ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

“VIRUS Y SEGURIDAD TECNOLÓGICA EN LA DOCENCIA”

AUTORÍA
Mª JOSÉ PALOMAR SÁNCHEZ

TEMÁTICA
TIC´S

ETAPA
ESO, BACHILLER, F.P.

Resumen

En este artículo se pretende dar una amplia visión sobre los virus informáticos más comunes y como se pueden prevenir. De este modo nuestros centros educativos estarán más seguros ante los ataques informáticos.

Palabras clave

Virus.

Ataque.

Seguridad.

Software malintencionado.

Antivirus.

Cortafuegos.

1. INTRODUCCIÓN.

La seguridad es uno de los problemas más importantes que existe en Internet. Cada día aparecen nuevos virus que afectan a miles de usuarios, y por tanto al profesorado, alumnado y consecuentemente a los centros educativos. Estos hacen que se pierda mucho tiempo solucionándolos y recuperando la información perdida, en el mejor caso. Todo docente y alumno/a que están expuestos a los nuevos avances tecnológicos y están trabajando diariamente con las herramientas informáticas deben conocer como proteger sus equipos. En este artículo se expondrán que son los virus, que tipos de ataques puede recibir nuestros equipos, tanto personales como lo de los centros educativos, y cómo podemos defendernos de ellos con las herramientas de seguridad que se encuentran en el mercado actual.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

2. VIRUS.

Lo que comúnmente es llamado como virus lo deberíamos llamar software malintencionado, pues el virus sólo es un tipo dentro de esta definición. El término de virus malintencionado o malware (del inglés “malicious software”) se utiliza como denominación colectiva para hacer referencia a los virus, gusanos y troyanos que realizan tareas mal intencionada en un sistema y/o equipo informático.

Una vez el código malintencionado se ha introducido en nuestro equipo, intentará instalarse en lugares donde el usuario pueda ejecutarlos sin darse cuenta. Hasta que no se ejecuta el programa infectado o se cumple una determinada condición, el código malintencionado no actúa. Incluso los efectos producidos por éste, se aprecian mucho tiempo después de su ejecución.

2.1 Tipos de Software mal intencionado.

a) Troyano.

Es un programa aparentemente útil o inofensivo que en realidad contiene código oculto diseñado para generar daños o beneficiarse del sistema en el que se ejecuta. Los troyanos se envían normalmente a través de mensajes de correo electrónico. Una de las tareas más habituales de un troyano es permitir el acceso a nuestro ordenador, con lo que nuestros datos pueden ser dañados, robados, manipulados o eliminados.

b) Gusano.

