3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio – septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529
DOI: http://dx.doi.org/10.17993/3ctic.2016.52.1-12

Recepción: 17 de septiembre de 2015
Aceptación: 13 de junio de 2016
Publicación: 29 de junio de 2016

¿SE PUEDE USAR UNA PC SIN ANTIVIRUS?

CAN YOU USE A PC WITHOUT ANTIVIRUS?

Romel Vera Cadena [1]

1. Consultor de Seguridad Informática. Ecuador. E-mail: romel.vera.cadena@gmail.com

3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

RESUMEN

En la actualidad el uso de la tecnología es imprescindible para la mayoría de las actividades que se realizan a lo largo del día, sin embargo existen amenazas latentes capaces de interrumpir estas actividades e incluso lucrar a costa nuestra. Dada esta situación el presente documento tratará acerca del *malware*, antivirus y expondrá estrategias claves de seguridad de la información para evitar ser infectados por *malware*. Se establecerá además, los motivos de la existencia de estas amenazas.

ABSTRACT

Currently the use of technology is essential for most of the activities that take place throughout the day, however there are latent threats that can disrupt those activities and even profit at our expense. Given this situation, this paper will address malware, antivirus, security strategies and will present key information to avoid being infected by malware. Also we will explain the motives of existence of these threats.

PALABRAS CLAVE

Antivirus; Seguridad informática; Educación; Entrenamiento; Estadísticas Malware.

KEYWORDS

Antivirus; Information Security; Education; Security Awareness; Malware Statistics.

3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

INTRODUCCIÓN

Desde antes que las computadoras se conviertan en equipos populares e importantes, han existido los virus informáticos cuyo fin para la época era destruir la información almacenada o saturarla para que se quede sin espacio disponible. Ante tal situación, se creó un software capaz de eliminar estas amenazas de los sistemas denominado antivirus. Pero con la masificación del internet, los problemas con los virus dejan de ser simples puesto que ahora existen nuevos tipos de amenazas llamadas *malware* (Panda, s.f.).

Como nuevos *malwares* que se han encontrado tenemos del tipo bancario que roba dinero de las tarjetas de crédito o de las cuentas bancarias de las víctimas, también existen del tipo que secuestran datos denominados *ransomware* que cifran los datos de la víctima con una clave única y les piden dinero a cambio de ella, del tipo *botnet* que reúne un conjunto de equipos infectados y los ponen a realizar operaciones ilegales, entre otros (Kaspersky, s.f.).

Por consiguiente, las empresas antivirus de todo el mundo hacen seguimiento al *malware* y elaboran estadísticas de infecciones de *malware* y hay que tener en cuenta estas estadísticas, como la de Microsoft del año 2014, en donde se observa que Ecuador tiene un porcentaje de infección de *malware* del 23.5% versus el resto del mundo con un 15.9%. Es decir, que de cada 1,000 equipos que se escanean, 13.3 tienen *malware* versus el resto del mundo con una cifra promedio de 5.9 (Microsoft, 2015).

Como consecuencia de las infecciones por *malware* en los medios de comunicación, se difunden noticias como robos masivos de tarjetas de crédito, robo de claves personales, filtraciones de información empresarial e incluso fotos privadas de artistas conocidos. Sin embargo todos estos casos pudieron haber sido evitados.

Por esta razón existen lineamientos de seguridad de la información dirigidos a usuarios del hogar y a usuarios empresariales en las que explican estrategias simples para evitar ser infectados por *malware* (Broida, 2014*;* Gee, 2014).

El presente documento discute acerca del *malware*, antivirus y expone estrategias básicas que se usan para evitar ser infectados por *malware*. Estas técnicas sirven tanto para usuarios del hogar como para los usuarios que laboran en empresas.

.

3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

ANTIVIRUS Y MALWARE

CÓMO FUNCIONA UN ANTIVIRUS EN UNA PC?

Los antivirus son programas que sirven para proteger a los equipos informáticos de virus, *trojans*, *worms*, *adwares*, entre otros programas maliciosos denominados *malware* que puedan infectar el sistema operativo de su computador. La protección que se brinda cubre todas las actividades comunes tales como navegación por internet, redes sociales, juegos en línea, entre otras. Normalmente, los programas antivirus monitorean las actividades del *malware* en tiempo real realizando escaneos constantes o, a petición del usuario, el antivirus realiza una búsqueda contra *malware* y si son detectados entonces el antivirus los elimina o los pone en cuarentena (Microsoft, n.d; Kaspersky, n.d.).

