QUÉ PAPEL JUGAMOS, SI DE VIRUS Y ANTIVIRUS SE TRATA.

Lic. Yuri González Nieves.

RESUMEN

El siguiente trabajo pretende, a través de reflexiones y recomendaciones prácticas, elevar la preparación de nuestro personal docente y usuarios de manera general, en aspectos relacionados con la seguridad informática.

Ha sido concebido de manera clara y sencilla para que el lector con un mínimo de conocimientos en materia de informática sea capaz de realizar las operaciones propuestas; lo cual no solo elevará su preparación teórico-práctica en este sentido, sino que estará preparado para ser un ente activo en la protección y configuración de su sistema y el sistema de la institución.

PALABRAS CLAVE

SEGURIDAD INFORMÁTICA, CÓDIGOS MALIGNOS, VIRUS, GUSANOS, TROYANOS, SEGURIDAD WINDOWS, EXTENSIONES DE ARCHIVO, ATRIBUTOS DE ARCHIVOS, AUTORUN, ANTIVIRUS, PROTECCIÓN EN TIEMPO REAL.

Sí, de virus y antivirus se trata, pero no es nuestra intención hacer un análisis exhaustivo de sus características ni mucho menos, sino reflexionar acerca de qué papel jugamos en su prevención.

Es muy común hoy en el ISP Félix Varela encontrar personas que se preocupan por el tema e incluso quienes se sienten culpables por creer que contribuyeron a una infección, amén de otros que nos juzgan y acusan por no «acabar con todos los virus», las situaciones mencionadas no nos preocupan ya que en estas personas se ha encendido la llama de la «responsabilidad informática», más nos preocupan aquellos que se muestran indiferentes y que no se detienen al poner su pendrive en cualquier computadora, sin pensar que pueden estar diseminando un programa que pudiera hacer colapsar no solo a esa máquina sino a un sistema informático en su totalidad.

A través de este trabajo se desea dar a todos los profesores del instituto una serie de recomendaciones que pudiesen contribuir a elevar su preparación para enfrentar una realidad que existe y que empeora día a día: la aparición de programas malignos o como los clasifican los especialistas en seguridad informática: códigos malignos, a la vez se demanda de los profesores la diseminación, al igual que hacen los códigos malignos, de estas recomendaciones entre sus colegas, estudiantes y todos aquellos que emplean los medios informáticos.

En realidad los virus, troyanos, gusanos, etc, son programas informáticos que están diseñados para «dañar» el correcto funcionamiento de los sistemas informáticos; si bien en sus orígenes se utilizaron básicamente para deteriorar el software hoy, debido al desarrollo de las tecnologías de la información y la comunicación (TIC) y su empleo con disímiles fines, como el comercio electrónico, han diversificado sus objetivos, que sin abandonar los originarios ahora se concentran en el robo de informaciones, lo cual permite a sus creadores aumentar su poderío o su riqueza material.

Windows, inseguro «por defecto».

No se afilen los dientes los detractores de Windows y seguidores de Linux se trata solo de un cometario. Windows sin duda es el sistema operativo más utilizado en nuestro contexto y en el mundo; a pesar de que con el surgimiento de nuevas versiones se mejora la seguridad de este sistema, en su instalación «por defecto»: instalación predeterminada por sus programadores, no se muestra al usuario las extensiones de los archivos, lo cual se considera una fisura de seguridad, pues esto constituye una sustancial ayuda para que los fabricantes de códigos malignos puedan introducir sus programas en los sistemas con relativa facilidad.

El siguiente ejemplo servirá para ilustrar este planteamiento:

Usted crea un documento utilizando Microsoft Word y lo titula *Tesis*, solo le será mostrado el nombre y un icono con una «W» que identifica que este programa está asociado a Word; si Windows ha sido instalado «por defecto», de lo contrario, a continuación del nombre del fichero se mostrará un punto y tres letras, en este caso en particular las letras (doc), esto se conoce como extensión de fichero o archivo. La extensión de un fichero es la que realmente permite identificarlo, tanto por Windows como por usted, en este caso su fichero sería Tesis.doc más el icono de Microsoft Word. Ahora bien si su Windows fue instalado «por defecto», usted solo verá el fichero así: 

. . Si apareciese un código maligno que no fuese detectado por el antivirus y que se llamase Tesis.exe o Tesis.doc.exe y que muestre un icono de Word, ¿Pudiera usted identificarlo trabajando con Windows instalado «por defecto»?

