|  |  |  |
| --- | --- | --- |
| **VIRUS INFORMATICO**    Un Virus es un programa que en poco más de uno o dos Kbytes (es una unidad de almacenamiento de información ) consiguen realizar acciones inimaginables; desde mostrar diversos mensajes o gráficos en pantalla hasta formatear el disco duro o hacernos perder todos los datos en él guardados.  Un virus de computadora es un programa -o código- que se replica añadiendo una copia de sí mismo a otro archivo ejecutable. Particularmente da debido a que, sin detección o protección antivirus, el usuario no se percata que su sistema está siendo invadido hasta que ve los resultados que pueden ir desde anuncios inocuos hasta la pérdida total del sistema.  **Bombas lógicas o de tiempo:** Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.  **Joke:** Al igual que los hoax, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a cerrar es posible que salga una ventana que diga: No se puede cerrar!.  **Virus de Macro:** vinculan sus acciones a modelos de documentos y a otros archivos de modo que, cuando una aplicación carga el archivo y ejecuta las instrucciones contenidas en el archivo, las primeras instrucciones ejecutadas serán las del virus.  **http://antivirus.es/wp-content/uploads/2010/02/gusano.jpg** | **SÍNTOMAS**    -Reducción del espacio libre en la memoria  - El disco duro aparece con sectores en mal estado    **Virus residentes:** La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados    **Virus de sobre-escritura** Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.  **Virus de boot (bot\_kill) o de arranque**  Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco o unidad de almacenamiento CD, DVD, memorias USB etc. En ella se guarda la información esencial. No infecta ficheros, sino los discos que los contienen. Actúan infectando el sector de arranque.  Virus Pasivos: son aquellos que se infectan por medio de e-mails de direcciones desconocidas, instalación de software “piratas”, entre otros. | -Cambios en las características de los ficheros ejecutables -Aparición de anomalías en el teclado  **TIPOS DE VIRUS**  **Troyano:** Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.  **http://publicdomainvectors.org/photos/virus4.png**  **http://i46.photobucket.com/albums/f127/anecdota/dv539009.jpgHackers:** "secuestran" navegadores de Internet, principalmente el Internet Explorer. Cuando eso pasa, el hacker altera la página inicial del navegador e impide al usuario cambiarla, muestra publicidad en pop-ups o ventanas nuevas, instala barras de herramientas en el navegador  **Zombie** ocurre cuando es infectada y está siendo controlada por terceros. Pueden usarlo para diseminar virus, keyloggers, y procedimientos invasivos en general. Usualmente esta situación ocurre porque la computadora tiene su Firewall y/o sistema operativo desactualizado.  **METODOS DE PROTECCIÒN:**  **C:\Users\Invitado\Desktop\proteccion.jpg**No se puede garantizar la seguridad de su equipo, pero existen muchas formas de disminuir las posibilidades de que su equipo se infecte con un virus. Se pueden proteger con un: **ANTIVIRUS:** Que ayudan a la herramienta a identificar y eliminar amenazas. **FILTROS DE FICHEROS:** consiste en generar filtros de ficheros dañinos si el computador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.  **INTEGRANTES:**  ANGIE MANUELA FRANCO FLOREZ  CAROLINA GIRALDO MAZO  ANDREA GONZALEZ VASQUEZ  CAROLINA HORTUA SANCHEZ  DAIANA URREGO |