QUÉ ES EL MALWARE?

El *malware* es conocido también como software malicioso y es un término que se le otorga a varios tipos de amenazas como virus, *worms* y *trojans*. De todos estos, el que predomina en la lista de amenazas es el *trojan*.

Las personas tienden a creer que estos tipos de *malware* son lo mismo cuando en realidad cada uno tiene una función en específica, por ejemplo:

El virus está diseñado para infectar objetos en un disco y se propaga automáticamente de computadora a computadora. Usualmente, la forma de infección se debe a la interacción del usuario al abrir un correo con un archivo infectado.

Los *worms* también se propagan automáticamente aunque en lugar de infectar varios objetos en el disco, éste se instala una sola vez y luego busca otro equipo para infectar. Algunos *worms,* por ejemplo, el *worm* de los emails, para propagarse requiere la interacción del usuario, en cambio los *worms* de red no necesitan la interacción del usuario para infectar computadoras.

Los *trojans* poseen este nombre proveniente del mítico "Caballo de Troya" porque igual como en la historia los *trojans* se escudan en algo que aparentemente parece benigno o útil cuando en realidad una vez ejecutados o instalados estos realizan operaciones maliciosas sin consentimiento del usuario. Algunos *trojans* se instalan de manera oculta cuando el usuario navega en una página de internet que haya sido comprometida. Los *trojans,* a diferencia de virus y *worms,* no se replican pero dependen de la conexión de internet.

Los *trojans* del tipo puerta trasera conocidos como *backdoors* permiten control remoto del equipo, es decir, acceso total al ordenador por medio del internet. Algunos incluyen *keylogger,* que graban la actividad del teclado en busca de contraseñas o algún otro tipo de información confidencial con el fin de realizar actividades ilegales como los *trojans* bancarios que están diseñados para robar dinero de las cuentas bancarias de las víctimas.

También existe *malware* hibrido que mezcla funcionalidades de otros tipo de *malware* creando nuevas funciones o dándoles una mejor flexibilidad al momento de infectar nuevos equipos, como es el caso de la *Botnet.* Ésta conecta computadoras entre sí creando una red de equipos infectados para luego el delincuente informático darles órdenes por medio del internet para que realicen operaciones ilegales que van desde el envío de correos no deseados hasta realizar ataques a organizaciones específicas (Kaspersky, s.f; US-CERT, n.d.).

MOTIVACIONES DETRÁS DEL MALWARE

En la actualidad, el *malware* es creado con el fin de obtener dinero de forma ilegal; usualmente obteniendo información privada de las víctimas. Para lograrlo, el *malware* se instala de una manera discreta, es decir, se está ejecutando sin molestar las actividades que realiza el usuario. Existe especulación del impacto financiero de los delitos informáticos, buscando en internet *el costo del cibercrimen*[1] le aparecerán cifras que van desde millones hasta billones de dólares. Lo que sí es seguro es que, debido al incremento de ataques de ciberdelincuentes[2], se han creado mercados negros en todo el mundo; que son lucrativos para los que son miembros del cibercrimen.

Desde el año 2003 en el mercado negro del cibercrimen existen servicios que contratan las personas por diferentes motivos, tales como: robo de datos confidenciales, robo de propiedad intelectual, daño a la reputación, sabotaje a las funciones de alguna entidad o para realizar declaraciones políticas (Rosenthal, 2014).

Otra forma en la que los ciberdelincuentes obtienen dinero es cuando hacen uso de un *malware* denominado *Ransomware,* que es usado para extorsionar por medio del secuestro de archivos; que consiste en la encriptación de sus contenidos usando una clave única y piden dinero a cambio de la clave. El *Ransomware* es muy lucrativo porque según la importancia del contenido de los equipos secuestrados las empresas o personas estarían predispuestas a pagar el valor que pide el ciberdelincuente (McDermott, 2015).

[1] Cibercrimen: Delitos que involucra el uso de computadoras.

