LOS VIRUS INFORMÁTICOS: UNA AMENAZA PARA LA SOCIEDAD

Yansenis López Matachana

Página legal

621.39-Lop-V

Los virus informáticos: una amenaza para la sociedad. -- Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9. -- 33 pág.

1. López Matachana, Yansenis
2. Ingeniería de computadores

Edición: López Matachana, Yansenis (yansenis@ispetp.rimed.cu)

Digitalización: Dr. C. Raúl G. Torricella Morales (torri@reduniv.edu.cu)

Calle 23 entre F y G, No. 564. El Vedado, Ciudad de La Habana, CP 10400, Cuba

e-mail: eduniv@reduniv.edu.cu

Sitio Web: http://revistas.mes.edu.cu

Dedicatoria

Dedico esta obra a mis padres, en especial a mi padre, quien me enseñó a ser profundamente martiano. Siempre decía que todo hombre debe crear y aportar a la sociedad para enriquecerla.

Índice general

Prólogo del autor

Varios años de recopilación de información, investigación, deducción y aplicación, me ha guiado para poder culminar este trabajo. En su mayoría se realizó mediante ensayo y error, poniendo a prueba los criterios del autor y sus propias experiencias. Para ello se realizó dicho trabajo en el pedagógico ISPETP “Héctor Alfredo Pineda Zaldivar”, en un laboratorio de computación, dedicado por completo al tiempo de máquina para los estudiantes y profesor. En los años comprendido entre 2001 y 2003. En estos momentos el autor aspira al título de Master en la UCI (Universidad de Ciencias Informáticas).

El tema de los virus informáticos es cada vez de mayor importancia porque son mayores los riesgos que se corren con los programas malignos. Los riesgos son enormes y no podemos darnos el lujo de que nuestra sociedad, que está entrando en la era de la informatización, no esté preparada para enfrentar este fenómeno. Todos los que manipulen una máquina tienen que saber lo que tiene que hacer para evitar contagios y propagaciones de virus, tomar medidas de contingencia y reparar los daños causados por dichos organismos. Mi aspiración es que cada usuario de computadora sea un conocedor sobre estos temas y esté preparado para cualquier eventualidad.

Agradecimientos

A mis padres, por velar tan celosamente por mi preparación para la vida.

A la revolución, a la que le debo la vida y mis estudio.

Introducción

Hoy en día, la rapidez de las comunicaciones y los modernos sistemas con que contamos, nos permiten un flujo de información prácticamente igual en cualquier lugar del mundo donde nos encontremos.

Se dice que la información y el conocimiento es poder, pues para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir información y hasta realizan el comercio en forma electrónica, para ser más eficientes. Pero al unirse en forma pública, se han vuelto vulnerables, pues cada sistema de computadora involucrado en la red es un blanco potencial para obtener información.

La tendencia en el contexto informático actual, es el aumento de organizaciones que conectan sus redes internas a la Internet. Al conectar una red a la Internet se tiene acceso a las redes de otras organizaciones que también estén conectadas. De la misma forma que accedemos a un ordenador de nuestra entidad, se puede recibir información de un servidor en Japón, conectarnos a una computadora en Venezuela o desde muchos otros lugares del mundo. El mundo informático cuenta con varias decenas de millones de computadoras interconectadas, no sería imprudente pensar que exista más de una persona con intenciones perversas. Por eso se debe tener la red protegida adecuadamente, toda precaución tomada nunca será suficiente.

Cada día que pasa es más frecuente escuchar noticias sobre las redes de importantes organizaciones que han sido violados sus sistemas de seguridad por desconocidos, alguno de ellos se denominan “Hackers”, aunque en este mundo de la informática existen otros grupos como los “Lamers” , “Crackers”, entre otros. A pesar de que la prensa extranjera a publicado que tales intrusiones son solamente obras de adolescentes con propósito de entretenerse o de jugar ya no se trata de un incidente aislado, pues esto son solo los que han sido capturados por la ley. A diario se reciben reportes de ataques a redes informáticas, los que se han vuelto cada vez más siniestros, los archivos son alterados, las computadoras se vuelven inoperables, se ha copiado información confidencial sin autorización, se ha reemplazado el “software” para agregar puertas traseras de entradas y miles de contraseñas han sido capturadas a usuarios inocentes, con todo el peligro potencial que esto representa.

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en los Laboratorios “Bell”. Hacia finales de los años 60 Douglas Mcllory, Victor Vysottky y Robert Morris, idearon un juego llamado “Core War” (guerra en lo central) aludiendo a la memoria de la computadora, que se convirtió en el pasatiempo de alguno de los programadores de los laboratorio BELL, de AT & T. El juego consistía en que dos jugadores escribieran cada uno un programa llamado “organismo”, cuyo habitad fuera la memoria de la computadora, a partir de una señal, cada programa forzaba al otro a realizar una función inválida, ganando el primero que lo consiguiera. Al termino del juego, se borraba de la memoria todo rastro de la batalla ya que estas actividades estaban severamente sancionada por los jefes, por ser un gran riesgo que quedara un “organismo” suelto que acabara con las aplicaciones del día siguiente. De esta manera surgieron los programas destinados a “dañar” en la escena de la computación.

En 1983, el ingeniero eléctrico estadounidense, Fred Cohen, acuñó el término "virus" para describir un programa informático que se reproduce a sí mismo.

¿Cómo nacieron los virus?

En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUME-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos

Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la universidad estadounidense *Delaware* notaron que tenían un virus porque comenzaron a ver (© *Brain*) como etiqueta de los disquetes. La causa de ello era *Brain Computer Service*, una casa de computación paquistaní que desde 1986 vendía copias ilegales de software comercial infestadas, para según los responsables de la firma, dar una lección a los piratas.

Los especialistas de *Brain Computer Service* habían notado que el sector de boteo de un disquete contenía código ejecutable y que dicho código se ejecutaba cada vez que la máquina se inicializaba desde un disquete. Lograron reemplazar ese código por su propio programa residente y que este instalara una replica de sí mismo en cada disquete que fuera utilizado de ahí en lo adelante.

También en 1986 un programador llamado *Ralph Burger*, se dio cuenta de que un archivo podía ser creado para copiarse así mismo, adosando una copia de él a otros archivos. Escribió una demostración de este efecto a la que llamó VIRDEM, que podía infestar cualquier archivo con extensión (COM). Esto atrajo tanto interés que se le pidió que escribiera un libro. Debido a que él desconocía lo que estaba ocurriendo en Pakistán, no mencionó a los virus del sector de arranque (*boot sector*). Para este entonces ya se había empezado a diseminar el virus VIENNA.