Un factor de suma importancia para que usted pueda contribuir a elevar la protección de su sistema o el sistema de la institución es no solo conocer que extensión identifica a cada archivo sino poder visualizarlas.

Las siguientes recomendaciones le ayudarán a solucionar esta situación.

1. Desde la ventana de una carpeta cualquiera acceda al menú Herramientas/Opciones de Carpeta y en la ficha Ver/Configuración

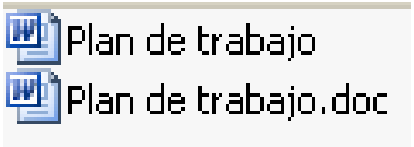
avanzada: desmarque la casilla *Ocultar las extensiones de archivo para tipos de archivo conocidos*. Posteriormente presione el botón: Aplicar a todas las carpetas / Aplicar / Aceptar.

Es necesario ser cuidadosos al tener configurado el sistema para mostrar las extensiones de los ficheros ya que un cambio de extensión de manera intencional o por error puede ocasionar la desasociación de un fichero a un programa, lo cual produciría efectos indeseados.

La siguiente situación está basada en un hecho que ocurre con relativa frecuencia en la práctica:

> Se informa a todos lo usuarios, por el administrador de la red u otra persona oficialmente reconocida para hacerlo, que está circulando un código maligno dentro de un fichero nombrado **Plan de Trabajo.doc.exe** y que no es identificado por los productos antivirus del instituto. Se advierte además, que puede llegar al usuario por la vía del Email, dispositivo de almacenamiento, carpeta compartida, etc, y que debe ser eliminado inmediatamente, si por error este es ejecutado (haciendo doble clic, Enter o abriéndolo con Microsoft Word) la Computadora quedará infectada inmediatamente.

Si Windows está instalado «por defecto» en la computadora que usted se encuentra trabajando y en una carpeta existen los siguientes ficheros cuál de los dos será el código maligno.



¿Está usted en condiciones de resolver esta situación u otras con características muy similares? Si su respuesta es afirmativa es señal que asimiló el contenido, de ser negativa no se detenga vuelva a estudiar este tema y recuerde: «el que persevera triunfa».

¿Conoce el contenido de su pendrive?

Los pendriver, memorias flash, discos externos o como prefiera llamarlos son los dispositivos de almacenamiento más utilizados por estos días para el traslado de información.

La ingeniería del software ha estado en función de acomodar el uso de estos dispositivos de tal manera que los usuarios de las tecnologías de la información y la comunicación con solo introducirlos en sus sistemas les es mostrada automáticamente la información que contienen. Esta peculiaridad, por llamarla de algún modo, ha sido aprovechada por los fabricantes de códigos malignos para invadir los sistemas informáticos.

Si bien hace algunos años el transporte favorito de los códigos malignos era los disquetes flexibles hoy son los pendriver. En este sentido se ponen de manifiesto dos cuestiones, que en una instalación «por defecto» de Windows atenta contra la seguridad de los referidos medios de almacenamiento y contra el sistema informático de manera general.

La primera está relacionada con las propiedades o atributos de los ficheros o archivos. A un fichero o archivo en Windows puede asignársele las siguientes propiedades o atributos especiales:

1. Solo lectura (Read only)
2. Oculto (Hidden)
3. De sistema (System)

Solo lectura (Read only): Esta propiedad hace que un fichero no pueda ser modificado en su contenido, e incluso si deseara su eliminación, Windows le pediría una confirmación de eliminación. Para ser modificado y en algunos casos eliminado es necesario retirar esta propiedad al archivo.

