Juliaca, 09 ENE. 2023

OFICIO MÚLTIPLE No 006 - 2023-ME-DREP/DUGELSR-JAGP-D/EETIC.

SEÑORES(AS) : DIRECTORES(AS) DE LAS INSTITUCIONES EDUCATIVAS PÚBLICAS DE EBR, EBE Y EBA DEL ÁMBITO DE LA UGEL SAN ROMÁN.

PRESENTE.-

ASUNTO : REMITO INFORME TÉCNICO DE LOS RIESGOS DE NO UTILIZAR UN ANTIVIRUS EN COMPUTADORAS DE LAS II. EE.

REF. : **OFICIO MÚLTIPLE N° 00057-2022-MINEDU/SPE-OTIC**

Es muy grato dirigirme a usted, para saludarle cordialmente y comunicar que, en atención al documento citado en referencia y en el marco del desarrollo del Gobierno Digital y la seguridad digital en el sector educación, se remite el **informe técnico N°00183-2022-MINEDU/SPE-OTIC-UCSI** enviado por la Unidad de Calidad y Seguridad de la información del MINEDU, mediante el cual informa sobre **LOS RIESGOS DE NO UTILIZAR UN ANTIVIRUS EN COMPUTADORAS** de las Instituciones educativas y otros órganos del sector educación, así mismo, ***recomienda el uso del ANTIVIRUS***. En aquellos órganos que no cuenten con antivirus corporativo se adjunta el link donde se detalla los pasos para realizar la protección de las computadoras que tienen sistema operativo Windows 10:

1. https://support.microsoft.com/es-es/windows/activar-o-desactivar-el-firewall-demicrosoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f
2. https://www.formacionprofesional.info/guia-rapida-de-windows-defender/

Sin otro en particular, aprovecho la ocasión para expresar a usted, las consideraciones más distinguidas y estima personal.

Atentamente,

Lic. Luis Jarid Mamani Llanc
DIRECTOR

LJML/DUGEL
LSSC/JAGP
JCRQO/EESTIC-S
c.c arch.

PERÚ | Ministerio de Educación

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

UGEL SAN ROMAN
AREA DE GESTION PEDAGOGICA
RECEPCION
29 NOV 2022
Reg. N°:
Hora: Firma:

UGEL SAN ROMAN
DIRECCION
28 NOV 2022
RECIBIDO
Fol. Hora: Firma:

Lima, 28 de septiembre de 2022

OFICIO MÚLTIPLE N° 00057-2022-MINEDU/SPE-OTIC

Sr(a).
DIRECCIÓN REGIONAL DE EDUCACIÓN
GERENCIA REGIONAL DE EDUCACIÓN

Presente.-

Asunto: INFORME SOBRE LOS RIESGOS DE NO UTILIZAR UN ANTIVIRUS EN LAS COMPUTADORAS.

Referencia: INFORME TÉCNICO N° 00183-2022-MINEDU/SPE-OTIC-UCSI

De mi consideración:

Tengo el agrado de dirigirme a usted para saludarlos cordialmente y, a su vez, en el marco del desarrollo del Gobierno Digital y la Seguridad Digital en el sector educación, se remite el Informe Técnico N° 00183-2022-MINEDU/SPE-OTIC-UCSI, elaborado por la Unidad de Calidad y Seguridad de la Información, mediante el cual informa sobre los riesgos de no utilizar un antivirus en las computadoras de las instituciones educativas y otros órganos del sector educación.

Por lo antes expuesto, se recomienda el uso del antivirus en las computadoras de las instituciones educativas y otros órganos del sector educación; para aquellos órganos e instituciones educativas que no cuenten con antivirus corporativo, se adjunta el link, en el cual podrán encontrar los pasos para poder realizar la protección de las computadoras que tienen instalado el sistema operativo Windows 10 con el software antivirus Windows Defender, que viene como parte del propio sistema operativo Windows, que es gratuito:

1.-https://support.microsoft.com/es-es/windows/activar-o-desactivar-el-firewall-demicrosoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f
2.- https://www.formacionprofesional.info/guia-rapida-de-windows-defender/

En caso de tener alguna consulta respecto a la activación del antivirus, favor de remitir al correo electrónico soporteiiee@minedu.gob.pe.

Atentamente,

Ing. CESAR VILCHEZ INGA
Jefe de la Oficina de Tecnologías de la Información y Comunicación

(MDCRIOS)

UGEL SAN ROMAN EXP.
DIRECCIÓN

AL DIRECTOR:
A: SOPORTE TECNOLOGICO

PARA:

- [ ] PARA TRAMITACIÓN INMEDIATA:
- [x] PARA CONOCIMIENTO Y TOMAR ACCIÓN
- [ ] OPINAR Y RECOMENDAR:
- [ ] ATENDER DE ACUERDO A LO SOLICITADO:
- [ ] PARA COORDINACIÓN:
- [ ] POR CORRESPONDER:
- [ ] PROYECTO DE RESOLUCIÓN:
- [ ] AGREGAR A ANTECEDENTES:
- [ ] OTROS.....

JULIACA, 29 NOV 2022

DIRECCIÓN REGIONAL DE EDUCACIÓN PUNO - UNIDAD DE GESTIÓN EDUCATIVA LOCAL - DIRECCIÓN SAN ROMAN - PUNO

Lic. Luis Jurid Mamani Llano
DIRECTOR

UGEL SAN ROMAN
AREA DE GESTIÓN PEDAGÓGICA

Visto el documento que antecede: .....

- Especialista de TIC

Juliaca, 29-11-2022

DIRECCIÓN REGIONAL DE EDUCACIÓN PUNO - ÁREA DE GESTIÓN PEDAGÓGICA - UGEL SAN ROMAN - FIRMA Y SELLO

Dr. L. Severo Suctupuca Chinchapaza
JEFE DEL ÁREA DE GESTIÓN PEDAGÓGICA
UGEL - SAN ROMÁN

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

INFORME TÉCNICO N° 00183-2022-MINEDU/SPE-OTIC-UCSI

A : **CESAR VILCHEZ INGA**
JEFE-DIRECTOR - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

De : **LUIS GASTULO SALAZAR**
JEFE(e) DE LA UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN

IVAN ALIOSCAR GONZALES TINTAYA
ESPECIALISTA DE SEGURIDAD DE LA INFORMACIÓN

Asunto : INFORME SOBRE LOS RIESGOS DE NO UTILIZAR UN ANTIVIRUS EN LAS COMPUTADORAS

Referencia : Microsoft Security Intelligence Report Volume 14 Key Findings Summary Spanish

Fecha : Lima, 28 de septiembre de 2022

Tengo el agrado de dirigirme a usted, en atención al asunto del rubro y los documentos de la referencia, para informarle lo siguiente:

I. ANTECEDENTES

1.1 Microsoft ha publicado una nueva edición de su informarme "Microsoft Security Intelligence Report (SIRv14)", el cual contiene un análisis de las amenazas más extendidas en el mundo y el estudio del uso del antivirus, en la que evidencia que, de cada 10 computadoras, 2,5 no han utilizado nunca un antivirus. Resaltando que, sin esta protección imprescindible, el riesgo de que una computadora sea infectada con malware es de 5,5 veces superior.

II. ANÁLISIS

2.1 Microsoft en su reporte muestra estadísticas de las amenazas más frecuentes que pueden llegar a sufrir las computadoras, las cuales se presentarán a continuación.

