# VIRUS INFORMATICOS

## ¿Qué son los Virus informáticos?

Un virus informático es un **programa de computadora**, que tiene como objetivo causar una alteración en un sistema de cómputo. Al igual que otras amenazas, un virus informático puede causar la alteración total de programas e información, o comprometer su integridad. A diferencia de otras amenazas, un virus informático puede propagarse de programa en programa, de sistema en sistema, sin intervención premeditada de las personas.

El componente esencial de un virus informático es un **conjunto de instrucciones** (programa de computadora) las cuales, cuando se ejecutan, se propagan por si mismas a otros programas o archivos, no infectados.

Un virus informático típico ejecuta dos funciones:

- Se copia a sí mismo a un programa, no infectado.
- Ejecuta cualquier instrucción que el autor del virus incluyó en él. Las instrucciones las puede ejecutar en una fecha predeterminada, o luego de un número de ejecuciones. También lo puede hacer en forma alterna e imprevista (random). Dependiendo de los motivos que tuvo el autor para crearlo, las instrucciones de un virus pueden ser de cualquier tipo. Desde desplegar un inocente mensaje en la pantalla a borrar y/o alterar completamente la información almacenada en un medio magnético (disquete, disco fijo). En algunos casos, un virus puede contener instrucciones que no sean destructivas, pero puede causar daño al replicarse a sí mismo, utilizando recursos limitados del sistema, como espacio en discos, tiempo de la memoria principal o conexiones de una red.

Estos programas tienen algunas características muy especiales:

- Son muy pequeños.
- Casi nunca incluyen el nombre del autor, ni el registro o Copyright, ni la fecha de creación.
- Se reproducen a sí mismos.
- Toman el control o modifican otros programas.

A diferencia de los virus biológicos que causan resfriados y enfermedades en humanos, los virus informáticos no ocurren en forma natural, cada uno debe ser programado. No existen virus benéficos.

## Clasificación de los Virus informáticos

Los virus informáticos pueden ser clasificados por su comportamiento, origen, o tipo de archivo que atacan:

- **Virus de Macros/Código Fuente**. Se adjuntan a los programas Fuente de los usuarios y, a las macros utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hojas de Cálculo (Excel, Quattro, Lotus).
- **Virus Mutantes**. Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (NATAS o SATÁN, Miguel Angel, por mencionar algunos).
- **Gusanos**. Son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos.

- **Caballos de Troya**. Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.
- **Bombas de Tiempo**. Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que los contiene.
- **Autorreplicables**. Son los virus que realizan las funciones mas parecidas a los virus biológicos, ya que se autorreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programadas o cada determinado tiempo, contado a partir de su última ejecución, o simplemente al "sentir" que se les trata de detectar. Un ejemplo de estos es el virus del Viernes 13, que se ejecuta en esa fecha y se borra (junto con los programas infectados), evitando así ser detectado.
- **Infectores del área de carga inicial**. Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.
- **Infectores del sistema**. Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros que se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).
- **Infectores de programas ejecutables**. Estos son los virus más peligrosos, porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras). La infección se realiza al ejecutar el programa que contiene al virus, que en ese momento se posiciona en la memoria de la computadora y a partir de entonces infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos. Aunque la mayoría de estos virus ejecutables "marca" con un byte especial los programas infectados, para no volver a realizar el proceso en el mismo disco, algunos de ellos (como el de Jerusalén) se duplican tantas veces en el mismo programa y en el mismo disco, que llegan a saturar su capacidad de almacenamiento.

Una clasificación aceptada en la actualidad, es la que hace John MacAfee y Asociados; la cual divide los virus de acuerdo al lugar donde atacan, al daño que hacen:

- 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 Ejecutables con extensión EXE o COM.
- Programa COMMAND.COM del Sistema Operativo.
- Los que se instalan a sí mismo en la memoria de la computadora.
- Los que usan técnicas de bloqueo.

- Por el tipo de daño que producen:

- Sobre−escribe o borra archivos o programas.
- Corrompe o borra sector de carga inicial o BOOTeo.
- Corrompe datos en archivos.
- Formatea o borra todo/parte del disco.
- Directa o indirectamente corrompe relación de los archivos.

- Afecta sistema tiempo−operación.
- Corrompe programas o archivos relacionados.

Naturalmente hay virus que no solo caen en una, sino en varias clasificaciones. Entendiendo que existe mas de 54.000 virus identificados, y cada día aparecen nuevos virus, les ayudará a comprender la magnitud y complejidad de los problemas que se tendrá en el futuro con los virus. Un mismo virus puede ejecutar diferentes daños a diferentes partes de las unidades de almacenamiento, o archivos.

