¿Qué es un Virus Informático?

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras.

Es importante señalar que la palabra "Virus" es un vocablo latín y su equivalencia a nuestro lenguaje actual es "veneno".

Es capaz de tomar el control de la maquina o aplicación en algún momento modificándola para incluir una versión de si mismo y auto replicarse, alojándose en un soporte diferente al que se encontraba originalmente.

Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

La estructura de un virus es tripartita

Mecanismo de reproducción Infección que genera copias del virus "pegadas" en ficheros ejecutables o en el sector de arranque de discos (en realidad son programas también).

Detonante (trigger) Esta parte del virus (de su código) se encarga de comprobar si se cumplen las situaciones previstas por el programador. Cuando se cumplan una o varias circunstancias: puede ser una fecha concreta, una acción por parte del usuario, etc.

Carga (payload) La acción que realiza el virus. No tiene por qué ser destructivo: puede ser mostrar una ventana, un mensaje, etc. Entre los payload destructivos o perjudiciales pueden encontrarse desde el borrado de ficheros hasta el envío de información confidencial a destinos no autorizados.

El virus intentará sobrevivir el máximo tiempo posible e infectar al mayor número de ficheros y/o ordenadores. Para esto, desde el sencillo "Brain" en 1986, se usan las llamadas técnicas de ocultación, que buscan engañar al usuario y a los antivirus.

Uno de los mitos más persistentes hacen referencia a las llamadas "mutaciones" de los virus, que en la mayoría de las ocasiones son cambios que realizan determinados programadores sobre el código de un virus o gusano exitoso (y los medios de comunicación no se refieren al polimorfismo sino a lo citado).

Otro es que la infección vírica destruye, pero la realidad es que no es destructora salvo errores (bugs) de programación. Lo que puede destruir es el "payload".