- **Amenaza de manipulación**

www.gob.pe/minedu
Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511) 615 58000

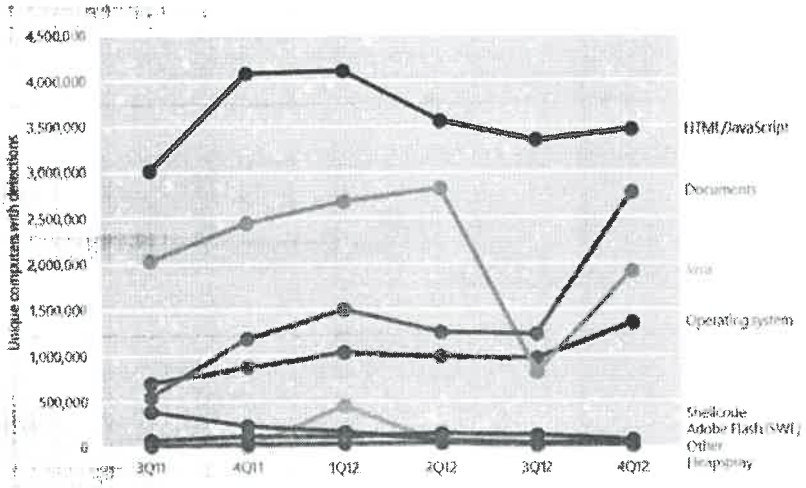


Ilustración 1 Equipos únicos que informan de distintos tipos de manipulaciones

La tendencia indica que las amenazas más frecuentes son los vectores de ataque que provienen de aplicaciones web en formatos HTML/JavaScript, carga de archivos como documentos infectados, programas java y programas ejecutables.

- **Malware y software potencia mente no deseados y sistemas operativos más atacados.**

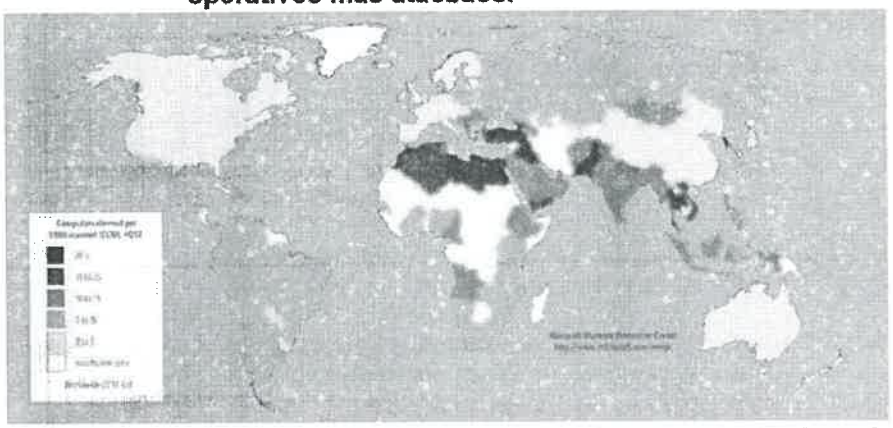


Ilustración 2 Tasas de infección por país/región el en tasa de medición CCM (equipos limpiados por millares)

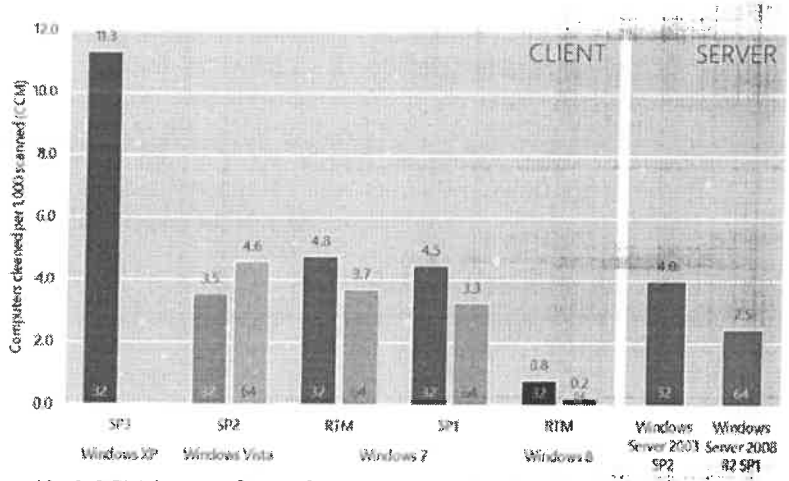


Ilustración 3 CCM (equipos limpiados por millares) por sistema operativo y Service Pack

En la imagen número 3, se muestra la cantidad de desinfecciones que se realiza gracias a la utilización de antivirus en sus computadoras, también se observa que, los sistemas operativos más atacados son: Windows XP de 32 bits, Windows Vista de 32 y 64 bits, Windows 7 32 y 64 bits, Windows 8 de 32 y 64 bit; asimismo, los Windows server 2003 y 2008 en sus plataformas de 32 y 64 bits.

- **Amenaza de correo electrónico**

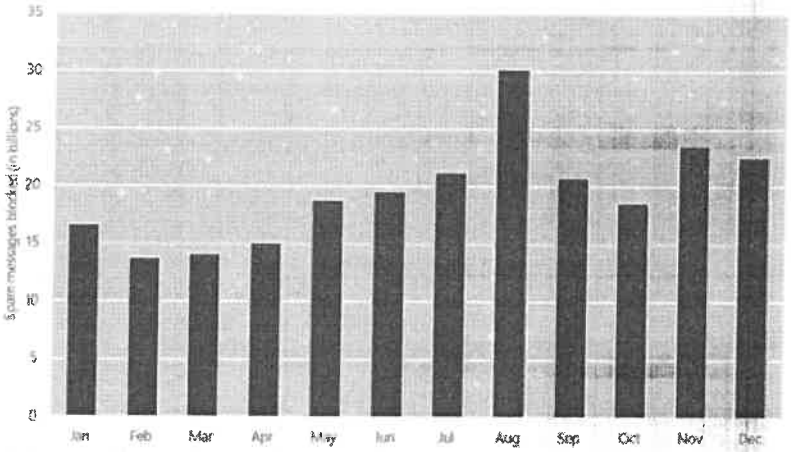


Ilustración 4 Mensajes bloqueados por el servicio de protección en línea de Exchange cada mes de 2012.

Una de las formas más utilizadas y con mayor llegada al público es la utilización del correo electrónico para infectar, engañar y suplantar identidades de los usuarios. La imagen número 4 nos muestra la importancia de un control como el antivirus, el cual muestra una gran reducción del riesgo ante ataques de spam y contenido malicioso.

2.2 Microsoft afirma que, el uso de un antivirus instalado en los computadores es fundamental; ya que elimina infecciones, protege contra virus y salvaguarda la privacidad de la persona.

2.3 Gracias a estas estadísticas podemos llegar a informar respecto a la importancia de la instalación de un antivirus de pago y/o el "por defecto" de Microsoft como es el Windows defender; el cual debe encontrarse habilitado y activo con una licencia oficial de la marca para su sistema operativo base. Como se puede apreciar, en el cuadro siguiente, el antivirus por defecto de Microsoft se encuentra dentro de los líderes del segmento, según el "Cuadrante Mágico de Gartner EPP 2021".

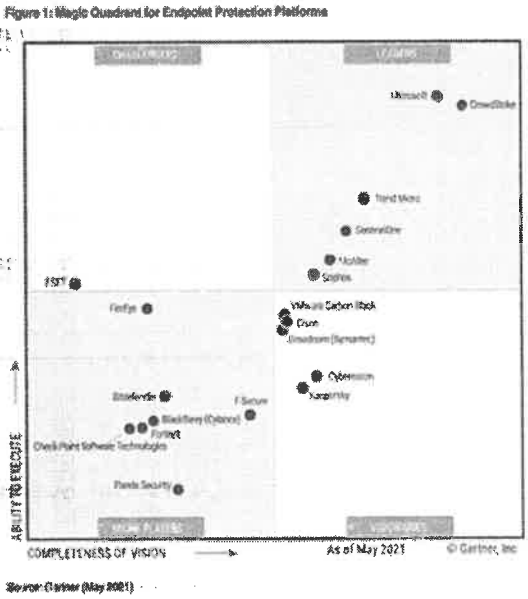


Ilustración 5 Cuadrante Mágico de Gartner EPP 2021

2.1 En la URL https://www.formacionprofesional.info/guia-rapida-de-windows-defender/ , https://support.microsoft.com/es-es/windows/activar-o-desactivar-el-firewall-de-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f#ID0EFD=Windows_10 , podemos encontrar los pasos para poder realizar la protección de Windows 10 con Windows defender, adicionalmente se adjunta un enlace de YouTube donde se visualiza un ejemplo práctico https://www.youtube.com/watch?v=YmqQddE1wh4.