Actual mente los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta, algunos de ellos dicen hacerlo por diversión o pasatiempo, otros quizás por probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

Con relación a la motivación de los autores de virus para llevar a cabo su obra, existe en Internet un documento escrito por "*Freelance Marcus Salo*", en el cual, se exponen varios conceptos entre los que podemos encontrar los siguientes:

- "Algunos de los programadores de virus, especialmente los mejores, sostienen que sus interés por el tema es puramente científico, que desean averiguar todo lo que se pueda sobre virus y sus usos"
- "El hecho de escribir programas virales dan al programador cierta fuerza coercitiva, lo pone fura de las reglas convencionales de comportamiento. Este factor es uno de los más importantes, pues el sentimiento de pertenencia es algo necesario para todo ser humano y está probado que dicho sentimiento pareciera verse reforzado en situaciones marginales"
- "Por otro lado ciertos programadores parecen legalizar sus actos poniendo sus creaciones al alcance de mucha gente, (vía Internet, BBS especializada, etc.) haciendo la salvedad de que el material es peligroso por lo cual el usuario debería tomar las precauciones y que ellos no se hacen responsables de los usos que otras personas pudieran hacer"
- "Existen programadores de los cuales generalmente, provienen los virus más destructivos, que alegan que sus programas están creados para hacer notoria la falta de protección que sufren la mayoría de los usuarios de computadoras"

En otros contextos también se ha manejado que la producción inicial de virus informáticos, haya sido obra de personas inescrupulosas con ansias de hacer dinero con posteriores curas, es decir, antivirus. Aunque esto son solo especulaciones y posibilidades, no existe la posibilidad real de probar que esto haya sucedido así. Lo cierto es que ya hoy en día las corporaciones están tan ocupadas en hacer las vacunas para los virus que aparecen en cualquier lugar del mundo que ya no tendrían tiempo de fabricar los suyos. En definitiva sea cual fuere el motivo por el cual se sigue produciendo virus, se debe destacar que su existencia no ha sido solo perjuicios: Gracias a ellos, muchas personas ha tomado conciencia de que es lo que tiene y de cómo protegerlo.

Desarrollo

CAPÍTULO 1

1- Conociendo a los virus

1.1- ¿Qué es un virus?

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el consentimiento o el permiso de este. Se dice que es un programa parásito porque ataca a los archivos o al sector de arranque cuyo nombre en ingles es (Boot) y se replica a sí mismo para continuar su esparcimiento hacia otras máquinas.

Algunos se limitan solamente a replicarse, mientras que otros pueden afectar a los sistemas.

Los virus tienen diferentes finalidades o propósitos: Algunos solo infestan, otros alteran datos, otros los eliminan, otros destruyen el hardware, otros destruyen los softwares, algunos solo muestran mensajes, pero todos persiguen un propósito en común “propagarse”.

1.2- Potencial de daño

Es importante destacar que el potencial de daño de un virus informático no depende de su complejidad, sino del entorno donde actúa.

La definición más sencilla y completa que hay de virus corresponde al modelo “DAS” y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

1. Dañino.
2. Auto-reproductor.
3. Subrepticio.

Así mismo, se pueden distinguir tres módulos principales de un virus informático:

- Módulo de reproducción.
- Módulo de ataque.
- Módulo de defensa.

Módulo de reproducción: Se encarga las rutinas de infección de programas ejecutables (archivos de datos, en el caso de los virus macros) afín de que el virus pueda ejecutarse subrepticiamente, pudiendo de esta manera tomar control del sistema e infestar a otros programas permitiendo su traslado de una computadora a otra a través de estos archivos.

Módulo de ataque: Es optativo. En caso de estar presente es el encargado de manejar las rutinas de daños adicional del virus. Por ejemplo, un virus además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica una fecha determinada.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

Módulo de defensa: Tiene la misión de proteger al virus y como el de ataque puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar en todo lo posible su detección.

1.3- Clasificación de los Virus

En 1984 el *Dr. Fred Cohen* clasificó a los emergentes virus de computadoras en tres categorías:

- Caballos de Troya
- Gusanos
- Virus

Empleó el término "gusano" porque los consideraba programas despreciables.

En 1984 al sustentar su tesis para un Doctorado en ingeniería eléctrica en la universidad al sur de California, demostró como se podrían crear virus, motivo por el cual es considerado como el primer autor auto identificado de virus de computadoras.

Cabe mencionar que la IBM PC (computadora personal) fue lanzada en agosto de 1981 y a partir de esa fecha los *Hackers* comenzaron a tomar mayor interés en los virus. Ese mismo año presentó su libro "Un pequeño curso de virus de computadoras", para posteriormente escribir y publicar "*The Gospel according to Fred*" el cual significa "El evangelio según *Fred*".

1. **Caballos de Troya**: Por la forma subrepticia que usaban para ingresar a un sistema.
2. **Gusanos**: Por las técnicas que se usaban para ingresar a los sistemas que eran consideradas fuera de toda ética, repugnantes y despreciables.
3. **Virus**: Un programa que tiene la capacidad de infestar a otros programas incluyendo una copia de su código dentro de este programa.

1.4- Tipos de virus

La tipología de los virus se define por el modo en que actúan infectando la computadora. Es decir ¿a quién está dirigido el daño?:

1. **Programas**: Estos virus parásitos, infectan ficheros y ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado cuando se ejecuta dicho programa.
2. **Boot**: Los virus del sector de arranque inicial, residen en la primera parte del disco duro, disquetes o medios de almacenamientos masivos, conocida como sector de arranque inicial, ellos sustituyen o modifican la información sobre el contenido del disco o de los programas que arrancan el ordenador. Estos virus suelen difundirse mediante cualquier medio de almacenamiento..
3. **Multiples**: Estos virus combinan las capacidades de los virus de programas y de sector de arranque inicial. Pueden infectar tanto ficheros como sectores de arranque inicial.
4. **Acompañantes**: Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo engañando al sistema operativo para que lo ejecute.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

5. **Bios**: Este grupo de virus atacan directamente al Bios de la máquina modificando la información contenida en ellos provocando un mal funcionamiento de la máquina, que puede hacer que no se reconozcan los dispositivos en ella instalados hasta la destrucción de esta pieza provocando la inutilización de la máquina, hasta que se reponga dicha pieza.
6. **Hoax**: Los Hoax están diseñados únicamente para asustar, es decir jugarle una broma al usuario.

1.5- Características de los virus

El virus es un pequeño software (cuanto más pequeño es más fácil de esparcir y más difícil de detectar) que permanece inactivo hasta que un hecho hace que el programa sea ejecutado. De esa forma el programa del virus es activado se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "boteo". Menos comunes son los no residente que no permanecen en la memoria después que el programa huésped es cerrado.

Los virus pueden llegar a "camuflarse" y esconderse para evitar la detección y reparación. ¿Cómo lo hacen?

1. **Re-orientación**: El virus reorienta la lectura del disco para evitar ser detectado.
2. **Desinformación**: Los datos sobre el tamaño del directorio infestado son modificados en la FAT, para evitar que se descubra bites extras, que aporta el virus.
3. **Encriptamiento**: el virus se encripta en símbolos sin sentidos para no ser detectado, pero para destruir o replicarse debe desencriptarse siendo entonces detectable.
4. **Polimorfismo**: Muta cambiando segmento del código para parecer distinto en cada nueva "generación", lo que lo hace muy difíciles de detectar y desinfectar.
5. **Gatillables**: Se relaciona con un evento que es el encargado de la ejecución del virus que puede ser el cambio de fecha, una determinada combinación de teclas, una macro o la apertura de un programa específico o uno asociado al virus (generalmente son troyanos).

