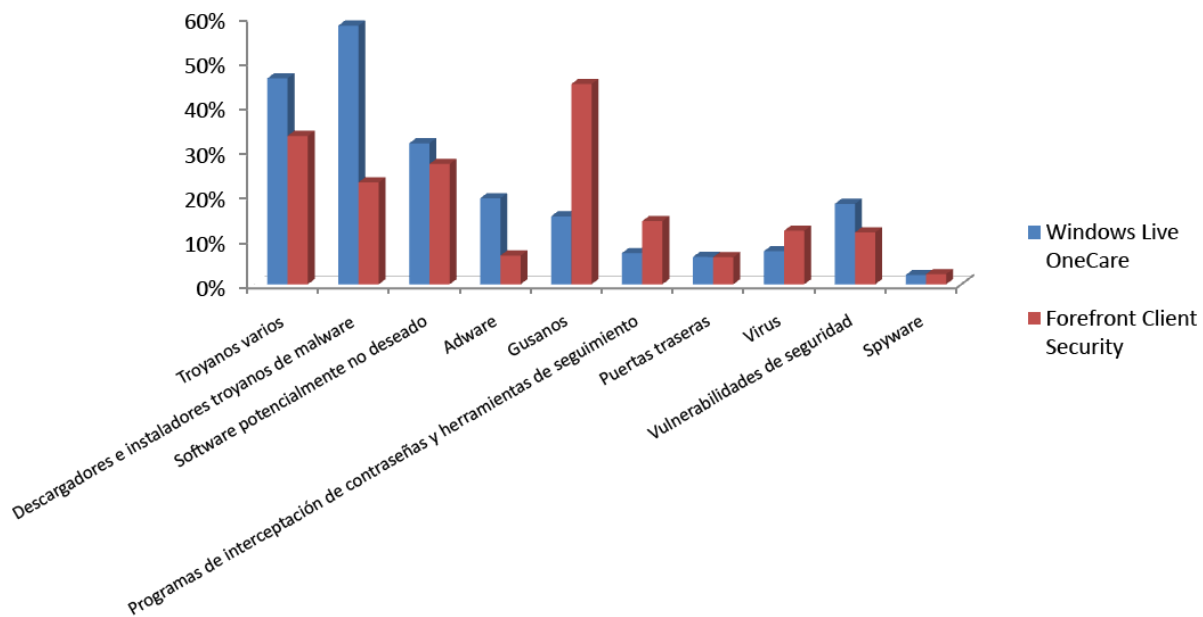
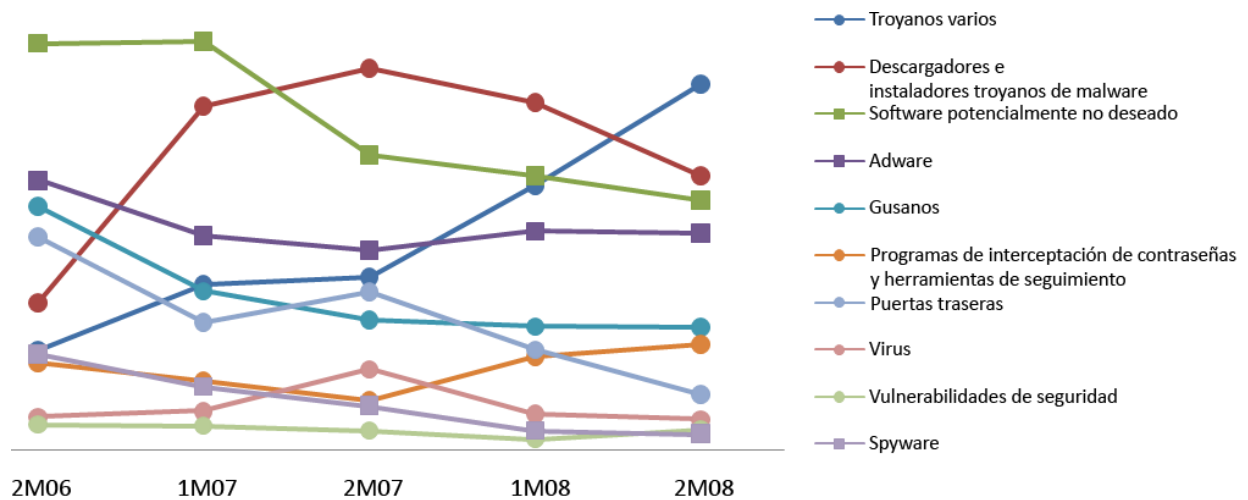