III. CONCLUSIONES

3.1 Por medio del presente informe se comunica de la importancia de la utilización de los antivirus en las computadoras de los usuarios, y para ello se agrega unos enlaces y una guía para la configuración del antivirus por defecto de Windows el cual lleva como nombre "Windows Defender".

IV. RECOMENDACIONES

4.1 Se recomienda trasladar el presente informe a las UGELEs para que puedan realizar la configuración del antivirus Windows defender.

Es todo cuanto debo informar.

Atentamente,

IVAN A. GONZALES TINTAYA
ESPECIALISTA DE SEGURIDAD DE LA INFORMACIÓN
UCSI – OTIC – MINISTERIO DE EDUCACIÓN

Con la conformidad del funcionario que suscribe remítase el presente Informe y sus antecedentes a la Oficina de Tecnologías de Información y Comunicación, para su atención.
Correspondiente.

LUIS GASTULO SALAZAR
JEFE(e) DE LA UNIDAD DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN
UCSI – OTIC – MINISTERIO DE EDUCACIÓN

Guía rápida de Windows Defender:

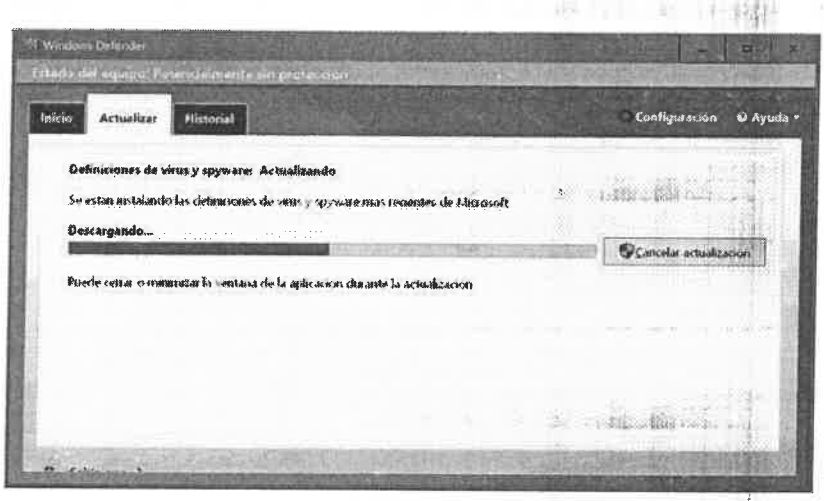
Protección de Windows 10 con Windows Defender

Windows Defender es una utilidad gratuita que Windows 10 incluye de serie y que nos ofrece los siguientes servicios de protección ante todo tipo de malware; virus, troyanos, spyware, ransomware, entre otros malwares.

- Protección en tiempo real. Siempre alerta, nos avisa de cualquier cambio sospechoso en los archivos de nuestro sistema o sin autorización. Puede activarse de forma temporal o definitiva.
- Análisis del sistema. Podemos lanzar un análisis rápido que escanea sólo determinados archivos, servicios y procesos cargados en memoria o el análisis completo mucho más lento pero que consigue escanear todo nuestro sistema en busca de malware.
- Si se detectan ficheros infectados los envía a cuarentena (un espacio seguro que impide la ejecución de programas malintencionados). El tercer tipo de análisis es el personalizado.
- En Configuración podemos agregar exclusiones de archivos y carpetas. También podemos filtrar por tipo de archivos o por procesos.
- Las definiciones son catálogos de virus detectados al momento y que permite su localización, en ocasiones por comparación con

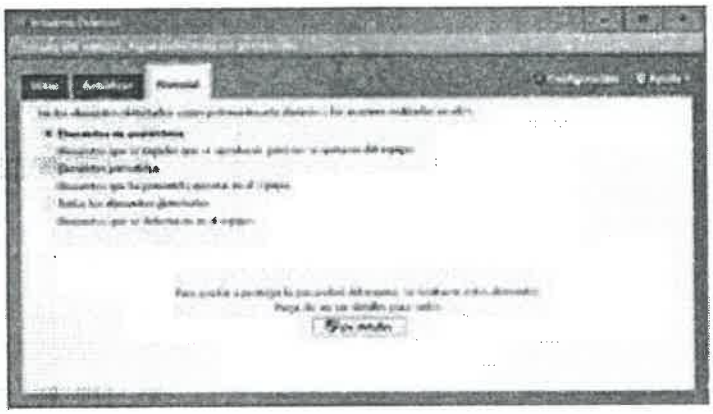
fragmentos de código. Se recomienda activar la actualización automática de las definiciones.

- Para actualizar los catálogos manualmente solo tenemos que pulsar el botón Actualizar definiciones en la ficha de Actualizar.
- Podemos consultar en la información de configuración de Windows Defender la Versión del cliente antimalware, la versión del motor, la fecha de definición de antivirus y antispyware. También dispone de un sistema de Inspección de red.
- Windows Defender también permite el análisis de unidades externas de almacenamiento o discos duros de red.
- Puede avisar a todos los usuarios de un sistema de una posible amenaza.



- En Windows 10 es posible activar la Protección basada en la nube. Un sistema que reporta información de problemas encontrados a Microsoft de manera anónima y que ayuda a la mejora de este servicio.
- También se incluye la posibilidad de enviar muestras de los archivos infectados en Ayuda / Enviar muestra de software malintencionado.
- Permite la Exclusión de archivos especificados por los usuarios.
- Permite el escaneo manual si tener activado el servicio de protección continua.

- La ficha Historial, ofrece información sobre los Elementos en cuarentena, los Elementos permitidos y Todos los elementos detectados en el equipo analizador.



Configuración de Windows Defender

Si vamos a inicio y tecleamos Configuración Defender podremos abrir la pantalla de Actualización y seguridad que permite activar o desactivar servicios de protección antivirus.

Si desactivas todos los servicios de Windows Defender y no utilizas otras medidas de seguridad te arriesgas a exponer a tu equipo a una infección por virus o troyanos.

No obstante, no se recomienda utilizar más de un antivirus pues el sistema puede quedar inestable por los errores provocados entre ambas aplicaciones. Ya que, como método de detección, ciertos antivirus guardan fragmentos de código de virus en sus bases de datos lo que puede ser interpretado como una amenaza por otro antivirus que escanee dichos archivos.

Defender, dispone de una opción de análisis offline para intentar eliminar algunos virus resistentes a ser eliminados. Para ello, simplemente selecciona dicha opción, será necesario que el sistema reinicie, ejecute dicho análisis y una vez terminado, vuelva a reiniciar en modo normal.

Descargas:

Windows Defender viene incluido por defecto en tu sistema operativo Windows, pero si lo has borrado o deseas actualizarlo tienes la descarga directa en el siguiente enlace windows.microsoft.com. (http://windows.microsoft.com/es-es/windows/what-is-windows-defender-offline)

Enlace Original:
https://www.formacionprofesional.info/guia-rapida-de-windows-defender/

Micro

Una perspectiva en detalle acerca de las vulnerabilidades y manipulaciones de software, malware, software potencialmente no deseado y sitios web malintencionados

Microsoft Security Intelligence Report

Volumen 14

De julio a diciembre de 2012

RESUMEN DE CONCLUSIONES PRINCIPALES

Resumen de conclusiones principales de Microsoft Security Intelligence Report

Microsoft Security Intelligence Report, volumen 14

El volumen 14 del *Microsoft® Security Intelligence Report* (*SIRv14*) presenta en detalle perspectivas acerca de las vulnerabilidades de software en programas de software de Microsoft y de terceros, manipulaciones, amenazas de código malicioso y software potencialmente no deseado. Microsoft ha elaborado estas perspectivas basándose en detallados análisis de tendencias realizados en los últimos años, haciendo hincapié en el segundo semestre de 2012.

Este documento resume las principales conclusiones del informe. El *SIRv14* incluye un completo artículo donde se demuestra que ejecutar software de seguridad de un proveedor de reconocido prestigio en tiempo real y mantenerlo actualizado es uno de los pasos más importantes para reducir la exposición al malware.

El sitio web del *SIR* 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.

