ACIMED
ISSN 1024-9435 *versión impresa*

ACIMED v.11 n.5 Ciudad de La Habana sep.-oct. 2003

Como citar este artículo

Elementos teórico-prácticos útiles para conocer los virus informáticos

Lic. Ramón Orlando Bello Hernández1 y Ms C. Ileana R. Alfonso Sánchez2

Resumen

El vertiginoso avance de las comunicaciones, la conexión entre las computadoras, las posibilidades de transmisión de datos entre ellas, así como del uso de la llamada autopista mundial de información, Internet, ha causado no pocos problemas, tanto a usuarios aislados como a pequeñas y grandes redes. Ellas reciben constantes ataques de los llamados cracker. Estos producen grandes pérdidas en materia de información, recursos, tiempo y dinero; se violan los sistemas de seguridad de los proveedores de servicios y la red se llena de códigos malignos; virus o malware (malicious software). Sin embargo, muchos cibernautas carecen de los conocimientos mínimos necesarios para comprender los virus y, peor aún, para reducir sus efectos negativos. Se trata un conjunto de aspectos importantes sobre los virus informáticos: historia, conceptos, tipos, entre otros. Se demuestra la relevancia del uso de las listas de distribución, así como las experiencias obtenidas en la educación de los usuarios de Infomed con la lista Virus-l, para elevar la educación de los usuarios en los temas relacionados con la seguridad de la información que circula por la red.

Clasificación: Artículo docente

Descriptores (DeCS): SEGURIDAD COMPUTACIONAL; MEDIDAS DE SEGURIDAD; CAPACITACION DE USUARIO DE COMPUTADOR
Descriptores (DeCI): VIRUS INFORMATICO/historia; VIRUS INFORMATICO/clasificacion; SEGURIDAD COMPUTACIONAL; PROGRAMAS ANTIVIRUS; EDUCACION USUARIOS

Abstract

The giddy advance of the communications, the connection among the computers, the data broadcast possibilities among them, as well as, the use of the so called world freeway of information, Internet, has caused not few problems to remote users and small and large networks. They receive constant attacks of the called cracker. They produce large losses of information, resources, time and money; the systems of security of the service suppliers are violated and the network become infected with harmful codes; virus or malware (malicious software). Nevertheless, many websurfers lack the necessary most minimum knowledge to understand the virus and, worse still, to reduce its negative effects. An important assembly of aspects on the data processing virus: history, concepts and types, are provided. The importance of the use of the lists of distribution is shown, as well as the experiences obtained in the education of the users of Infomed with the list Virus l, to elevate the users education in the themes related to information security.

Classification: Learning article

Subject headings (DeCS): COMPUTER SECURITY; SECURITY MEASURES; COMPUTER USER TRAINING

Subject headings (DeCI): COMPUTER VIRUS/history; COMPUTER VIRUS/ clasification; COMPUTER SECURITY; ANTIVIRUS PROGRAMS; USER EDUCATION

El escenario mundial actual en el campo de las redes se caracteriza por un crecimiento acelerado del número de organizaciones y empresas que se enlazan con Internet.Este crecimiento es actualmente superior al 10 % cada mes.1 En la medida en que se suman nuevas redes crece el volumen de información disponible. El número de computadoras que pueden conectarse al mismo tiempo es del orden de los millones. Es fácil entonces suponer que existan, entre millones de usuarios de la red, individuos con perversas intenciones, dispuestos a penetrar la seguridad de las empresas u organizaciones o a lanzar ataques contra miles de cibernautas mediante programas con códigos malignos.

Los virus informáticos son uno de los principales riesgos para los sistemas informáticos actuales, su ritmo de crecimiento es de diez nuevos virus por día y no existe ningún programa detector de virus que sea perfecto, capaz de proteger totalmente a un sistema. No existe un algoritmo universal que permita arreglárnoslas de una vez por todas y para siempre con estos bichitos.1
El propósito del presente trabajo es tratar ciertos aspectos importantes relacionados con el surgimiento y desarrollo de los virus informáticos; así como valorar la función que realizan las listas de distribución y los sitios web que alertan, aconsejan y educan a los usuarios en materia de protección contra los virus informáticos.

Los virus informáticos

Los virus informáticos nacieron al mismo tiempo que las computadoras. En fecha tan lejana como 1949, el famoso científico matemático John Louis Von Neumann (1903-1957), escribió un artículo, donde presentaba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros con una estructura similar.2 En 1944, *Von Neumann* ayudó a *John Mauchly* y *J. Presper Eckert*, en la fabricación de la ENIAC, una de las computadoras de primera generación. En 1950, construyeron la famosa UNIVAC.3

En su libro "Virus Informáticos: teoría y experimentos", el doctor Fred Cohen, quien es reconocido como el primero en definir los virus informáticos, señaló: "Se denomina virus informático a todo programa capaz de infectar a otros programas, a partir de su modificación para introducirse en ellos". A su vez, planteó la imposibilidad de desarrollar un programa que fuera capaz de detectar y eliminar todos los virus informáticos.4

En 1984, en su tesis para optar por el título de Doctor en Ingeniería Eléctrica, presentada en la Universidad del Sur de California, Cohen demostró cómo se podía crear un virus, motivo por el que es considerado como el primer autor de un virus "autodeclarado".5 En el mismo año, editó el libro titulado "Un pequeño curso sobre virus de computadoras". Posteriormente, escribió y publicó "The Gospel according to Fred" (El evangelio de acuerdo a Fred).5

