***LOS VIRUS***

Integrantes:

* Víctor Astorga
* Franco Santini

Asignatura: TIC

Profesora: Romina Iragorre

**¿Qué es un virus informático?**

Un virus informático es un programa o software que se auto-ejecuta y se propaga insertando copias de sí mismo en otro programa o documento.

Un virus informático se adjunta a un programa o archivo de forma que pueda propagarse, infectando los ordenadores a medida que viaja de un ordenador a otro.

Como los virus humanos, los virus de ordenador pueden propagarse en gran medida: algunos virus solo causan efectos ligeramente molestos mientras que otros pueden dañar tu hardware, software o archivos.

Casi todos los virus se unen a un fichero ejecutable, lo que significa que el virus puede estar en tu ordenador pero no puede infectarlo a menos que ejecutes o abras el programa infectado. Es importante observar que un virus no puede continuar su propagación sin la acción humana, (por ejemplo ejecutando un programa infectado).

 La gente contribuye a la propagación de los virus, muchas veces sin saberlo, al compartir archivos infectados o al enviar e-mails con virus como archivo adjunto en el email.

La inserción del virus en un programa se llama infección, y el código infectado del archivo (o ejecutable que no es parte de un archivo) se llama hospedador (host).

Los virus son uno de los varios tipos de Malware o software malévolo.

Algunos virus tienen una carga retrasada, que a veces se llama bomba. Por ejemplo, un virus puede exhibir un mensaje en un día o esperar un tiempo específico hasta que ha infectado cierto número de hospedadores. Sin embargo, el efecto más negativo de los virus es su auto-reproducción incontrolada, que sobrecarga todos los recursos del ordenador.

Debido a Internet, hoy en día son más comunes los gusanos que los virus. Los programas antivirus, diseñados originalmente para proteger los ordenadores contra virus, se han ampliado para cubrir gusanos y otras amenazas tales como el spyware.

# *¿Cómo funciona un virus informático?*

El funcionamiento de los virus coincide en sus líneas esenciales con el de los demás programas ejecutables, toma el control del ordenador y desde allí procede a la ejecución de aquello para lo que ha sido programado.

Generalmente están diseñados para copiarse la mayor cantidad de veces posible, bien sobre el mismo programa ya infectado o sobre otros todavía no contaminados, siempre de forma que al usuario le sea imposible o muy difícil darse cuenta de la amenaza que está creciendo en su sistema. El efecto que produce un virus puede comprender acciones tales como un simple mensaje en la pantalla, disminución de la velocidad de proceso del ordenador o pérdida total de la información contenida en su equipo.

En la actuación de un virus se pueden distinguir tres fases:

1. El contagio: El contagio inicial o los contagios posteriores se realizan cuando el programa contaminado está en la memoria para su ejecución. Las vías por las que puede producirse la infección de su sistema son disquetes, redes de ordenadores y cualquier otro medio de transmisión de información. Los disquetes son por el momento, el medio de contagio más extendido en nuestro país. Estos disquetes contaminantes suelen contener programas de fácil y libre circulación y carecen de toda garantía. Es el caso de los programas de dominio público, las copias ilegales de los programas comerciales, juegos, etc.

El virus activo: Cuando se dice que un virus se activa significa que el virus toma el control del sistema, y a la vez que deja funcionar normalmente a los programas que se ejecutan, realiza actividades no deseadas que pueden causar daños a los datos o a los programas.

El virus pasivo: Generalmente, suelen enviar "fotos" por la web, que dicen llamarse "mifoto.jpg", tienen un ícono cuadrado blanco, con una línea azul en la parte superior. En realidad, no estamos en presencia de una foto, sino de una aplicación Windows (\*.exe). Su verdadero nombre es "mifoto.jpg.exe", pero la parte final "\*.exe" no la vemos porque Windows tiene deshabilitada (por defecto) la visualización de las extensiones registradas, es por eso que solo vemos "mifoto.jpg" y no "mifoto.jpg.exe". Cuando la intentamos abrir (con doble clic) en realidad estamos ejecutando el código de la misma, que corre bajo MS-DOS.