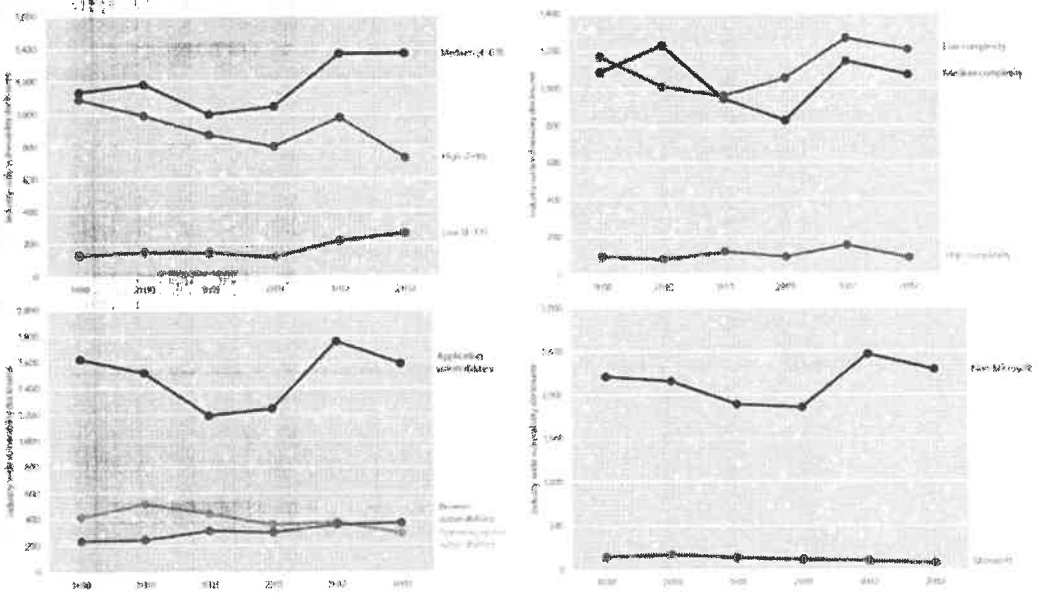
Puede descargar el informe *SIRv14* desde www.microsoft.com/sir.

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 tipo y por productos de Microsoft y de otros fabricantes, en todo el sector del software, 1S10-2S12[1]



- Las denuncias de vulnerabilidad del sector descendieron un 7.8% desde el 1S12, principalmente por la reducción de las denuncias de vulnerabilidad de las aplicaciones. A pesar de este descenso, las denuncias de vulnerabilidad crecieron un 20% en el 2S12 con respecto al 2S11, un año antes.

[1] En el documento, se hace referencia a períodos semestrales y trimestrales mediante los formatos *nSaa* o *nTaa*, donde *aa* indica el año natural y *n* indica el semestre o trimestre. Por ejemplo, 2S12 denota el segundo semestre del año 2012 (del 1 de julio hasta el 31 de diciembre), en tanto que 4T12 representa el cuarto trimestre de 2012 (desde el 1 de octubre hasta el 31 de diciembre).

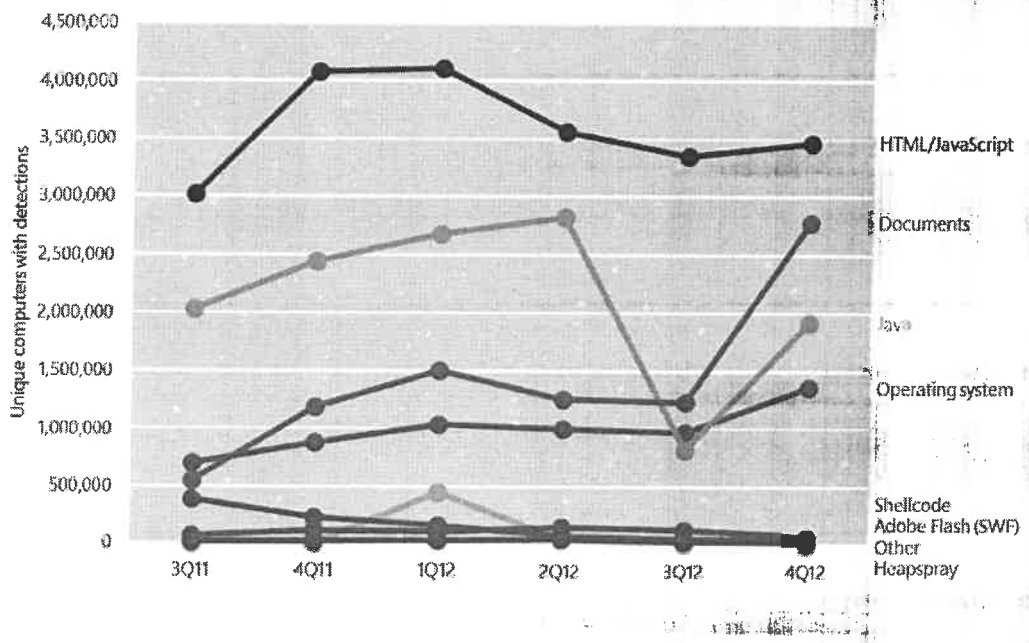
- La reducción general de las denuncias de vulnerabilidad del sector estuvo causada de forma íntegra por una reducción de las vulnerabilidades de alta gravedad, que disminuyeron un 25,1% desde el 1S12. Las vulnerabilidades de alta gravedad representaron el 30,9% de las denuncias totales del 2S12, frente al 38% del período anterior.
- El aumento de las denuncias de vulnerabilidad de las aplicaciones en el 1S12 interrumpió una tendencia de reducciones sistemáticas entre períodos desde el 2S09.

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 *SIRv14* 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 3T11 al 4T12, por número de equipos únicos afectados.

Figura 2. Equipos únicos que informan de distintos tipos de manipulaciones, 3T11-4T12



- El número de equipos que informaron de manipulaciones ejecutadas a través de HTML o de JavaScript se mantuvo alto durante el segundo semestre de 2012, impulsado principalmente por la prevalencia continuada de la familia de manipulaciones multiplataforma Blacole.
- Las manipulaciones dirigidas a vulnerabilidades de lectores y editores de texto se incrementaron súbitamente durante el 4T12, debido al incremento en las detecciones de Win32/Pdfjsc.
- Las detecciones de manipulaciones de Java durante el 3T12 quedaron reducidas a menos de la tercera parte de su total en el 2T12, si bien durante el 4T12 llegaron a constituir la mitad de la diferencia para convertirse en el tercer tipo de manipulación más habitual durante la segunda mitad del año.

Familias de manipulaciones

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

Figura 3. Tendencias trimestrales de las familias de manipulaciones más importantes detectadas por los productos antimalware de Microsoft en el 2S12, por número de equipos únicos con detecciones, sombreadas según la prevalencia relativa

Manipulación	Plataforma o tecnología	1T12	2T12	3T12	4T12
Win32/Pdfjsc*	Documentos	1.430.448	1.217.348	1.187.265	2.757.703
Blacole	HTML/JavaScript	3.154.826	2.793.451	2.464.172	2.381.275
CVE-2012-1723*	Java	—	—	110.529	1.430.501
IFrame malintencionado	HTML/JavaScript	950.347	812.470	567.014	1.017.351
CVE-2010-2568 (MS10-046)	Sistema operativo	726.797	783.013	791.520	1.001.053
CVE-2012-0507*	Java	205.613	1.494.074	270.894	220.780
CVE-2011-3402 (MS11-087)	Sistema operativo	42	24	66	199.648
CVE-2011-3544*	Java	1.358.266	803.053	149.487	116.441
Código shell*	Código shell	105.479	145.352	120.862	73.615
JS/Phoex	Java	274.811	232.773	201.423	25.546

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

- Las detecciones de Win32/Pdfjsc, una detección de archivos PDF especialmente diseñados que manipulan vulnerabilidades en Adobe Reader y Adobe Acrobat, aumentaron más del doble desde el 3T12 al 4T12. Esta fue la manipulación más detectada durante el último trimestre del año y la segunda más habitual durante el semestre en general.
- Blacole es el nombre que Microsoft asigna a la detección de componentes del llamado kit "Blackhole", que carga software malicioso a través de páginas web infectadas. Blacole fue la familia de manipulaciones más detectada en el segundo 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 carga 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 1.000 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 4T12, por CCM

