Conciencia Tecnológica
ISSN: 1405-5597
contec@mail.ita.mx
Instituto Tecnológico de Aguascalientes
México

Correa Medina, Juan Gabriel; Carlos Pérez, Héctor de Jesús; Velarde Martínez, Apolinar
Virus informáticos
Conciencia Tecnológica, núm. 31, enero-junio, 2006, pp. 54-57
Instituto Tecnológico de Aguascalientes
Aguascalientes, México

Conciencia Tecnológica No. 31, Enero-Junio 2006

Virus Informáticos

Nota de Divulgación

M.C. Juan Gabriel Correa Medina [1], Lic. Héctor de Jesús Carlos Pérez [2], M.C. Apolinar Velarde Martínez [2]
(1) Colaborador del Cuerpo Académico de Sistemas Distribuidos del Instituto Tecnológico de Aguascalientes Departamento de Sistemas de Información de la Universidad Autónoma de Aguascalientes, Av. Universidad #940, Cd. Universitaria Aguascalientes, Ags.Tel. (449) 9108417 C.P. 20100, gabriel_correa@yahoo.com.mx
(2) Miembro del Cuerpo Académico de Sistemas Distribuidos del Instituto Tecnológico de Aguascalientes Departamento de Sistemas y Computación del Instituto Tecnológico de Aguascalientes, Av. A. López Mateos 1801, Fracc. Bonagens, Aguascalientes, Ags., C.P. 20256 Tel. (449) 9105002, Fax (449) 9700423, hjcarlos@hotmail.com, avelarde@ita.mx

Resumen

Cada día que transcurre, la computadora se vuelve una herramienta indispensable. Inherentemente, la consecuencia lógica esperada, es que hay cada vez mas usuarios, los cuales ya comienzan a ser conscientes de los beneficios de utilizar dicha herramienta, pero, ¿serán conscientes de los riesgos de utilizarla, cómo son los virus informáticos?, y si conocen el riesgo, ¿qué tan informados están sobre la variedad de éstos?

Palabras clave

Virus informático, infección, estado de latencia, estado activo.

Introducción

Podría decirse que el fenómeno de los virus informáticos (en lo posterior, referidos solo como virus) en nuestro país, pasó de ser un "problema técnico" a un problema popular, a partir de las elecciones presidenciales de 1994, cuando aparece el virus *Natas* alterando el proceso de conteo del IFE. Por aquel entonces, para muchos el fenómeno era desconocido y para otros tantos representó la aparición de una "nueva amenaza tecnológica". Lo cierto es que dicha problemática ya existía desde hacía varios años.

A la fecha, cada vez es más común que un usuario normal u ocasional ya no desconozca sobre el tema y tenga que aprender a convivir con él, puesto que al transcurso del tiempo, la computadora ha invadido e impuesto su presencia en escenarios como la educación, la investigación y la vida en el hogar, por mencionar sólo algunos ejemplos.

Incluso, para muchos usuarios es normal culpar a los virus informáticos de daños y/o contratiempos ocasionados a su trabajo, desestimando su participación en su situación particular, cuando en realidad existe la probabilidad de que el usuario sea el culpable de daños ocasionados a sus propios archivos y hardware, buscando con esto expiar su responsabilidad. Aunque por otro lado, no se puede abandonar la posibilidad, de daños realmente causados por virus, los cuales son cada vez más poderosos al paso del tiempo.

Si bien, el problema puede verse aumentado por la visión y desconocimiento que el usuario tenga sobre los virus, es importante informar a la sociedad en general, sobre lo que son, cómo surgieron y por qué surgieron, lo cual es el tema principal de este artículo, como una forma de convivir con el problema que está latente cuando se utiliza una computadora [1].

¿Qué es un virus informático?

Etimológicamente, la palabra *virus* procede del latín y significa veneno. Técnicamente hablando, un virus es un programa (software) que cumple con al menos una función básica, la *reproducción autónoma* (infección), para asegurar de esta manera su supervivencia. Dicha supervivencia puede llevarse a cabo en dos formas básicas distintas: en *estado de latencia*, es decir, se encuentra almacenado en dispositivos de almacenamiento secundario, como discos flexibles por ejemplo, pero sin implicar que está en posesión de recursos de la computadora; y, un *estado activo*, donde previamente le ha sido posible apoderarse de recursos, tanto del sistema operativo como de ciertos elementos de hardware de una computadora en particular, y de esta forma "infectar" a otros dispositivos, ya sean computadoras u otras unidades de almacenamiento. De esta manera, es claro que se necesita un huésped que albergue al virus.

