Carta a nuestros lectores

Cumpliendo la nueva política establecida por Chasqui de hablar del comportamiento de los medios en los sucesos de mayor importancia acaecidos en América Latina y el mundo, analizamos ahora los avances tecnológicos de comunicación que serán utilizados durante el campeonato mundial de fútbol en Corea del Sur y Japón.

Coherentes con esta política, tratamos de descubrir qué hay detrás de la aseveración del Presidente Hugo Chávez, respecto a la falta de profesionalismo de los medios de comunicación venezolanos, en la cobertura informativa que tiene que ver con las actividades del Gobierno. En la portada nos preguntábamos si se trataba de un golpe mediático o BUROCRÁTICO, para luego recoger en el título y cuerpo del artículo de Ted Cordova-Claure su respuesta que nos habla, más bien, de un golpe BRUTOCRÁTICO.

Como siempre, Eduardo Galeano nos ofrece un artículo incisivo y rico, en nuestra columna de Opinión, sobre la forma en la que actúa la maquinaria del poder para presentar la información de acuerdo a su peculiar conveniencia.

De importancia especial para la región andina es el problema de la guerrilla revolucionaria de Colombia y, por eso, Chasqui analiza la confusión semántica que impide un diálogo productivo entre los alzados en armas y el Gobierno, para lograr la tan deseada paz y evitar que sea estéril el derramamiento de sangre de más de un millón de muertos.

En España ha despertado sorpresivo interés el programa de televisión "Operación Triunfo", que marca un contraste -para muchos saludable- con otro programa de similar audiencia, pero manchado por el escándalo: "El Gran Hermano". Este programa parecería demostrar que es posible alcanzar altísimos niveles de sintonía sin recurrir a temas morbosos como es la costumbre de los "REALITY SHOWS" y los "TALK SHOWS", tristes alternativas que ya han sido objeto de nuestro análisis.

Finalmente, sin abandonar una vieja costumbre investigativa de nuestra revista, damos a conocer a nuestros lectores la imagen que la televisión española proyecta de América Latina.

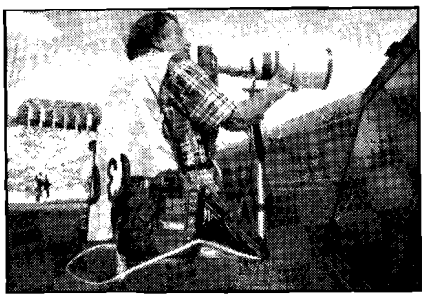
CHASQUI

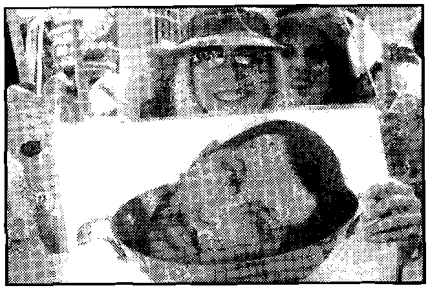
Revista Latinoamericana de Comunicación

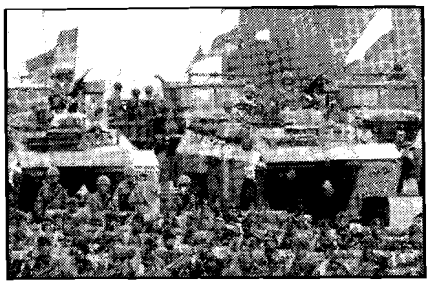
Chasqui

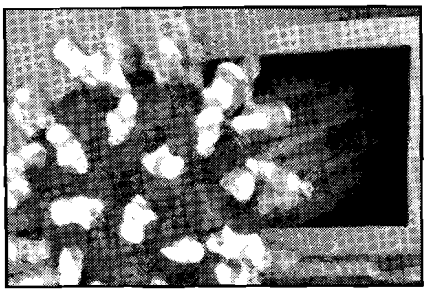
Nº 78 Junio 2002

Chasqui es una publicación de CIESPAL
Telf.: (593-2) 2506149 – 2544624
Fax (593-2) 2502487
e-mail: chasqui@ciespal.net
chasqui@ciespal.org.ec
web: www.ciespal.net
www.comunica.org/chasqui
Apartado 17-01-584
Quito – Ecuador
Registro M.I.T.,S.P.I.027
ISSN 13901079

