

## **¿Qué es un virus informático?**

### **Los Virus Informáticos, una "Peste Electrónica"**

Los virus informáticos, que reciben ese nombre debido a la forma en que se desarrollan y transmiten de computadora a computadora, comparable al modo en que lo hace un virus biológico, no son en realidad otra cosa que pequeños programas desarrollados por un programador. Estos virus se propagan ocultos en los disquetes, o entre los datos de una transmisión a distancia (como ser la red Internet) e infectan los equipos de computación en el momento de ser leídos estos datos. Desde allí se reproducen, atacan y "contagian" al copiar datos de la máquina infectada en otra máquina. Algunos virus provocan la simple aparición de mensajes en la pantalla, pero otros destruyen la información contenida en el disco rígido o impiden el acceso a ella.

Existen miles de estos virus, la gran mayoría de ellos catalogados, y con fechas de activación distintas. La fecha de ataque del virus Michelangelo, por ejemplo, es el 6 de Marzo; otros virus, en cambio, se activan apenas ingresados al sistema. Muchos se alojan en la memoria al momento de encender el equipo, lo que hace mucho más dificultosa su detección. Algunos actúan repentinamente. Otros, en cambio, producen daños progresivos.

### **Como han surgido los virus a lo largo de su historia y su cronología .**

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en la década de 1950 en los Laboratorios Bell, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él.

En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término de "virus" para describir un programa informático que se reproduce a sí mismo. En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos.

El virus llamado Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infectador rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

Los virus tienen la misma edad que las computadoras. Ya en 1949 John Von Neumann, describió programas que se reproducen a sí mismos en su libro "Teoría y Organización de Autómatas Complicados". Es hasta mucho después

que se les comienza a llamar como virus. La característica de auto-reproducción y mutación de estos programas, que las hace parecidas a las de los virus biológicos, parece ser el origen del nombre con que hoy los conocemos.

Antes de la explosión de la micro computación se decía muy poco de ellos. Por un lado, la computación era secreto de unos pocos. Por otro lado, las entidades gubernamentales, científicas o militares, que vieron sus equipos atacados por virus, se quedaron muy calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaron millones, al bolsillo de los contribuyentes. Las empresa privadas como Bancos, o grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Lo que se sabe de los virus desde 1949 hasta 1989, es muy poco.

Se reconoce como antecedente de los virus actuales, un juego creado por programadores de la empresa AT&T, que desarrollaron la primera versión del sistema operativo Unix en los años 60. Para entretenerse, y como parte de sus investigaciones, desarrollaron un juego llamado "Core Wars", que tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa tenía instrucciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento. Al mismo tiempo, desarrollaron un programa llamado "Reeper", que destruía las copias hechas por Core Wars. Un antivirus o antibiótico, como hoy se los conoce. Conscientes de lo peligroso del juego, decidieron mantenerlo en secreto, y no hablar más del tema. No se sabe si esta decisión fue por iniciativa propia, o por órdenes superiores.

En el año 1983, el Dr. Ken Thomson, uno de los programadores de AT&T, que trabajó en la creación de "Core Wars", rompe el silencio acordado, y da a conocer la existencia del programa, con detalles de su estructura.

La Revista Scientific American a comienzos de 1984, publica la información completa sobre esos programas, con guías para la creación de virus. Es el punto de partida de la vida pública de estos programas, y naturalmente de su difusión sin control, en las computadoras personales.

Por esa misma fecha, 1984, el Dr. Fred Cohen hace una demostración en la Universidad de California, presentando un virus informático residente en una PC. Al Dr. Cohen se le conoce hoy día, como "el padre de los virus". Paralelamente aparece en muchas PCs un virus, con un nombre similar a Core Wars, escrito en Small-C por un tal Kevin Bjorke, que luego lo cede a dominio público. ¡La cosa comienza a ponerse caliente!