Los virus son capaces de hacer daño y reproducirse, esto precisamente los ha convertido en una verdadera pesadilla para las redes y sus usuarios. Pero, no es hasta mucho después de escrito el libro de Cohen, que adquieren esa propiedad y, a consecuencia de ello, se les comienza a llamar virus. Sus posibilidades de autorreproducción y mutación, que los asemejan con los virus biológicos, todo lo cual parece ser el origen de su nombre. Se le adjudica a Len Adleman, el haberlos llamado virus por primera vez.1

Antes de la explosión de la microcomputación se hablaba muy poco sobre ellos. La computación estaba sólo al alcance de investigadores y científicos que trabajaban, tanto en universidades como en instituciones privadas y estatales, que manejaban fuertes sumas de dinero y podían pagar los altos costos de sus programas. A su vez, las entidades gubernamentales, científicas o militares, que experimentaron ataques de virus, se quedaron muy calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaban millones de dólares a sus contribuyentes. Las empresas privadas, como los bancos y las grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Por tanto, puede decirse que entre 1949 y 1987 el conocimiento sobre los virus informáticos estuvo bastante limitado.

El primer antecedente reconocido de los virus actuales es un juego creado por programadores de la empresa AT&T, *Robert Thomas Morris, Douglas McIlory y Victor Vysottsky*, como parte de sus investigaciones y su

entretenimiento. El juego, llamado "*Core Wars*",6 tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa disponía de 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*6 un antivirus o vacuna, como hoy se le 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.7

En el año 1983, el Dr. *Keneth Thomson*8, uno de los creadores del famoso sistema operativo UNIX y los programadores de AT&T, que trabajaron en la creación de *Core Wars*,6 rompieron el silencio acordado, informaron la existencia del programa y ofrecieron detalles sobre su estructura. A comienzos de 1984, la revista Scientific American, 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, donde presentó un virus informático residente en una PC. Al Dr. *Cohen* se le conoce hoy, como "el padre de los virus". Paralelamente, aparecieron virus en muchas PCs, se trataba de un virus, con un nombre similar a *Core Wars*,6 escrito en Small-C por *Kevin Bjorke*, que luego lo cedió al dominio público. ¡La cosa comenzaba a ponerse caliente!7

Con posterioridad, los virus se multiplicaron con gran rapidez. Cada día creció el número de virus existentes y hoy son tantos que es imposible registrarlos todos. Aunque cientos de ellos son prácticamente desconocidos, otros gozan de gran popularidad, debido a su extensión y daños causados. Algunos de los virus más conocidos son:8,9,10

Viernes 13

Es el virus más conocido dentro y fuera del mundo de la informática, debido a su gran difusión y al protagonismo que adquiere en los medios informativos cada vez que se acerca un viernes con la fecha trece. Su gran expansión se debe a que respeta las funciones habituales de los programas que lo albergan. La primera versión fue descubierta en diciembre de 1987 en las computadoras de la Universidad Hebrea de Jerusalén.

El descubrimiento se debió a lo que se supone un fallo en el diseño del programa. El virus no detectaba los programas .EXE contaminados y, por tanto, volvía a infectarlos. Cada vez, su tamaño crecía unos 2 Kb, hasta que estos alcanzaban un tamaño imposible de manejar por el sistema operativo DOS. El resto de los programas ejecutables sólo se infectaban una vez. Si un programa contaminado se ejecutaba, el virus pasaba a la memoria de trabajo de la computadora y, a partir de ese momento, se contaminaba cualquier programa que se ejecutase.

El virus, totalmente desconocido, se extendió por Israel rápidamente, debido principalmente a que este país dispone de extensas y potentes redes de computadoras. Las computadoras personales mostraban claros síntomas de un mal funcionamiento, manifestaban lentitud y largo tiempo de respuesta. Debido a su tamaño, algunos programas no podían ejecutarse por falta de espacio suficiente en la memoria de trabajo. Estos síntomas llevaron a los expertos, pertenecientes a la Universidad Hebrea, a investigar el fenómeno, hasta que a finales de diciembre de 1987, dieron con el virus. Pudieron así, desactivar la pequeña bomba de relojería cuya detonación estaba preparada para el 13 de mayo de 1988. Su objetivo era borrar programas militares y científicos, así como innumerables programas pertenecientes a los usuarios de computadoras personales. La vacuna preparada por los expertos de la Universidad Hebrea redujo considerablemente sus efectos.

Existen dos teorías sobre el origen y el objetivo principal del virus. Ambas hacen referencia a su fecha de activación. La primera de ellas, y más convincente, se deduce de las instrucciones relativas a la obtención de la fecha de la computadora para su comparación con la fecha de activación. El programa ignora todos los posibles viernes con fecha trece que pudieran existir en 1987, año en que se dedicaría únicamente a la multiplicación y propagación. Esta teoría, atribuida a un origen político, juega con la posibilidad de que el virus fuese un nuevo tipo de arma lógica creada contra el pueblo judío, posiblemente por seguidores palestinos. El l primer viernes trece del año 1988 fue en el mes de mayo y coincidió con el cuadragésimo

aniversario del final de la guerra de Yom Kippur. Las consecuencias de dicha guerra fueron la desaparición de Palestina y la constitución del estado de Israel el 14 de mayo. Por tanto, el 13 de mayo de 1988 se celebraba el cuadragésimo aniversario del último día de la existencia de Palestina.