[2] Ciberdelincuente: Delincuente que comete actos ilegales mediante uso de computadoras.

3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

SEGURIDAD DE LA INFORMACIÓN

¿EN QUÉ CONSISTE LA SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información es el proceso de proteger la disponibilidad, privacidad y la integridad de los datos. Sin embargo, este término es usado usualmente para describir medidas y métodos para aumentar la seguridad de las computadoras.

Uno de los dichos de los expertos en el área es que ningún sistema es a prueba de todo pero al tomar medidas elementales y prácticas se pueden proteger mejor los datos (Montenegro, s.f.).

Uno de los peligros más graves de la seguridad de la información es el error humano y la ignorancia. Las personas deben tener un entrenamiento elemental de seguridad para evitar dar acceso accidental a los ciberdelincuentes. Se considera obligatorio que las personas responsables de información crítica en una empresa reciban entrenamiento elemental de seguridad de la información. En el hogar, los miembros de la familia deben poder identificar las amenazas más comunes del internet con el fin de proteger al equipo y la información personal (Wagner, 2006).

ANTIVIRUS VS ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN

La razón principal por la que muchos entusiastas y profesionales de la seguridad de la información no usan antivirus es que si alguien va a intentar atacarlos lo más probable es que usen técnicas nuevas y seguramente el antivirus no los va a proteger. Aunque a nivel empresarial el uso del antivirus es obligatorio debido a las exigencias de los estándares de industria, muchos de estos profesionales actualmente creen que en las empresas el uso del antivirus no es efectivo (McMillan, 2012).

El antivirus solo detecta amenazas viejas o conocidas, es decir, que siempre va a estar un paso atrás versus los miles de nuevos *malware* que se construyen a diario por los ciberdelincuentes. Sin embargo, el factor humano (errores humanos) dado a la falta de una educación elemental de seguridad de la información hace posible que el antivirus sea una línea adicional de seguridad (Broida, 2014; McMillan, 2012).

3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

ESTRATEGIAS PARA EVITAR INFECTARSE DE MALWARE

Aprendiendo de los estándares, lineamientos y artículos de los profesionales de la seguridad de la información, se consigue evitar ser víctimas de *malware* tanto en el hogar como en la empresa.

A continuación expongo tres estrategias esenciales que sirven contra el *malware.*

1. RECONOCER LOS ARCHIVOS EJECUTABLES

Un archivo ejecutable contiene un programa con la habilidad de realizar tareas automatizadas. A diferencia de otros tipos de archivos que solo contienen datos para ser mostrados o reproducidos como un video o audio. Es decir, que si abre un archivo ejecutable en una computadora este podría realizar cualquier tipo de acción sin requerir su permiso continuo y si fuera un *malware* serían acciones dañinas.

En el caso del sistema operativo, Windows se puede identificar el tipo de archivo por su extensión. Se llama extensión porque va al final del nombre del archivo y siempre va después de un punto. Por ejemplo en un archivo que se llame *léeme.txt* la extensión es *txt* y esta extensión le dice al Windows que se trata de un archivo de texto y que se puede abrir con el programa *notepad* (Microsoft, s.f.).

Los archivos ejecutables que los *malware* comúnmente abusan son los que tienen extensiones: exe, bat, cmd, vb y vbs.

Por ejemplo el archivo *informatica.exe* sería un ejecutable porque su extensión es un *.exe*

Hay que tener en cuenta que Windows por defecto no muestra las extensiones de los archivos para verlos siga los siguientes pasos:

1) Abra el explorador, o presione las teclas Windows+E.
2) Vaya a la pestaña *Vista*.
3) En el lado derecho habilite *extensiones de nombre de archivo.*
4) Opcionalmente habilite *elementos ocultos*