Los archivos de datos como los de textos (TXT, DOC Y HTML), no pueden contener virus, aunque pueden ser dañados por estos. Aunque debemos tener especial cuidado con los documentos de tipo DOC, ya que estos incluyen una funcionalidad que pueden ser de gran ayuda, como son las macros, pero estas macros si pueden contener virus, por los que se recomienda desactivar las macros para leer los documentos de Word.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

CAPÍTULO 2

2- Una mirada más profunda

2.1- ¿A quien puede afectar cada uno de estos grupos de virus?

Los virus de Programas: Se manifiestan cuando la aplicación infestada es ejecutada, el virus se activa y se carga en la memoria, infestando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos, o permanecer inactivos por largos períodos de tiempo, infestan archivos ejecutables con extensión tales como: COM, EXE, DRV, SYS, BIN, BAT, entre otras.

Los virus de sectores de Boteo: Se instalan en estos sectores y desde allí se van trasladando a los sectores equivalentes de cada uno de los discos de la PC. Pueden dañar el sector o sobrescribir, cuando su desinfección es imposible, lamentablemente obligan al formateo del disco infestado, incluyendo disco de 3,5 " y todo tipo de unidades de almacenamiento.

Los virus múltiples: Estos virus tienen la capacidad de infestar el sector de arranque de la máquina así como a un programa ejecutable.

Acompañantes: Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo engañando al sistema operativo para que lo ejecute. Puede hacerlo en los archivos del sistema o de otros programas ya instalados en la computadora personal.

Los virus que infectan los Bios: Estos atacan al bios y los inutilizan o desde allí sobrescriben los discos duros, ellos por lo general atacan al hardware de la máquina.

Los virus Hoax: Se distribuyen por correo electrónico y una de las formas de eliminarlos es el uso del sentido común aunque muchos antivirus incorporan la revisión del correo electrónico, este tipo de virus es capaz de entrar vía correo y expandirse de forma solapada. Es la forma más usada por los Hackers le envían un virus por correo, cuyo propósito no es destruir información sino obtenerla de usted.

2.2- Daño de los virus

Se define como daño a la acción indeseada sobre un fichero que altere su integridad sin el consentimiento del usuario o mediante artificios para que se acepte su acción y deteriore la información contenida en él y de una manera u otra perjudica al usuario o al sistema.

Los daños se clasifican según la cantidad de tiempo necesaria para repararlos. Existen seis categorías de daños hechos por los virus de acuerdo a la gravedad:

1. **Daños triviales**: Sirva como ejemplo la forma de trabajo del virus *Form* (el más común) en el día 18 de cada mes cualquier tecla que presionemos hace sonar el *beep*. Deshacerse del virus implica generalmente segundos o minutos.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

2. **Daños menores**: Un buen ejemplo de este tipo de daños es el Jerusalem. Este virus borra los viernes 13 todos los programas que uno trate de usar después de que el virus haya infestado la memoria residente. En el peor de los casos tendremos que reinstalar los programas perdidos esto nos llevará alrededor de 30 minutos.
3. **Daños moderados**: Cuando un virus formatea el disco duro mezcla los componentes de la FAT por sus siglas en inglés (*File Allocation Table*) traducido al español (Tabla de Ubicación de Archivos), o sobrescribe el disco duro. En este caso, sabremos inmediatamente que es lo que está sucediendo y podremos reinstalar el sistema operativo y utilizar el último Backup (copia de respaldo). Esto quizás nos tome una hora.
4. **Daños Mayores**: Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibido, pueden lograr que ni siquiera restaurando de un Backup recuperemos el último estado bueno de los datos, un buen ejemplo de esto es el virus "*Dark Avenger*" , que infesta archivos y acumula la cantidad de infecciones que realizó cuando este contador llega a 16 elige un sector del disco a la zar y en el escribe la frase "*Eddy live ... somewhere in time*" (Eddy vive … en algún lugar en el tiempo) . Esto puede haber estado pasando por algún tiempo sin que lo notemos, pero el día que detectemos la presencia del virus y queramos restaurar el último Backup notaremos que también el está infestado. Puede que lleguemos a encontrar una copia de respaldo limpia, pero será tan vieja que probablemente hayamos perdido una gran cantidad de información o archivos que fueron creados con posterioridad a él.
5. **Daños severos**: Los daños severos son hechos cuando un virus realiza daños mínimos graduales y progresivos. No sabemos cuando los datos son correctos o han cambiado.
6. **Daños ilimitados**: Algunos programas como "Cheeba", "Vacsina44.Log-in" y "GPL1" entre otros, destinados a obtener la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos son Troyanos. En el caso de Cheeba, crea un nuevo usuario con los privilegios máximos fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que se le antoje.

2.3- Síntomas típicos de una infección

- El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente (en máquinas de alta velocidad).
- El tamaño del programa cambia sin razón aparente.
- El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea real.
- Su Windows comienza a informar de forma incorrecta las capacidades de disco, disquetes y CD al igual que los espacios vacíos y llenos aumentando este último por encima de lo real.
- En Windows aparece: "32 bits error".
- La luz del disco duro en la torre continúa parpadeando aunque no se esté trabajando ni haya protectores de pantallas activados. (se debe tomar este síntoma con mucho cuidado, porque no siempre es un virus).
- No se puede "botear" desde la disquetera o torre (A:), ni siquiera con los disco de rescate.
- Aparecen archivos con nombres y extensiones extrañas.
- Los caracteres de texto se caen "literalmente" a la parte inferior de la pantalla como la lluvia, especialmente en sistema operativo MS DOS.
- En la pantalla del monitor pueden aparecer mensajes absurdos tales como "Tengo hambre", "Introduce un *Big Mac* en la unidad A:".

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

- En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrio repartidos de colores y una leyenda en negro que dice “Windows 98” (No puedo evitarlo, es mas fuerte que yo … !!)
- Al salvar documento de texto descubre que tiene otros nombre como : “El elefante gordo”, “La vieja loca”, “Un elefante bailarín”, entre otros nombres absurdos los cuales usted no ha creado. En la mayoría de los casos los textos contenidos son ilegibles o contienen repetidas veces el mismo nombre del documento y otros más.

Una infección se soluciona con las llamadas ”vacunas” (que impiden la infección) o con los remedios que desactivan o eliminan (o tratan de hacerlo) a los virus de los archivos infestados. Hay ciertos tipos de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infestado.

2.4- ¿Qué hacen algunos virus informáticos?