Adicionalmente, se ha hablado de que los virus poseen otra característica adicional, aunque ésta no siempre es indispensable, y esa es la de *causar daño* a la información y/o hardware. Pues en el transcurso del tiempo, han existido virus que sólo muestran un mensaje con una finalidad especifica, aunque se faltaría a la verdad si no se expresa que los hay (y habrá) tan dañinos como el Chernobyl, que fue capaz de causar estragos en discos duros hasta el grado de

quedar inservibles para uso, aunque la información en un alto porcentaje de los casos pudiese recuperarse.

¿De dónde surgen los virus?

Los virus no surgieron de la nada, o así como así. Al ser software, debe existir un programador, quien es una persona que debe tener conocimientos amplios y bastos sobre temas relacionados con el hardware y un lenguaje de programación en particular, éste último puede ser un lenguaje de bajo nivel como el lenguaje ensamblador o un lenguaje de alto nivel como el lenguaje C, aunque a últimas fechas ha devenido en el uso de lenguajes script, como es el caso de Visual Basic para Aplicaciones (VBA) que acompaña al Office de Microsoft.

Debido a que existen infinidad de programadores de virus en la actualidad, los virus no son iguales entre sí, por lo que el comportamiento, la infección y el objetivo y/o alcance de ataque es diverso en la mayoría de los casos. De ahí la enorme cantidad de virus que existen en la actualidad, al menos los conocidos.

¿Por qué surgen los virus?

Está quizá es la pregunta más difícil de contestar, pues existan tan amplias y diversas razones que han argumentado tanto especialistas como creadores de virus, unas escépticas y otras hasta absurdas. Pero desde un punto de vista técnico y filosófico, solo nos recuerda que todas las cosas construidas por el hombre tienen vulnerabilidades y sólo es cuestión de tiempo, el descubrir cómo violar la frontera de la protección, y de esta manera crear caos y miedo.

Cabe resaltar, que recientemente, la creación de virus se ha vuelto también un problema de seguridad pública, pues nuestros datos pueden ser “secuestrados” y por ende recibir una petición de rescate. Parece absurda esta noticia, pero ya existen grupos criminales o mafias que se dedican a contratar a especialistas en el área con dicha finalidad. En realidad ésta es una de tantas facetas de la mafia “informatizada” por llamarla de alguna manera.

Aunque en algunos otros casos, se han debido a investigaciones formales, con la finalidad de demostrar la seguridad implementada en lenguajes script (también conocidos de lenguajes de macros) como es el caso de Office, con el primer virus de macro (macrovirus) llamado Concept, que apareció en 1995 y que era operable en el Microsoft Word versión 6.

Clasificación de los virus

Desde los inicios hasta la fecha, la clasificación de los virus se ha basado en características funcionales que han innovado cada uno de los virus. Tales características que se han considerado, frecuentemente suelen ser su forma de infección, su peligrosidad, técnicas de protección y entorno de trabajo.

Una condición necesaria para la latencia y reproducción es tener tanto memoria principal (RAM) como memoria auxiliar (discos flexibles, discos duros y otro tipo de unidades de almacenamiento).

Básicamente existen virus *residentes en memoria* o simplemente virus *TSR*, los cuales están activos en la computadora y tienen cierto nivel de control sobre ésta, es decir, mientras esté encendida.

Los virus *no residentes en memoria* o virus *NTSR*, sólo permanecen en memoria el tiempo indispensable para su infección. No se apropian de recursos adicionales hasta que llegue el tiempo de activar algún suceso en particular, como puede ser mostrar un simple mensaje o hasta formatear un disco duro.

El medio que proporciona la supervivencia a los virus frecuentemente suelen ser los archivos en disco y los discos propiamente. De esta manera se tienen virus *infectores de archivos*, los cuales pueden ser ejecutables o en documentos. El primer caso implica que el virus está oculto en un archivo ejecutable, y al momento de poner en ejecución dicho programa, éste buscará a otros programas ejecutables (archivos cuya extensión es COM, EXE, SYS y DLL, por ejemplo) para su infección. Su forma de infección era incluirse dentro de dicho programa.

Cabe señalar que surgió una variación de este tipo de archivos conocida como virus *acompañante*. Los cuales no infectaban directamente los programas y eran exclusivos de programas cuya extensión fuese EXE. Su forma de infección consiste en crear otro archivo con el mismo nombre que el archivo con extensión EXE, pero con una extensión COM. De esta forma, cuando el usuario deseaba ejecutar el programa (sin incluir la extensión) el primer archivo en ejecutarse era el del virus (archivo con extensión COM) y éste terminada su ejecución, pasaba el control del programa al otro archivo con extensión EXE. Esta propiedad de priorizar la ejecución de programas era exclusiva del sistema operativo MS DOS, por lo que está técnica ha quedado obsoleta en los sistemas MS WINDOWS.