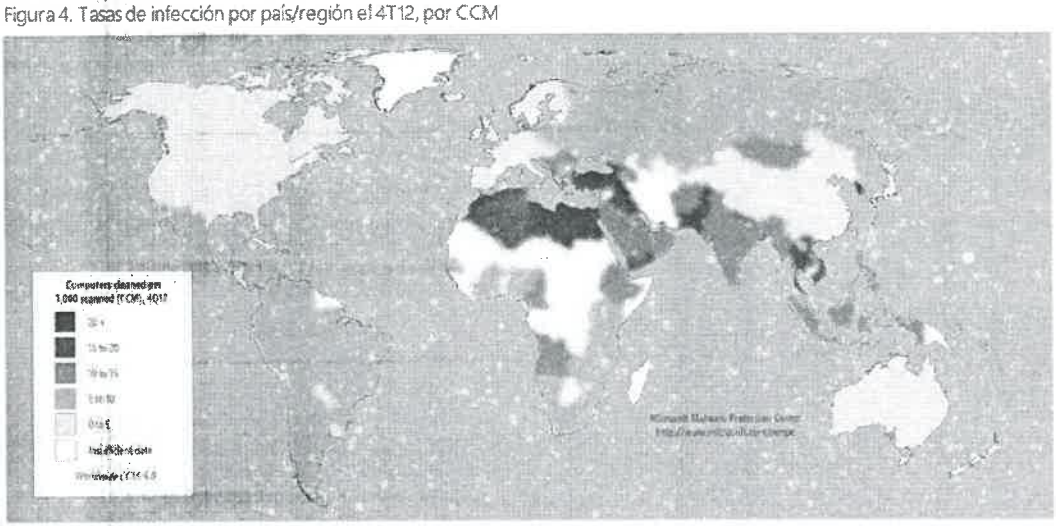
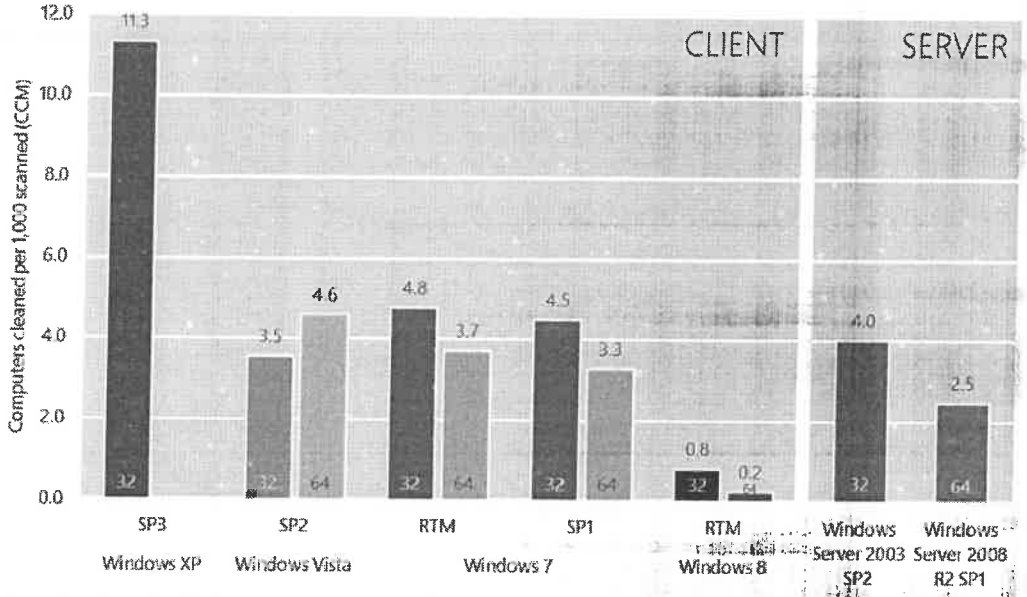


Figura 5. Tasas de infección (CCM) por sistema operativo y Service Pack el 4T12

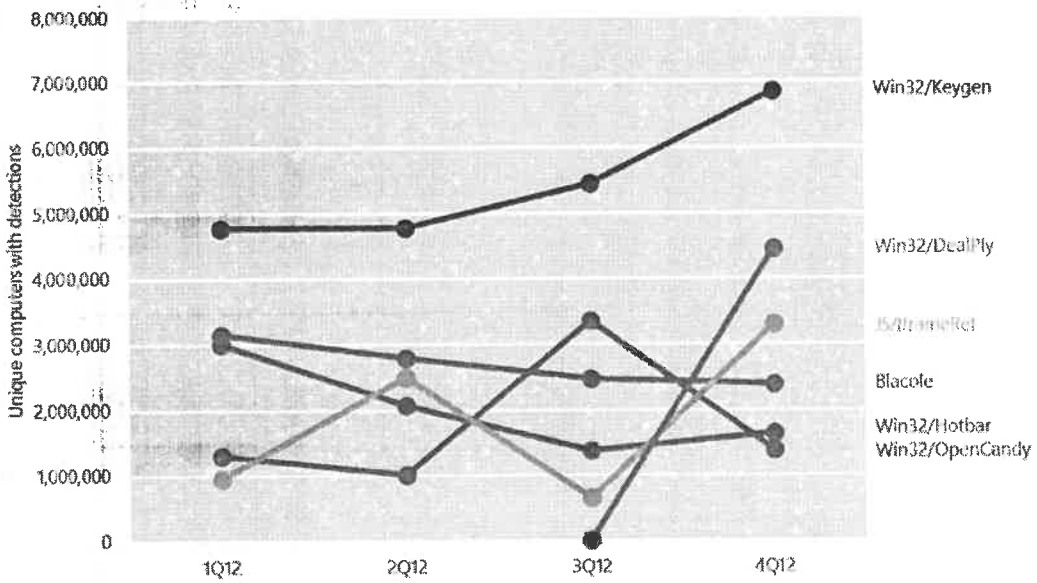


"32" = edición de 32 bits; "64" = edición de 64 bits. SP = Service Pack. RTM = enviado a producción. Se indican los sistemas operativos con al menos un 0,1% de ejecuciones totales de la MSRT en el 4T12.

Estos datos han sido normalizados; es decir, la tasa de infecciones por cada versión de Windows se calcula comparando un número equivalente de equipos por versión (por ejemplo, 1.000 equipos con sistema operativo Windows XP SP3 con 1.000 equipos con Windows 8 RTM).

Familias de amenazas

Figura 6. Tendencias de detección de determinada cantidad de familias destacadas en 2012



- Las detecciones de Win32/Keygen, la detección general más común en el 2S12, aumentaron en cada trimestre: de 4,8 millones de equipos en el 2T12 a 6,8 millones en el 4T12. Keygen es una detección de herramientas que generan claves para diversos productos de software, las cuales pueden permitir a los usuarios ejecutar los productos de forma ilícita.
- La detección de adware Win32/DealPly, que apareció por primera vez durante el 4T12, se convirtió rápidamente en la segunda más común del trimestre. DealPly es un programa de adware que muestra ofertas relacionadas con los hábitos de exploración web del usuario. Se ha observado que se incluye con determinados programas de instalación de software de otros fabricantes, como Win32/Protlerdob.
- Las detecciones de la familia de genéricos JS/IframeRef se multiplicaron por cinco en el 4T12 tras haber descendido de forma significativa entre el 2T12 y el 3T12. IframeRef es una detección genérica de etiquetas de marco flotante (IFrame) HTML con formato especial que redirigen a sitios web remotos con contenido malintencionado. El incremento de las detecciones de IframeRef durante el 2T12 y el 4T12 fue resultado del descubrimiento de un par de nuevas variantes ampliamente usadas en abril y noviembre de 2012. (En enero de 2013, estas variantes se reclasificaron como Trojan:JS/Seedabutor.A y Trojan:JS/Seedabutor.B, respectivamente).

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.

