Boletín 2-2001, artículo 6º

¿Qué es un virus informático?

Ing. Gustavo Rojas García

Un virus informático es un programa que después de copiarse o duplicarse a si mismo causa problemas de operación en un computador.Estos problemas pueden ser mínimos, como que aparezcan imágenes o mensajes extraños en la pantalla, o causar daños mucho mayores como lo son la alteracióno destrucción de los datos almacenados en el disco duro.Además de los daños a la información, los virus consumen espacio del disco duro, memoria y recursos de la Unidad Central de Procesamiento ("Central Unit Processing", CPU) y por consiguiente afectan el desempeño del computador infectado.

1.1.Tipos de virus

Existen varias clases de virus, una característica común a todos ellos es que actúan sin el conocimiento del usuario causándole daños intencionales. Dentro de los tipos de virus se incluyen los denominados gusanos, los Caballos de Troya y cuentagotas.Todos éstos programas son parte de una categoría de programas conocida como "malware".

Un gusano ("worm") es un programa que se reproduce pero no infecta a otros programas.Se transmite a otras computadoras por medio de diskettes o vía conexiones de redes.

Un Caballo de Troya ("Trojan horse") es un programa que está oculto dentro de otro programa aparentemente inofensivo.Cuando este último se ejecuta, el Caballo de Troya comienza a correr para realizar acciones en contra del usuario.El nombre de Caballo de Troya proviene del mito griego relatado en "La Odisea" en que el ejército griego dejó un caballo gigante de madera como regalo a los Troyanos, escondiendo varios soldados dentro del caballo.Cuando los troyanos estaban desprevenidos, los griegos saltaron fuera y capturaron la ciudad de Troya.El principio es el mismo para las computadoras.

Los Cuentagotas ("droppers") son programas diseñados para dificultar su descubrimiento por los programas antivirus, de los cuales hablaremos más adelante. Entre las funciones típicas de los cuentagotas están transportar e instalar otros virus.Los cuentagotas esperan a que ocurra un evento específico dentro del sistema y cuando ocurre se ejecutan e infectan el sistema con el virus contenido.

Relacionado con estos programas destructivos tenemos un concepto muy interesante conocido como la bomba.Para activarse en un momento determinado, la bomba chequea constantemente el reloj del sistema y podría programarse para borrar todos los archivos almacenados en el disco duro con la extensión *.DOC.La bomba puede activarse en una fecha determinada, por ejemplo en el fin de año.

1.2.Propagación de virus

En el pasado los virus se propagaban por medio de la distribución de diskettes infectados. Hoy, también se transmiten por medio de las conexiones de redes, lo que incluye el Internet.Un virus puede alojarse en el "attach" de un correo electrónico ("e-mail").El propio mensaje en el e-mail no puede considerarse un virus, puesto que el viruses un programa y como tal debe ejecutarse en el sistema para volverse activo.

Si usted baja y ejecuta software de Internet, o incluso si recibe archivos anexos de correo electrónico, hay muchas probabilidades de contraer uno de estos virus.Si un virus se encuentra agregado al "attach" de un e-mail, este no puede causar daño alguno hasta que usted lo ejecute dando doble click en él.Una manera de protegerse es NUNCA ABRIR attach que incluyan archivos ejecutables (*.EXE,*.COM, *.BAT) o archivos de datos sospechosos. Una vez activo, el virus inmediatamente inicia su trabajo destructivo, el que comienza en un computador y luego desemboca en una reacción en cadena sobre cientos de computadores.

Otro posible foco de infección de virus consiste en la utilización de software ilegal o "pirateado", es decir, aquellos programas que no cuentan con las respectivas licencias de uso de su dueño.Algunos vendedores y distribuidores instalan estas copias no autorizadas de "software" en el disco duro de las computadoras, las que a su vez ofrecen sin ningún costo para el usuario, con el propósito de inducir su compra.Muchos usuarios utilizan estos programas "gratuitos" sin saber el peligro a que se enfrentan.

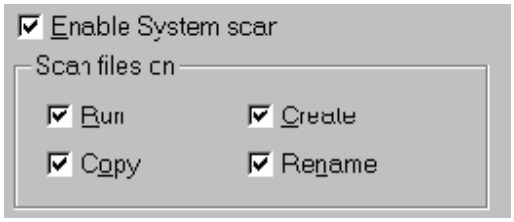
Los virus son diseñados por personas que cuentan con amplios conocimientos técnicos y que actúan por diferentes motivaciones, entre ellas tenemos las emociones que experimentan al desafiar los sistemas de seguridad de las organizaciones y no ser descubiertos.También se sabe que actúan para vengarse, chantajear y extorsionar a las personas o Instituciones.En contra de estas personas es muy difícil tomar medidas legales ya que actualmente es extremadamente difícil rastrearlas, debido a que se aprovechan de la tecnología informática para permanecer ocultos.