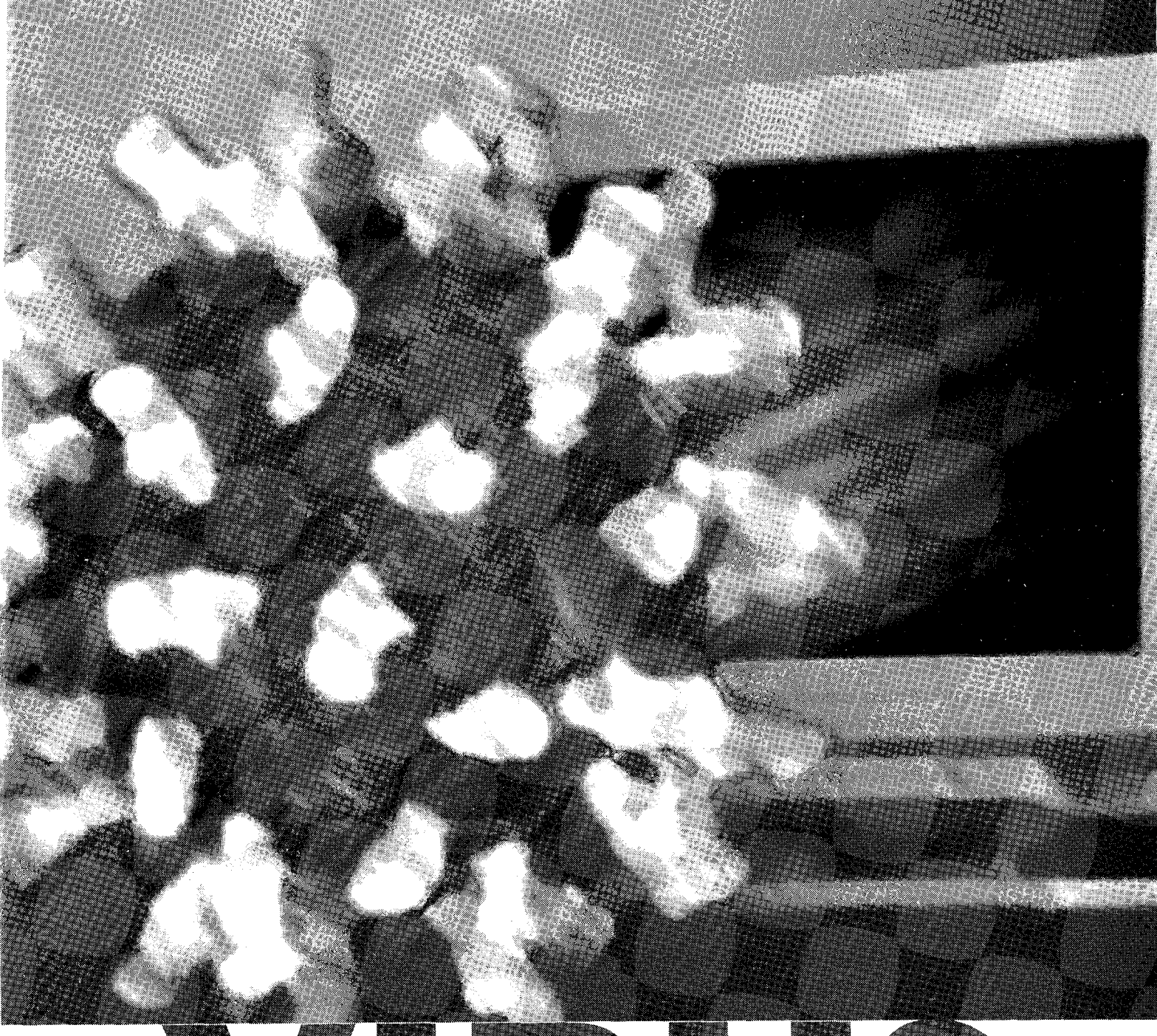








CIESPAL



VIRUS INFORMÁTICOS:

Entre el negocio y el temor

Francisco Ficarra ■

En nuestros días son muchos los medios de comunicación que hablan con términos tales como: Norton, McAfee, Panda, Caballo de Troya, gusanos, bombas lógicas, y un largo etcétera. Sin embargo, son muchas las personas que realmente empiezan a preocuparse de la seguridad del propio sistema, luego de padecer alguna mala experiencia del ataque de un virus. La categoría de los programas nocivos o también denominados "malware" incorpora a los mismos, en particular a los de tipo gusano y Caballo de Troya. A lo largo de estas líneas se pretende dar una primera panorámica del tema virus informáticos y todas sus derivaciones.