**Origen corriente de los Virus informáticos**

- Archivos recibidos vía e−mail, con archivo adjunto o no.
- Software introducido o usado en los sistemas por un extraño a la organización, y que tiene acceso a las computadoras.
- Software traído de su casa, por un empleado que tiene un sistema infectado, sin saberlo él.
- Software recibido (regalado o comprado) de alguna persona que tiene su computadora infectada.
- Software intencionalmente infectado por un empleado descontento o malicioso.
- Cualquier otro tipo de software (incluyendo Sistemas Operativos, Programas de Aplicación, Juegos, Utilidades, etc.), que se trae de fuera de la organización, de cualquier fuente externa.

**La historia de los virus**

**¿Cómo surgieron los virus?.**

No se sabe exactamente cuál fue el primer virus en la historia de las computadoras, aunque sí se sabe cuál fue posiblemente el primero en una computadora con sistema operativo.

Algunos llevan este comienzo a los primeros conceptos de programas autoreplicantes, o sea programas que se reproducen, los cuales se describen en el trabajo: "Theory and Organization of Complicated Automata" de John Von Newman, ya en el año de 1942. Pero claro, en ese tiempo las computadoras se programaban "con alambres" (literalmente), es decir los programas eran conexiones que se hacían entre las diversas partes electrónicas de la computadora. Hasta que precisamente John Von Newman creó el concepto de "programa almacenado", en el cual los programas y datos se almacenan juntos en la memoria del ordenador. Esto dio una gran flexibilidad a las grandes computadoras de entonces, pero al poder modificar las instrucciones surgió también la posibilidad de "sabotear" el código.

A finales de los años 50, en los laboratorios Bell, tres programadores, H. Douglas Mcllroy, Víctor Vysottsky y Robert Moris inventaron un juego llamado "Core Wars", el cuál consiste en elaborar "programas" para una computadora ficticia simulada. El objetivo es que los programas sobrevivan usando técnicas de ataque, ocultamiento y reproducción semejantes a los virus.

Enla década del 70, aparecieron otros programas del mismo tipo.

John Shoch y Jon Hupp, investigadores de Palo Alto Research Center (PARC) de Xerox aseguran que ya en 1970 habían elaborado programas con ciertas técnicas virales de reproducción. Aunque estos programas podrían ser considerados "virus buenos", ya que controlaban continuamente la "salud" de las redes.

A uno de ellos lo llamaron "el gusano vampiro" porque se escondía en la red y sólo se activaba en las noches para aprovechar las computadoras que no se estaban utilizando. También en 1970, en lo que eran los inicios de Internet, en ARPAnet la red militar y universitaria, un investigador

llamado Bob Thomas liberó un programa llamado 'Creeper' (rastrero), el cual se "arrastraba" por toda la red desplegando este mensaje: "Soy el 'Rastrero', atrápame si puedes!". Otro programador escribió otro "virus" llamado "Reaper" (segador) el cual se reproducía en la red "matando" Creepers. Esos primeros virus no causaban daño o destrucción, sólo eran experimentos sobre ideas curiosas de programas que generaban copias de sí mismos.

En 1981 apareció un programa para Apple II llamado "El Cloner" el cual se duplicaba escribiendo en la pantalla un pequeño verso. En 1982, también para microcomputadoras Apple II fue diseñado otro programa que estaba destinado solo a viajar y no a causar daños, y que fue denominado por su autor Jim Hauser, como un caminante electrónico (electronic hitchhicker) que se pegaba a programas sin ser detectado.

En 1983 Ken Thompson cuando recibía el premio A. M. Turing de A.C.M. (Asociation of Computing Machinery) en su discurso basado en el juego "Core Wars" instó a experimentar con esas pequeñas "criaturas lógicas".

Tal vez el primer virus, o al menos el primero en recibir esa denominación, fue ideado en noviembre de 1983. En un seminario sobre seguridad en computadoras a Fred Cohen se le ocurrió el experimento (en una minicomputadora VAX 11/750) de hacer un programa que "pudiera modificar otros para incluir una copia (posiblemente evolucionada) de si mismo".