En el segundo de los casos, los virus están albergados en documentos. Estos documentos dependen de otras aplicaciones (como el caso del Office de Microsoft) que proporcionen un lenguaje de macros. De esta manera, al abrir un documento infectado, éste buscará a otros documentos que estén en uso, para infectarlos o activar alguna función de destrucción especifica. A este tipo se le suele denominar virus de macro o simplemente *macrovirus*.

En el caso de virus que infectan a los discos, el virus que ha sobrevivido desde MS DOS, es el virus de *arranque* o *boot*. Estos virus se caracterizan por ser de

tamaño pequeño, pues se almacenan en un sector especial de un disco flexible, el *boot record*. El boot record es un sector donde se almacena una estructura de datos denominada BPB (BIOS Parameter Block) la cual contiene información referente a atributos del disco como el formato y sistema de archivos que soporta el medio; y un programa cargador de inicio del sistema operativo denominado *IPL* (Initial Program Loader).

Tal vez en alguna ocasión habrá observado un mensaje similar al siguiente:

Disco sin sistema reemplace y presione una tecla

Generalmente esto sucede debido a que usted ha introducido un diskette en su unidad de 3 ½" y encendido del CPU de su computadora. Lo que significa que la computadora debe buscar el sector de arranque y cargar el programa para comenzar a preparar el sistema operativo, y al no encontrarlo, el mismo programa le avisa que el disco en cuestión no tiene sistema operativo.

Esta característica de cargar el sistema operativo en cualquier PC, sigue existiendo a la fecha, lo que ha posibilitado que este tipo de virus sigan existiendo, pues se intenta cargar el sistema operativo, pero el virus aprovecha para establecerse en memoria RAM y desde ahí verificar que cualquier disco que sea leído, si no está infectado, a partir de ese momento lo estará. De ahí, que tanto discos flexibles (diskettes) y discos duros puedan ser infectados con este tipo ataque.

Una variación de este tipo de técnica y que es exclusiva de discos duros, son los virus *MBR*. El MBR (Master Boot Record) es un sector especial del disco duro, que es leído primeramente por la PC, para establecer los límites de dicho disco. Esto posibilita que un disco duro funcione como si se tuviesen instalados varios discos duros, es decir, permite que un disco duro *sea particionado*, o seccionado y que cada sección funcione como un disco duro independiente. Una vez reconocidos el o los disco(s) duro(s), se prosigue con la ejecución del IPL encontrado en el boot sector del disco y la forma de propagarse es similar a la del virus de arranque.

Tanto en discos flexibles como en discos duros existe un conjunto de sectores consecutivos llamados *directorio*, los cuales contienen un registro de los archivos (*entrada de directorio*) disponibles, cuyos datos generalmente suelen ser el nombre y extensión del archivo, el tamaño, la fecha y hora de creación, atributos, así como el sector donde inicia cada archivo. Teniendo esto en mente, un virus puede alojarse en otros sectores que puede registrar como dañados o para uso del sistema operativo, y redireccionar hacia su código (en el sector del disco propiamente) cada entrada a un archivo ejecutable y almacenar la entrada original en otro sector del disco. De esta manera, al ejecutar un programa, este ejecutará primero el código del virus y éste habiendo finalizado su ejecución, redirige la ejecución al código ejecutable original. A este tipo de virus se le conoce como virus de *directorio*.

Si bien, ésta es una técnica que fue algo novedosa, también lo era muy peligrosa, pues en algunos casos, la lectura de discos infectados en distintas versiones del mismo sistema operativo (MS DOS por ejemplo) no permitía la correcta ejecución del programa y en casos extremos un daño físico al disco debido a la constante lectura repetitiva sobre el sector en particular del disco por parte de la unidad de disco (drive). Por otra parte, el virus dependía en gran medida del sistema de archivos que era implementado por el sistema operativo. Cuestión que hizo que los programadores de virus abandonasen esta forma de infección.

De los tipos de virus anteriores se han derivado algunos otros, como los virus *bipartitas*, los cuales enlazan la característica de infectar tanto archivos como sectores de arranque. Un caso similar, lo conforman los virus *multipartitas*, los cuales tienen la capacidad de infectar tanto el MBR, el sector de arranque y archivos ejecutables.