La segunda de las teorías, menos difundida, asegura que las especulaciones de la anterior son pura coincidencia. Basa la existencia del Viernes13, tanto en Israel como en Estados Unidos, en que ellos son países con extensas redes de telecomunicaciones, y no a consecuencia de un objetivo político. Se ampara en que esta fecha es símbolo de la mala suerte para la cultura anglosajona, como lo es en España, el martes13.

La razón de que el virus no se activase durante el año 1987 se debe a la necesidad de una etapa de incubación. Si el virus hubiera actuado en el mismo momento en que infectó un programa, su efecto sería mínimo. Además, al detectarse con rapidez, pudiera haberse descubierto a su creador. Por eso, su programador extendió el período de incubación a un año en espera de que su alcance fuera el mayor posible.

Brain

Brain es uno de los virus más extendidos entre los usuarios del sistema operativo DOS. Sus creadores, los hermanos *Basit* y *Alvi Amjad*, de Pakistán, elaboraron una primera versión del virus que se instalaba en el sector de arranque de los disquetes. Algunos de sus sectores aparecían marcados como si estuviesen en mal estado. Aparentemente no producía daños. Cambiaba la etiqueta de volumen de los disquetes de 5,25 pulgadas, que contenían el sistema operativo, por la de "(c) Brain". No infectaba el disco duro y sólo atacaba los disquetes con el sistema operativo mencionado y una versión inferior a la 2.0. Destruía pequeñas cantidades de datos, sólo si los discos estaban casi o totalmente llenos. Pero, como ocurre con la mayoría de los virus, comenzó a volverse molesto. Posteriormente, surgieron versiones mejoradas que inutilizaban los datos almacenados e infectaban el disco duro, así como las nuevas versiones del sistema operativo.

Aunque se establece su creación en 1986, se hizo público el 16 de mayo de 1988 en Estados Unidos, cuando un periodista del Journal-Bulletin de Providence, *Rhode Island*, no podía recuperar un fichero almacenado en el disquete en el que había guardado el trabajo de varios meses. Llevó entonces el disquete deteriorado a la casa que lo fabricaba, donde un analista detectó que el bloque de inicialización del disco contenía un programa vírico.

El virus, actualmente activo, se caracteriza por la aparición de un mensaje en el primer sector del disquete contaminado. El mensaje, que varía según la versión del virus, es similar al siguiente: "Welcome to the Dungeon ... (c) 1986 Brain & Amjads (pvt) Ltd ... VIRUS_SHOE RECORD V9.0 ... Dedicated to the dynamic memories of millions of virus who are no longer with us today - Thanks GOODNESS !! ... BEWARE OF THE er ... VIRUS...".

Su traducción podría ser: "Bienvenido a la mazmorra ... [Marca del copyright de los hermanos Amjad], [posible fecha de creación del virus] 1986 [versión del programa] ... Dedicado a las memorias dinámicas de los millones de virus que ya no están con nosotros [se supone que por haberse detectados y desactivados] - ! GRACIAS A DIOS! ... CUIDADO CON EL ... VIRUS ...".

En algunas versiones, el mensaje menciona un número de teléfono de una compañía de computadoras pakistaní. El ingeniero de la Providence *Journal Corporation* se puso en contacto con dicho teléfono, que correspondía a la empresa de los hermanos Amjad, quienes tras excusarse de los daños ocasionados, afirmaron que el virus se escribió originalmente para que les ayudara a seguir el rastro de las copias "pirateadas" del software cuyo copyright disponían desde 1986. También aseguraron que no comprendían cómo el virus se había extendido de esa forma, se había alejado de las copias de sus programas, ni cómo había llegado hasta Europa y Estados Unidos, porque sólo debía afectar a aquellos usuarios que utilizasen alguno de sus programas de forma pirata.

El gusano de la NASA

El gusano de la NASA y el Pentágono es el caso más espectacular de contaminación informática producido por un gusano. Su entorno fue la red ARPANET (*Advanced Research Projects Administration Network*), con miles de terminales en varios continentes y en lugares tan estratégicos como el Pentágono o la NASA.

El 2 de noviembre de 1988, *Robert Tappan Morris*, hijo de uno de los precursores de los virus y recién graduado en *Computer Science* en la Universidad de Cornell, difundió un virus a través de ArpaNet, precursora de Internet. La propagación se realizó desde una de las teminales del Instituto Tecnológico de Massachussets.

Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de 10 000 dólares de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario.

Los hechos pudieron ocurrir de la siguiente manera: tras meses de estudio y preparación, en la primera semana de noviembre de 1988, *Robert T. Morris* decidió hacer la prueba final. Con la intención de ocultar un programa en la red a la que pertenecía su universidad, puso manos a la obra la noche de un miércoles. Cuando terminó de cenar y volvió a sentarse frente a su terminal con la intención de averiguar lo que ocurría con su programa, descubrió que la prueba se había desbordado: el programa activaba el correo electrónico, se copiaba en la memoria de las computadoras y se "autoenviaba" a todas las terminales que aparecían en su lista de correo. Esta operación, al repetirse en cada computadora, hacía que se volviera a enviar y copiar, incluso en aquellas computadoras por los que había pasado. En pocas horas, el programa viajó, ida y vuelta, por las mismas computadoras miles de veces y se copiaba una vez más en cada computadora. Esto supuso una saturación de las líneas de comunicación y de las memorias de las computadoras conectadas a la red, que quedaron bloqueadas.