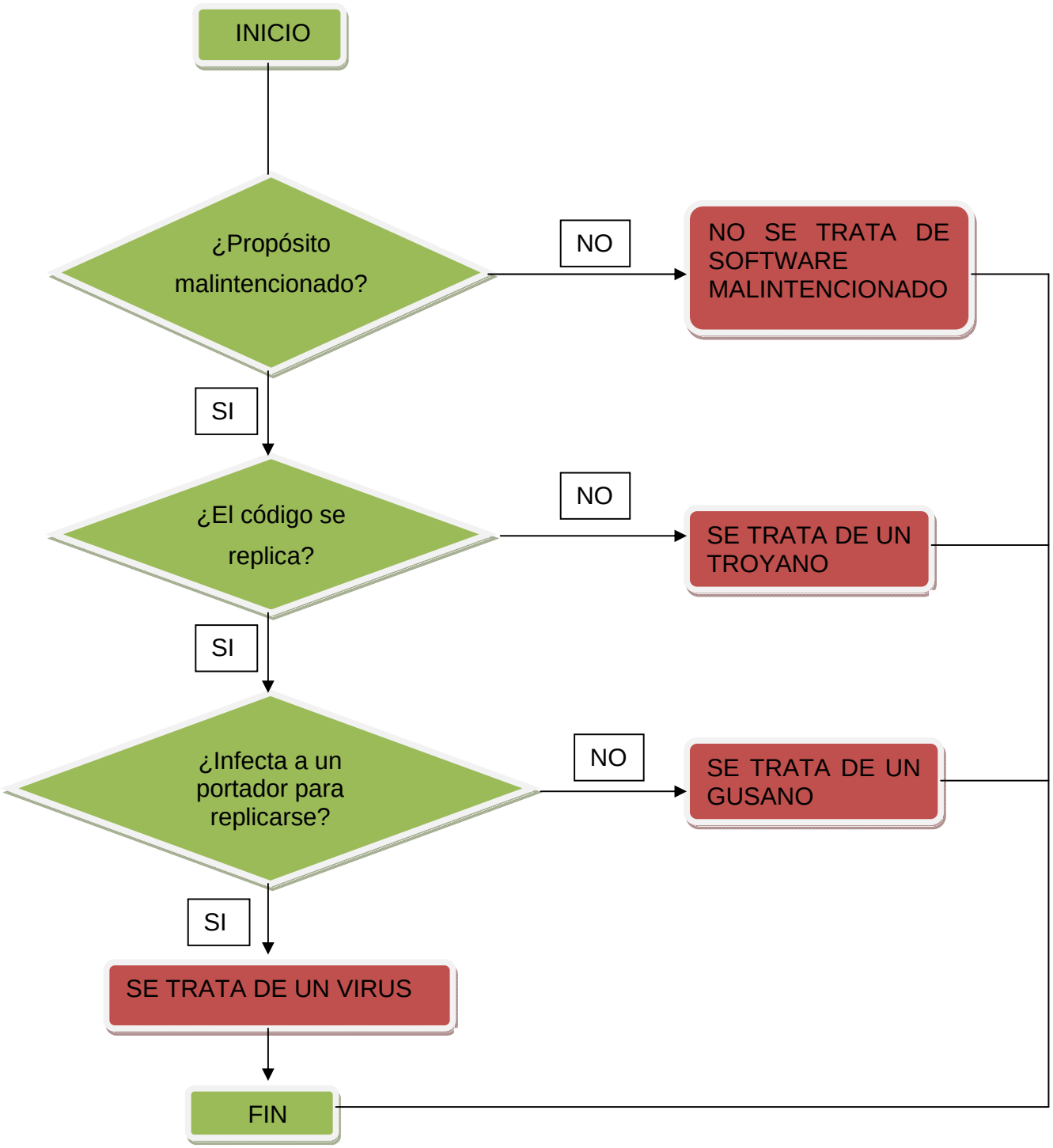
Los gusanos utilizan código malintencionado de propagación automática capaz de distribuirse de un equipo a otro a través de correo electrónico. Los gusanos pueden realizar acciones dañinas como consumir los recursos de internet o de nuestro propio sistema, eliminar información o instalar otro software mal intencionado. Una vez que el gusano se ha instalado en nuestro equipo es capaz de acceder a nuestra libreta de direcciones y auto enviarse a todos los contactos de la libreta de direcciones

c) Virus.

Los virus ejecutan código escrito con la única idea de replicarse. Se intentan propagar de un equipo a otro adjuntándose a un programa. Son más peligrosos que los troyanos y gusanos ya que pueden estropear, además de datos, hardware y software. Cuando el programa se ejecuta también lo hace el código del virus, infectado nuevos programas.

Estas definiciones de las distintas categorías de software malintencionado permiten presentar las diferencias entre ellos en un simple gráfico de flujo. En la figura siguiente se muestran los elementos que permiten determinar si un programa o una secuencia de comandos se incluyen dentro de alguna categoría de software malintencionado:

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

2.2 Medios de propagación más habituales para el Software mal intencionado.

La primera pregunta que nos debemos hacer es a través de que medio un software malintencionado puede atacar o introducirse en nuestro ordenador. Si conocemos la respuesta, seremos capaces de proteger las distintas vías de entrada para evitar posibles infecciones. El software malintencionado utiliza las siguientes vías de propagación:

a) Unidades de almacenamiento.

Son aquellos medios de almacenamiento en la que se guarda información, mediante archivos. Con ellos se puede trabajar en un ordenador y luego utilizarlos en otro diferente. Algunas de estas unidades pueden ser DVD. Cd, pen drive, tarjetas de memoria. Si alguno de ellos se encontrase infectado, al trabajar con él en algún ordenador éste se podría infectar.

b) Redes de ordenadores.

Una red es un conjunto o sistemas de ordenadores conectados físicamente entre sí, para facilitar el trabajo de varios usuarios. Esto quiere decir que existen conexiones entre cualquiera de los ordenadores que forman parte de la red, pudiéndose transferir información entre ellos. Si alguna de esta información transmitida de un equipo a otro está infectada, el ordenador en el que se recibe será infectado.

c) Internet.