- **El Pin pon**: Fue descubierto en marzo de 1988 y en poco tiempo estuvo en Cuba, donde se convirtió rápidamente en epidemia. La falta de conocimiento sobre los virus ayudó a que se diseminara ampliamente y fuera incontrolable en un principio. Ese mismo desconocimiento llevó a que pasara bastante tiempo hasta que se empezara a tomar medidas. Solo después de algunos meses, en revistas especializadas en informática empezaron a publicar formas de desinfectar los discos y como consecuencia de ello se aplicaron políticas de seguridad en las unidades y entidades del estado. Lo positivo de esto fue que las personas comenzaran a conocer sistema operativo MS DOS más profundamente, por ejemplo el “boot sector” ¿qué es? y ¿para qué sirve? Ya que las máquinas eran utilizadas pero pocos sabían como funcionaban internamente. Este virus mostraba un síntoma muy evidente (una pelotita que rebotaba por la pantalla) se pensó que todos los virus debían ser visibles, pero las siguientes generaciones fueron más subrepticios y se limitaban a reproducirse o destruir sin avisar al usuario o si que este se diera cuenta. El Pin pon original no podía infestar discos duros, pero la versión que se popularizó en el país fue la “B” que si podía hacerlo. Se creó una variante en argentina, el Pin pon C, que no mostraba la pelotita en la pantalla. Este virus está extinto en este momento ya que solo podía funcionar en máquinas cuyo procesador fueran 8088 y 8086, porque ejecutaba una instrucción no documentada en estos e incorrecta en los modelos siguientes.
- **Avispa**: Escrito en noviembre de 1993, en muy poco tiempo se convirtió en epidemia, infesta archivos “exe”. Al ejecutarse, si no se encontraba ya residente en memoria intenta infestar los archivos: xcopy, mem, setver y emm386, para maximizar sus posibilidades de reproducción ya que estos archivos son de los más frecuentemente utilizados. Este virus está encriptado siempre con una clave distinta (polimórfico), para dificultar su detección por medios de antivirus eurísticos.
- **Menem Tocoto**: Esta adaptación del virus “Michelangelo” apareció en 1994. en los disquetes se aloja en el sector de arranque y en los discos duros en la tabla de particiones, es muy sencillo y fácil de detectar.
- **Camuflage II**: Apareció por primera vez en 1993, infesta el sector de arranque de los disquetes ubicados en la unidad “A:” y la tabla de partición de los discos duros. Es un virus simple y fácil de detectar.
  - **Leproso**: Creado en 1993, en rosario, provincia de santa Fe, se activa el día 12 de enero (cumpleaños del autor), hace aparecer un mensaje que dice: “Felicitaciones, su máquina está infestada por el virus leproso creado por J. P. Hoy es mi cumpleaños y lo voy a

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

festejar formateando su disco duro. Bye … Vamos Ne well´s que con Diego somos campeones.

- **Pindonga**: Virus polimórfico residente en memoria que se activa los días 25 de febrero, 21 de marzo, 27 de agosto y 16 de septiembre, cuando ataca borra toda la información contenida en el disco duro.
- **Teddy**: Es el primer virus argentino interactivo. Apareció hace algún tiempo, infesta archivos con extensión ".exe" y se caracteriza por hacerle una serie de preguntas al usuario. Una vez activado, se muestra una pantalla con el siguiente cartel: !*Teddy*, el primer virus interactivo de la computación¡ Responda el siguiente cuestionario:
  - ¿Los programas que usted utiliza son originales? (S/N)
  - ¿Los de Microsoft son unos ladrones? (S/N).
  - Si se responde afirmativa mente a la primera pregunta, el virus contestará "Cinco archivos menos por mentiroso".
  - En caso contrario "Dos archivos menos por ladrón"
  - En cuanto a la segunda pregunta, el único mensaje que se ha visto es: "Te doy otra oportunidad para responder". Con este virus los archivos infestados aumentarán su tamaño en 4 310 bites.
- Natas: Alias (Satán) su nombre al revés, infesta la Tabla de Particiones y sector de arranque del DOS así como ficheros con extensión (.exe y .com). Tipo: Residente (6 Kbytes en memoria RAM). Tamaño: 4744 bytes. Reparación: Siempre. Activación: Si. Infecta ficheros con formato ejecutable, incrementando sus tamaños en 4744 bytes. El código del virus está cifrado. El sector de arranque original no es salvado. En los discos duros el resto del código es almacenado en la zona de los sectores especiales ocultos y en los disquetes está en los primeros 9 sectores de la última pista de la cara 1. Utiliza la técnica STEALTH para ocultarse, trampas para evitar el *debugger* y el código cifrado varía en cada nueva infección (polimorfismo). Disminuye la cantidad de memoria RAM en 6 K bytes. El año de creación de los ficheros infectados es incrementado en 100. Bajo ciertas condiciones formatea todos los discos duros.

2.5- ¿Qué no es un virus?

Existen algunos programas que sin llegar a ser virus ocasionan problemas al usuario. Estos programas, carecen de por lo menos una de las tres características que identifican a un virus (Dañino, Auto reproductor y Subrepticio).

Hace algunos años la red de IBM, encargada de conectar más de 130 países, fue virtualmente paralizada por haberse saturado con un correo electrónico que contenía un mensaje de felicitación navideña que una vez leído por el destinatario, se enviaba a sí mismo a cada uno de los integrantes de la libreta da direcciones de correo del usuario, sin ocasionar daño alguno. Al cabo del tiempo fueron tanto los mensajes que esperaban ser leídos por sus destinatarios que el trafico se volvió demasiado alto, lo que ocasionó la caída de la red.

Otro ejemplo de algunos ingeniosos, es que han querido convertirnos en parte de sus virus, de una forma nunca antes pensada, imposible de detectar por los antivirus actuales, quizás parezca increíble pero es muy posible que usted haya sido partícipe de estas técnicas, veamos:

Recibe usted un correo con un mensaje de cualquier tipo que debe enviarlo posteriormente a 10 personas o a sus amigos, si no lo hace será usted objeto de mala suerte durante una cantidad de años

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

determinados o que usted no tiene corazón si no reenvía ese mensaje, o que algo bueno le sucederá dentro de un lapso de tiempo después de enviar el correo entre otras tácticas.

Ahora analizamos, usted recibe el mensaje, no sabemos cuantas personas antes que usted han recibido ese mensaje, por lo que partamos de la idea que usted es el primero. Usted se dice, no tengo nada que perder, solo son 10 mensajes, lo cierto es que sus 10 correos si todos piensan y actúan como usted se convertirán instantáneamente en 100 pues esos 10 se lo enviarán a otros 10 cada uno y nunca faltará el exagerado, luego esas 100 se lo enviarán a otras 10 cada uno y así sucesivamente.

Para que tenga una idea más cercana de lo que sucede vea la siguiente tabla.

Envíos	Personas	Correos resultantes en tráfico
1	1	10
2	10	100
3	100	1 000
4	1 000	10 000
5	10 000	100 000
6	100 000	1 000 000
7	1 000 000	10 000 000
8	10 000 000	100 000 000
9	100 000 000	1 000 000 000
10	10 000 000 000	100 000 000 000

Esto trae como consecuencia indiscutible el colapso de las redes sin necesidad de virus, pues somos nosotros mismos los virus. Una verdadera ironía.