La vulnerabilidad de las redes

Los acontecimientos del mes de septiembre del 2001, en los Estados Unidos, abrieron la carrera de las inversiones en cuestiones de seguridad. Uno de los sectores que están viviendo una época de oro son las empresas de servicios y desarrollos de sistemas de seguridad informática, especialmente ante un eventual ataque a nivel internacional de virus informáticos.

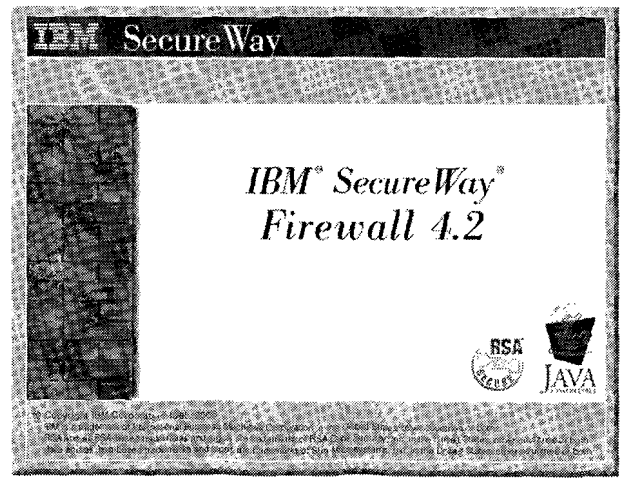
En nuestros días son vulnerables las redes Intranet e Internet, los datos almacenados, el software, la trasmisión de la información, etc. Por lo tanto, hay que preparar el sistema para evitar que los intrusos al sistema informático puedan causar daños (incluido entre ellos los programas o archivos portadores de virus). Existen varios mecanismos y metodologías de seguridad, en donde Europa está invirtiendo grandes sumas de dinero:

1. Muro anti-incendio (firewall).
2. Redes privadas virtuales.
3. Zonas desmilitarizadas.
4. Trampas.
5. Sistemas de escansión de la vulnerabilidad.
6. Criptografía.
7. Seguridad del correo electrónico.

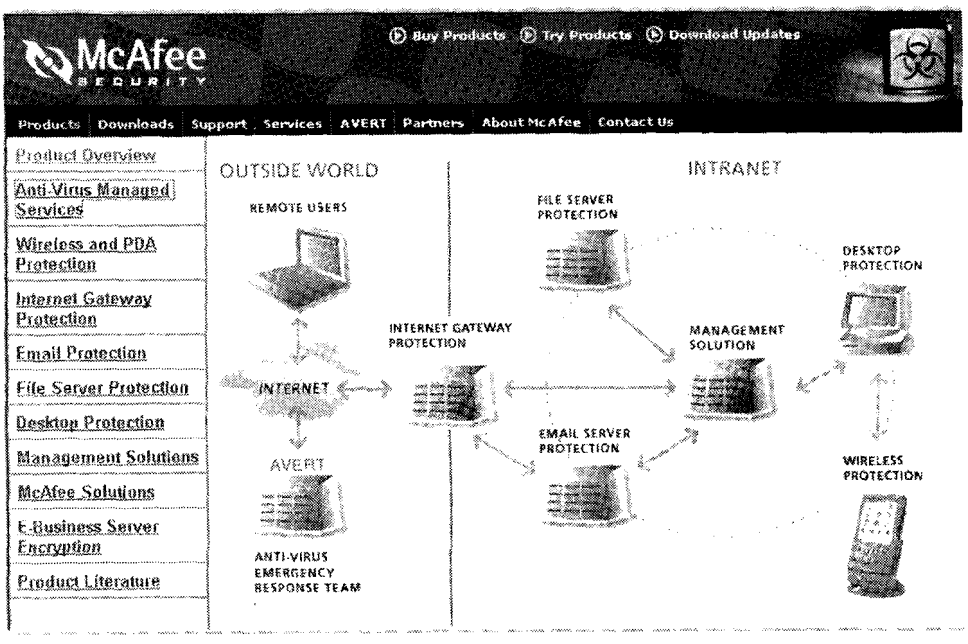
Sin entrar en detalles técnicos, todas las miradas apuntan al primero de ellos (firewall). El muro anti-incendio sirve para impedir el acceso a los extraños. El firewall representa el límite entre una red privada y una red pública. Sin embargo, es factible saltarse esta protección mediante el uso de datos ocultos pero autorizados. Dependerá del tipo, modelo y configuración del firewall para que la intromisión tenga lugar o no. El nombre firewall deriva de las viejas locomotoras a vapor que protegían el carbón o leña de la zona de la caldera.