- Seis familias son comunes en ambas listas, notablemente las familias de genéricos Win32/Keygen e INF/Autorun, y la familia de manipulaciones Blacole. Keygen, la familia más detectada en equipos no unidos a un dominio en el 2S12, se detectó aproximadamente en el doble de equipos no unidos a un dominio que en los que sí lo estaban, si bien su prevalencia en los últimos fue suficiente para ocupar el tercer puesto en la lista para equipos unidos a un dominio en ambos trimestres.
- Las detecciones en la categoría Gusanos se mantuvieron altas en el caso de los equipos unidos a un dominio, encabezadas por Win32/Conficker y si bien se redujeron ligeramente durante el transcurso del año, se mantuvieron como la segunda familia más detectada en equipos unidos a un dominio. Vea "Cómo sigue propagándose Conficker" en Microsoft Security Intelligence Report, volumen 12 (julio-diciembre 2011) para obtener más información.
- Las detecciones de adware suelen ser más habituales en equipos no unidos a un dominio que en los que sí lo están. La familia de adware Win32/DealPly fue la segunda familia de amenazas más detectada en equipos no unidos a un dominio en el 4T, con otra familia de adware, Win32/Hotbar, en el décimo puesto. Sin embargo, ninguna de las 10 familias principales detectadas en equipos unidos a un dominio eran familias de adware.

Figura 7. Tendencias trimestrales de las 10 familias principales detectadas en equipos unidos a un dominio en el 2S12, por porcentaje de equipos unidos a un dominio que informan de detecciones

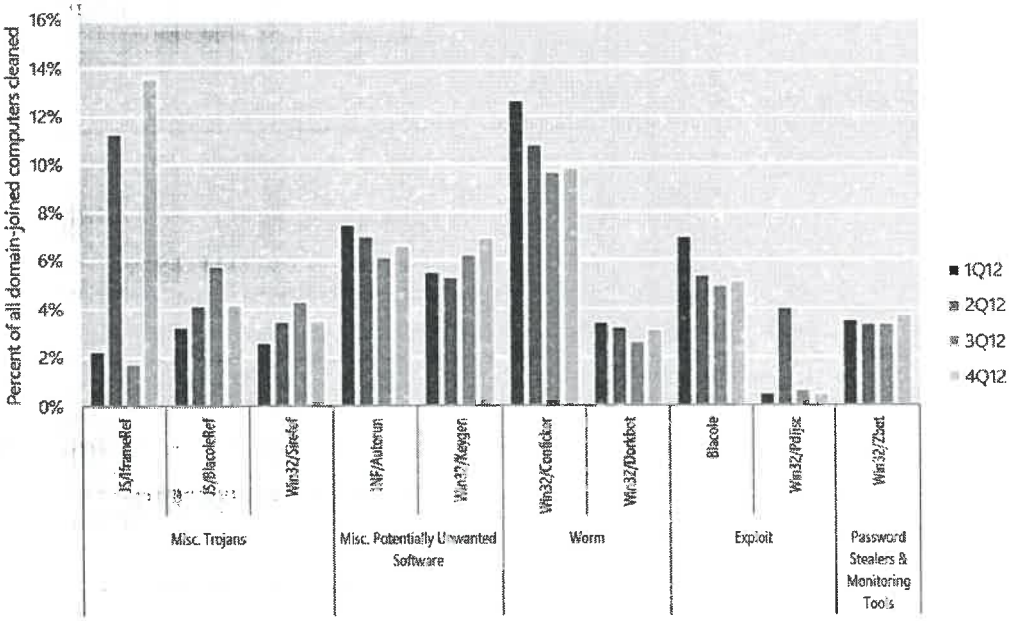
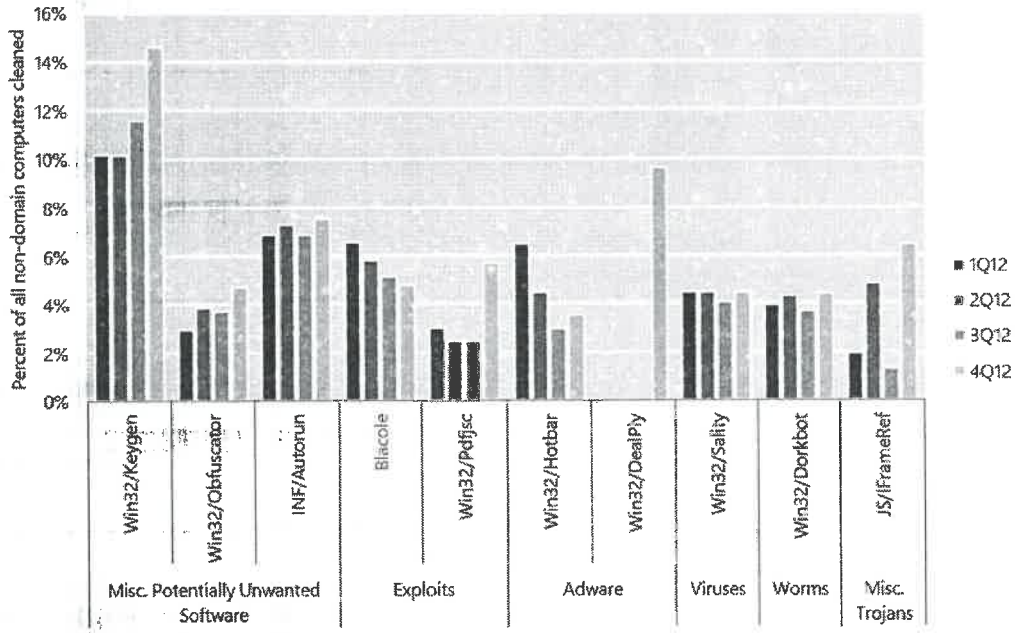


Figura 8. Tendencias trimestrales de las 10 familias principales detectadas en equipos no unidos a un dominio en el 2S12, por porcentaje de equipos no unidos a un dominio que informan de detecciones

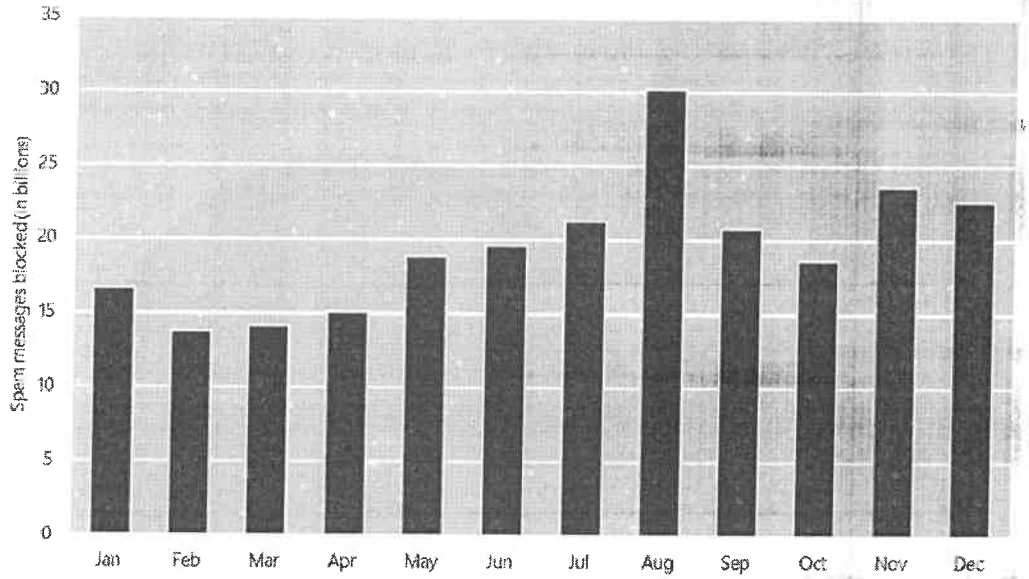


Amenazas de correo electrónico

Mensajes de correo no deseado bloqueados

La información de esta sección del informe 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 (phishing) y de malware a miles de clientes empresariales de Microsoft que procesan decenas de miles de millones de mensajes cada mes.