En mayo de 1984, en la revista "Scientific American", A.K.Dewdney en su sección "Computer Recreations" describe el juego "Core Wars" con lo que le da amplia difusión. Varios lectores escriben sus experiencias al experimentar con programas de tipo virus. Uno de ellos comenta: "Nunca conseguí eliminar completamente esa peste electrónica"

En enero de 1986 aparece el virus "Brain", originario de Paquistán, el que es considerado el primer virus para PCs con sistema operativo MS−DOS. Al principio no causaba daño, sólo mostraba un mensaje de advertencia: "Bienvenido al calabozo. (c)1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES", luego la dirección y teléfono, y "Cuidado con este virus... Contáctenos para vacunarse...."

Comienza aquí la historia más reciente de los virus informáticos, la que continuaremos desarrollando en nuestra próxima entrega.

La literatura científica se anticipó tímidamente a la historia de los virus de computadoras. Cuando a finales de la década del sesenta, se realizaron tal vez los primeros ensayos de programas con el poder de "autoduplicarse" (basado en el concepto del matemático húngaro John von Neumann en los años cuarenta), los diseñadores John Shoch y Jon Hupp del PARC, tomaron su nombre de una novela de ciencia−ficción llamada "The Shockwave Rider", del escritor inglés John Brunner. En ella se hablaba de un programa que se reproducía hasta el infinito, y no podía ser eliminado. El programa se llamaba algo así como "tenia" (nombre común a diversos gusanos que se convierten en parásitos), y Shock y Hupp, denominaron a su primer "programa autoreplicante" como "gusano" (worm).

Ambos trabajaban para el Xerox's Research Center (PARC) de Palo Alto, y su principal idea era simplemente aliviar sus labores, con un programa que realizara tareas de mantenimiento automático a las más de cien computadoras que poseía la red informática del centro. Estas tareas consistían en copias de seguridad, diagnóstico, borrado de archivos en desuso, etc.

Sin embargo ocurrió algo que ni siquiera se imaginaron. El "gusano" iba a ser probado en principio solo en las computadoras de los propios creadores (en su laboratorio existían 6 de

ellas). Lo único que debería hacer esta primera versión de su programa era dejar una copia de si mismo en cada máquina, ya que no tenía incluido aún ninguna otra tarea específica. Sin embargo, al otro día los investigadores se encontraron con una alarmante sorpresa. El "gusano" no solo estaba en sus máquinas, sino que se había propagado por todas las máquinas de la red del PARC. Y lo que era peor, había crecido tanto que todas las máquinas estaban "colgadas" por falta de memoria. Al intentar reactivar el sistema, nuevamente el programa actuó por si mismo, y volvió a expanderse por toda la red. Sin preverlo habían sido víctimas de la primera infección de un "virus", o por lo menos de sus síntomas. Para eliminar el "gusano", debieron crear otro programa que lo borrara, inventando así el primer "antivirus" del mundo. El proyecto fue abandonado por no poder controlar la "infección".

¿Pero cuando se usó el término virus, relacionado con estos programas de computadora ?. Otra vez la novela de ciencia ficción parece adelantarse a la realidad. Emulando a otros grandes escritores que "vaticinaron" el futuro, como Julio Verne, David Gerrold creó en 1972 una novela llamada "When HARLIE was One" (Cuando HARLIE era uno). HARLIE (que significa "Equivalentes de Entrada de Vida Robótica Análoga a la Humana" en inglés) se trataba de una computadora capaz de duplicar las funciones del cerebro humano. También podía conectarse con otras computadoras e intercambiar datos vía telefónica. Y justamente, el programa que usaba para hacer este intercambio fue llamado "virus".

Corría el año 1985, cuando en la Universidad de California del Sur, en Estados Unidos, Fred Cohen desarrolló una tesis basada en programas "autoduplicadores", en la que aparece por primera vez la definición más moderna de los virus: "se trata de un programa que puede llegar a infectar a otros programas modificándolos de tal modo que incluyan una copia modificada de si mismos que puedan infectar a su vez a otros programas hasta el infinito". Pero Cohen preveía ya que esto también se convertiría en una gran amenaza para la seguridad informática, por el poder de destrucción implícito en estas acciones.

En si, la tesis no agregó nada nuevo, salvo el definir a estos programas autoreplicantes como virus, en clara analogía a los virus biológicos y a su poder de "infección" y "reproducción".

Basado en esta tesis, un año después, un ingeniero llamado Ralf Burger, creó un virus informático realmente operativo, al que llamó "Virdem" (por "demostración de virus", al menos era esa su "inocente" intención). "Virdem" estaba preparado para borrar gradualmente todos los archivos de la computadora huésped, causando su paulatina destrucción, pero solo luego que el mismo se hubiera reproducido en cuanto archivo encontrara. Tal vez se trató del primer virus que utilizó una de las principales características con las que hoy día los conocemos: la de reproducirse a si mismos para luego causar algún tipo de daño.