Oculto (Hidden): Este atributo es el de mayor relevancia para la diseminación de códigos malignos, ya que un fichero que posea esta propiedad no será mostrado en el explorador de Windows si este ha sido instalado «por defecto», por lo que el usuario no se percatará que en su pendrive, u otros dispositivos de almacenamiento, pudiera existir un software del cual no es propietario.

De sistema (System): De asignarse esta propiedad a un fichero, Windows lo asume como imprescindible para el correcto funcionamiento del sistema. Si desease eliminar un archivo que tenga incluida esta propiedad el sistema le advertirá y le pedirá una confirmación.

La segunda cuestión está vinculada con este atributo, ya que determinados archivos de sistema son ejecutados automáticamente por Windows en su arranque o posteriormente al ser introducidos desde una unidad de disco.

Ejemplo de ello son entre otros los siguientes archivos:

AUTOEXEC.BAT
boot.ini } *Ejecutados al arrancar Windows*
CONFIG.SYS
AUTORUN.INF **---** *Ejecutado desde una unidad extraíble o CD*

La combinación de estos tres atributos en un fichero más los nombres de ficheros ejecutados por Windows automáticamente son explotados de manera organizada por los fabricantes de códigos malignos para infectar sistemas sin la participación directa del usuario. En otras palabras, no es necesario el *doble clic o* el *Enter* del usuario para ejecutar el código maligno; Windows se encarga de ello.

Visto de esta manera parece prácticamente imposible escapar de las garras de los fabricantes de software malintencionados, pero no es necesariamente así, en nuestra calidad de usuario se puede evitar la infección del sistema por códigos malignos que utilizan esta vía de propagación, incluso si el producto antivirus no está preparado para reconocerlos.

Si bien en estos momentos no es nuestro interés hacer un análisis de un código maligno en particular, aspecto que reservamos para una próxima publicación, sí se desea realizar una serie de recomendaciones a los lectores, las cuales le servirán para evitar la infección de su sistema a través de los pendrive.

Es necesario que se conozca estrictamente el contenido del pendrive, para ello debe cerciorase que pueda ver a través del explorador de Windows todos los archivos,incluyendo los posibles ocultos y de sistema. En una instalación «por defecto», al igual que en el tema de la extensiones, estos no son mostrados al usuario. Para ver realmente el contenido de su pendrive tenga en cuenta las siguientes recomendaciones:

1. Desde la ventana principal de su pendrive acceda al menú Herramientas/Opciones de Carpeta y en la ficha Ver/Configuración avanzada: Seleccione *Mostrar todos los archivos y carpetas ocultos* y desmarque la casilla *Ocultar archivos protegidos del sistema operativo***.** Posteriormente presione el botón: Aplicar a todas las carpetas / Aplicar / Aceptar.

Si al realizar está acción se encontró en su pendrive archivos y carpetas que nunca guardó es casi seguro que estos sean códigos malignos o complementos de estos, por ejemplo: bibliotecas (.dll), autoejecutables (autorun.inf) etc. Puede eliminar con toda seguridad estos archivos pues excepto los pendriver de última generación (U3 y otros) que tienen software incluido, el resto no debe poseer otro software al introducido por usted.

El fichero **autorun.inf** es un caso particular, este tipo de fichero es ejecutado por Windows desde una unidad extraíble con solo introducirlo en el sistema. Este archivo tiene en su contenido indicar al sistema la ejecución automática de determinado software. Si bien el principio de creación de este archivo es ejecutar un software de manera automática, lo cual es muy utilizado para software de tipo multimedia, promocional, etc, los fabricantes de virus lo han utilizado para la ejecución de sus códigos malignos de manera automática e infectar el sistema si este no está protegido por un antivirus o si el antivirus no está actualizado para dicho código.

Por tanto, una forma de detener la infección automática por códigos malignos que aprovechan esta particularidad puede resolverse con solo indicar al sistema que no reproduzca de manera automática archivos **autorun.inf**. Pero, ¿es posible?, ¿cómo?

Sí es posible. Para detener la ejecución automática de ficheros **autorun.inf** y así evitar la infección por virus que aprovechan esta característica siga las siguientes instrucciones.