Ilustración 16. Porcentajes de equipos limpiados según la categoría de amenaza, de 2M06 a 2M08



Distribución geográfica de las páginas de malware

El hospedaje de malware tiende a ser más estable y menos disperso geográficamente que el hospedaje de la suplantación de identidad (phishing). Esto puede ser el resultado del uso relativamente reciente de la caída de servidores y la reputación web como armas en la lucha contra la distribución de malware. Esto significa que los distribuidores de malware no se han visto forzados a diversificar sus medidas de hospedaje. Las ilustraciones 17 y 18 muestran la distribución geográfica de los sitios de hospedaje de malware puestos en conocimiento de Microsoft en 2M08 en todo el mundo y dentro de los Estados Unidos.

Ilustración 17. Sitios de hospedaje de malware detectados por país/región en 2M08, según la media de todas las ubicaciones

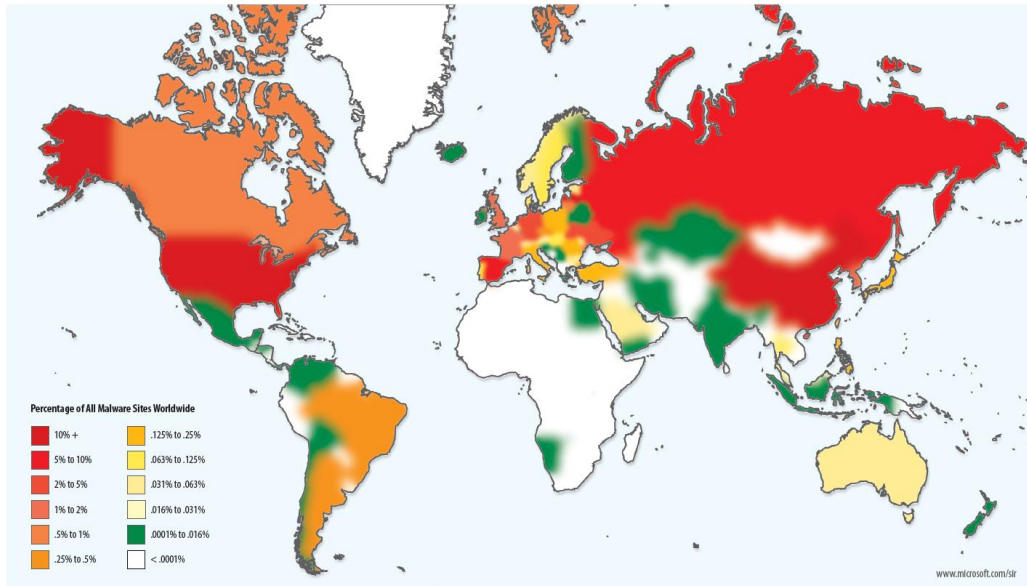
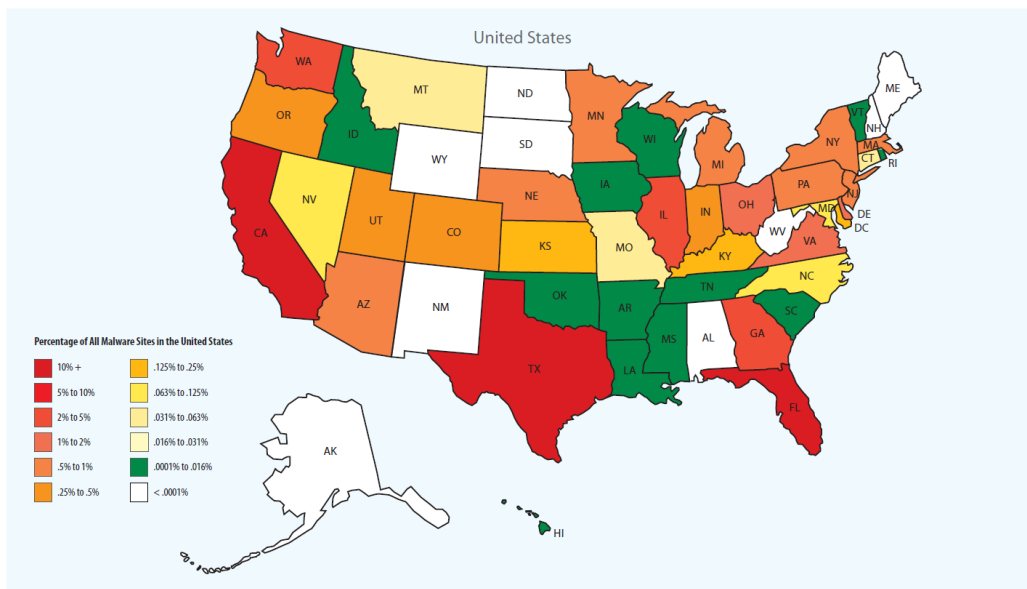