Ya corría 1986 cuando Burger participó en una convención anual realizada en Hamburgo, Alemania. Esta convención era organizada por el "Chaos Computer Club", una organización creada por un programador alemán (Herwert Wau Holland−Moritz) como pasatiempo. Según Holland, la razón del Club era extender la libertad de información y "traer luz al gran caos en las aplicaciones de las computadoras". El "Chaos Computer Club" reúne desde investigadores, hasta sociólogos que consideran a las computadoras como armas para los cambios sociales, pasando por simple fanáticos de juegos o aquello que solo quieren ganar dinero.

En el año que Burger participó (1986), poco se sabía de los virus informáticos, y los organizadores de la conferencia solo deseaban contribuir a la comprensión del problema ocasionado por los mismos. La idea de "programa dañino" fue insertada en el contexto de que su creación se debía principalmente a la "mala posición social de los programadores", expresándose que "el problema no son los virus, sino la dependencia de la tecnología". En la conferencia,

Burger distribuyó copias de su "Virsim" entre aquellos interesados en trabajar con "virus informáticos". Una novedad para muchos.

En 1987, el propio Burger escribió el primer libro que trató sobre los virus informáticos. Allí decía : "Los programas que viajan a lo que parece ser la velocidad de los electrones en movimiento, algunas veces en forma cómica, otras destructivos, y que son conocidos como virus, se han extendido por toda la comunidad informática mundial como plaga incontrolable". Sin embargo más adelante agregaba: "Hasta ahora no se han encontrado pruebas de un ataque de virus". Pero eso pronto iba a cambiar.

El 2 de noviembre de 1988, el caos cundió por la red ARPANET. Un "monstruo dañino" estaba comiéndose la memoria de cada computadora conectada a la misma, y hacían que funcionaran cada vez más despacio. A las tres horas todas las computadoras de costa a costa de los Estados Unidos estaban afectadas.

Pascal Chesnais del MIT de Massachusetts, descubrió que las copias del virus llegaban a través del correo electrónico. Un día después otro mensaje sobre el virus llegaba desde Harvard. Esta vez se explicaba como detener el ataque. Pero era tal el caos de la red, que el mismo no fue difundido a tiempo. Si alguien le hubiera prestado atención, hubieran descubierto la solución al problema, ya que el mensaje tenía que ver con el creador del programa dañino. Pero pasó desapercibido...

Mientras tanto, integrantes de la Universidad de Berkeley y del MIT de Massachusetts y de Pardue, intentaron trabajar en forma coordinada para capturar una copia del programa y analizarlo.

Descubrieron que no todas las computadoras eran afectadas, sino solo las Sun 3 y VAX con Unix y variantes del Unix2. En todas las computadoras afectadas aparecían mensajes nada comunes provenientes del gestor de correo electrónico (el Sendmail). Sin embargo el virus seguía pasando de computadora en computadora a una gran velocidad, reinfectándolas sucesivamente.

El 3 de noviembre en la madrugada, Gene Spafford de la Universidad de Purdue envió un mensaje avisando que todas sus computadoras Vaxen3 y algunas Sun se habían infectado y que "el virus hacía copias repetidas de si mismo mientras intenta propagarse, logrando que muchas veces las computadoras se queden sin espacio". El programa estaba aprovechando algunos defectos de la versión de la Universidad de Berkeley del sistema UNIX.

El Sendmail, el programa que enviaba el correo, era el culpable, ya que permitía que las instrucciones del correo electrónico fueran enviadas junto con los propios mensajes de computadora a computadora. En estas instrucciones viajaba el virus. El programa intentaba averiguar las claves de acceso (passwords) de otras computadoras, usando una rutina de búsqueda que permutaba los nombres de usuarios conocidos, una lista de los passwords más comunes y también búsqueda al azar.

Los técnicos de Berkeley crearon un parche para este error. Sin embargo a esta altura ya se sabía que el virus estaba hecho para reproducirse y propagarse y no causaba ningún otro daño a los datos.

Luego de divulgarse las formas de corregir el daño, se analizó el ataque, llegándose a la conclusión de que había sido premeditado. Se usó un programa que utilizaba defectos poco conocidos del sistema UNIX, estaba encriptado, y borraba su presencia luego de culminar su ataque.