Más de 6 000 computadoras quedaron infectadas. Entre ellas, las del Pentágono, la NASA, el Mando Aéreo Estratégico (SAC), la Agencia Nacional de Seguridad (NSA), el Ministerio de Defensa, los Laboratorios Lawrence Livermore de Berkeley (California), donde se desarrollaban varios componentes de la Iniciativa de Defensa estratégica, también llamada "guerra de las galaxias", y en las universidades de Princenton, Yale, Columbia, Harvard, Illinois, Purdue, Wisconsin y el Instituto de Tecnología de Massachussets. Incluso se infectaron computadoras de la República Federal de Alemania y de Australia.

La legislación que existe para sancionar estos delitos es inmadura. Pero no por ello Robert T. Morris, quedó exento de culpa y se le tomó como "cabeza de turco" para impedir que se realizaran posteriores prácticas similares. Fue acusado de violar el código de Integridad Académica de la Universidad de Cornell, y es juzgado por ello en la actualidad.

Clasificación

La clasificación de los virus es muy variada. Pueden agruparse por la entidad que parasitan -sector de arranque o archivos ejecutables-, por su grado de dispersión a escala mundial, por su comportamiento, por su agresividad, por sus técnicas de ataque o por la forma en que se ocultan. En 1984, el Dr. *Fred Cohen* clasificó a los nacientes virus de computadoras en tres categorías:3,11

1. Caballos de Troya (Troyan horses)
   Los caballos de Troya son impostores, es decir, archivos que parecen benignos pero que, de hecho, son perjudiciales. Una diferencia muy importante con respecto a los virus reales es que no se replican. Los caballos de Troya contienen códigos dañinos que, cuando se activan, provocan pérdidas o incluso robo de datos. Para que un caballo de Troya se extienda es necesario dejarlo entrar en el sistema, por ejemplo, al abrir un archivo adjunto de correo.
2. Gusanos (worms)
   Los gusanos son programas que se replican de sistema a sistema, sin utilizar un archivo para hacerlo. En esto se diferencian de los virus, que necesitan extenderse mediante un archivo infectado. Aunque los gusanos generalmente se encuentran dentro de otros archivos, a menudo documentos de Word o Excel, existe una diferencia en la forma en que los gusanos y los virus utilizan el archivo que los alberga. Normalmente el gusano generará un documento que contendrá la macro del gusano dentro. Todo el documento viajará de un equipo a otro, de forma que el documento completo debe considerarse como gusano.
3. Virus

Un virus informático es un pequeño programa creado para alterar la forma en que funciona un equipo sin el permiso o el conocimiento del usuario. Un virus debe presentar dos características:

- Debe ser capaz de autoejecutarse. A menudo coloca su propio código en la ruta de ejecución de otro programa.
- Debe ser capaz de replicarse. Por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado.

Los virus pueden infectar tanto equipos de escritorio como servidores de red.

A partir de 1988, los virus empezaron a infectar y dañar archivos con diferentes extensiones: DLL, DBF, BIN, VBS, VBE, HTM, HTML, etcétera. Hoy, los virus no infectan áreas del sistema o tipos de archivos en forma específica y limitada. Sucede de acuerdo con cómo lo deseen sus creadores, dejando a un lado las clasificaciones tradicionales. Los virus requieren ejecutarse para lograr sus objetivos y por esa razón buscan adherirse a los archivos .COM, .EXE, .SYS, .DLL y .VBS, entre otros o a las áreas vitales del sistema: sector de arranque, memoria, tabla de particiones o al MBR. Una vez activados atacarán a otros archivos ejecutables o áreas, haciendo copias de sí mismos, sobrescribiéndolos o alterando archivos de cualquier otra extensión, no ejecutables. Los ficheros con extensiones diferentes a .COM, .EXE, .SYS, .DLL, .VBS y otras, sólo servirán de receptores pasivos, no activos,y pueden quedar alterados o inutilizados, pero jamás contagiarán a otros archivos.3