En ciudades en donde el grado de informatización de las actividades equivale hasta más del 90%, un virus con un elevado poder destructivo podría causar cortes en el suministro eléctrico, agua, gas, etc. Acontecimientos de este tipo, sumados al rigor del invierno en muchos países del planeta, podrían ser de consecuencias nefastas para gran parte de la población.

Curiosamente, la última difusión a escala mundial del virus "Sircam" se produjo en los meses de vacaciones en el hemisferio norte (julio y agosto 2001). Un hecho que tomó desprevenidos a numerosas empresas de servicios técnicos de informática, porque el personal estaba disfrutando



Francisco V.C. Ficarra, italiano, profesor, periodista y escritor. Residente actualmente entre la costa mediterránea española y los Alpes italianos.
Corre-e: ficarra@ctv.es - f_ficarra@libero.it



de sus vacaciones anuales. Un sinfín de empresas tuvieron que parar la producción para erradicar definitivamente dicho virus de la red de computadoras. Hoy, ante la lección vivida, dichas empresas están optando incrementar los presupuestos en seguridad informática. El antecesor gran virus "I love you" en el año 2000 causó daños por un valor superior a los 9.000 millones de dólares estadounidense.

Una etimología y evolución poco saludable

El término virus hace referencia indirecta a la vida artificial (artificial life o alife) pero poco tiene que ver con las nuevas formas de vida biológica, creada en los laboratorios de genética en nuestros días. Este campo de estudio nació en 1987, cuando el biólogo Cristopher Langton organizó la primera conferencia sobre el tema en Los Álamos (EE.UU.).

Luego de reflexionar sobre preguntas tales como: ¿qué es la vida? ¿es factible realizar un programa que esté vivo?, se planteó la gran pregunta del tema que estamos tratando: ¿puede un programa en una computadora ser un ente vivo? A priori, sí; porque es capaz de replicarse a sí mismo y es capaz de realizar operaciones complejas.

La idea de desarrollar una cosa similar a un virus informático, pero sin ningún objetivo destructivo, es decir, dar vida a criaturas artificiales como un modo de desafío entre los programadores, nació en los centros de investigación de la AT&T Bell Lab. y en la Xerox Corporation. Fue a comienzos de 1970 cuando surgió en esos ámbitos la moda de jugar a la guerra de los núcleos (core wars), en la cual los participantes creaban organismos siempre más agresivos, con la finalidad de destruir a los generados por los adversarios.

En 1983 el Dr. Fred Cohen definió el término "virus informático". Es un programa que permite copiarse o replicarse y ha sido creado para cometer algunas acciones. Cuando un archivo es atacado por un virus, este incorpora sus propias líneas infectadas en las líneas del código del programa, por consiguiente, cada vez que se pone en marcha el programa o archivo infectado, el virus entra en acción. En pocas palabras, un virus se engancha a un fichero o archivo.

En sus orígenes, el atributo de autoreplicarse o autoreproducirse, no estaba todavía en capacidad de difundirse entre las computadoras conectadas a Intranet o Internet. Evidentemente, con el paso de los años, algunos programadores lograron este objetivo.