1.3.Eliminación de virus

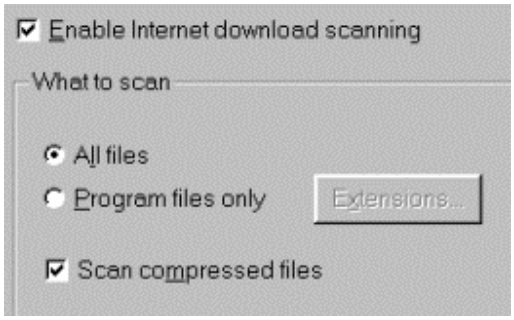
La eliminación de un virus debe hacerse lo más rápido posible y tratando de causar el mínimo daño a la información almacenada. Para remover los virus se utilizan los programas de protección denominados "antivirus" que actúan como especie de vacunas de inmunización.Para que los programas de protección controlen la infección también deben consumir los recursos del computador para detectar y eliminar los virus descubiertos en el sistema, por consiguiente se ve afectado el desempeño del computador.

Seguidamente, se mencionan varias recomendaciones básicas para protegerse contra los virus:

1. Configure el "software" antivirus para que examine en forma automática todos los archivos almacenados en el sistema.Deben escogerse los siguientes parámetros para el programa[1]:



2. En gran cantidad de sitios de Internet se permite bajar ("download") información que se encuentran en formato comprimido, por lo que el software antivirus debe configurarse para examinar este tipo de archivos.Deben escogerse los siguientes parámetros para el programa:



3. Aunque el software antivirus examina los archivos comprimidos, como se mencionó anteriormente, existen posibilidades de que un virus se encuentre oculto dentro de un archivo comprimido y sólo será descubierto después de que el archivo se ha descomprimido.

4. Establezca una rutina periódica para examinar regularmente los archivos almacenados en el computador.Es cierto que esto puede consumir algún tiempo dependiendo del tamaño de la unidad de disco duro, sin embargo, esta previsión bien merece la pena, dado que se tiene la garantía de que el sistema se encuentra libre de virus.

5. Diariamente se registran nuevos virus, así que es muy importante mantener actualizado el software anti-virus.La mayoría de las compañías que venden los programas antivirus proporcionan actualizaciones por lo menos una vez al mes, mientras otras proporcionan actualizaciones cuando surge la necesidad.Usted se preguntará porqué constantemente aparecen nuevos virus, la respuesta es muy simple:los autores de los virus siempre buscan nuevas formas de infectar las computadoras.Esta situación se asemeja al juego del gato y ratón entre los autores de los virus y los fabricantes del software antivirus.

[1] *Tome en cuenta que los parámetros de configuración de un programa antivirus varían de un producto a otro puesto que son fabricados por diferentes empresas proveedoras.*

6. Es aconsejable visitar periódicamente el sitio del fabricante para enterarse de las nuevas versiones de programas antivirus y conocer las recomendaciones del proveedor para combatir los nuevos virus .

7. La empresa Symantec AntiVirus Research Center, una de las compañías líderes en software de anti-virus, cuenta con el sitio web www.Symantec.com (en inglés) y provee un servicio de consulta en donde se puede efectuar una revisión sobre el tema de los virus.Otros sitios interesantes de consulta para productos antivirus sonwww.McAfee.com, www.sophos.com y www.pandasoftware.com (todos en inglés).

8. Si el computador no cuenta con este tipo de protección contra virus, es aconsejable comunicarse con el encargado técnico para que le instale uno de estos programas.

Además de las anteriores recomendaciones, tome en cuenta el establecimiento de una rutina periódica de respaldos (“back-up”) para los archivos de trabajo y de la configuración del sistema.En caso de que su computadora se infecte, existirá la posibilidad de recurrir a copias limpias de información.Relacionado con el tema de los respaldos, es muy importante que tome en cuenta las siguientes dos previsiones:1) los respaldos de información deben estar libres de virus y 2) deben ser almacenados en un lugar seguro.

Finalmente, es necesario dejar claro que en muchas ocasiones el mal funcionamiento de un computador, la alteración de archivos o la pérdida de información no tienen nada que ver con la presencia de un virus en el sistema.Entre las situaciones que pueden originar problemas de operación y que no pueden considerarse ataques de virus está la aparición de las denominadas pulgas (“bugs”).Existe una gran variedad de circunstancias por las que se originan las pulgas dentro de un sistema.Pueden suceder debido a que tanto el software como el hardware no han sido instalados y configurados correctamente. Por esta razón, en ambientes informáticos de compleja operación es necesario el diagnóstico del encargado técnico para resolver el verdadero problema.

Esperamos que este artículo constituya un punto de partida para la reflexión y el debate acerca los mecanismos de protección que deben implementarse en los equipos computacionales de la Institución para combatir efectivamente los virus informáticos.