1. En el menú *Inicio* opción *Ejecutar* teclee: **gpedit.msc**

En el árbol de consola que se muestra siga la siguiente secuencia:

Configuración del equipo/Plantillas administrativas/Sistema/Desactivar reproducción automática**.** Haga clic en botón de opción: *Habilitada* y en la lista desplegable *Desactivar reproducción automática en***:** Todas las unidades/ Aplicar/Aceptar.

Ahora su PC no se infectará por virus de esta naturaleza

¿Funciona el antivirus?

No existe un antivirus perfecto ni un fin para los virus. Si usted preguntara a un médico si pretende acabar con los virus que afectan a los seres vivos que cree que le respondería; le diría que es imposible, porque si incluso se acabaran los que aparecen de forma natural siempre a nivel de laboratorio se pudieran crear más y más e incluso modificar los conocidos; qué decir entonces de los virus informáticos que no se forman de manera natural, sino que son creados y modificados al antojo del hombre y que además se ponen a disposición de todos en su código fuente, a través de internet, para que quien lo desee con un mínimo de conocimientos informáticos pueda modificarlos y obtener nuevas versiones.

No se debe dejar a la casualidad el trabajo del antivirus, pues este no siempre estará actualizado ciento por ciento, cuestión que es del todo normal, ya que primero surgen los virus y después se agrega su modo de desinfección a las bases antivirales y, por supuesto, en este espacio aparecen «víctimas». Un aspecto determinante es que el antivirus esté controlando toda la información que se almacene o transite por nuestro sistema. Este proceder del antivirus se conoce como *Protección en tiempo real* (Realtime protection), es el proceso «transparente al usuario» mediante el cual el producto antivirus antes de mostrar, por ejemplo: un programa, documento, etc, que ha solicitado el

usuario, lo chequea en busca de código maligno. Se dice que este proceso es «transparente al usuario» porque realmente el usuario no se percata qué está ocurriendo

Para comprobar que su antivirus está controlando todas las operaciones de su sistema se pone a su disposición este pequeño código que, a pesar de ser identificado como virus, es un contenido benigno, es una prueba o test para verificar la protección en tiempo real.

Para realizar la prueba siga las siguientes instrucciones:

1. Copie para un fichero de texto vacío la siguiente cadena de caracteres, teniendo cuidado de omitir alguno o agregar espacios en blanco.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

2. Guárdelo con cualquier nombre y trate después de abrirlo, si su antivirus sea cual fuera está realmente trabajando lo detectará como el virus Eicar.

Si bien es necesario disponer de un conjunto de privilegios en un sistema para poder efectuar las operaciones anteriormente descritas, en otras palabras ser administrador del equipo, está en todo su derecho de exigir a los «privilegiados» que el sistema al cual usted accede sea configurado de forma que responda a su seguridad. Si usted fue capaz de comprender lo que este trabajo quiere hacerle llegar ya es uno más de aquellos a los cuales se le ha encendido la llama.

BIBLIOGRAFÍA

BELLO R., ALFONSO I. *Elementos teórico-prácticos útiles para conocer los virus informáticos* Disponible en: http://bvs.sld.cu/revistas/aci/vol11_5_03/aci04503.htm Acceso: 10 de septiembre del 2007.

BENAVIDES, J. «Historia de los sistemas operativos», en Revista *GIGA* No1, 2002.

GLADIS, E. «Virus altamente destructivo: Win95.CIH», en Revista *GIGA* No 2,1999.

MÁRQUEZ, G « Ojo con el doble clic y los virus», en Revista *GIGA,* No 3, 2001.

MASHEVSKY, Y. «Bestiario virtual», *Miscelánea de virus informáticos* (№8, septiembre de 2007). Disponible en: http://www.viruslist.com/sp/analysis?pubid=207270950 Acceso: 27 de septiembre del 2007.

Moreno, A. *Conozca los distintos antivirus*. Disponible en: http://www.vsantivirus.com/am-conozcaav.htm Acceso: 10 de septiembre del 2007.