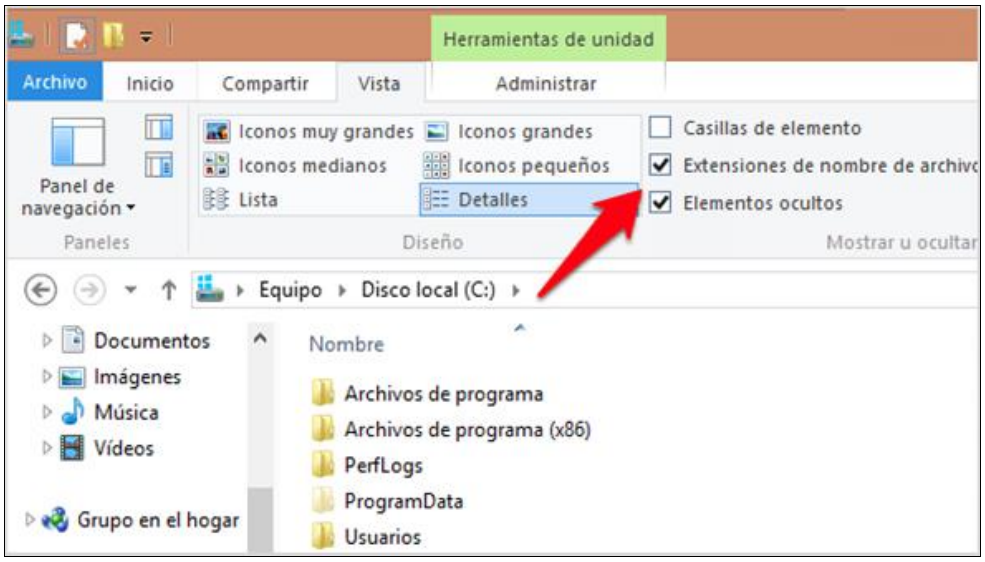

Figura 1: Procedimiento para habilitar las extensiones de los archivo.

Una vez que haya habilitado la opción de ver las extensiones de los archivos, entonces podrá identificar fácilmente los diferentes tipos de archivo.

2. DISTINGUIR TRAMPAS COMUNES DE LOS CIBERDELINCUENTES

La trampa más común de los ciberdelincuentes consiste en disfrazar ejecutables de *malware* como si fueran archivos de documentos, audios o videos ejemplo:

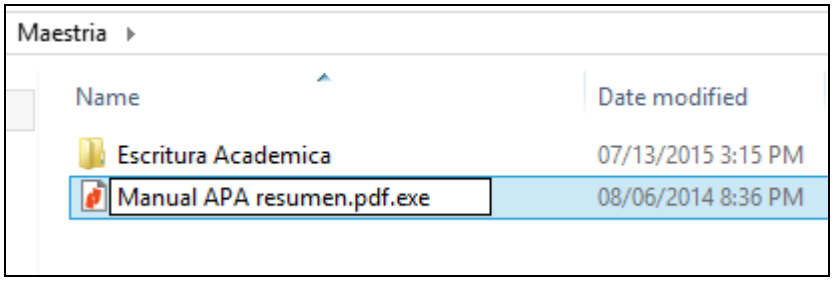

Figura 2: Un ejecutable que aparenta ser un documento pdf.

En la Figura 2 se puede distinguir con facilidad que el archivo aparenta ser un documento PDF cuando en realidad es un ejecutable porque termina en *.exe*.

Evite prestar atención al ícono del archivo porque los archivos ejecutables pueden tener cualquier gráfico como ícono. Sin embargo, solo podrá distinguir un documento original de un ejecutable siempre y cuando tenga habilitada la opción de ver las extensiones ocultas.

Al descargar documentos por internet deberá fijarse en el nombre completo del archivo, si el archivo supuestamente es un documento entonces no deberá terminar con una extensión de un ejecutable, ejemplo:

3C TIC ***(Edición núm. 17)*** *Vol.5 – Nº 2*
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

Figura 3: Error ortográfico en un ejecutable.

A veces, los creadores de *malware,* al realizar traducciones cometen faltas ortográficas al momento de ponerle nombre a los ejecutables, como se puede apreciar en la Figura 3.

3. CONFIRMAR FUENTES

Siempre debe confirmar el origen de los documentos o programas, es decir, antes de descargar un archivo o programa deberá hacerlo de su sitio oficial o de algún sitio externo pero que sea avalado por el oficial. Por ejemplo:

El software WinRAR de RARLAB es un programa compresor de archivos muy popular. El sitio web oficial es www.rarlab.com. Sin embargo, existen varios sitios no oficiales que permiten descargarlo y en muchos de estos sitios el archivo es un malware.