Tal es así que en 1984 la revista estadounidense "Scientific American" dio a conocer la existencia de los virus informáticos y los grados de peligros que ello implicaba. Fue en 1986 cuando se produjo el salto en las computadoras personales por medio de la BBS (bolletin board system), o sea, un tipo de banco de datos con el cual se intercambian mensajes y archivos de datos y/o programas. A partir de ese momento una visión diacrónica y escueta es la siguiente:

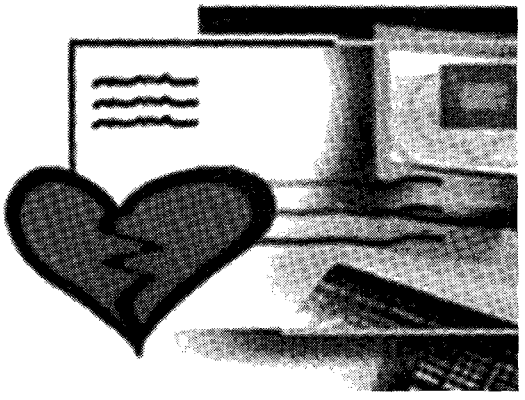
• 1986. Los hermanos Alvi en Pakistán crean un programa llamado "Brian". Este fue el primer virus que infectaba el sector de autoarranque de los clásicos floppy de 5" (cinco pulgadas y un cuarto). Para tal fin recurría al uso del método Stealth. Se trataba pues, de un programa que adjuntaba el propio código ejecutable en otras aplicaciones. De

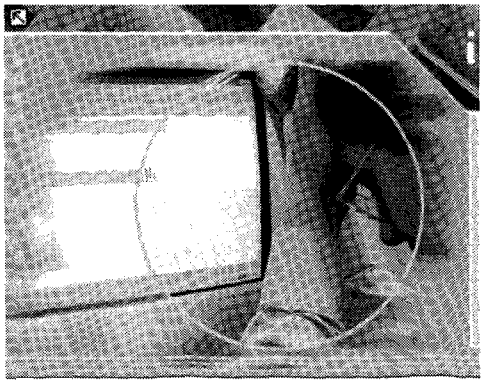
esta manera, cada programa infectado tenía la facultad de duplicarse a su vez. A finales de 1986, nacía el virus "Stoned" que dañaba definitivamente el sistema operativo, motivo por el cual se perdía toda la información almacenada en los archivos, como los programas.

• 1988. Se presenta el primer programa Antivirus.

• 1989. Nace el virus "Dark avenger" que causa un daño lento en el sistema operativo. Ese mismo año IBM comercializa el primer programa antivirus y "oficialmente" se pone en marche la carrera de un gran negocio, con una bonanza comercial a partir del siglo XXI.

• 1990. Surgen los primeros virus poliformes, es decir, mutantes, capaces de autoreproducirse y generar una copia diferente a la anterior. Consecuentemente, detectar estos virus es casi imposible.





• 1992. Hace la aparición "Micheangelo" que en la misma fecha del nacimiento del artista italiano infecta parte del disco duro.

• 1995. La legislación británica lleva a la cárcel al autor del virus "Pathongen" durante 18 meses.

• 1999. El uso del programa Outlook para difundir virus a través de las direcciones del Email es la base del virus "Melissa". En este mismo año nace el virus "Chernobyl" con gran difusión en Asia y Europa, el cual causa unos daños económicos cifrados en cientos de millones de dólares americanos.

• 2000. Debut del famoso "I love you". Estas tres palabras causan temor en el sector informático, porque ha sido el virus que más pérdidas económicas ha causado en la industria del software.

• 2001. El virus "W32/Sircam" (popularmente conocido como Sircam) llegó a infectar millones de computadoras en cuestión de horas. Otro virus "Nimda" infectó a cientos de miles de ordenadores en todo el mundo, especialmente en Estados Unidos. El principal efecto de este virus es que ralentiza el funcionamiento de las computadoras

Lo primero que llama la atención de las personas dedicadas a generar y difundir virus en la red, en nuestros días, es el afán de publicidad. En la mayor parte de los casos se trata de jóvenes cuyas edades oscilan entre los 22 y 35 años de edad, con gran conocimientos de informática, particularmente expertos en lenguaje Assembler y C.