También se contagian cuando ponemos en nuestro equipo algún medio de almacenamiento el cual esta infectado; cuando abrimos un e-mail de un remitente desconocido; a través del software pirata…

Lo primero que suele hacer el virus es cargarse en la memoria del ordenador y modificar determinadas variables del sistema que le permiten "hacerse un hueco" e impedir que otro programa lo utilice. A esta acción se le llama "quedarse residente". Así el virus queda a la espera de que se den ciertas condiciones, que varían de unos virus a otros, para replicarse o atacar.

2. La replicación, que es el mecanismo más característico y para muchos expertos definitorio de la condición de virus, consiste básicamente en la producción por el propio virus de una copia de si mismo, que se situará en un archivo. El contagio de otros programas suele ser la actividad que más veces realiza el virus, ya que cuanto más deprisa y más discretamente se copie, más posibilidades tendrá de dañar a un mayor número de ordenadores antes de llamar la atención.

3. El ataque: Cada virus tiene una estructura de ataque diferente, pero generalmente todos tratan de sobrevivir encubriéndose en algún archivo o auto-ejecutándose cuando hacemos doble clic sobre la carpeta contenedora, alguno apagan el equipo y otros la paralizan utilizando todos sus recursos.

**“Tipos de virus”**

**Según su propagación**

Aquellos que infectan archivos. A su vez, estos se clasifican en:

          Virus de acción directa. En el momento en el que se ejecutan, infectan a otros programas.

* Virus residentes. Al ser ejecutados, se instalan en la memoria del ordenador. Infectan a los demás programas a medida que se accede a ellos. Por ejemplo, al ser ejecutados.
* Los que infectan el sector de arranque (virus de boot). Recordemos que el sector de arranque es lo primero que lee el ordenador cuando es encendido. Estos virus residen en la memoria.

Existe una tercera categoría llamada multipartite, pero corresponde a los virus que infectan archivos y al sector de arranque, por lo que se puede decir que es la suma de las dos categorías anteriores.

La clasificación de los virus también se divide en dos categorías, pero el método de clasificación utilizado es diferente:

* Virus de archivos, que modifican archivos o entradas de las tablas que indican el lugar donde se guardan los directorios o los archivos.
* Virus de sistema operativo, cuyo objetivo consiste en infectar aquellos archivos que gobiernan el ordenador.

Existe una tercera clasificación, promovida por CARO, para unificar la forma de nombrar a los virus. En esta clasificación se atiende a la plataforma en la que actúa el virus y a algunas de sus características más importantes.

Por ejemplo, el W32/Hybris.A-mm es un virus que funciona en la plataforma win32 en su variante A (primera) que tiene capacidad mass mailing o de envío masivo de correo electrónico infectado.

### Según su comportamiento

En función de su comportamiento, todos los virus anteriores pueden a su vez clasificarse en otros subgrupos:

* Virus uniformes, que producen una replicación idéntica a sí mismos.
* Virus encriptados, que cifran parte de su código para que sea más complicado su análisis. A su vez pueden emplear:
  + Encriptación fija, empleando la misma clave.
  + Encriptación variable, haciendo que cada copia de sí mismo esté encriptado con una clave distinta. De esta forma reducen el tamaño del código fijo empleable para su detección.
* Virus oligomórficos, que poseen un conjunto reducido de funciones de encriptación y eligen una de ellas aleatoriamente. Requieren distintos patrones para su detección.
* Virus polimórficos, que en su replicación producen una rutina de encriptación completamente variable, tanto en la fórmula como en la forma del algoritmo. Con polimorfismos fuertes se requiere de emulación, patrones múltiples y otras técnicas antivirus avanzadas.
* Virus metamórficos, que reconstruyen todo su cuerpo en cada generación, haciendo que varíe por completo. De esta forma se llevan las técnicas avanzadas de detección al límite. Por fortuna, esta categoría es muy rara y sólo se encuentran en laboratorio.
* Sobre-escritura, cuando el virus sobre-escribe a los programas infectados con su propio cuerpo.
* Stealth o silencioso, cuando el virus oculta síntomas de la infección.

**Daños**

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir replicándose. Las redes en la actualidad ayudan a dicha propagación.

Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Hay que tener en cuenta que cada virus plantea una situación diferente.

<http://megavirtual.galeon.com/index3.htm>

<http://www.clasificadosenbolivia.com/internet/tipos_de_virus_informatico/>

<http://www.masadelante.com/faqs/virus>