Con la aparición de Internet y la oferta de servicios como el Chat y el correo electrónico, surgieron nuevos especimenes, entre los que destacaron en su tiempo fueron los virus *mIRC*. Estos virus sólo funcionaban bajo programas cliente IRC, cuya uso principal recaía en el Chat e intercambio de archivos. De hecho, estos virus estaban codificados en el lenguaje script del propio cliente, y una de sus características principales era el envío masivo de un archivo script de configuración del cliente IRC a una lista enorme de destinatarios, lo cual provocaba que el sistema se congestionara a tal grado que la computadora se bloqueaba. Otra de sus funciones consistía en robar passwords.

Los virus de *email* hacen su aparición aprovechando las capacidades del Visual Basic Script (VBS) que se incluye con el cliente de correo Microsoft Outlook. Éste lenguaje script se puede fusionar con otros como es el caso de JavaScript (JS) y Windows Scripting Host (WSH), este último creado en equivalencia de los archivos por lote de MS DOS (archivos con extensión BAT). Siendo el más celebre el virus *I Love You*.

De esta forma, al llegar un mensaje con código viral, el cliente automáticamente puede ejecutar ciertas acciones, entre estas, el envío masivo de correos electrónicos según la lista de contactos con que cuente el Outlook. Dentro de este tipo de virus teóricamente podían albergar otros códigos de virus cuyas formas de infección ya se han comentado con anterioridad.

Tradicionalmente, tenían una característica especial y particular, consiste en que su diseño e implementación estaban en función directa del sistema operativo, así el parásito aseguraba su correcto funcionamiento. Con esto se quiere decir, que un virus diseñado para un sistema operativo como Windows, no podría en la mayoría de los casos, ejecutarse en Linux, por ejemplo. La parte que no se descarta, se debe al uso de programas emuladores de sistemas operativos. Dichos programas "imitan" a otro sistema operativo, con respecto al soporte en la ejecución de programas, aunque de está forma el virus tendría una seria limitación al momento de su reproducción.

Dentro de un contexto particular, esto evitó que la mayoría de virus diseñados para MS DOS fuesen funcionales y que sólo los virus infectores de arranque sobreviviesen al cambio en sistemas operativos.

Otro claro ejemplo de esto, es que los virus de directorio, no lograron la supervivencia en MS DOS, debido a que el manejo y administración del sistema de archivos cambió, particularmente entre las versiones 5 y 6.

Adicionalmente, también dependen del microprocesador de la computadora en cuestión, esto refuerza la dependencia inclusive del sistema operativo. Esto se debe a que cada microprocesador define un conjunto de instrucciones particular, aun entre diversos modelos de un mismo fabricante. Concretamente, un virus escrito en lenguaje ensamblador para un microprocesador Intel (propio de las PC) no podría ejecutarse de manera adecuada en un microprocesador Motorota (predominante en computadoras Apple).

A últimas fechas, se han realizado experimentos de virus *interplataforma*, lo que ha llevado a fracaso en éste ámbito de acción, pero se ha podido comprobar que un virus escrito para un microprocesador Intel, puede ejecutarse tanto en Windows como en Linux, pero no en un microprocesador distinto.

Conclusiones

Es importante hacer notar que el conocimiento de la diversidad de los virus a menudo ayuda a "reparar" o "corregir" el riesgo que cualquier usuario puede tener en un momento determinado, es decir, según el tipo de virus, existen diferentes formas de erradicación, aunque en la mayoría de los casos esto suele ser transparente para el usuario de un producto antivirus comercial.

También, es necesario remarcar que la amenaza continuará en los años por venir, con la aparición de nuevas técnicas de infección y de nuevas variantes para algunos virus ya conocidos, contando con la adaptabilidad que los autores de virus respecto a las nuevas tecnologías de software y hardware, como son los teléfonos celulares o los PDA. Esto dependerá de las motivaciones psicológicas de personas (o grupos de éstas) que decidan crearlos.

Es necesario aclarar, que existen virus para casi todas las variedades de computadoras (PC o compatibles, Apple, Atari, Commodore, etc.) y es un hecho parcialmente conocido que se puede atribuir a la popularidad de la PC de IBM y al sistema operativo MS DOS en su momento. Esto implica una incompatibilidad para que un espécimen de "cierta computadora" pase a otro "tipo de computadora", debido principalmente a el microprocesador empleado en cada tipo y a la arquitectura particular de cada rubro de computadoras.

Referencias

[1] Correa, J. G., (1998), *Antivirus Mexicano para DOS*, Tesis de Licenciatura en Informática, Instituto Tecnológico de Aguascalientes.

Agradecimientos. Queremos agradecer al *Cuerpo Académico de Sistemas Distribuidos* del Instituto Tecnológico de Aguascalientes por brindar todos los recursos necesarios para llevar a cabo el desarrollo de este trabajo.