Figura 9. Mensajes bloqueados por el servicio de protección en línea de Exchange cada mes de 2012



Los volúmenes de correo bloqueado en el 2S12 crecieron ligeramente respecto al 1S12, pero se mantienen en niveles muy inferiores a los obtenidos antes de finales de 2010. El espectacular descenso de correo no deseado observado en los dos últimos años 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).[2] En el 2S12, aproximadamente uno de cada cuatro mensajes de correo electrónico se envió a las bandejas de entrada de los destinatarios sin bloquear ni filtrar, frente a la cifra de uno de cada 33 mensajes en 2010.

[2] Para obtener más información acerca de las medidas para Cutwail, vea *Microsoft Security Intelligence Report, volumen 10 (julio-diciembre 2010)*. Para obtener más información acerca de las medidas para Rustock, vea "Battling the Rustock Threat" ("La lucha contra la amenaza Rustock"), disponible en el Centro de descarga de Microsoft.

Figura 10. Mensajes bloqueados por la protección en línea de Exchange cada semestre, 1S09-2S12

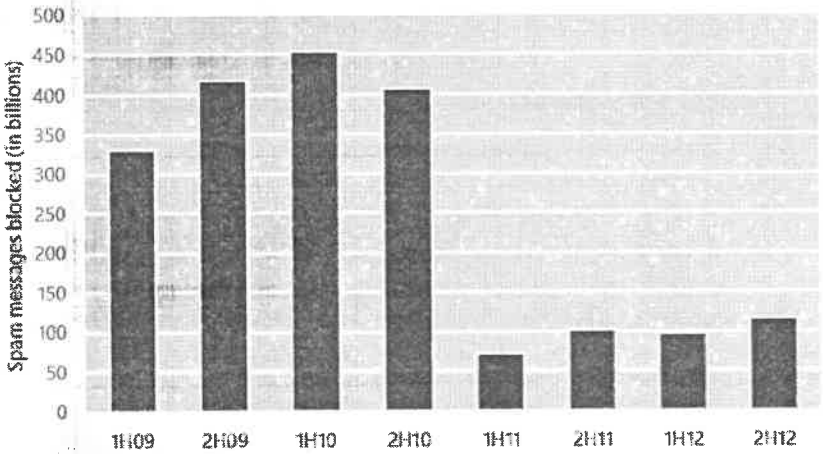
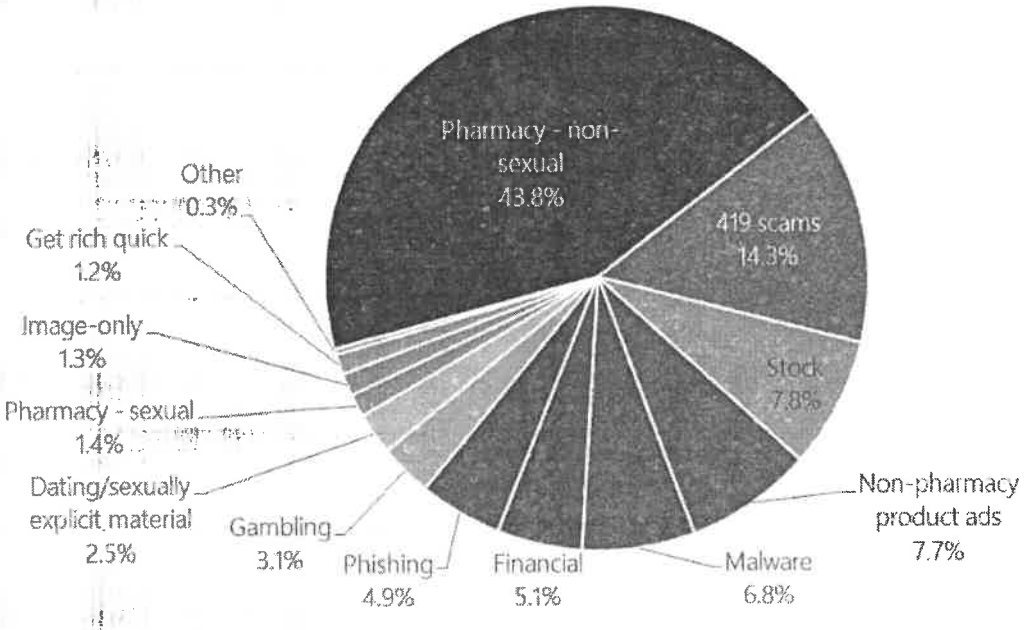


Figura 11. Mensajes entrantes bloqueados por los filtros de la protección en línea de Exchange el 2S12, por categoría.



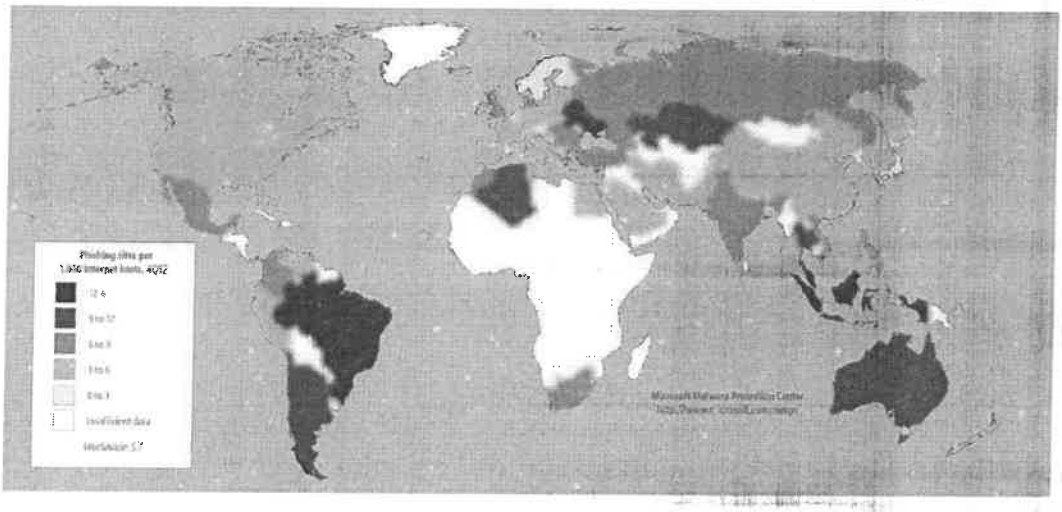
Los filtros de contenido del servicio de protección en línea de Exchange reconocen diversos tipos comunes de mensajes de correo no deseado. La figura 11 muestra la prevalencia relativa de los tipos de mensajes no deseados que se detectaron en el 2S12.

Sitios web malintencionados

Sitios de suplantación de identidad (phishing)

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 12. Sitios de suplantación de identidad por cada 1.000 hosts de Internet ubicados en todo el mundo durante el 4T12

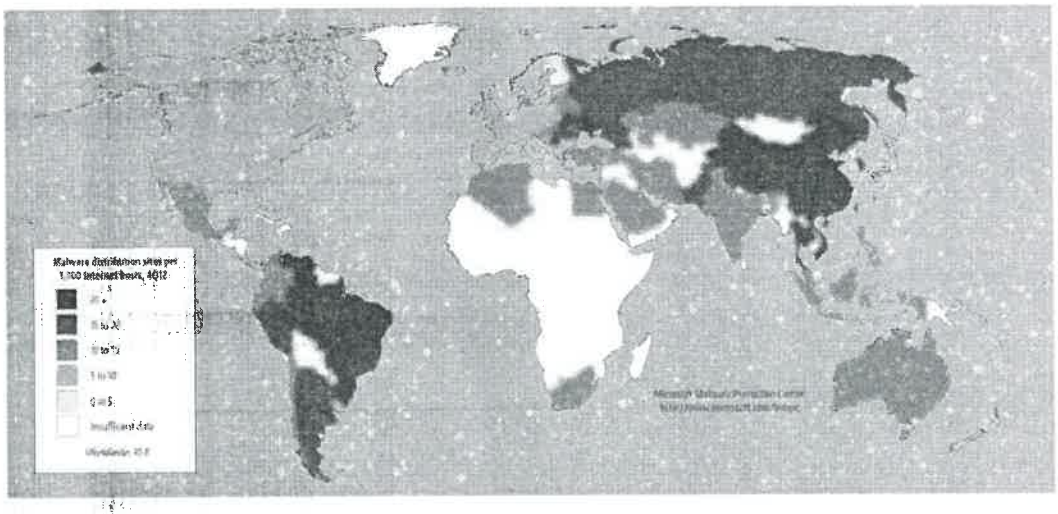


- El filtro SmartScreen detectó 5,1 sitios de suplantación de identidad por cada 1,000 hosts de Internet ubicados en todo el mundo durante el 4T12.
- Entre los lugares con concentraciones de sitios de suplantación de identidad superiores a la media se incluyen Brasil (12,6 por cada 1.000 hosts de Internet en el 4T12), Australia (9,1) y Rusia (8,3). Entre los lugares con concentraciones bajas de sitios de suplantación de identidad se incluyen Japón (1,8), Finlandia (1,9) y Suecia (2,8).