Tipología de virus

Ahora mismo hay entre 10.000 y 60.000 tipos de virus. Todos ellos se pueden insertar en alguna de estas supercategorías: virus que contaminan los archivos, virus que fastidian el sector boot o de autoarranque de la computadora y virus macro. Una clasificación basada en la bibliografía de los virus informáticos es la que se presenta a continuación:

- Virus por correo electrónico.
- Virus gusanos.
- Virus polimorfos.
- Virus invisibles.
- Virus lentos.
- Virus de ataque múltiple.
- Virus acorazados.
- Virus de acompañamiento.

Entre ellos los más difundidos o clásicos en la historia de los virus informáticos son:

- Virus por correo electrónico

Los virus que se difunden en la actualidad utilizan como plataforma de lanzamiento al programa Outlook de Microsoft, para alcanzar una máxima difusión de infección a través de la red. Sin embargo, otros productos para el envío de Email no están exentos de dicho fenómeno.

- Virus gusanos (worm)

Es un virus que se divulga por medio de los correos electrónicos, como es el caso del Sircam. El primer virus gusano lo realizó Robert Morris, en 1988. En ese entonces tenía 23 años y era estudiante universitario, curiosamente su padre era un experto en seguridad informática de la NSA (National Security Agency). Sin embargo, Morris fue el primero en probar la ley estadounidense sobre criminalidad informática de los Estados Unidos de América.

- Virus Caballo de Troya (Trojan Horse)

Son los más peligrosos desde el punto de vista de la seguridad, porque una vez instalado el virus en la computadora, los teleoperadores del sistema denominados "crackers" son capaces de manejarla a distancia. Quizás sea el momento oportuno para diferenciar estos últimos de los hacker, que entran en el sistema unas milésimas de segundo, por ejemplo, para poner de manifiesto que no hay seguridad. Cuando un Caballo de Troya está en el sistema, es posible observar cómo el cracker puede leer, modificar, borrar, copiar archivos y programas, por ejemplo. Pero la situación límite es ver cómo el cracker puede destruir el sistema poco a poco.

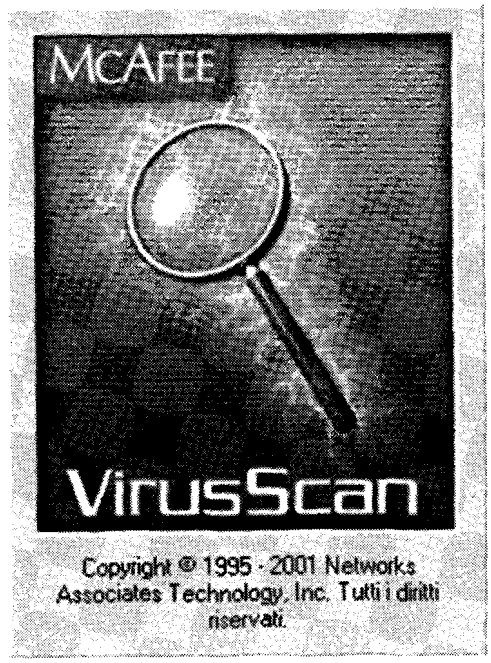
Los antídotos

Como si de una farmacia se tratase, una vez que aparece un virus, automáticamente salta la alarma (por ejemplo, en España es el Consejo Superior de Informática, órgano dependiente del Ministerio de Administraciones Públicas) y velozmente se crea el antídoto al virus.

Lo que llama poderosamente la atención es la velocidad de su fabricación. En varios portales especializados del tema como Panda, McAfee, Norton, etc., se suele descargar gratuitamente, vía Internet, un set para erradicar el virus. A veces, puede suceder que en un primer momento dicho antídoto sea parcial y por ende, no sirva para nada.

En el caso del Sircam, hubo toda una secuencia de pasos que nadie publicó "on-line" hasta pasado unos días. Mientras tanto, no hubo una metodología para seguir paso a paso. Este material es vital para numerosas empresas, para evitar la parada técnica de la actividad y los costes que ello implica.