Estamos seguros que en el futuro seremos más cuidadosos para intentar combatir este tipo de ataque a las redes. Los servicios de correo han ideado una forma de hacerle frente a este fenómeno, poniendo una denominación al correo cuando detecta en su lista a múltiples destinatarios y múltiples envíos, entonces los catalogan como SPAM y lo notifica al usuario para que tenga conocimiento de ello, pero no toma ninguna acción.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

CAPÍTULO 3

3- Armas de combate

3.1- ¿Qué es un antivirus?

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

Es importante aclarar que todo antivirus es un programa y que como todo programa solo funcionará correctamente si es adecuado y está bien configurado, además un antivirus es una herramienta para el usuario y no será eficaz para el 100 % de los casos y nunca debe considerar que será una protección total ni definitiva o inexpugnable.

La función de un programa antivirus es detectar de alguna manera la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independiente mente de las prestaciones adicionales que pueda ofrecer, puesto que solo el hecho de detectar la presencia de un virus informático, detener el accionar del mismo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una computadora personal infestada.

El modelo primario de las funciones de un programa antivirus es la detección de su presencia y en lo posible su identificación. La primera técnica que se popularizó para la detección de virus informáticos y que todavía se sigue utilizando, aunque cada vez con menos eficiencia es la técnica del "*scanning*" lo que traducido al español significa (escandir). Esta técnica consiste en revisar el código de todos los archivos contenidos en las unidades de almacenamiento, fundamentalmente los archivos ejecutables, en busca de pequeñas porciones de código, que puedan pertenecer a un virus informático. Este procedimiento, denominado "escaneo" se realiza a partir de una base de datos que contiene porciones de códigos representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda.

Esta técnica de escaneo fue bastante eficaz en los primeros tiempos, cuando habían pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los que desarrollaban antivirus escaneadores tuvieran tiempo de analizar el virus extraer la porción de código que lo iba a identificar y se agregaba a la base de datos del programa antivirus.

El primer punto grave de este sistema radica en que siempre brinda una solución posterior, es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado por usuarios capacitados, especialistas o distribuidores de producto a los analistas de virus estos lo analizarán, extraerán la porción de código que lo identificará y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comience a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

Además este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas cuya sumatoria jamás constituirá una solución definitiva, que debe actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis la técnica de escanear es hoy en día poco eficaz, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y como son estos los de mayor dispersión permite una importante gama de posibilidades.

Un ejemplo típico de un antivirus de esta clase es el "Virus scan" de MC Afee.

En virtud del agotamiento de la técnica de escanear, los desarrolladores de software antivirus han dotado a sus programas de otros métodos para la búsqueda de virus informáticos y sus actividades, que no identifican específicamente al virus sino algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastre rutinas de alteración de información que no puedan ser controladas por el usuario, tales como (modificaciones de sectores críticos de las unidades de almacenamiento como el "sector maestro de arranque" , "sector de arranque", "FAT", entre otras). Un ejemplo de este tipo de métodos es el que utiliza algoritmos heurísticos.

Este tipo de procedimientos busca de manera bastante eficiente códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en que puede llegar a sospechar de muchísimas cosas que no son virus. Esto hace necesario que el usuario que lo utiliza conozca un poco a cerca de la estructura del sistema operativo afín de poseer conocimientos que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico. Algunos de los antivirus de esta clase son: F-Prot, Norton antivirus y Dr. Solomon´s Toolkit.

Otra forma de detectar la presencia de un virus informático en un sistema consiste en el monitoreo de las actividades de la computadora personal, señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denomina de chequeo de integridad.

Sobre la base de estas consideraciones, podemos decir que un buen sistema antivirus debe estar compuesto por un programa detector de virus, que siempre este residente en memoria y un programa que verifique la integridad de los sectores críticos del disco duro y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

3.2- Modelos antivirus

La estructura de un programa antivirus, está compuesta por dos módulos principales, el primero denominado de (control) y el segundo de (respuesta). A su vez, cada uno de ellos se divide en varias partes.

1. **Módulo de control**: Posee la técnica de verificación de integridad que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco duro. Se trata en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco duro que no son modificados a menos que el usuario lo requiera. Otra opción dentro de este módulo es la identificación de virus, que incluye diversas técnicas para la detección de virus informáticos. Las formas más

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

comunes de detección son el escaneo y los algoritmos, como por ejemplo los heurísticos. Así mismo la identificación de códigos dañinos es otra de las herramientas de detección que en este caso busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco duro. Esto implica descompilar o desensamblar en forma automática los archivos almacenados o ubicar sentencias o grupos de instrucciones peligrosas. Finalmente, el módulo de control también posee una administración de recursos para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a discos, etc). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.

2. **Módulo de respuesta**: La función alarma se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla. Algunos programas antivirus ofrecen una vez detectado un virus informático, la posibilidad de erradicarlo. Por consiguiente, la función reparar se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada. Por otra parte existen dos técnicas para evitar el contagio de entidades ejecutables, evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

CAPÍTULO 4

4- Más vale prevenir

4.1- Medidas de prevención

La primera medida de prevención que se debe tener en cuenta es, contar con un sistema antivirus y utilizarlo correctamente, por tanto la única forma en que se logra un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos, conocido en nuestro país como lineamientos a seguir dentro del plan de seguridad informática dentro de cada institución.

Estas normas tienden a controlar la entrada de archivos al disco duro de la computadora, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y por supuesto disminuyendo al mínimo posible todo tipo de tráfico.

Además de utilizar un sistema antivirus y controlar el trafico de archivos al disco duro, una forma muy eficaz de proteger los archivos ejecutables es utiliza un programa chequeador de integridad que verifique que estos archivos no sean modificados, es decir que mantengan su estructura, de esta manera antes que puedan ser infestados por un virus convencional se impediría su accionar.

Para prevenir la infección con un virus del sector de arranque, lo más indicado es no dejar disquetes olvidados en la disquetera y contar con un antivirus, pero además pueden aprovecharse dos características que incorporan los *setup* de las computadoras modernas:

1. Variar la secuencia de arranque de la computadora "Primero disco duro y luego disquetera" (C: , A:) o simplemente "solo disco duro" (C:). De esta manera, la computadora no intentará leer la disquetera en el arranque aunque tenga cargado un disquete.
2. En el *setup* también podemos encontrar una característica que nos brindará protección contra este tipo de virus y es la protección "Virus Warning". Si usted activa esta protección ningún virus podrá infestar su sector de arranque (boot) pues cuando inicie la máquina y el virus intente hacer esto la computadora personal le mostrará un mensaje en pantalla en el cual le pondrá al corriente sobre este intento y le da la opción de si usted admite que se modifique o no este sector, ¡lógicamente deberá denegar! ¿Cómo?, muy simple la máquina le preguntará que oprima la tecla (S) para permitir la modificación o la tecla (N) para impedir este cambio. Su variante en ingles sería (Y) para admitir y (N) para negar. Nuestra opción sería siempre (N). Debemos tener presente que si vamos a instalar un sistema operativo en la máquina primero revíselo con algún antivirus o con más de uno pues para instalar los sistemas Windows estos necesitan escribir en estos sectores y si está activada la protección "*Virus Warning*" del setup puede bloquear la instalación y provocar que no se instale el sistema en su equipo.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

4.2- ¿Quién certifica los productos antivirus en el ámbito internacional?

