MITOS Y REALIDADES DE LOS VIRUS INFORMÁTICOS

Johnny A. Tamayo Arias[1], Alonso Tamayo Alzate[2]

P.C: virus, antivirus, detección, prevención.

RESUMEN

Con el surgir de la informática también han hecho presencia nuevas amenazas, convirtiéndose los virus informáticos en un problema que nos aqueja a todos los usuarios de los equipos de computación, entorpeciendo nuestra labor diaria y desencadenando incertidumbre y zozobra. Desde la primera aparición su crecimiento ha sido sorprendente, prestándose mucho al sensacionalismo y la desinformación, por eso se hace necesario conocer sobre su forma de actuar para poderlos prevenir, detectar y eliminar oportunamente.

ABSTRACT

With arising of the computer science they have also made presence new threats, becoming the virus computer specialist a problem that it suffers us to all the users of the calculation teams, hindering our daily work and unchaining uncertainty and it keels. From the first appearance their growth has been surprising, being lent a lot to the sensationalism and the disinformation, for that reason it becomes necessary to know on its form of acting to be able to them to prevent, to detect and to eliminate appropriately.

---

1 Doctorando Ingeniería de Proyectos. Universidad Politécnica de Catalunya. Barcelona.

2 Profesor Asociado. Depto. Informática y Computación. Universidad Nacional de Colombia. Sede Manizales.

Introducción

No existe información exacta sobre el origen de los virus informáticos, algunos autores señalan que el padre de la computación John Von Newmann escribió en su libro Theory and Organization of Complicated automata(Teoría y organización de autómatas complejos) en 1949, varios programas que se autoreproducían, concepto que sirvió de base para la elaboración de los virus. En 1983, el Dr. Fred Cohen presentó los primeros virus residentes en una computadora personal a los que bautizó Trojan Horses y Worms (Caballos de Troya y Gusanos respectivamente), por lo cual se le conoce como el Padre de los Virus Informáticos. De todas maneras se considera que los virus informáticos han sido desarrollados por programadores irresponsables desubicados laboral y socialmente.

Virus Informáticos. Definición.

Un virus electrónico es básicamente una alteración de la información que consiste en un pequeño programa, generalmente escrito en lenguajes de bajo nivel (ensambladores), que ha sido desarrollado con el propósito de realizar acciones generalmente nocivas que alteran el desempeño normal de la computadora, modificando los programas ejecutables a los que contamina consiguiendo así una ejecución parasitaria, es decir, siempre necesitará de otro programa para poder existir y se activa de forma involuntaria por el usuario cuando ejecuta el programa contaminado y presenta como característica básica la autoejecución y reproducción; generalmente están diseñados para copiarse la mayor cantidad de veces posible, bien sobre el mismo programa ya infectado o sobre otros todavía no contaminados, ocasionando daños a los demás programas residentes en el sistema. Es así como la infección puede propagarse de una computadora a otra a través de los mismos usuarios cuando éstos intercambian disketes o discos o envían archivos por medio de la red, o adquieren software de dudosa procedencia.

Es importanter señalar que los archivos de datos y el correo electrónico no se contagian de virus, pero si los archivos adjuntos infectados enviados por algunos usuarios que al ser "bajados" de la red transmitirán el contagio. En la actualidd los virus informáticos afectan tanto a los archivos ejecutables de extensión .EXE y .COM, así como a los procesadores de texto y hojas de cálculo.

En la actuación de un virus se pueden diferenciar tres fases:

- ***El contagio.*** Se realiza cuando el programa contaminado pasa a la memoria del computador y el sistema se ejecuta tomando el control del mismo, después de intentar inicializar el sistema con un disco o con el sector de arranque infectado o al ejecutar un archivo infectado. El programa funciona aparentemente con normalidad, de esta forma el usuario no se da cuenta que su sistema está siendo infectado. Los medios por los que puede producirse la infección del sistema son: a través de las copias ilegales o "piratas"; llevando disquetes a lugares públicos donde se realicen trabajos tales como digitación, impresión gráfica, prácticas de estudio, etc; intercambio de disquetes entre diferentes equipos de una misma entidad sin haberlos revisado previamente con un buen antivirus; redes de computadoras y cualquier otro medio de transmisión de información. Los disquetes se constituyen actualmente en el medio de contagio más extendido; éstos disquetes contaminantes suelen contener programas de fácil y libre circulación y carecen de toda garantía; es el caso de los programas de dominio público, las copias ilegales de los programas comerciales, juegos, etc.

- ***La activación.*** Se produce cuando el virus toma el control del sistema y despliega todo su potencial destructivo realizando actividades no deseadas que pueden causar daños a los datos y/o a los programas, a la vez que deja ejecutar normalmente los programas. Lo primero que suele hacer el virus es cargarse en la memoria del computador residenciándose y modificando determinadas variables del sistema, así el virus queda a la espera de que se cumplan ciertos condicionamientos que varían de unos virus a otros para replicarse o atacar. Algunos virus se activan después de ocurrir un cierto número de ejecuciones de un programa infectado o de encender el sistema operativo; otros simplemente esperan a que se escriba el nombre de un archivo o de un programa. La mayoría de los virus se activan mediante el reloj del sistema tras comprobar la fecha o mediante el cumplimiento de determinada condición previamente concebida.