Cada día se utilizan más las posibilidades que ofrece internet para obtener información, realizar envíos y recepciones de mensajes de correo, recibir y publicar noticias, o descargar ficheros. Odas estas operaciones se basan en la transferencia de información, así como en la conexión de diferentes ordenadores de cualquier parte del mundo. Por tanto, cualquier virus puede introducirse en nuestro ordenador al mismo tiempo que la información es recibida. A través de internet la infección podría realizarse empleando diferentes caminos como los siguientes:

- Correo electrónico: en un mensaje enviado o recibido se pueden incluir documentos o ficheros (fichero adjunto). Estos ficheros podrían ser infectados, contagiando al ordenador destino.
- Páginas Web: las páginas que visitamos en internet son ficheros de texto o imágenes escritos en un lenguaje denominado HTML. No obstante también pueden contener cierto tipo de código ejecutable, como los controles ActiveX y Applets de Java, que son programas. Estos sí pueden ser infectados y podrían infectar al usuario que se encuentre visitando esa página.

2.3 Ubicación del Software mal intencionado.

El software malintencionado utiliza sus propias medidas de ocultamiento, pudiendo “esconderse” en diferentes lugares. Algunos de ellos podrían ser los siguientes:

a) En memoria principal.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

En este caso el software malintencionado se colocará automáticamente en la memoria principal (memoria RAM) esperando que se ejecute algún programa (fichero con extensión EXE o COM) para infectarlo. Este tipo de software malintencionado, se denomina residente.

b) Documentos con macros.

Por regla general, los ficheros que no sean programas, no son infectados por ningún tipo de software malintencionado. Sin embargo, existen determinados tipos de archivos con los que el usuario puede trabajar, que permiten incluir en ellos lo que se denomina macro. Una macro es un conjunto instrucciones o acciones que otro programa puede llevar a cabo. Pues bien, estas macros pueden formar parte del documento (texto, hoja de cálculo o base de datos) y por tratarse de programas pueden ser infectados por el software malintencionado (virus de macro).

c) Sector de arranque (Boot y Master Boot).

El sector de arranque es una sección concreta de un disco (disquete o disco duro) en la que se guarda la información sobre las características de disco y sobre el contenido del mismo. Cuando se habla del sector de arranque de un disquete su utiliza el término BOOT, mientras que si se trata del sector de arranque de un disco duro, se emplea el término Master BOOT (MBR). En ocasiones, esta sección de un disco contiene un programa que permite arrancar el ordenador. Cierto tipo de software malintencionado, se denominan virus de Boot, se esconden en este lugar, y por consiguiente consiguiendo que se ejecute el virus en cada arranque del ordenador.

2.4 Spam.

Aunque no se puede considerar software malintencionado, el Spam es uno de los problemas más extendidos actualmente a través de las comunicaciones por vía electrónica. Se denomina Spam o “correo basura” cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar. Comercializar o tratar de despertar el interés respecto de un producto, servicia o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Esta conducta es particularmente grave cuando se realiza en forma masiva.

El bajo coste de los envíos vía internet (mediante el correo electrónico) o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades en el volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada. Existen varias formas de Spam que se detallan a continuación.

a) Correo electrónico.

Debido a la facilidad, rapidez y capacidad en las transmisiones de datos, la recepción de comunicaciones comerciales a través de este servicio de la sociedad de la información es la más usual, y el medio más utilizado por los spammers.

b) Spam por ventanas emergentes (Pop ups).

Se trata de enviar un mensaje no solicitado que emerge cuando navegamos por internet por medio de un explorador. Su contenido es variable pero generalmente se trata de un mensaje de carácter publicitario.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

En la plataforma de Windows, el Service Pack 2 de Windows XP corrige esta vulnerabilidad, siendo el usuario el que decide si permite la aparición de los popups o no.

c) Hoax.

El Hoax es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos Hoax informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de suerte. Los objetivos que persigue quien inicia un Hoax son normalmente captar direcciones de correo o saturar la red o los servidores de correo.

d) Scam.

El Scam no tiene carácter de comunicación comercial. Este tipo de comunicación no deseada implica un fraude por medios telemáticos, bien vía teléfono móvil o por correo electrónico.

e) Spam en el móvil.

Además de las comunicaciones del operador de telefonía mediante mensajes de texto o mensajes multimedia, existen otros tipos de comunicaciones publicitarias en las que no media un consentimiento previo ni una relación contractual, por lo que son considerada comunicaciones comerciales no solicitadas. Este tipo de comunicaciones generan un gasto de tiempo y de dinero.