Sitios que alojan malware

El filtro SmartScreen de Internet Explorer ayuda a proporcionar protección frente a sitios conocidos por hospedar malware, además de sitios de suplantación de identidad (phishing). Dicho filtro emplea datos sobre la reputación de las direcciones URL y las tecnologías antimalware de Microsoft para determinar si los sitios distribuyen contenido no seguro. Al igual que con los sitios de suplantación de identidad (phishing), Microsoft realiza un seguimiento de la cantidad de personas que visitan cada sitio que aloja malware y usa dicha información para mejorar el filtro SmartScreen y combatir la distribución de malware de forma más adecuada.

Figura 13. Sitios de distribución de malware por cada 1.000 hosts de Internet ubicados en todo el mundo durante el 4T12



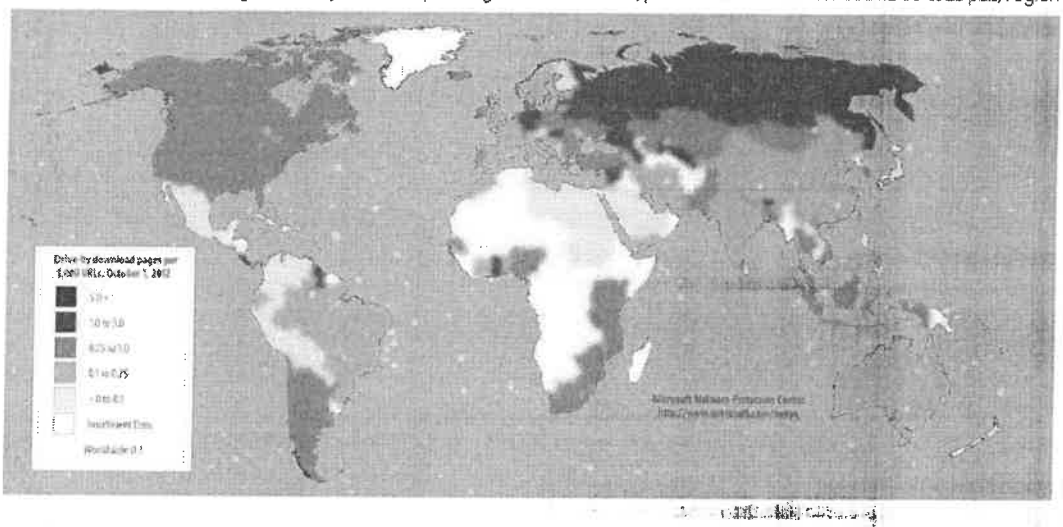
- El filtro SmartScreen detectó [3] 10,8 sitios que alojan malware por cada 1.000 hosts de Internet ubicados en todo el mundo durante el 4T12.
- China, que tenía una concentración de sitios de suplantación de identidad (phishing) muy inferior a la media (3,4 sitios de este tipo por cada 1.000 hosts de Internet en el 4T12), también tenía una concentración muy alta de sitios que alojan malware (25,1 sitios de este tipo por cada 1.000 hosts en el 4T12). Entre otros lugares con altas concentraciones de sitios que alojan malware se incluyen Brasil (32,0), Corea (17,9) y Rusia (15,9). Entre los lugares con concentraciones bajas de sitios que alojan malware se incluyen Japón (5,3), Suecia (5,4) y Polonia (6,1).

[3] Para proporcionar una perspectiva más precisa en relación con el panorama de la suplantación de identidad (phishing) y el alojamiento de malware, se ha revisado la metodología empleada para calcular el número de hosts de Internet en cada país o región. Por este motivo, las estadísticas que aquí se presentan no deben compararse directamente con las conclusiones de volúmenes anteriores.

Sitios de descargas drive-by

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 malware por el solo hecho de visitar estos sitios, incluso sin intentar descargar nada.

Figura 14. Páginas de descargas drive-by indizadas por Bing a finales del 4T12, por cada 1.000 direcciones URL de cada país/región



Este documento resume las principales conclusiones del informe. El sitio web del *SIR* 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 *SIRv14* desde www.microsoft.com/sir.

Outlook

Buscar

Reunirse ahora

Mensaje nuevo | Eliminar | Correo deseado | Informar sobre suplantación de identidad | Mover a | Categorizar | ...

Carpetas

- Bandeja d... 4
- Correo ... 136
- Borradores 30
- Elementos... 1
- Elemento... 13
- Archivo
- Notas
- Conversatio...

Crear carpeta...

Grupos

Actualizar a Microsoft 365 con Características de Outlook Premium

Cerrar

USO DE SOFTWARE ANTIVIRUS EN PC O LAPTOP DE LAS INSTITUCIONES EDUCATIVAS - MINEDU

Este mensaje se movió a la carpeta Correo electrónico no deseado debido a que solo confía en los mensajes de correo electrónico de los remitentes incluidos en la lista de remitentes seguros. No es un correo no deseado | Mostrar contenido bloqueado

Mensaje enviado con importancia Alta.

OTIC009 <OTIC009@minedu.gob.pe>
Para: OTIC009
CC: JAIME IVAN VELARDE CORDOVA

Jue 24/11/2022 17:24

20221003_103116_20220926... 960 KB | OFICIO_MULTIPLE-00057-20... 398 KB | 20221003_103051_INFORME... 1 MB

3 archivos adjuntos (3 MB) Guardar todo en OneDrive Descargar todo

Estimado Director(a):

La oficina de Tecnologías de la Información y Comunicación - OTIC del Ministerio de Educación tiene el agrado de dirigirse a usted para saludarlo cordialmente y, a su vez, en el marco del desarrollo del Gobierno Digital y la Seguridad Digital en el sector educación, se remite el Informe Técnico N° 00183-2022-MINEDU/SPE-OTIC-UCSI, OFICIO_MULTIPLE-00057-2022-MINEDU-SPE-OTIC elaborado por la Unidad de Calidad y Seguridad de la Información, y la perspectiva en detalle acerca de las vulnerabilidades, manipulaciones de software, malware, software potencialmente no deseado y sitios web malintencionados, mediante el cual informa sobre los riesgos de no utilizar un software antivirus en las computadoras de las instituciones educativas y otros órganos del sector educación, a nivel nacional. Por lo antes expuesto, se recomienda el uso del software antivirus en las computadoras de las instituciones educativas y otros órganos del sector educación; para aquellos órganos e instituciones educativas que no cuenten con software antivirus corporativo, se adjunta el link, en el cual podrán encontrar los pasos para poder realizar la protección de las computadoras que tienen instalado el sistema operativo Windows 10 con el software antivirus Windows Defender, que viene como parte del propio sistema operativo Windows, que es gratuito:

1.- SOPORTE ACTIVAR O DESACTIVAR SOFTWARE ANTIVIRUS

https://support.microsoft.com/es-es/windows/activar-o-desactivar-el-firewall-de-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f

2.-GUIA RAPIDA DE SOFTWARE DE ANTIVIRUS

https://www.formacionprofesional.info/guia-rapida-de-windows-defender/

En caso de tener alguna consulta respecto a la activación del antivirus, favor de remitir al correo electrónico soporteiiee@minedu.gob.pe

Atentamente,