Existen cinco tipos de virus conocidos:11

- Virus que infectan archivos: atacan a los archivos de programa. Normalmente infectan el código ejecutable, contenido en archivos .COM y .EXE, por ejemplo. También pueden infectar otros archivos cuando se ejecuta un programa infectado desde un disquete, una unidad de disco duro o una red. Muchos de estos virus están residentes en memoria. Una vez que la memoria se infecta, cualquier archivo ejecutable que no esté infectado pasará a estarlo.
- Virus del sector de arranque: infectan el área de sistema de un disco, es decir, el registro de arranque de los disquetes y los discos duros. Todos los disquetes y discos duros (incluidos los que sólo contienen datos) tienen un pequeño programa en el registro de arranque que se ejecuta cuando se inicia el equipo. Los virus del sector de arranque se copian en esta parte del disco y se activan cuando el usuario intenta iniciar el sistema desde el disco infectado. Estos virus están residentes en memoria por naturaleza. La mayoría se crearon para DOS, pero todos los equipos, independientemente del sistema operativo, son objetivos potenciales para este tipo de virus. Para que se produzca la infección basta con intentar iniciar el equipo con un disquete infectado. Posteriormente, mientras el virus permanezca en memoria, todos los disquetes que no estén protegidos contra escritura quedarán infectados al acceder a ellos.
- Virus del sector de arranque maestro: residen en memoria e infectan los discos de la misma forma que los virus del sector de arranque. La diferencia entre ambos tipos de virus es el lugar en que se encuentra el código vírico. Los virus del sector de arranque maestro normalmente guardan una copia legítima de dicho sector de arranque en otra ubicación.
- Virus múltiples: infectan tanto los registros de arranque como los archivos de programa. Son especialmente difíciles de eliminar. Si se limpia el área de arranque, pero no los archivos, el área de arranque volverá a infectarse. Ocurre lo mismo a la inversa. Si el virus no se elimina del área de arranque, los archivos que se limpiaron volverán a infectarse.
- Virus de macro: atacan los archivos de datos.

Con la aparición de los virus Macro, a mediados de 1995, y en 1998 con los virus de *Java, Visual Basic Scripts*, Controles ActiveX y HTML, se hizo necesario, además, una clasificación por sus técnicas de programación.12

Una de las últimas técnicas empleadas es la llamada Ingeniería social. En ella no se emplea ningún software o elemento de hardware, sólo grandes dosis de ingenio, sutileza y persuasión para lograr que otra persona revele información importante con la que, además, el atacante puede dañar su computadora.

En la práctica, los creadores de virus utilizan esta técnica para que sus ingenios se propaguen rápidamente. Para ello, atraen la atención del usuario inexperto y consiguen que realice alguna acción, como la de abrir un fichero, que es el que ejecuta la infección, mediante la alusión a un fichero o página con explícitas referencias eróticas, personajes famosos, relaciones amorosas, alternativas para encontrar parejas, juegos, entre otros.

Algunos virus que utilizan la técnica de ingeniería social son:

- W32/Hybris: reclama la curiosidad de los usuarios mediante un mensaje sugerente sobre una posible versión erótica del cuento de Blancanieves y los siete enanitos.
- W32/Naked: atrae la atención del usuario al intentar mostrarle un archivo cuyo nombre (NakedWife.exe) sugiere la imagen de una mujer desnuda.
- "AnnaKournikova" alias VBS/SST.A o "I-Worm/Lee.O"-: trata de engañar al usuario haciéndole creer que le ha recibido un fichero con la fotografía de la tenista Anna Kournikova.
- Trojan.Butano: aprovecha la imagen del conocido locutor de radio José María García, para esconder un programa que elimina todos los archivos existentes en el directorio raíz del disco duro.
- VBS/Monopoly: se autoenvía por correo electrónico en un mensaje que tiene como asunto "Bill Gates joke" ("Broma sobre Bill Gates"), y como cuerpo "Bill Gates is guilty of monopoly. Here is the proof.:" (Bill Gates es culpable de monopolio).
- I-Worm/Pikachu: se envía por correo electrónico en un mensaje cuyo asunto es "Pikachu Pokemon", en clara referencia al popular personaje infantil de videojuegos y series de animación.
- W32/Matcher: utiliza como reclamo -en el cuerpo del mensaje en el que se envía- un texto que ofrece una alternativa para encontrar pareja.
- VBS/LoveLetter -alias "Iloveyou"-: se envía por correo electrónico en un mensaje cuyo asunto es "ILOVEYOU" y el fichero que incluye se denomina "LOVE-LETTER-FOR-YOU.TXT.VBS". Dicho fichero utiliza doble extensión para engañar a los usuarios de Windows, porque este sistema no emplea las extensiones de los archivos.

Los virus pueden causar diferentes daños y molestias, como son:

En software

- Modificar programas y datos (virus Black Box: agrega un número de bytes a los programas infectados.)
- Eliminar programas y datos (Melissa: Macrovirus de Word). Se envía a sí mismo por correo. Daña todos los archivos
- DOC; virus JERUSALEM: borra, los viernes 13, todos los programas que el usuario trate de utilizar después de haberse infectado la memoria residente.
- Agotar el espacio libre del disco rígido.
- Demorar el trabajo del sistema.
- Sustraer información confidencial (Mighty: gusano para Linux:, Troj/Backdoor.Netdex.A: trojano, W32/Daboom): gusano de Internet, caballo de Troya tipo RAT.
- Producir mensajes o efectos extraños en pantalla (WinWord.Concept): Macrovirus que infecta la plantilla Normal.dot. Hace aparecer mensajes en la pantalla y el WORD funciona incorrectamente.
- Emitir música o ruidos (virus FORM): el día 18 de cada mes cualquier tecla que se presione hace sonar el beep.

En hardware

- Borrar el BIOS (Chernobyl (W95.CIH): Intenta reescribir el BIOS de la PC lo que obliga a cambiar la motherboard.
- Formatear el disco rígido (FormatC): Troyano que infecta el Word, al abrir un archivo infectado formatea el disco rígido.
- Borrar la FAT (tabla de partición de archivos), Chernobyl (W95.CIH): Borra el primer Mb del diso duro, donde se encuentra la FAT. Obliga a formatear el disco duro. Además intenta reescribir el BIOS de la PC lo que obliga a cambiar la motherboard. Se activa el 26 de abril. Michelangelo: Virus del sector de arranque. Se activa el 6 de marzo.
- Sobreescribe la FAT, deja el disco inutilizable.
- Alterar el MBR (Master Boot Record), Troj/Killboot.B. Trojano que borra el MBR llenándolo de ceros.