2.5 Phising.

El Phising es la duplicación de una página web para hacer creer al visitante que se encuentra en la página original en lugar de la lícita. Se suele utilizar con fines delictivos duplicando páginas de bancos y enviando indiscriminadamente correos mediantes Spam para que se acceda a esta página con el fin de actualizar los datos de acceso al banco, como contraseñas, fechas de caducidad, etc. Al actualizar los datos, en realidad lo que estamos haciendo es escribir esta información en el servidor de los estafadores. A partir, de este momento pueden realizar operaciones con nuestra cuenta bancaria.

2.6 Pharming.

El Pharming es una nueva amenaza, más sofisticada y peligrosa, que consiste en manipular las direcciones DNS (Domain Name Server) que utilizamos. Los servidores DNS son los encargados de conducirnos a la página que deseamos ver. Pero a través de esta acción, los ladrones de datos consiguen que la páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online.

A través del “pharming”, cuando tecleamos en nuestro navegador la dirección de la página a la que queremos acceder, en realidad podemos ser enviados a otra creada por el hacker, que tiene el mismo aspecto que la original. Así, el internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

3. MEDIDAS DE SEGURIDAD.

Una vez que ha sido detallado los distintos tipos de problemas que nos podemos encontrar al conectarnos a internet. A continuación, se detallarán algunas de las herramientas que nos pueden a ayudar a prevenir o solucionar los problemas que se nos plantean.

3.1 Antivirus.

Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los archivos adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que puedan ejecutarse en un navegador web (ActiveX, Java, JavaScript).

3.2 Cortafuegos.

Los Cortafuegos (firewall) son programas que instalamos de forma residente en nuestro ordenador y que permiten filtrar y controlar la conexión a la red. En general necesitamos un conocimiento adecuado de nuestro ordenador, pues en la actualidad son muchos los programas que realizan conexiones a la red y que son necesarios. Es por ello que no son recomendables para usuarios inexpertos ya que podrían bloquear el funcionamiento de sus aplicaciones (incluso hasta la propia posibilidad de navegación por internet), aunque siempre se tenga la posibilidad de desactivarlos.

La instalación de un cortafuegos requiere además un proceso de “entrenamiento para usarlo” ya que al principio deberemos ir elaborando las reglas de acceso en función del empleo que le demos a la red. Así lo normal es que nuestro Firewall Personal nos pregunte si queremos dar permiso a distintos programas de red a medida que los usamos. Esto al principio puede resultar un poco complicado o incluso molesto.

Los cortafuegos no impiden por sí solos que entren troyanos, virus y gusanos a nuestro ordenador. Lo ideal es que también tengamos instalado un potente antivirus residente en memoria, actualizando y bien configurado. Adicionalmente es deseable tener al día todas las actualizaciones en seguridad que nuestro sistema operativo requiera.

En general, estas son las características principales de los cortafuegos:

- Que proteja el sistema de acceso no autorizado a través de internet.
- Capacidad de alertar de intentos de intrusión y mantener un registro para seguir sus pistas.
- Cierto grado de protección frente a virus a través de correo electrónico.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº26 – ENERO DE 2010

- Bloqueo de contenidos peligroso en internet: ActiveX, cookies, etc.
- Filtrado al nivel de la aplicación para conexiones hacia el exterior.

3.3 Otras herramientas.

Además de las mencionadas anteriormente, existen muchas más que nos ofrecen la posibilidad de solucionar problemas derivados del uso de internet. Algunas de estas herramientas son:

- Escaneadores de puerto.
- Mata emergentes.
- Anti marcadores.
- Anti espías.

Además de todas estas herramientas, debemos tener en cuenta que es muy importante, realizar copias de seguridad de nuestros datos y ser cuidadosos a la hora de crear y mantener nuestras contraseñas, pues debemos recordar que las contraseñas son las llaves que impiden que otros usuarios accedan a nuestra información.

4. CONCLUSIÓN.

Con este artículo se ha pretendido dar una serie de recursos de seguridad informática para que tanto docentes como alumnado tengan protegidos sus trabajos tanto en su vida académica, profesional y personal.

5. BIBLIOGRAFÍA.

- Montero Ayala, Ramón. (2007). *Protección ante Internet (como proteger el ordenador).* Creaciones Copyright.
- Smith, Ben y Komar, Brian. (2003). *Seguridad en Microsoft Windows: Kit de recursos.* Editorial McGraw Hill/ Interamericana de España, S.A.

Autoría

- Nombre y Apellidos: Mª JOSÉ PALOMAR SÁNCHEZ.
- Centro, localidad, provincia: CÓRDOBA.
- E-mail: mjpalomarsanchez@hotmail.com.