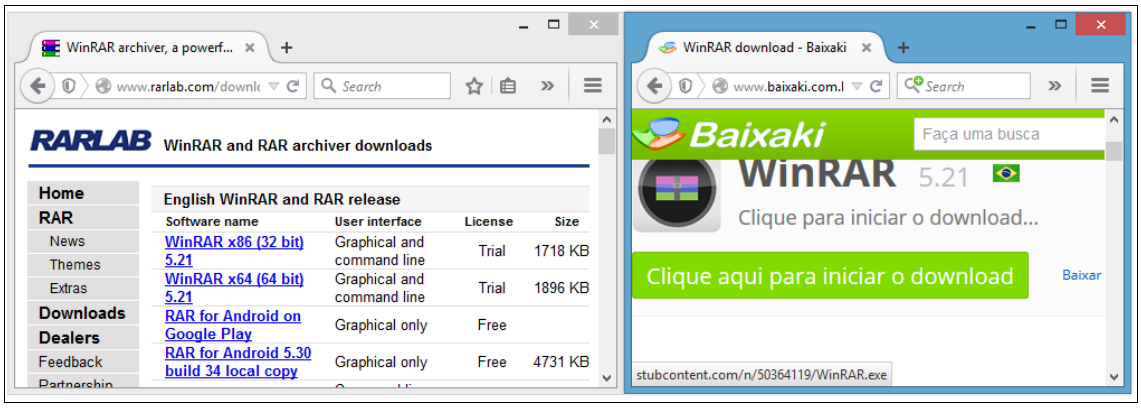

Figura 4: Descarga de un ejecutable.

En este caso, al hacer la descarga del sitio *Baixaki;* como se muestra en la Figura 4, el archivo que se descarga del sitio web no oficial es un ejecutable lo cual es correcto porque se trata de un programa y si comparamos el archivo es evidente que el tamaño en KiloBytes (KB) del archivo es diferente del original. Incluso la procedencia del archivo es otra; su nueva procedencia es *pocodoctor.com.*

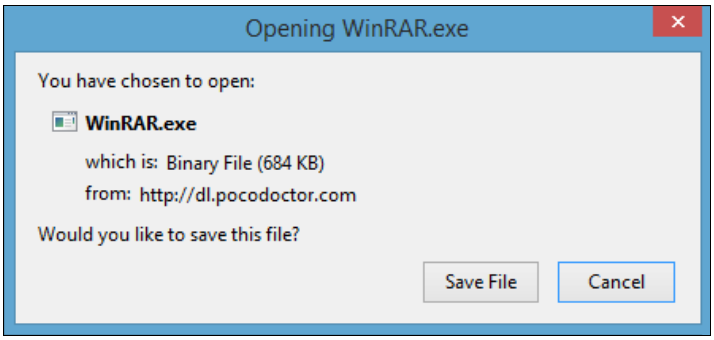

Figura 5: Opción para abrir un ejecutable.

Si realizamos un escaneo contra virus el resultado será obvio.

ESET-NOD32	a variant of Win32/TrojanDropper.Addrop.J	20150716
Emsisoft	Gen:Variant.Adware.Graftor.190520 (B)	20150716
F-Prot	W32/S-018f1eb2!Eldorado	20150716
F-Secure	Gen:Variant.Adware.Graftor	20150716
GData	Gen:Variant.Adware.Graftor.190520	20150716

Figura 6: Archivo ejecutable descargado.

Este archivo ejecutable descargado de la web de *Baixaki* cuya procedencia es de un sitio que se llama *pocodoctor.com* y que simula ser el programa WinRAR, en realidad es un *malware.*

En este caso los anti-virus lo han detectado, sin embargo si el *malware* fuera nuevo no se contaría con la misma suerte.

En cuanto a los emails, es preferible no abrir archivos extraños y si es un email de alguna entidad conocida aplicar las mismas estrategias para evitar *malware*.

También evite abrir vínculos que encuentre en un email, por ejemplo: si en un mail le dicen que *haga clic para ver su estado de cuenta del banco,* no lo haga y abra el navegador y escriba la dirección oficial del banco para ver su estado de cuenta de forma segura.