- ***El ataque.*** Los virus comprueban si determinada condición se ha cumplido para atacar mientras que se van copiando en otros programas. Es importante tener en cuenta que los virus son diseñados con la intención de no ser descubiertos por el usuario y generalmente no lo son hasta que se produce el daño con la consiguiente pérdida de información o pueden ser inofensivos como el despliegue de ciertos mensajes que, aunque molestos, no representan daños graves.

Síntomas de la existencia de virus

Para detectar el contagio de algún virus informático se debe observar detenidamente el funcionamiento habitual del equipo de cómputo. El comportamiento de los virus es

bastante errático, cada uno de ellos realiza acciones diferentes, por lo que son difíciles de detectar. Muchos virus pueden permanecer en la computadora sin activarse por largos períodos de tiempo.

Algunos síntomas que pueden indicar la existencia de virus son:

- Problemas en la iniciación del equipo(booteo).
- Menor memoria disponible a la habitual.
- Destrucción del directorio y/o de la tabla de localización de archivos Fat de los discos fijos.
- Destrucción de la tabla de particiones de los discos fijos.
- Aumento injustificado del tamaño de los archivos ejecutables.
- Demoras excesivas en los accesos al disco.
- Aparición en la pantalla de mensajes, gráficas y/o caracteres no justificados con o sin bloqueo parcial o total del funcionamiento del equipo.
- Desaparición de programas y archivos sin que exista causa justificada.
- Al correr el programa CHKDSK, da menos de 655.360 bytes de memoria total.
- Alteración del funcionamiento de programas ejecutables.
- Interrupción inexplicada de algunos procesos.

En todo caso la mejor forma de salir de dudas sobre el origen del problema, es hacer una revisión del sistema con un programa que busque la existencia de virus en la memoria y en todas las unidades de disco.

¿Cómo se clasifican los virus informáticos?

Según el Dr. Fred Cohen, en 1987 clasificó a los virus informáticos en dos grupos:

Virus Informáticos Benignos. Consiste en un pequeño programa residente en memoria que realiza una broma informática sin consecuencias importantes y son fácilmente controlables, por ejemplo sonidos, alarmas, despliegue por pantalla de algún mensaje amenazante, etc., pero no va más allá, quedando todo en un simple pánico.

Virus Informáticos Malignos. Se les culpa de generar importantes desastres en los archivos y/o sistemas. Dañan la pista de arranque incluyendo el sector y deteriorando archivos, además pueden formatear el disco duro; a esta clasificación pertenecen la gran mayoría de virus que existen en la actualidad.

John MacAfee y asociados, clasifica los virus de acuerdo al lugar donde atacan y al daño que producen, así:

Lugar donde se ubican o atacan:

- Tabla de partición del disco fijo.
- Sector de carga inicial de los discos fijos.
- Sector de carga inicial de discos flexibles.
- Programas overlay.
- Programas ejecutables con extensión .EXE o .COM
- Programa COMMAND.COM del sistema operativo
- Los que se instalan a sí mismo en memoria.
- Los que se auto-encriptan.
- Los que usan técnicas de bloqueo.

Por el tipo de daño que producen:

- Sobre - escribe o borra archivos o programas.
- Corrompe o borra el sector de carga inicial o BOOT.
- Corrompe datos en archivos
- Formatea o borra todo / parte del disco.
- Directa o indirectamente corrompe la relación de los archivos.
- Afecta el sistema tiempo- operación.
- Corrompe programas o archivos relacionados.

La clasificación de los virus en donde concuerdan la gran mayoría de los expertos es: los de sector de arranque: obviamente son aquellos que modifican el sector de arranque reemplazándolo por su propia versión, de tal forma que cuando arranca el sistema les permite cargarse en memoria y tomar el control de la computadora; y los de programa, que infectan los archivos ejecutables tomando el control y residenciándose en la memoria.

Programas antivirales - vacunas

Hay numerosos programas que realizan la función de detectar virus en un sistema y consiste en aquellos programas que tienen como función proteger nuestro sistema de computación del ataque inesperado de un virus, cumpliendo la tarea de eliminarlo; actúan de manera similar a las vacunas biológicas, con el agravante que todos los días aparecen nuevos virus informáticos y/o mutaciones de los ya existentes, para lo cual es necesario desarrollar nuevas vacunas que estén en capacidad de combatirlos; según parece, este es un proceso de nunca acabar.

Los antivirus vacunan los programas colocando en ellos la etiqueta que caracteriza al virus, de tal forma que al ingresar un virus y comparar su propia etiqueta con la que está colocada en el programa a ser contaminado, crea que éste ya está contaminado y desiste de hacerlo.