Era el ataque del que fue llamado "Gusano de Internet", y la prensa cubrió el tema con frases como "el mayor asalto jamás realizado contra los sistemas de la nación".

Se calculó en más de 2.000 computadoras las realmente infectadas en Internet, y erradicarlo costó casi un millón de dólares, sumado a las pérdidas por haberse detenido casi toda la red.

El autor fue Robert Morris Jr, un graduado de Harvard de 23 años en ese entonces. Creó un programa con gran capacidad de reproducirse, pero sin embargo jamás pensó que se propagaría tan rápida y extensamente. El mismo calificó su "invento" como un "fallo catastrófico", su idea no era hacer que las computadoras se enlentecieran. Al parecer quería que el programa se copiara una vez en cada máquina, y luego se escondiera en la red.

Cuando se percató que su programa estaba propagándose por la red, pidió a un amigo (Andrew Sudduth) que enviara un correo electrónico pidiendo disculpas y las instrucciones para acabar con el programa. Pero en el caos que se originó, su mail, al que hacemos referencia más arriba, pasó desapercibido.

Morris fue acusado de acceder en forma intencional y sin autorización a computadoras "con intereses federales", impidiendo su uso y causando pérdidas de miles de dólares (aunque se especificaba 1.000 dólares, debido a que es la cifra mínima por ley para presentar una acusación). El cargo que aparece expuesto en una ley norteamericana de 1986 sobre Fraudes y Abusos informáticos, tiene como pena multas de un cuarto de millón de dólares y un mínimo de cinco años de cárcel. El juicio fue en enero de 1990, y aunque sus abogados aseguraban que Morris "intentaba ayudar a la seguridad de Internet cuando su programa se salió de su control por accidente", la fiscalía argumentó que el gusano "no se trató de un error, sino de un ataque contra el gobierno de los Estados Unidos".

Finalmente el 22 de enero, Morris fue declarado culpable por un jurado federal, lo que se convirtió en la primer condena por la ley de fraudes informáticos de 1986. Sin embargo, el juez del caso expresó que "no creía que los requisitos de la sentencia se daban en el caso del acusado", y por lo tanto las circunstancias no presentaban "fraude y engaño", por lo que lo sentenció a tres años de libertad condicional, una multa de 10.000 dólares y 400 horas de servicio as la comunidad.

Corría el año de 1987, cuando se tuvo noticias del primer caso de un "Caballo de Troya". Ello ocurrió en Alemania, y también tuvo mucho que ver el correo electrónico.

El día 9 de diciembre, varios estudiantes de la Universidad de Clausthal−Zellerfeld, recibieron en un mensaje de Navidad unas líneas de código de un programa informático. El mensaje los invitaba a ejecutarlo, y les deseaba "una Feliz Navidad y un Próspero Año Nuevo". Las instrucciones decían que debían teclear la palabra "Christmas" (Navidad en inglés) para disfrutarlo. Llevados por su curiosidad, los estudiantes hicieron lo que se les pedía. Solo vieron el dibujo de un gran árbol de Navidad y simplemente terminaron borrando el archivo.

Pero al volver a revisar su correo, se encontraron con más copias del mensaje, y lo mismo le sucedió al resto de los usuarios de la universidad.

No sospechaban que al ejecutar el programa que mostraba la imagen del árbol de Navidad, este programa también había leído las direcciones electrónicas de todos los estudiantes, guardadas en la computadora, y se había encargado también de enviar una copia de si mismo a cada uno de esas direcciones. De ese modo, cada vez que el programa se ejecutaba, podía generar entre cincuenta y cien copias o más de si mismo.

Pero el autor del programa (un desconocido estudiante) no había previsto que algunos usuarios poseían direcciones electrónicas externas que enlazaban la universidad con otros países, incluso con Estados Unidos. En este caso la red de Investigación Europea (EARNet), se enlazaba con BitNet, una red académica con más de 1300 sedes en EE.UU, y lo que era peor, con Vnet, la red de correo electrónico privado de IBM (las computadoras en la Universidad eran por supuesto de IBM en esa época), llegándose a conectar un total de más de 4000 computadoras.

El mensaje se distribuyó por toda esa red con su programa infeccioso. Los usuarios de IBM tenían más nombres en sus agendas, que los existentes en la universidad de Alemania donde se originó todo, por lo que a los 6 días de la primera infección, miles de mensajes y copias del archivo estaban dando la vuelta al mundo, llegando incluso al Japón, y terminando por paralizar a toda la red IBM.