Cuando alguno de estos daños ocurre en una computadora aislada, las pérdidas pueden ser insignificantes, pero cuando se trata de una gran empresa, universidad, banco, institución militar, centro de salud, aeropuerto, proveedor de servicios de Internet u otro, los daños pueden ser incalculables e irreparables.

Ahora bien, es oportuno señalar que los virus son controlables y que, si se cumplen una serie de normas, que no varían mucho, establecidas por las entidades que se dedican a la protección de las redes y sus usuarios, puede lograrse una protección aceptable. Baste con recordar que ningún virus es capaz de hacer daño alguno, si antes no se ejecuta.

Situación actual

La cantidad de virus que circulan actualmente en la red no puede precisarse con exactitud. Algunos autores calculan el total de virus existentes en más de 300 000.13 La mayoría de los virus que forman parte de la historia de la computación se crearon para DOS; un sistema obsoleto en nuestros días.

A pesar de la creación constante de nuevos virus, son pocos los que llegan a ser realmente efectivos y logran contaminar un número considerable de usuarios de la red. Los expertos en virus informáticos, respaldan los informes sobre la existencia de no más de 300 virus esparcidos y en libertad.15 Al repetirse en forma cíclica su proceso de extinción, la cantidad de virus mencionados nunca es mayor y se mantiene aproximadamente igual.

A pesar de los estragos causados por el reciente torrente de ataques de virus, como el mortal "Love Bug", o el famoso "CIH" son muchos los usuarios, individuales e institucionales, que no actualizan regularmente sus programas antivirus.

Se plantea que casi una cuarta parte de los usuarios norteamericanos no actualizan sus programas, al menos, una vez al mes. Un examen, realizado a cerca de medio millón de usuarios de PCs en los Estados Unidos, reveló que la mayoría de estos (un 65 %) fueron infectados con, al menos un virus, en los últimos doce meses. De estos, un 57 % perdió un buen número de datos. Un 18 % afirmó que había perdido "moderadas" o "grandes" cantidades de datos y un 14 % sostuvo que había sufrido más de cinco ataques de virus al año. Según Steve Sundermeier, cuando "el público que no adquiere la última protección contra virus, abre un enorme agujero de seguridad. Los usuarios necesitan actualizar sus programas diariamente para salvaguardarse de los virus que los atacan diariamente".13 Cada día se crean 30 nuevos virus como promedio, desde inofensivos hasta muy peligrosos.14

Los softwares antivirus, líderes en el combate de virus, pueden descontaminar distintas cifras de códigos malignos. Por ejemplo, Norton Antivirus, 63 076, McAfee, 64 686, AVP, 64 156, SAV, 513 y F-Prot, 73 350.16-19

Uno de estos productos, el SAV, comercializado por la firma Segurmática, y que descontamina los virus identificados en la isla, es el resultado de las necesidades nacionales, surgidas como resultado del amplio programa de informatización desplegado por Cuba durante los últimos años.

Sin embargo, como los planes de informatización del país, son cada vez más abarcadores, el énfasis fundamental debe situarse no sólo en la creación y la adquisición de los recursos técnicos y humanos, sino en el desarrollo de una cultura informática que permita a los usuarios prepararse para enfrentar los peligros de la red, en especial, para minimizar los efectos dañinos de los virus informáticos que provocan pérdidas considerables de tiempo, esfuerzo y recursos de gran valor.

Las listas de discusión o distribución de información

El conocimiento adquirido por los usuarios de la red para enfrentar los virus es el resultado, en gran medida, de la creación de boletines y listas que los alertan sobre la aparición de nuevos virus y la forma de eliminarlos, además de las medidas aprendidas para el uso correcto del correo y la navegación en el web.

Las listas son muchas y tienen un lugar muy importante en la educación de los usuarios. Entre las listas dedicadas a la difusión oportuna de información sobre los virus informáticos, se encuentran:

- VSAntivirus: El boletín diario de VSANTIVIRUS - http://www.vsantivirus.com (Uruguay).
- Virus Attack: Un excelente sitio para obtener información en la lucha contra los virus. http://www.virusattack.com.ar (Argentina).
- AlertaVirus: Un servicio gratuito de AlertaVirus.com. http://www.alertavirus.com (Chile).

- Per Systems: Boletín sobre alerta de virus. http://www.perantivirus.com/ (Perú).
- Alerta - Antivirus: Centro de Alerta Temprana sobre Virus y Seguridad Informática http://www.alerta-antivirus.es/ (España).
- VirusProt: Boletín sobre seguridad informática. http://www.virusprot.com/ (España).
- Infovirus: Boletín que informa sobre lo último en virus informáticos. http://www.espanadir.com/drwebsp/index.shtml (España).
- Virus-l: Boletín sobre virus informáticos. http://www.sld.cu/mailman/listinfo/virus-l (Cuba).