El primer virus destructor y dañino plenamente identificado que infecta muchas PC's aparece en 1986. Fue creado en la ciudad de Lahore, Paquistán, y se le conoce con el nombre de BRAIN. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Supercalc o Wordstar, por suma bajísimas. Los turistas que visitaban Paquistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20,000 computadoras.

Los códigos del virus Brain fueron alterados en los EE.UU., por otros programadores, dando origen a muchas versiones de ese virus, cada una de ellas peor que la precedente. Hasta la fecha nadie estaba tomando en serio el fenómeno, que comenzaba a ser bastante molesto y peligroso.

En 1987, los sistemas de Correo Electrónico de la IBM, fueron invadidos por un virus que enviaba mensajes navideños, y que se multiplicaba rápidamente. Ello ocasionó que los discos duros se llenaran de archivos de origen viral, y el sistema se fue haciendo lento, hasta llegar a paralizarse por mas de tres días.

La cosa había llegado demasiado lejos y el Big Blue puso de inmediato a trabajar en los virus su Centro de Investigación Thomas J. Watson, de Yorktown Heights, NI.

Las investigaciones del Centro T. J. Watson sobre virus, son puestas en el dominio público por medio de Reportes de Investigación, editados periódicamente, para beneficio de investigadores y usuarios.

El virus Jerusalem, según se dice creado por la Organización de Liberación Palestina, es detectado en la Universidad Hebrea de Jerusalem a comienzos de 1988. El virus estaba destinado a aparece el 13 de Mayo de 1988, fecha del 40 aniversario de la existencia de Palestina como nación. Una interesante faceta del terrorismo, que ahora se vuelca hacia la destrucción de los sistemas de cómputo, por medio de programas que destruyen a otros programas.

El 2 de Noviembre del '88, dos importantes redes de EE.UU. se ven afectadas seriamente por virus introducidos en ellas. Mas 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados se ven atacados.

Por 1989 la cantidad de virus detectados en diferentes lugares sobrepasan los 100, y la epidemia comienza a crear situaciones graves. Entre las medidas que se toma, para tratar de detener el avance de los virus, es llevar a los tribunales a Robert Moris Jr. acusado de ser el creador de un virus que infectó a computadoras del gobierno y empresas privadas. Al parecer, este muchacho conoció el programa Core Wars, creado en la AT&T, y lo difundió entre sus amigos. Ellos se encargaron de diseminarlo por diferentes medios a redes y equipos. Al juicio se le dio gran publicidad, pero no detuvo a los creadores de virus.

La cantidad de virus que circula en la actualidad no puede llegar a ser precisada pero para tener una idea los últimos antivirus pueden identificar alrededor de cincuenta mil virus (claro que en este valor están incluidos los clones de un mismo virus).

Es importante señalar que la palabra "Virus" es un vocablo latín y su equivalencia a nuestro lenguaje actual es "veneno".

La Teoría y Organización de un Autómata Complicado (1949) de John Von Neumann, uno de los primeros miembros de la comunidad informática y padre

del modelo actual de computadoras, presentó con esta teoría el modelo de programa de un virus, explicando que los programas de los computadores se podían multiplicar, nadie pensó en ese momento la repercusión que tendría esta teoría en un futuro no muy lejano.

Diez años más tarde, en la atmósfera enrarecida de los laboratorios AT&T Bell, tres jóvenes programadores desarrollaron un juego denominado "Core-Wars".

Estos jóvenes genios, Douglas McIlroy, Victor Vysotsky y Robert Morris, comprendieron magníficamente el funcionamiento interno de los computadores. "Core-Wars", consistía en una batalla mano a mano entre los códigos de dos programadores, cada programador desarrollaba un conjunto de programas que se reproducían, llamados Organismos. Tras el tiro de salida, cada jugador soltaba sus Organismos en la memoria del computador. Los Organismos de cada uno trataban de destruir a los del oponente y el jugador que mantuviera mayor número de supervivientes al finalizar el juego era declarado ganador.

Los jóvenes genios como buenos empleados, al finalizar borraban los juegos y se iban a casa.