El virus fue llamado por supuesto "Arbol de Navidad de IBM", pero como necesitaba la acción de un usuario para poder funcionar (se debía escribir la palabra "Christmas" para accionarlo), no se podía considerar exactamente como un virus. Y debido al disfraz que presentaba, se le ocurrió a alguien asociarlo con el famoso "Caballo de Troya".

Había nacido así el primer "Caballo de Troya" en la historia de los virus.

Al poco tiempo de la aparición del gusano de Internet, cuya historia mencionábamos en entregas anteriores, otro muy diferente apareció en la red de la NASA (SPAN, Space Physics Astronomy Network), y en las redes del departamento de energía de los EE.UU.

Se parecía al "Caballo de Troya" por su mensaje navideño, pero como el gusano de Arpanet, su objetivo eran los ordenadores VAX de Digital Equipment.

El gusano fue conocido como "Papá Noel" y dejó éste mensaje a los usuarios de la red en la noche del 24 de diciembre: "Hola como estás ?. He tenido mucho trabajo preparando todos los regalos, lo que no es tarea fácil, porque cada vez recibo más cartas... Ahora deja de trabajar en tu computadora y diviértete un poco en tu casa. Feliz Navidad y Próspero Año Nuevo... Tú Papá Noel".

Esto se consideraba una molestia, pero no causaba ningún otro daño más que el aparecer sin que fuera solicitado. Pero en 1989, la red SPAN volvió a ser infectada con una variante de este gusano, aunque en este caso, los usuarios descubrieron que la pantalla que debería aparecer al identificarse en su sistema, había sido sustituida por otra con un gran dibujo realizado alrededor de la palabra "Wank" y el siguiente mensaje: "GUSANOS CONTRA LOS ASESINOS NUCLEARES. Su sistema ha sido WANKeado oficialmente. Ustedes hablan mucho de la paz, pero después se preparan para la guerra".

Esto coincidió con una manifestación en contra del lanzamiento por parte de la NASA de un transbordador impulsado con energía nuclear.

Sin embargo este gusano (llamado "Gusano Wank"), se propagó mucho más lentamente, causando mucho menos daño que el que había causado el anterior gusano de Arpanet.

Así llegamos a los años 90. Ya no solo existían los virus, sino una completa variedad de gusanos, Caballos de Troya y bombas informáticas.

Al comienzo había sido un simple programa capaz de autoreproducirse, pero ya era una verdadera amenaza para el mundo informático.

Sin embargo, no fue hasta unos años después, cuando la aparición del "Michelangelo", un virus de sector de booteo que debía activarse un 23 de marzo, fecha del nacimiento del famoso artista, en que el manejo casi sensacionalista de la prensa, logró que mucha gente tomara conciencia de su peligrosidad, si no se tomaban las mínimas precauciones. Es que las historias de los "gusanos" y otros virus de Internet, tan lejanos para muchos aún, ya estaba en cualquier simple computadora, aunque aún no estuviera conectada a la red.

Y desde entonces la industria de los antivirus también tuvo su gran auge...

**Algunos virus**

**Icecubes − "Icecubes" simula buscar datos secretos en el sistema − 03/08/2000**

**EPOC − Virus para los ordenadores de mano. − 03/08/2000**

**Autocad2k\Star − Primer virus para AutoCAD 2000 − 19/07/2000**

**Timofónica − El i−worm "Timofónica" envía mensajes a móviles − 06/06/2000**

**W97M.Resume − Un curriculum vitae muy peligroso − 27/05/2000**

**VBS.NEWLove.A − Un nuevo gusano vuelve a causar la alerta − 21/05/2000**

**VBS.LoveLetter − Un gusano escrito en Visual Basic Script − 05/05/2000**

**Melting − El primer gusano "salvapantallas" − 08/03/2000**

**WebExt − Copia del "Plage" − 21/02/2000**

**Unicle − Copia del "BubbleBoy" − 18/02/2000**

**Plage − Nuevo i−worm español**

**The Fly − Una aparente broma electrónica**

**Babylonia − Un virus actualizable**

**Remote Explorer − Este virus es capaz de infectar una red entera**

**Deep Throat − Troyano desapercibido − 27/06/1999**

**Subseven 2.1 − Nueva versión de este troyano (altamente peligroso)**

**PrettyPark − Es una mezcla ente gusano y troyano**

**CIH − Es capaz de borrar la BIOS − 15/03/1999**

**Happy 99 − El primer gusano de E−Mail − 08/02/1999**