La NCSA (*Nacional Computer Security Association*) por sus siglas en ingles, su traducción al español sería (Asociación Nacional de Seguridad de Computadoras). Ellos son los encargados de certificar los productos antivirus.

Para obtener dicha certificación los productos deben tener una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario.

Antiguamente el esquema de certificación requería que se detectara (incluyendo el numero de versión de los virus) el 90% de la librería de virus del NCSA y fue estipulado para asegurar optimas capacidades de detección. Pero esta metodología no era completamente eficiente.

Actualmente el esquema de certificación enfoca la amenaza a las computadoras empresariales. Para ser certificados, el producto debe pasar las siguientes prueba:

- Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.
- Deben detectar como mínimo, el 90% de la librería de virus del NCSA (más de 6000 virus).

Estas pruebas son realizadas con el producto ejecutándose con su configuración por defecto.

Una vez que un producto ha sido certificado la NCSA tratará de recertificar el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación. Si un producto no pasa la primera o segunda prueba su distribuidor tendrá siete días para proveer la corrección. Si este límite de tiempo es excedido el producto será eliminado de la lista de productos certificados. Una vez que se ha retirado la certificación de un producto, la única forma de recuperarla es que el distribuidor envíe una nueva versión completa y certificable.

Acerca de la lista de virus de la NSCA, aclaremos que ningún desarrollador de antivirus puede obtener una copia, cuando un antivirus falla en la detección de algún virus incluido en la lista, una cadena identificatoria del virus le es enviada al productor del antivirus para su inclusión en futuras versiones.

En el caso de los virus polimórficos, se incluyen múltiples formas del virus para asegurar que el producto testeado los detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.

La A. V. P. D. (Antivirus Product Developers) por sus siglas en ingles cuya traducción sería (Desarrolladores de Productos Antivirus) es una asociación formada por las principales empresas informáticas del sector entre las que se encuentran:

- Cheyenne Software
- IBM
- McAfee Associates
- On Tecnology
- Stiller Research inc
- S & S Internacional
- Symantec Corp
- Thunder Byte

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

4.3- Algunos antivirus

4.3.1- Dr. Solomon´s Anti virus Toolkit

Certificado por la NCSA, detecta más de 6500 virus, gracias a su propia estructura de detección llamada "Vir Tran", con una velocidad de detección entre 3 y 5 veces mayor que los antivirus tradicionales.

Uno de los últimos desarrollos S & S es la tecnología G. D. G. (*Generic Decryption Engine*) por sus siglas en ingles lo cual traducido al español significa (Motor de desencriptación Genérica), que permite detectar virus polimórficos sin importar el algoritmo de encriptación utilizado.

Permite detectar modificaciones producidas tanto en archivos como en la tabla de partición del disco duro. Para ello utiliza *Check sums* criptográficos lo cual, sumado a una clave personal de cada usuario, hace casi imposible que el virus pueda descubrir la clave encriptada.

Elimina virus en archivos en forma sencilla y efectiva, con pocas falsas alarmas y en sectores de boteo y tablas de partición, la protección es genérica, es decir independiente del virus encontrado.

Otras características que presenta este antivirus son:

- Ocupa nueve Kb de memoria extendida o expandida.
- Documentación amplia y detallada en español y una enciclopedia sobre los virus más importantes.
- Actualizaciones mensuales o trimestrales del software y manuales.
- Trabaja como residente bajo Windows.
- A. H. A. por sus siglas en ingles (Advanced Heuristic Analysis) en español significa (Análisis Heurístico Avanzado).

4.3.2- Norton Antivirus

Certificado por la NCSA, posee una protección automática en segundo plano. Detiene prácticamente todos los virus conocidos y desconocidos a través de una tecnología propia denominada "Novi" que implica control de las actividades típicas de un virus, protegiendo la integridad del sistema, antes de que causen algún daño o pérdida de información, con una amplia línea de defensa que combina búsqueda, detección de virus e inoculación, (se denomina inoculación al método por el cual este antivirus toma las características principales de los sectores de boteo y archivos para luego chequear su integridad. Cada vez que se detecta un cambio en dichas áreas, Norton Antivirus, avisa al usuario y provee las opciones de (reparar, volver a usar la imagen guardada, continuar, no realizar cambios, inocular y actualizar la imagen).

Utiliza diagnósticos propios para prevenir infecciones de sus archivos y de archivos comprimidos.

El escaneo puede ser lanzado manual mente o automáticamente a través de la planificación de fecha y hora, también permite reparar los archivos infestados por virus desconocidos. Incluye información sobre muchos de los virus que detecta y permite establecer una contraseña para aumentar así la seguridad.

La lista de virus conocidos puede ser actualizada periódicamente (sin cargos adicionales) a través de servicios en línea como Internet, America on Line, Compuserver, The Microsoft Network o el BBS propio de Symantec, entre otros.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

4.3.3- VirusScan

Este antivirus de McAfee Associates, trabaja por el sistema de *scanning* descrito anteriormente y es el mejor en su estilo.

Para escanear hace uso de dos técnicas propias CMS por sus siglas en ingles (*Code Matrix Scanning*) lo cual traducido al español significa (escaneo de códigos de Matriz) y CTS por sus siglas en ingles significa (*Code Trace Scanning*) lo cual traducido al español significa (escaneo de seguimiento de código).

Una de las principales ventajas de este antivirus es que la actualización de los archivos de bases de datos de strings es muy fácil de realizar, lo cual sumado a su condición de programa shareware, lo pone al alcance de cualquier usuario. Es bastante flexible en cuanto a la configuración de cómo detectar reportar y eliminar virus.

4.3.4- Sav 32 Versión 12.1

En documentación de la empresa de Consultoría y Seguridad Informática denominada "Segurmática" empresa netamente cubana, ofreció los siguientes datos sobre su producto que incluye:

- Protección permanente contra programas malignos, impidiendo que estos se ejecuten en la computadora.
- Es capaz de identificar y descontaminar utilizando datos de programas malignos conocidos y por medio de métodos heurísticos.
- Está preparado para identificar programas malignos dentro de ficheros comprimidos.
- Incorpora una enciclopedia con información sobre los programas malignos.
- Dispone de una herramienta adicional para detectar programas malignos en buzones de correos de Outlook Express.
- Detecta no solamente programas malignos sino también correos sospechosos que pudieran por ejemplo descargar un programa maligno desde Internet.
- Las actualizaciones se realizan desde Internet o la red local de forma automática o manual.
- La protección permanente utiliza muy pocos recursos y a diferencia de otros productos antivirus, no hace más lenta la máquina.