El concepto de juego se difundió por otros centros de alta tecnología, como el Instituto de Tecnología de Massachusetts (MIT) o el Centro de Investigación de Xerox en Palo Alto, California.

Cuando se jugaba al Core-Wars en una sola máquina, podía pararse y no se corría el riesgo de que se propagara. Esto se realizó no mucho antes de que el fenómeno que hoy conocemos como "conectividad" facilitara las comunicaciones entre computadoras. El fantasma de un juego divertido que se volviera perjudicial y se multiplicara entre las máquinas interconectadas rondó por sus cabezas.

El juego Core-Wars fue un secreto guardado por sus jugadores hasta 1983. Ken Thompson, el brillante programador que escribió la versión original en UNIX, lo develó a la opinión pública. Cuando Thompson recibió uno de los más altos honores de la industria, el premio A.M. Turing, su discurso de aceptación contenía una receta para desarrollar virus. Thompson contó todo sobre Core-Wars y animó a su audiencia a intentar practicar el concepto.

El número de Mayo de 1984 de la revista Scientific American (Científico Americano), incluyó un artículo describiendo Core-Wars y ofreció a los lectores la oportunidad de solicitar un conjunto de instrucciones para diversión y juegos en el hogar o la oficina.

En ese mismo año 1984, Fred Cohen expuso por primera vez por escrito, el concepto de virus informático, durante el desarrollo de una conferencia sobre seguridad.

El primer contagio masivo de microordenadores se dio en 1987 a través del MacMag Virus también llamado Peace Virus sobre ordenadores Macintosh. La historia, se describe a continuación:

Dos programadores, uno de Montreal, Richard Brandow, y el otro de Tucson, Drew Davison, crearon un virus y lo incluyeron en un disco de juegos que repartieron en una reunión de un club de usuarios. Uno de los asistentes, Marc Canter, consultor de Aldus Corporation, se llevó el disco a Chicago y contaminó su ordenador. Al realizar pruebas del paquete Aldus Freehand, contaminó el disco maestro el cual posteriormente devolvió a la empresa fabricante; allí la epidemia se extendió y el programa se comercializó con el virus incluido.

El virus era bastante benigno, el 2 de Marzo de 1988 (primer aniversario de la aparición del Macintosh II) hizo público en la pantalla un mensaje pidiendo la paz entre los pueblos, y se destruyó a sí mismo. Existe una versión de este virus detectada en alguna red de correo electrónico de IBM y al que se denomina IBM Christmas Card o Xmas, el cual felicita al usuario cada 25 de Diciembre.

Pero no todo fue felicitaciones y buenos deseos. El conocido virus Viernes 13 fue detectado por primera vez en la Universidad Hebrea de Jerusalén "casualmente" el primer Viernes 13 (13 de Mayo de 1988), era el cuarenta aniversario de la fundación del Estado Judío. El virus se difundió por la red de la Universidad e infectó ordenadores del ejército israelí, Ministerio de Educación, etc.

Aquí hay un caso más reciente. En 1987 un periodista de los Estados Unidos perdió la información de 6 meses de trabajo guardada en un disco, cuando trató de recuperarla se dio cuenta que era obra de un sabotaje. En el disco se encontraba el número telefónico de una tienda de computación pakistaní y el siguiente mensaje:

Bienvenidos al calabozo... llámenos para la vacuna.

La información había sido presa de un virus maligno. Investigando el caso se encontró que dicha tienda era Brain Computer Services y que vendía copias ilegales de algunos programas con un costo de cientos de dólares a sólo \$1.50 cada una (aproximadamente unos 1000 pesos chilenos). Durante 1986 y 1987, algunos de sus clientes fueron estudiantes estadounidenses atraídos por su bajo costo. Sin embargo, escondido en el disco había un virus; cada vez que el programa se ejecutaba, el virus contaminaba a la computadora y ésta a su vez, infectaba a los discos de otros usuarios. Los diseñadores son los hermanos Amjad y Basit Farooq Alvi, dueños de Brain Computer Services.