El antivirus se encarga de buscar, encontrar y eliminar los virus informáticos que existen en la computadora y se compone fundamentalmente de dos partes: un programa que rastrea (SCAN), si en los dispositivos de almacenamiento se encuentra alojado algún virus, el programa revisa primero en la memoria RAM, y luego en todas las unidades de almacenamiento, directorio por directorio, archivo por archivo, la existencia de virus conocidos y otro programa que desinfecta (CLEAN) a la computadora del virus detectado. En caso de encontrar algún virus, el programa produce un mensaje señalando el directorio, nombre del archivo infectado y nombre del virus detectado, procediendo luego a destruir el virus parásito. En algunas ocasiones el programa queda dañado, por lo que no volverá a correr.

No se debe creer que para estar libre de infecciones basta sólo con un antivirus, también es necesario que los usuarios entiendan que, además de mantener actualizados los antivirus, deben utilizar de forma segura su computadora, no abriendo archivos no solicitados, haciendo back-ups de los archivos dé datos, revisando el disco duro

con programas detectores, etc, como una de las primeras defensas contra los virus, además de disponer de los antivirus actualizados.

En el transcurso en que el virus comienza a infectar y es detectado por los antivirus, muchos usuarios pueden haber sido infectados, y haber sufrido los efectos del virus, sin que el producto que utilizan para defenderse de ellos lo haya percibido oportunamente, lo que demuestra la debilidad que tienen muchos de estos productos para la detección de virus; lo que implica que los antivirus como se conocen actualmente tienen varios puntos débiles que se deben mejorar a fin de brindar realmente esa protección imbatible contra los virus que tanto promocionan pero que no siempre cumplen.

Plan de prevención

Se debe desarrollar un plan para tratar con los virus, antes de que éstos ocasionen un serio problema, el cual debe considerar los siguientes aspectos:

- No permitir a ningún funcionario que introduzca software para ser utilizado en los equipos de la empresa sin que se encuentre debidamente probado como libre de contaminación.
- Mantener respaldos(back - ups) de programas y datos. Se debe guardar copia de todos los back - ups en lugares distantes al centro de informática, en instalaciones de alta seguridad.
- Se debe sacar back - up del sistema operativo mínimo cada dos meses o en su defecto cada que se presente un cambio de release o actualización del mismo. Los back - ups se deben guardar en lugares distantes al centro de informática y en instalaciones de alta seguridad.
- Controlar y limitar el acceso de personas no autorizadas a las computadoras, limitando la operación del equipo computacional solo a los operadores acreditados, debido a razones obvias de seguridad.
- Los disketes, cintas, discos u otros medios de almacenamiento deben estar etiquetados, tanto interna como externamente, para evitar confusiones y facilitar su identificación.
- Se debe responsabilizar la custodia de la cintoteca a un funcionario del centro de informática, que no tenga que ver con la operación del equipo.
- Se debe tener un estricto control sobre el préstamo y transporte de discos y/o cintas de la sala de cómputo al lugar de almacenamiento distante.

- Se debe capacitar al personal del centro de informática para la aplicación de controles y procedimientos de seguridad.
- Las aplicaciones sistematizadas deben estar totalmente documentadas por escrito y se debe optar como norma la permanente revisión de la documentación.
- La seguridad del centro de informática se debe asignar a una persona del mismo centro que recibe generalmente el nombre de oficial de seguridad o administrador de seguridad.
- Se debe diseñar un plan de contingencias y ponerlo en marcha lo más pronto posible, de tal manera que incluya convenios con otras entidades o instituciones que posean equipos con características similares, para que sirvan de respaldo en caso de presentarse una eventualidad. Así mismo se debe asignar al personal responsable de darlo a conocer a todos los funcionarios del centro de informática y adiestrarlos en su funcionamiento.

Conclusión

Toda organización debe evaluar su vulnerabilidad ante ésta amenaza y tomar las medidas necesarias para minimizar los riesgos; aunque la presencia de virus informáticos no debe acarrear pánico, tampoco se le debe restar importancia al hecho desconociéndolo. Una forma óptima de evitar el contagio consiste en no ejecutar programas o no arrancar el sistema con disketes que hayan sido usados en otras computadoras. El uso de software antiviral es útil, pero solo si es actualizado frecuentemente, lo importante en este caso es tratar de evitar por todos los medios posibles que ocurran infecciones por virus.

Debemos aprender a convivir con este mal, ya que entró a formar parte de la cultura informática y la mejor manera para combatir todos aquellos enemigos del uso adecuado y eficiente de la información es la prevención; pero es imposible prever cuanta situación se pueda presentar en un momento dado, por lo tanto es necesario estar siempre expectantes.

BIBLIOGRAFÍA

LOPEZ, Saucedo, José. Los virus informáticos. Unam
Instituto Nacional de estadística e informática. INEI. Perú.
SBAMPATO, M. Ignacio. Debilidades en los antivirus. DIARIORED.COM