4.3.4.1- Ventajas del Sav

- El mecanismo de protección permanente ha sido completamente rediseñado para ofrecer mayor robustez.
- Instalación única para todos los sistemas operativos soportados por el producto.
- Instalación más sencilla que incluye todos los componentes del producto, permitiendo seleccionar cual de ellos se desea instalar.
- Actualización menor en tamaño y con integridad garantizada con una firma digital.
- Nuevo programador de tares más eficiente.

4.3.4.2- Consideraciones sobre el Sav

A pesar de las nuevas mejoras incorporadas a este producto no ha podido establecer una seguridad alta a niveles competitivos en el ámbito internacional. Pero ha tenido una difusión en el mercado nacional, que ha dado respuesta a las necesidades de nuestros centros educativos y empresas del sector productivo.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

No ha brindado toda la protección que necesitamos en estos tiempos modernos pero, ¿qué sistema puede garantizarla?

Es frecuente obtener información de algún centro de enseñanza o llevarle información al mismo en el cual se encuentre instalado y actualizado el Sav y al revisar con otro sistema antivirus detectamos alguna manifestación de virus y en ocasiones más de una.

Pero también hemos podido constatar que el Sav ha detectado virus mayormente del tipo gusano y Caballos de Troya, que provienen de máquinas cuya protección está basada en sistemas con antivirus de renombre como Norton y Kaspersky los cuales no han detectado dichas amenazas y solo ha sido posible la detección y erradicación gracias a nuestro producto antivirus nacional Sav.

4.3.4.3- ¿Porqué es tan importante el Sav?

Por nuestro propio desarrollo y estima además de su demostración diaria en el enfrentamiento contra estos virus transgresores de la paz informática, nuestro antivirus ha demostrado muy buenos resultados, por lo que no debe ser despreciado, ni menospreciado por nadie, los científicos seguirán trabajando en su perfeccionamiento para nuestra tranquilidad informática.

Ningún producto antivirus nació siendo perfecto, es el producto del trabajo diario y el esfuerzo acumulado de muchos años y de muchas personas los que han hecho posible su calidad. El nuestro va por ese largo camino, ya que la informatización de nuestra sociedad empezó rezagada y aunque no vamos a la vanguardia, tampoco estamos en la retaguardia, estos momentos es muy evidente los esfuerzos que realiza nuestro país por colocarse entre los primeros en esta disciplina y ejemplos tenemos muchos desde los nuevos politécnicos de informática hasta la UCI (Universidad de Ciencias Informáticas) de reciente creación.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

CAPÍTULO 5

5- Eliminando amenazas

5.1- Recomendaciones para combatir a los virus

Algunos dicen que cualquier antivirus es mejor que el Sav, están errados, lo cierto es que ningún desarrollador de sistemas antivirales puede garantizar su producto al 100%, argumento más que suficiente para derribar el mito de cualquier antivirus.

Para poder poner una barrera antiviral que sea lo más segura posible, lo indicado es combinar las características antivirales que tienen varios de estos programas. La cuestión no es llenar la máquina con antivirus porque esto va en contra del buen desempeño de la Pc, pues se tomaría demasiado tiempo para ejecutar una instrucción, ya que estaría siendo revisada por un gran numero de programas rastreadores de virus y por diferentes técnicas. La idea es poner solo dos antivirus para mezclar diferentes técnicas de rastreo y detección. De esta forma la acción combinada de ellos nos provea de un entorno más seguro.

5.1.1- Las mejores combinaciones de antivirus

A continuación se enumeran las combinaciones de antivirus que tienen el mejor desempeño:

- Sav y Kapesky Antivirus
- Sav y Norton Antivirus
- Sav y McAfee
- Sav y Dr. Solomon´s Antivirus Toolkit
- Sav y VirusScan
- Sav y Panda Antivirus.

Muchos plantean que el sistema antivirus Sav no debe usarse porque existe antivirus con mayor calidad. La realidad no siempre es lo que parece, en múltiples ocasiones he presenciado la detección de un virus por el Sav y otros programas antivirus no lo han detectado, algunos tan prestigiosos como el Kapesky y el Norton. Es importante destacar que en nuestro país también se han creado virus por personas que quieren unirse a la comunidad de innovadores de la “destrucción” en nombre de la ciencia. Muchos de estos virus que hacen grandes estragos no son detectados por productos antivirus extranjeros.

Siempre que usted vaya a instalar una de las combinaciones recomendadas instale primero el Sav y luego cualquiera de los de más productos antivirales según recomendación del autor, esto no es capricho es una forma de evitar conflictos y bloqueos de las instalaciones ya que si primero instala cualquier otro producto antivirus cuando vaya a instalar el Sav deberá desactivar la protección permanente del producto antivirus que instaló antes para que permita así la instalación del Sav, una ves instalado y actualizado podrá reactivar la protección permanente y reiniciar la máquina y verá que no hay conflictos ni problemas. Si instala primero el Sav se ahorrará todas estas molestias ya que él no entrará en conflicto no el próximo producto que instalará. Eso sí el arranque inicial de la

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

máquina será un poco más lento que antes solo espere a que los dos antivirus hayan cargado la protección permanente antes de introducir cualquier medio de almacenamiento o cualquier dispositivo como Ipo, celulares, tarjetas de memorias de cámaras etc.

Muchos plantean que el sistema antivirus Sav no debe usarse porque existe antivirus con mayor calidad. La realidad no siempre es lo que parece, en múltiples ocasiones he presenciado la detección de un virus por el Sav y otros programas antivirus no lo han detectado, algunos tan prestigiosos como el Kapesky y el Norton. Es importante destacar que en nuestro país también se han creado virus por personas que quieren unirse a la comunidad de innovadores de la "destrucción" en nombre de la ciencia. Muchos de estos virus que hacen grandes estragos no son detectados por productos antivirus extranjeros.

Siempre que usted vaya a instalar una de las combinaciones recomendadas instale primero el Sav y luego cualquiera de los de más productos antivirales según recomendación del autor, esto no es capricho es una forma de evitar conflictos y bloqueos de las instalaciones ya que si primero instala cualquier otro producto antivirus cuando vaya a instalar el Sav deberá desactivar la protección permanente del producto antivirus que instaló antes para que permita así la instalación del Sav, una ves instalado y actualizado podrá reactivar la protección permanente y reiniciar la máquina y verá que no hay conflictos ni problemas. Si instala primero el Sav se ahorrará todas estas molestias ya que él no entrará en conflicto no el próximo producto que instalará. Eso sí el arranque inicial de la máquina será un poco más lento que antes solo espere a que los dos antivirus hayan cargado la protección permanente antes de introducir cualquier medio de almacenamiento o cualquier dispositivo como Ipo, celulares, tarjetas de memorias de cámaras etc.