Al respecto, la situación en Italia -por citar un país europeo- para poner en marcha una empresa que sufrió un ataque de virus, hasta finales del año



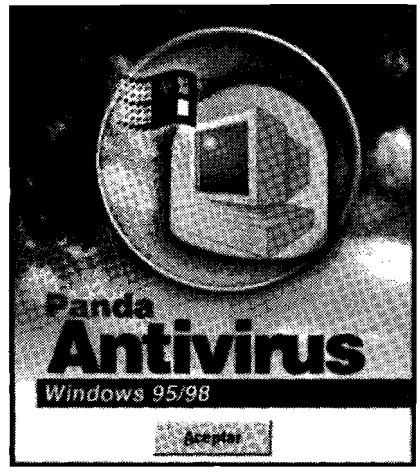
2000, era esta:

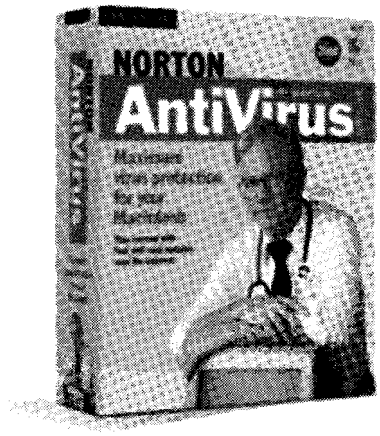
- 45% menos de un día.
- 24% menos de 3 días.
- 13% menos de una semana.
- 11% menos de un mes.
- 7% más de un mes.

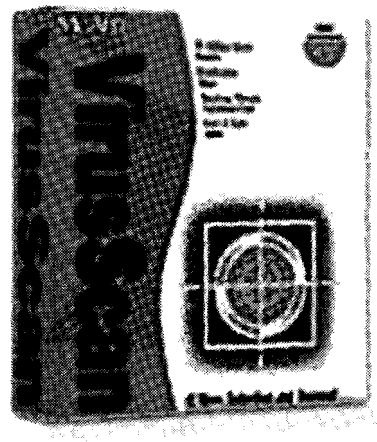
(Fuente EITO 2001)

Por último, he aquí una serie de consejos en caso de infección de virus:

1. Mantener la calma.
2. Llamar al experto informático más próximo.
3. No apagar y volver a encender la computadora.
4. Apuntar las últimas operaciones que se estaban realizando, para posteriormente tratar de recuperar la información en los soportes magnéticos de backup.
5. Poner en marcha el programa antivirus, optando siempre en lo posible por la opción limpieza del file o programa, antes que eliminarlo. Obviamente, si no hay otra solución que eliminar, pues se elimina, pero aquí se anota el nombre del archivo y/o programa







A modo de conclusión

En 1993 existían unos 3.000 virus. En la actualidad oscilan en casi 50.000 y crecen a una media de 2.000 a 6.500 nuevos virus al año, es decir, casi 18 virus al día. Por lo tanto, estamos en una situación de nunca acabar, si a ello le sumamos la venta o actualización de hardware y software para potenciar la seguridad informática. Lo cierto es que la red de redes tiene un gran talón de Aquiles con el tema de los virus informáticos.

De frente a esta realidad, la primera cosa que se espera encontrar en una computadora conectada a Internet es un programa antivirus (en una próxima entrega veremos cómo funcionan los tres más vendidos en el mundo) y la actualización semanal del antídoto. Por cierto, es curioso cómo en un mismo día, por la puerta nos llega el virus y por la ventana el antivirus (obviamente, este último, previo el pago respectivo).

UNA ESTRATEGIA ANTIVIRUS

QUÉ HACER PARA NO TENER VIRUS

1. Actualizar el antivirus en Internet todos los días, antes de comenzar con cualquier actividad. En Europa, lo habitual es realizar una actualización semanal y en automático del antivirus de la computadora principal o server. Un Pc con un sistema antivirus instalado y activo, cada vez que pone en marcha la computadora puede realizar en automático el control de cada unos de los archivos y programas residentes en el disco duro.

2. Una vez descargados los mensajes de correo electrónico, ejecutar el análisis del Antivirus sobre los programas de correo (Outlook, Lotus Domino, etc.) antes de comenzar a verlos.

3. Desconfiar de todos los archivos adjuntados a los e-mail, incluso los que vienen desde remitentes conocidos (pueden contener virus aunque ellos no lo sepan). Es fundamental contar con un antivirus instalado y actualizado en el PC para evitar inconvenientes en el envío y recepción de correspondencia electrónica.