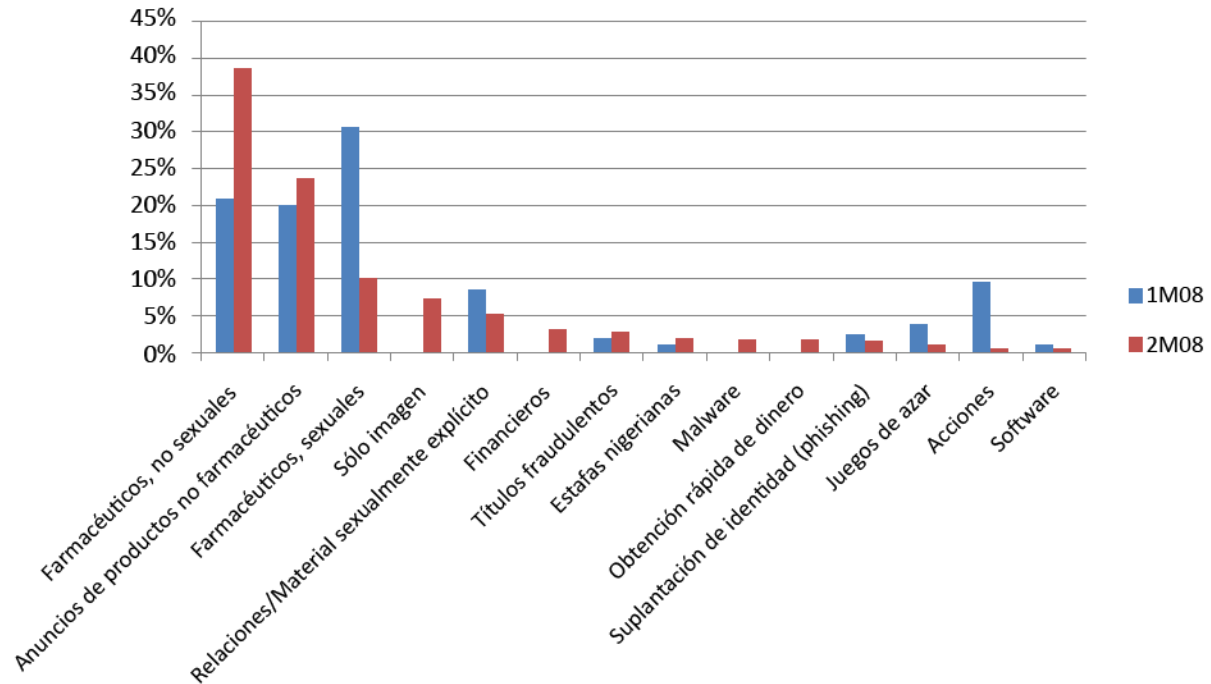
Ilustración 18. Sitios de hospedaje de malware detectados en Estados Unidos en 2M08, según la media de todas las ubicaciones