En las redes sociales, si al hacer *clic* a un video o algún otro tipo de vínculo le piden instalar algo adicional para proceder, no lo instale o si se le presenta una ventana para descargar un ejecutable entonces no lo haga porque se trata de *malware.*

3C TIC *(Edición núm. 17)* Vol.5 – Nº 2
Junio– septiembre '16, 1 - 12
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

CONCLUSIONES

El *malware* es una amenaza constante que no solo afecta a los equipos de computación, sino que también puede llegar a afectarnos convirtiéndonos en victimas de ciberdelincuentes.

Un ciberdelincuente crea *malware* por varios motivos tales como dañar, sabotear, lucrar e incluso hay quienes lo hacen por diversión. Aunque en la actualidad el motivo que prevalece sobre los demás es el de lucro.

Los antivirus son una línea de defensa obligatoria para las empresas que deben cumplir estándares de industria. Sin embargo, los antivirus están un paso por detrás de los ciberdelincuentes que crean a diario nuevos *malware* y es por este motivo que actualmente se está dando importancia a los temas de seguridad de la información que involucra directamente al usuario.

Los profesionales de seguridad de la información aconsejan que se de entrenamiento de seguridad a las personas que laboran en cualquier empresa y a las personas del hogar que se eduquen y ayuden a transmitir el conocimiento adquirido.

Existen varias estrategias de seguridad de la información que cubren diferentes áreas como son, la defensa contra ataques informáticos, prevención de infección por *malware*, seguridad de datos, respaldos de información entre otras.

En este artículo solo tratamos tres estrategias claves que sirven para evitar *malware* que es el principal vector de ataque de los ciberdelincuentes.

1. Reconocer los archivos ejecutables.
2. Distinguir trampas comunes de los ciberdelincuentes.
3. Confirmar fuentes.

Cabe destacar que estas estrategias se pueden aplicar en cualquier sistema operativo. Sin embargo, los ejemplos en este artículo se enfocan al sistema operativo Windows.

Para terminar, se concluye que haciendo uso de conocimientos esenciales de seguridad de la información es posible evitar *malware.*

REFERENCIAS BIBLIOGRÁFICAS

Broida, R. (2014, June 25). *I still don't use anti-virus software. Am I still nuts?* Recuperado de: <http://www.cnet.com/how-to/i-dont-use-anti-virus-software-am-i-nuts/>

Gee, G. (2014). *Cyber Security Principles.* Paper Street Publishing.

Kaspersky. (s.f.). *Seguridad 101: Los tipos de malware*. Recuperado de: <http://support.kaspersky.com/sp/viruses/general/614/>

Kaspersky. (n.d.). *Viruses & Worms*. Recuperado de: <https://usa.kaspersky.com/internet-security-center/threats/viruses-worms#.VaK1p_lOnIU/>

McDermott, I. E. (2015). Ransomware. *Online Searcher*, pp. 35-37.

McMillan, R. (2012). *Wired*. Recuperado de: <http://www.wired.com/2012/03/antivirus/>

Microsoft. (2015). *Microsoft Security Intelligence Report Volume 18.* Recuperado de: <http://download.microsoft.com/download/7/1/A/71ABB4EC-E255-4DAF-9496-A46D67D875CD/Microsoft_Security_Intelligence_Report_Volume_18_English.pdf/>

Microsoft. (s.f.). *Nombres de archivo y extensiones de nombre de archivo*. Recuperado de: <http://windows.microsoft.com/es-es/windows/file-names-extensions-faq#1TC=windows-7/>

Microsoft. (n.d.). *What is a computer virus?* Recuperado de: <https://www.microsoft.com/security/pc-security/virus-whatis.aspx/>

Montenegro, L. (s.f.). *Seguridad de la Información: Más que una actitud, un estilo de vida.* Recuperado de: <http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/>

Panda. (s.f.). *Classic Malware: su historia, su evolución.* Recuperado de: <http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/>

Rosenthal, A. (2014, September 15). *Security 101*. Recuperado de: <https://www.youtube.com/watch?v=sdpxddDzXfE />

US-CERT. (n.d.). *Virus Basics*. Recuperado de: <https://www.us-cert.gov/publications/virus-basics/>

Wagner, C. G. (2006). Information Security's Biggest Enemy. *Futurist*, 11.