Dichas listas alertan a sus usuarios mediante boletines diarios, semanales o mensuales y su objetivo principal es mantener informados a lectores sobre los nuevos virus, así como sobre la forma de eliminarlos, además de ofrecer consejos, publicar estadísticas, realizar encuestas comparativas sobre programas antivirus, etcétera.

Virus-l, por ejemplo, es la lista sobre virus de la Red Telemática de Salud en Cuba (Infomed). Cuenta con 1 199 miembros.20 Su objetivo esencial es la educación de sus miembros en materia de protección de los sistemas. Comprende desde el médico o técnico de la salud que se conecta desde su casa vía telefónica hasta los centros e instituciones, como los hospitales, facultades, policlínicos, y otros, que requieren de una seguridad mayor, debido a su importancia.

Infomed brinda servicios a una gran cantidad de profesionales del sector de la salud, crece muy rápidamente y tiene más de 9000 usuarios directos. Los planes del gobierno en el sector de la salud se proponen conectar todos sus centros e instituciones en el país.

Fidel Castro Ruz, Primer Secretario del Comité Central del Partido Comunista de Cuba y Presidente de los Consejos de Estado y de Ministros, en el acto de inauguración de obras del extraordinario programa de salud ya en marcha, que se realiza en Cuba, efectuado en el Teatro Astral, el 7 de abril del 2003, expresó:

> "Algo de gran trascendencia será la creación, ya iniciada, de Infomed, un servicio Intranet que comunicará a todos los centros de salud, hospitales, policlínicos, hogares de ancianos, farmacias, etcétera, a través de una densa red de computadoras que posibilitará la comunicación, consultas e intercambio científico entre todos los médicos, enfermeros y técnicos, y el acceso a todas las bases de datos e información médica con el empleo de miles de equipos de computación".21

De aquí, la importancia de una seguridad informática amplia y poderosa. Dentro de ella, la lucha contra los virus es un aspecto muy relevante. Es entonces necesario, desarrollar una cultura informática que permita estar preparados contra cualquier ataque proveniente de un programa o código maligno.

Virus-l dispone de un boletín semanal que divulga información sobre los virus más peligrosos, selecciona y promueve la consulta de artículos sobre el tema ubicados en distintos sitios, se alerta sobre fallos en sistemas o agujeros de seguridad y las formas de eliminarlos. Por supuesto, como en todas las listas de este tema no falta en cada boletín, una serie de consejos útiles para evitar la posibilidad de contaminarse por un virus informático.

La lista cuenta además, con un espacio en el servicio de FTP de la red donde se apoya su trabajo con material educativo sobre el tema, herramientas para eliminar ciertos virus y la posibilidad de descargar programas instaladores de antivirus y sus actualizaciones. Todo ello ha posibilitado elevar el nivel de protección de una gran parte de los usuarios de la red.

Por encuestas realizadas mediante la propia lista se han podido conocer cuáles antivirus utilizan los usuarios de Infomed, con qué frecuencia los actualizan, cómo actúan ante una infección y otros aspectos que han permitido trazar estrategias de trabajo para mejorar su protección.

Ante la pregunta, ¿cómo usted. actúa ante un mensaje con un fichero adjunto?, el 45 % de los 103 suscriptores encuestados el día 10 de junio del 2002, respondieron "Abro sólo ficheros adjuntos enviados por personas conocidas" y el 33 %, "No abro ningún adjunto sin revisarlo antes con un antivirus". Por su parte, a la pregunta, ¿qué hace si descubre que su PC está infectada?, el 48 % de los 139 usuarios consultados el día 28 de agosto del 2002, seleccionaron "Utilizo un antivirus y sigo las instrucciones de mi

lista". Entre los 104 suscriptores consultados el día 22 de noviembre del 2002, el 54 % respectivamente dijeron utilizar como antivirus el AVP y el NAV. Este mismo día, cuando se preguntó, ¿cada cuánto tiempo actualiza su antivirus?, del total de encuestados, el 65 % respondió "Una vez por semana" y el 23 % "Dos o tres veces por mes"

Para apoyar su tarea educativa de la lista, se imparte mensualmente una clase donde se orienta a los alumnos-usuarios sobre cómo evitar o eliminar las infecciones por virus. En ellas, se ofrecen también una serie de consejos prácticos relacionados con el tema.

Consideraciones finales

Como se ha tratado de evidenciar a lo largo de este trabajo, los virus informáticos no son un simple riesgo de seguridad. Son muchos los programadores en el mundo que se dedican a la creación de códigos malignos por distintos motivos, que causan pérdidas anuales millonarias en gastos de seguridad a las empresas. El verdadero peligro de los virus es su forma indiscriminada de ataque contra cualquier sistema informático, algo realmente lamentable.

Es muy difícil prever la propagación de los virus y cuáles máquinas infectarán. De ahí, la importancia de comprender cómo funcionan regularmente y tomar las medidas pertinentes para evitarlos.

La educación de los usuarios de la red es la mejor forma de controlar una infección. Es importante saber qué hacer en el momento justo para frenar un avance que podría extenderse y hacer colapsar una red. La consulta de las últimas noticias sobre el tema es una forma importante de mantenerse actualizado sobre su evolución y riesgos inmediatos.