Amenazas por correo electrónico

- Más del 97% de los mensajes de correo electrónico enviados a través de Internet son correos no deseados, tienen archivos adjuntos malintencionados o son ataques de suplantación de identidad (phishing).
- Como en periodos anteriores, el correo no deseado de 2M08 estuvo dominado por los anuncios de productos, principalmente productos farmacéuticos (un 48,6% del total). Junto con los anuncios de productos no farmacéuticos (23,6% del total), la publicidad de productos supuso el 72,2% del correo no deseado en 2M08.

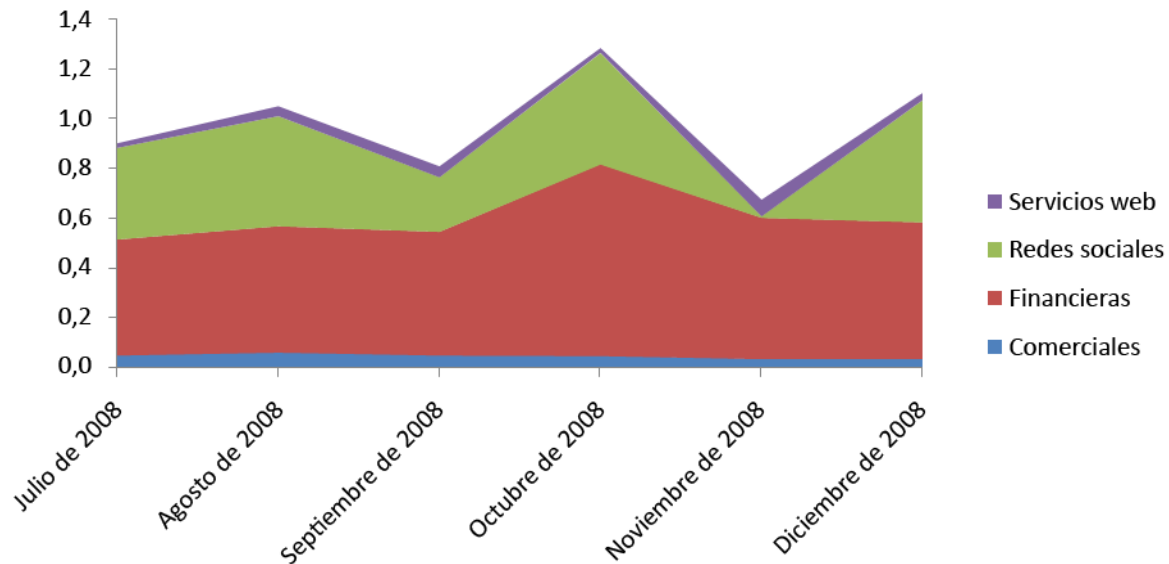
Ilustración 19. Mensajes entrantes bloqueados por los filtros de contenido de EHS, según categoría, de 1M08 a 2M08