5.1.2- Estrategias para enfrentar a los virus de forma efectiva

- Un disco de sistema protegido contra escritura y libre de virus: Se hace mediante el sistema operativo Windows 98, de la siguiente forma: Inicio/ configuración/panel de control/ agregar o quitar programas/ disco de inicio.
- Deberá contar con un disco de 3,5" vacío.
- Debe tener la instalación de este sistema operativo, pues para hacer el disco de inicio le pedirá la fuente de esta instalación o que inserte el CD de instalación.
- Puede contar con un CD booteable en el cual se encuentre un sistema operativo con antivirus para la desinfección de la máquina.
- Puede ser Linux o Windows. Para hacer un sistema operativo de Windows que trabaje desde una torre de CD sin necesidad de instalar usted puede usar un programa que se llama "PE Builder", el cual puede descargarlo desde : http://www.nu2.nu/download y el nombre del programa a descargar es : Pebuilder313.exe. Este programa le permite hacer un sistema operativo portátil es decir que puede hacer que la máquina cargue el sistema operativo desde el CD o desde una flash.
- Un programa antivirus actualizado: Se puede considerar a un programa antivirus actualizado si este no tiene más de 9 días desde su fecha de actualización de sus bases anti-virales.
- Un programa de respaldo de áreas críticas: Algún programa que ofrezca respaldo (backup) de los sectores de arranque de los discos duros. Muchos programas antivirus incluyen funciones de este tipo. También puede hacerse una copia (imagen) del disco duro y guardarlo en una partición diferente a la que le hizo la imagen, actualizándola cada dos semanas, un mes, tres meses o seis mese, en dependencia de las complejidades de los datos que se protegen y su importancia.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

- Tener un plan de seguridad informático establecido y de no existir hacerlo, que contemple todas las consideraciones sobre estos temas.
- El sistema de protección residente, tiene que estar activo, estos previenen en gran medida la intrusión de virus y de programas desconocidos a la computadora.
- Se deben tener respaldos en disco de los archivos de datos más importantes.
- Revisar todas las unidades antes de utilizarlas, todos los discos deben ser revisados incluyendo los programas de instalación originales. A veces ha sucedido que se distribuyen discos con programas originales infestados de virus, unas veces intencionales y otras veces desafortunadas.
- Revisar los programas que se obtengan de la red, CD o por cualquier otro medio de almacenamiento: Una de las grandes vías de contagio es la Internet y medios en los cuales es común la transferencias de archivos (CD regrabables o no, memorias flash y discos externos.
- Revisar periódicamente la computadora, se puede considerar como una buena frecuencia de análisis una vez al mes.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

Conclusiones

Con todo lo antes expuesto pueden ilustrarse algunas consideraciones que son necesarias para tener un conocimiento general sobre la materia de los virus informáticos.

- Es imprescindible contar con herramientas para la detección y desinfección de los virus informáticos.
- Todos los virus informáticos son programas y como tal deben ser ejecutados para activarse.
- Ningún sistema antivirus es 100% seguro, por eso todo usuario de computadora debe tratar de implementar la mejor estrategia de seguridad anti-viral, no solo para proteger su propia información, sino para no convertirse en un agente de propagación que puede producir grandes daños a otras máquinas.
- Toda entidad debe tener un plan de seguridad informático acorde con las características de su centro.
- Los usuarios de computadoras deben conocer como usar los medios o herramientas que permitan combatir los daños, lo más rápido posible.
- Las máquinas que posean información sensible de alto grado no pueden estar conectadas a Internet.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

Recomendaciones

- Las mejores combinaciones de antivirus son:
  - Sav y Kapesky Antivirus
  - Sav y Norton Antivirus
  - Sav y McAfee
  - Sav y Dr. Solomon´s Antivirus Toolkit
  - Sav y VirusScan
  - Sav y Panda
- Haga una imagen de la partición "C:" apenas tenga instalado el sistema operativo y los programas que usted trabajará. La ventaja de tener esta imagen hecha es que si por algún motivo debemos formatear y reinstalar nos tardaríamos alrededor de 1 hora o una hora y media en ponerlo todo a punto y con la imagen solo tardaremos a lo sumo 12 minutos, para tenerlo todo a punto. El tiempo de instalación de la imagen está estrechamente vinculado a la cantidad de información de "C".
- Haga un disco de herramientas para enfrentar las contingencias, con herramientas de diagnóstico reparación y comprobación. Una muy buena sugerencia es hacer un disco tipo: "Hiren's BootCD" sobre el cual se puede obtener información en : http://www.hiren.info
- Haga un sistema operativo portátil basado en la herramienta, "Pebuilder313.exe". Se sugiere que el disco utilizado para hacer un sistema operativo portátil sea regrabable para que pueda actualizar los antivirus que tendrá instalado en este disco puede tener instalados todos los antivirus que desee siempre y cuando no los tenga residente a todos solo a uno. A cualquiera de los otros solo lo ejecuta normalmente y lo pone a escanear la unidad o unidades que posea la máquina.
- Haga copia de respaldo de la información imprescindible en medios de almacenamientos externos o en otra partición.
- Nunca guarde información en la raíz del sistema operativo, si ocurriera algún inconveniente que obligara al formateo perdería usted todos los datos.
- Si posee un disco duro grande haga dos particiones una para el sistema y otra para los datos. Siempre el tamaño de la partición del sistema será menor que la de los datos. Aunque los tamaño para la partición del sistema está directamente relacionada a la carga o cantidad de programas que debe usted instalar para el trabajo diario.
- Mantenga actualizado los antivirus de su ordenador.
- Desactive las macros del office para trabajar, salvo que las necesite.

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

Bibliografía

http://es.wikipedia.org

http://www.hiren.info

http://www.segurmatica.cu

http://www.perantivirus.com/sosvirus/preguntas/clasific.html

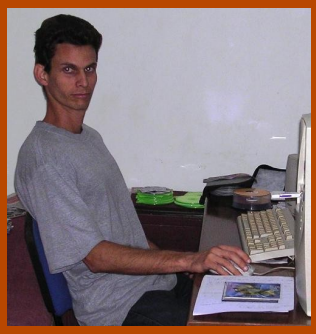
http://monografias.com

Hispasec – Seguridad informática

http://www.wikilearning.com/monografia/estudio_sobre_los_virus_informaticos-el_nuevo_escenario_informatico/3805-1

Ciudad de La Habana : Editorial Universitaria, 2009. -- ISBN 978-959-16-1136-9

Datos del autor



Lic. Yansenis López Matachana (yansenis@ispetp.rimed.cu)

Graduado de la Escuela José Martí de Técnico Medio en Construcción civil, en el año 1997, Fue eximido de la prueba estatal gracias a sus excelentes resultados académicos, por esta condición es seleccionado para comenzar a trabajar en la propia escuela como profesor en formación.

Comenzó sus estudios universitarios en el ISPETP en Septiembre de 1997, continuando su formación en la carrera de Construcción Civil.

Comienza a trabajar en el Instituto Universitario ISPETP como técnico de laboratorio, en el departamento de Informática, a la vez que estudiaba su Licenciatura en Construcción.

Es profesor del instituto al graduarse, en el año 2004, luego de dos años de licencia de estudio.

Desde sus comienzos decide reorientarse a la informática y es aceptado en dicho departamento, donde un año después es designado Jefe de la disciplina de programación, función que desempeña desde el 2005 hasta el 2009.

Es un entusiasta de los estudios informáticos y del conocimiento en general