LOS PROGRAMAS "VIRUS"

*Adolfo Ortiz Sedano**
*Víctor Campos Campos***

Resumen

Los programas "virus" son un tema de actualidad en los centros de cómputo mexicanos. Hay quienes opinan que pueden ser muy dañinos, otros dicen que son inofensivos. Aquí presentamos el resumen de nuestra experiencia con un programa de este tipo. Cómo se presentó, el impacto que causó y los recursos que se han utilizado para eliminarlo.

Introducción

En una plática entre clase y clase un maestro comentó haber leído un artículo en una revista extranjera acerca de un programa que se encuentra entre los "programas de uso común" que la mayoría de los usuarios adquiere a menudo como obsequio de alguien que a su vez lo adquirió por el mismo medio. Este programa –comentaba el maestro– fue creado por los fabricantes de *software* (programas, *paquetes* y lenguajes), que al no poder evitar la copia no autorizada de sus productos idearon un programa que daña la información en las unidades de almacenamiento (*diskettes* y discos duros).

El comentario nos pareció digno de crédito pero lo pensamos como algo ajeno a nuestro ambiente computacional.

De esto hace casi un año. Después nos enteramos, por algunos medios de comunicación, de noticias parecidas, pero en donde se mencionaban consecuencias alarmantes al grado que caían en lo absurdo. Esto en lugar de alertarnos vino a aumentar nuestra incredulidad.

A principios de agosto, al realizar diversas actividades en las computadoras del Centro de Cómputo de la Unidad de Economía y Estadística, los usuarios observaron la aparición de una pelotita, que al igual que en los juegos electrónicos de ping-pong rebotaba entre los caracteres y los bordes del monitor. Pero ¡oh sorpresa!, al revisar el contenido de los discos, algunos de sus archivos habían sido dañados.

* Integrante del Laboratorio de Asesoría Informática, Investigación y Desarrollo (LAIID) de la Facultad de Estadística e Informática de la U. V.

** Integrante del Laboratorio de Asesoría Informática, Investigación y Desarrollo (LAIID) de la Facultad de Estadística e Informática de la U. V.

Algunos usuarios, al notar la frecuencia de la situación anterior, revisaron los *diskettes* y encontraron en todos ellos la indicación de un sector dañado, que al examinarlo contenía el mensaje:

"Dos-Virus (v. 2.0) 21/10/87"

En ese momento la noticia se tomó a broma, pero al observar que el problema continuaba y que en algunos casos los usuarios tenían dañados todos sus *diskettes* (de 10 a 20), decidieron tomar medidas y la primera fue suspender el servicio en el Centro de Cómputo mientras no se determinara la gravedad del problema.

Avances

A continuación se reseña el trabajo que hemos realizado, esperando sea de utilidad para quienes tengan o deseen enfrentarse a los programas "virus".

Existen más de cuarenta programas "virus" diferentes por lo que, para realizar una investigación más a fondo, decidimos dividir el problema en las siguientes tareas:

I. Localizar el programa "virus".
II. Determinar cómo se recibe el programa "virus".
III. Establecer cómo y cuándo se propaga y ocasiona daños el programa "virus".
IV. Reparar los discos dañados.
V. Prevenir el daño en las unidades de almacenamiento.

Para determinar y realizar estas tareas recurrimos a artículos publicados en diversas revistas, pruebas en discos dañados y entrevistas a personas enteradas. Los resultados de nuestras indagaciones y las acciones que realizamos se resumen en los siguientes puntos:

1. El programa "virus" se encuentra generalmente en el sistema operativo; esto es, en los archivos "command.com", "bio.com" y "dos.com", y en el "boot" o en las "fats" (*file allocations table*), que son áreas necesarias para poder utilizar unidades de almacenamiento.

2. El programa "virus" no se encuentra agregado a un programa ejecutable.

3. El programa se recibe por medio de *paquetes computacionales piratas*, y se copia a los lugares antes mencionados, al utilizar algún comando del sistema operativo de uso frecuente, por ejemplo *DIR* (listar el contenido del directorio), *LOAD* y *SAVE* (realizar alguna lectura o escritura a las unidades de almacenamiento.)

4. El programa se propaga cuando en una sesión de computadora se utilizan archivos de *diskettes* sin programa "virus" junto a archivos de *diskettes* que sí lo contengan.

5. Al utilizar un *diskette* con el programa "virus" se copia un área de memoria de la computadora llamada *TRS (terminate and stay resident)* la cual permite utilizar los programas allí residentes sin necesidad de volver a introducir el *diskette* con el archivo original.

6. El programa se propaga de la misma forma en que se recibe, es decir, al utilizar algún comando del sistema operativo de uso frecuente.

7. Es importante señalar que los *diskettes* dañados no siempre contienen al programa "virus". Por lo tanto para salvar la información, ésta se debe copiar a otro *diskette*, teniendo siempre el cuidado de no copiar las áreas en donde reside el "virus".

8. Los *diskettes* dañados se pueden volver a utilizar, siempre y cuando sean "formateados" nuevamente para borrar todas las áreas en donde se pueda encontrar el programa "virus" y aquéllas que estén marcadas como dañadas.

9. Para evitar que nuevas unidades de almacenamiento sean dañadas se han creado programas que envían mensajes al programador cada vez que se intenta hacer una copia a dicha unidad o al *TRS*. Estos programas se conocen con el nombre de "vacunas" y son muy variados en su funcionamiento y en su precio (nosotros tenemos uno que es de distribución gratuita).

10. Otro tipo de programas llamados "antídotos" tiene como función localizar el programa "virus", borrarlo y en su lugar copiarse él mismo, para luego reproducirse de la misma manera que el programa "virus".