Sitios web malintencionados

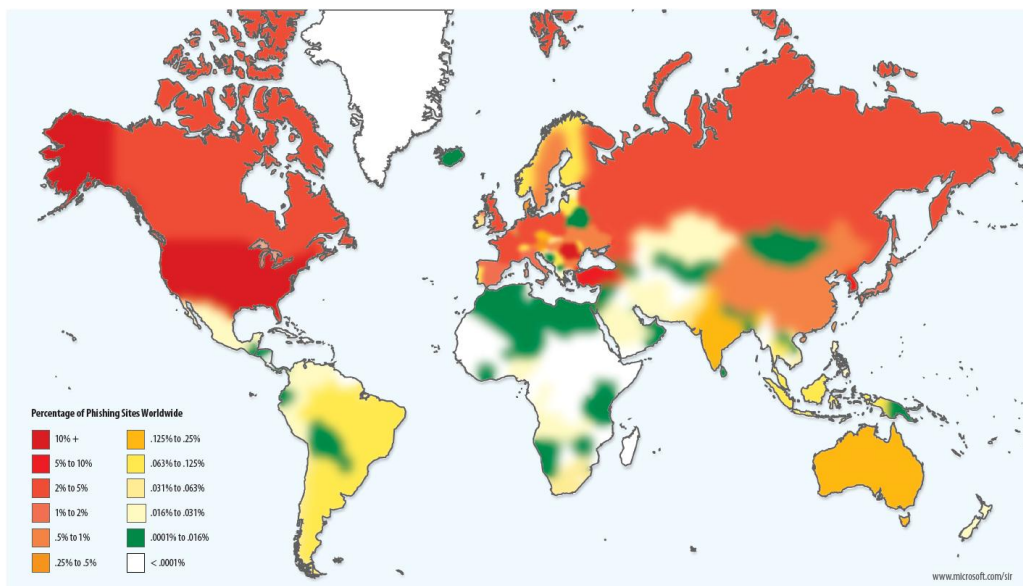
La mayoría de páginas de suplantación de identidad (phishing) tienen como objetivo organizaciones financieras, aunque en términos de impresiones (casos de usuarios que intentan visitar una página conocida de phishing), las redes sociales también son un objetivo frecuente.

Ilustración 20. Impresiones para cada tipo de página de suplantación de identidad (phishing) correspondientes a cada mes de 2M08, según la media de impresiones mensuales de dicho periodo.



- La interrupción de interconexiones de McColo a mediados de noviembre parece haber tenido un gran efecto en las impresiones de suplantación de identidad (phishing), que bajaron un 46,2% de octubre a noviembre. Las visitas a páginas de phishing dirigidas a sitios de redes sociales bajaron del 34,1% de todas las impresiones en octubre a sólo un 1,1% en noviembre.
- El país que hospedó el mayor número de páginas de suplantación de identidad (phishing) fue Estados Unidos con Texas como el estado con mayor cantidad de páginas.

Ilustración 21. Distribución mundial de las páginas de suplantación de identidad (phishing) en 2M08, según la media de todas las ubicaciones



Ayude a Microsoft a mejorar el informe de inteligencia sobre seguridad

Gracias por leer la última entrega del informe de inteligencia sobre seguridad de Microsoft. Esperamos que el informe sea lo más útil y relevante posible para nuestros clientes. Si tiene algún comentario acerca de esta entrega del informe o sugerencias acerca de cómo podemos mejorar las futuras entregas, háganoslas saber a través de la dirección de correo electrónico sirfb@microsoft.com.

Gracias y saludos,

Trustworthy Computing de Microsoft

La finalidad de este resumen es únicamente informativa. MICROSOFT NO OTORGA GARANTÍAS, NI EXPRESAS NI IMPLÍCITAS NI ESTATUTARIAS ACERCA DE LA INFORMACIÓN DE ESTE RESUMEN. Ninguna parte de este resumen puede ser reproducida, almacenada o introducida en un sistema de recuperación, ni transmitida de ninguna forma, ni por ningún medio (ya sea electrónico, mecánico, por fotocopia, grabación o de otra manera) con ningún propósito, sin la previa autorización por escrito de Microsoft Corporation.

Microsoft puede ser titular de patentes, solicitudes de patentes, marcas registradas, derechos de autor u otros derechos de propiedad intelectual sobre los contenidos de este resumen. La posesión de este resumen no le otorga ninguna licencia sobre estas patentes, marcas registradas, derechos de autor u otros derechos de propiedad intelectual, a menos que se prevea en un contrato de licencia por escrito de Microsoft.

Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

Microsoft, el logotipo de Microsoft, Windows, Windows XP, Windows Vista y Microsoft Office son marcas registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y/o en otros países. Otros nombres de productos y compañías reales mencionados aquí pueden ser marcas registradas de sus respectivos propietarios.