4. Guardar en el disco rígido de la PC aquellos archivos adjuntos que se reciben en los mensajes, cuando sospeche que sean virus y eliminar el mensaje. Recomendamos que la acción siempre sea sacrificar el mensaje eliminándolo, antes que investigar si es Virus o no. Otra recomendación puede ser abrir solo aquellos mensajes que el remitente declara haberlo enviado en el texto del mensaje.

El profesor Ficarra detecta una contradicción técnica en este aserto, porque si hay un antivirus actualizado DIARIAMENTE en el PC, en teoría la aplicación antivirus queda residente en la memoria y en automático se pone en marcha el mecanismo de alerta y erradicación del virus.

5. NO abrir archivos adjuntos que terminen en BAT, EXE, COM, VBS, SHS, PIF y otros, aunque los virus son cada vez más pícaros y utilizan otro tipo de extensiones.

6. Nunca abrir archivos que tengan doble extensión, recurso muy usado por los virus, por ejemplo: .bmp.exe

7. No abrir los mensajes que llamen su atención con propuestas como Sexo, Ofertas, Gratis, que actualice su software ingresando al sitio web indicado, etc. Siempre antes analícelos con su antivirus.

8. Descargar las actualizaciones de los programas de correo electrónico (por ejemplo, Outlook) desde Internet.

Fuente: Departamento de Investigaciones del Instituto Argentino de Computación, Email: azabalza@iac.com.ar, en coordinación con Panda Antivirus Argentina: argentina@pandaantivirus.com.ar. Se incluyen comentarios del profesor Francisco Ficarra

9. NO ingrese en el circuito de Advertencias de Virus reenviando mensajes (generalmente falsas alarmas - Hoax -). En este caso, el virus puede ser el usuario, porque estos mensajes implican eliminar parte del sistema operativo del PC. Mientras tenga su antivirus actualizado estará protegido.

10. Efectuar copias de seguridad periódicamente de la información, por lo menos la de mayor importancia. La frecuencia del backup o respaldo de la información está en función directa del valor de la información almacenada en caso de pérdida de la misma, por la acción destructiva de un virus.

REALIDADES QUE HAY QUE TENER EN CUENTA

1. Según estimaciones el 87% de las infecciones de Virus Informáticos es por medio del correo electrónico

2. Se descubren aproximadamente 600 virus por mes, entre nuevos, nuevas versiones o mutaciones de las anteriores.

3. Los antivirus shareware no son una protección duradera en el tiempo, solo lo protegerá de virus viejos, dependiendo de la antigüedad del software, dispuesto por la empresa que lo ofrece gratuitamente para probarlo.

4. Siempre es aconsejable tener a mano los CD originales de los programas disponibles en la computadora

5. No es lo mismo instalar un software antivirus en una computadora limpia de virus que en una que ya está infectada. Su desinfección puede ser muy fácil o muy compleja, todo depende del tipo de Virus, su complejidad y operatividad, como también de los problemas que haya ocasionado en la información de la PC.

6. Cuando se compra un Antivirus, el CD que se recibe está grabado en una fecha que seguramente es muy anterior a la de su compra. Consecuentemente, la actualización del antivirus es gratuita, ya que la tarea consiste en descargar vía Internet una aplicación que es una lista de antídotos (denominada, por ejemplo, "dat files" en el caso de McAfee -www.nai.com-). Estos archivos de datos son generados semanalmente por los fabricantes del software antivirus.

7. Si se posee una conexión de Banda Ancha no solo se necesita protección antivirus, sino también el software denominado FireWall (Pared de Fuego) para evitar que cualquier Hacker se introduzca en la información del PC, mientras esté conectado a Internet. El firewall es un software que evita en la medida de lo posible, la entrada de Hacker en el sistema informático, mientras se está conectado a Internet y se utiliza la banda ancha de la red. La visita de un Hacker puede producir mayores inconvenientes que un Virus.

8. Una computadora siempre corre peligro de verse infectada por un virus, que puede dañar los archivos que se encuentren en el disco duro. La contaminación puede ocurrir incluso con aquellas computadoras no conectadas a la red y que, por ejemplo, copian archivos de un disquete.

9. Una importante fuente de contaminación son los juegos. Es recomendable mantener una supervisión permanente de la computadora en la que se trabaja, en especial si en ella existe información muy importante, que no queremos que se vea afectada por un virus.