En 1985, se decidieron a hacer software, y para su desdicha, éste fue copiado y usado sin permiso. Así fue como a Amjad se le ocurrió hacer un programa que se autoduplicara, cuyo objetivo fuera infectar la computadora de un usuario desautorizado, forzándolo así a llamarles para reparar los daños. Al poco tiempo, tenían un virus que incluían en sus copias ilegales. Cuando un pakistaní deseaba una copia de un paquete se le vendía libre de virus, pero a los extranjeros se les vendían copias contaminadas.

Según declaraciones de los hermanos Alvi, en Pakistán, las leyes de derecho de autor no abarcan el software, por lo que vender software pirata no es ilegal. En cambio en EU, como en la mayor parte del mundo, es una práctica ilícita.

Ellos aseguran que dejaron de vender copias ilegales en 1987, pensando que los piratas ya debían haber tenido una lección.

Muy difundido también fue el caso de Robert Tappan Morris en Noviembre de 1988, el joven que contaminó (quizá sin ser su intención) la Red del Pentágono ARPAnet, paralizando gran número de computadoras estatales; los daños causados se calculaban en unos 80 millones de dólares.

Actualmente los virus son una de las principales causas de la pérdida de información en computadores. Sus propietarios deben estar invirtiendo cada vez más en los antivirus para la eliminación y erradicación de éstos, los antivirus no son nada más que programas especialmente diseñados para que batallen contra los virus, los identifiquen y posteriormente los eliminen.

Existe un incesante riesgo que corren hoy en día todos aquellos que se hacen partícipes de la red de redes (INTERNET), así sea por el mal uso que le dan algunos inescrupulosos al popular correo electrónico mediante el mail-bombing o sino por el solicitar de aquella red archivos, programas, fotos o todo lo que se pueda almacenar en nuestro disco maestro.

El primero consiste en recibir falsos correos electrónicos saludando o promocionando ciertos productos desconocidos, del cual el lector se hace partícipe sin saber que tras esto se oculta una verdadera amenaza de contagio para sus computadores. Y el segundo es adjuntar a los archivos de la INTERNET, programas especialmente diseñados para provocar errores en el huésped, es decir, añadirle un virus para que éste haga de las suyas con el computador que lo recibe.

### **Métodos de prevención**

Existen métodos de prevención, detección y, eventualmente, eliminación de los virus informáticos antes de que se activen. Como siempre, prevenir es mejor que curar, así que le recomendamos adoptar unas pocas pero seguras normas, como ser:

- Use software (programas) originales. No se deje tentar con programas de origen dudoso.
- Averigüe el origen de los datos que intercambie con otros usuarios. Nunca está de más ser precavido.
- Haga copias de respaldo de los datos importantes que tenga en su computadora.
- Tenga detectores y antivirus actualizados. Existen muchos económicos y seguros. Incluso hay antivirus que se pueden bajar de ciertas páginas en Internet, y son gratuitos.
- Ante el menor síntoma de problemas, consulte con un especialista.

Con el auge de Internet, se han agregado otras formas de contagio, por lo cual se recomienda estar alerta cuando está conectado a la red. Por ejemplo:

- Asegúrese del origen de un archivo que alguien quiere enviarle cuando esté "chateando".
- Baje archivos o programas de sitios seguros (su navegador puede "avisarle" cuando lo es)
- Cuidado con los archivos de Word o Excel que le envían adjuntos a los e-mail: Pueden contener virus de macros. Exija que usen antivirus aquellos con quienes intercambie archivos de este tipo usualmente.

Existen antivirus, incluso gratuitos como el F-Prot, que al instalarlos cargan aplicaciones que permanecen residentes y, a modo de escudo, le avisarán cuando le estén llegando por la red archivos infectados. Configúrelo para que impida el ingreso de un virus.

**Fuente de "Cómo han surgido los virus..." : Enciclopedia Encarta**

[© 2000 - Enrique A. Quagliano]

[www.recursos-pc.com.ar](http://www.recursos-pc.com.ar)