Referencias bibliográficas

1. Moreno Pérez A. La historia interminable- La génesis y el devenir de los virus. [sitio en Internet]. Disponible en: http://www.zonavirus.com/Detalle_Articulo.asp?Articulo=20. Consultado: 18 de febrero de 2003.
2. Von Neumann JL. Tutorial sobre virus informáticos. - nivel básico - [sitio en Internet]. Disponible en: http://sapiens.ya.com/herminiapaissan/virus/historia.htm. Consultado: 16 de febrero de 2003.
3. Machado J. Breve historia de los virus informáticos. [sitio en Internet]. Disponible en: http://www.perantivirus.com/sosvirus/general/histovir.htm . Consultado: 4 de Marzo de 2003.
4. Cohen F. "Virus Informáticos: teoría y experimentos" [sitio en Internet]. Disponible en: http://www.monografias.com/. Consultado: 16 de febrero de 2003.
5. Machado J. Fred Cohen el primer autor de virus. [sitio en Internet]. Disponible en: http://www.perantivirus.com/sosvirus/hackers/cohen.htm . Consultado: 4 de marzo de 2003.
6. Red Telemática de Salud en Cuba (Infomed). Versión adaptada a PC del juego COREWAR, precursor de los virus [sitio en Internet]. Disponible en: ftp://ftp.sld.cu/pub/antivirus/miscelaneas/corewar.zip . Consultado: 4 de Marzo de 2003.
7. Vanden Bosch L, Waisman N, Rojas F. "Virus informáticos". [sitio en Internet]. Disponible en: http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#historia . Consultado: 6 de marzo de 2003.
8. Jones Encyclopedia - Media & Information Technology. [sitio en Internet]. Disponible en: http://www.digitalcentury.com/encyclo/thompson.html. Consultado: 12 de marzo de 2003.
9. Judgment in U.S. vs. Robert Tappan Morris. [sitio en Internet]. Disponible en: http://www.rbs2.com/morris.htm . Consultado: 10 de marzo de 2003.
10. Bihar.net. [sitio en Internet]. Disponible en: http://www.biar.net/HistoriaInf/anecdotas.html . Consultado: 18 de febrero de 2003.
11. Symantec. Diferencias entre virus, gusanos y caballos de Troya. Disponible en: http://service1.symantec.com/SUPPORT/INTER/navintl.nsf/la_docid/pf/20010921095248905 Consultado: 10 de abril del 2003
12. Machado J. Cómo se clasifican los virus?. [sitio en Internet]. Disponible en: http://www.perantivirus.com/sosvirus/pregunta/clasific.htm . Consultado: 17 de febrero de 2003.
13. Machado J. ¿Cuántos virus existen?.[sitio en Internet]. Disponible en: http://www.perantivirus.com/sosvirus/pregunta/cuantos.htm . Consultado: 9 de Marzo de 2003
14. Zona Virus. Muchos usuarios ignoran el riesgo de los virus. [sitio en Internet]. Disponible

en:http://www.zonavirus.com/Detalle_ARTICULO.asp?ARTICULO=6 . Consultado: 6 de Marzo de 2003.
15. Synmatec Segurity Responce. Virus definition added. [sitio en Internet]. Disponible en:http://securityresponse.symantec.com/avcenter/defs.added.html . Consultado: 14 de febrero de 2003.
16. Networks Associates Technology. Top Selling Services. [sitio en Internet]. Disponible en:http://www.mcafee.com . Consultado: 25 de febrero de 2003.
17. Kaspersky Lab. Anti-Virus Updates. [sitio en Internet]. Disponible en: http://www.kaspersky.com/updates.html . Consultado: 25 de febrero de 2003.
18. Segurmática. Consultoría y Seguridad Informática. [sitio en Internet]. Disponible en: http://www.segurmatica.co.cu . Consultado: 18 de febrero de 2003.
19. FRISK Software Internacional. F-Prot Antivirus latest version and latest virus signature files. [sitio en Internet]. Disponible en: http://www.f-prot.com/currentversions.html. Consultado: 14 de febrero de 2003.
20. Virus-l mailing list administration General Options Section. [sitio en Internet]. Disponible en: http://www.sld.cu/mailman/admin/virus-l . Consultado: 13 de marzo de 2003.
21. Castro Ruz F. La idea esencial es acercar los servicios básicos a los ciudadanos. Discurso pronunciado el día 7 de abril en el Teatro Astral. Disponible en: http://www.granma.cubaweb.cu/2003/04/08/nacional/articulo01.html Consultado: 8 de abril del 2003.

Recibido: 9 de junio del 2003. Aprobado: 16 de julio del 2002.
Lic. *Ramón Orlando Bello Hernández*. Departamento Atención a Usuarios. Red Telemática de Salud en Cuba (Infomed).
Calle 27 No.110 e/ M y N. El Vedado. Plaza de la Revolución. Ciudad de La Habana, Cuba. CP 10 400. AP 6520.
Correo electrónico: bello@infomed.sld.cu

1 Licenciado en Educación. Especialista en Informática. Profesor Asistente. Red Telemática de Salud en Cuba (Infomed). Centro Nacional de Información de Ciencias Médicas.
2 Máster en Informática en Salud Pública. Profesora Auxiliar. Investigadora Agregada. Gestión Integral de Recursos Humanos. Red Telemática de Salud en Cuba (Infomed). Centro Nacional de Información de Ciencias Médicas.
