

MALWARE (SOFTWARE MALICIOSO)

Malware es un acrónimo de *Malicious Software*(Software Malicioso). Es un tipo de software dañino que se crea con malas intenciones. Uno de los primeros programas que encaja con la definición de malware es el **gusano** creado por Robert Morris en 1988. Fue el primer programa que se autoreproducía en una red informática. En esos primeros tiempos, muchos de los que creaban malware no eran mas que bromistas pesados que disfrutaban de la idea de borrar todo el contenido de los discos duros de los internautas. Al principio no se veía la manera de lucrar con el malware, sólo hacer daño. Les podía ser útil a servicios de inteligencia para la guerra electrónica. Pero con la evolución de internet vinieron los servicios bancarios en la red y algunos sitios Web empezaron a pedir a los usuarios que les dieran los datos personales que podían ser aprovechados por criminales y las mafias empezaron a interesarse en las posibilidades del malware.

Hoy en día, existe todo un submundo dedicado a este turbio negocio.

TIPOS DE MALWARE

VIRUS

Un **virus** informático es un software que, al igual que un virus biológico, infecta a una computadora y se propaga en ella con diversos propósitos como *daño, robo de información, molestia, etc.*

Por lo general intenta pasar desapercibido por el usuario el mayor tiempo posible.

El contagio por un virus suele producirlo el mismo usuario al ejecutar una aplicación(programa) que está infectado. Muchos virus usan internet para propagarse.

Los programas que protegen, detectan y eliminan virus son llamados **antivirus**. Son ejemplos de software antivirus el **Avast, McAfee , Bitdefender, Norton**.

Se aconseja no abrir los archivos adjuntos de personas desconocidas. No es recomendable conectar nuestro pen drive a computadoras desconocidas.

VIRUS Otra definición:

Este es un término genérico que se usa para referirse a software pernicioso que se autopropaga, copiándose de máquina en máquina cada vez que consiguen infectar una computadora nueva. El virus informático lleva normalmente lo que se llama una *carga* y que no es mas que una serie de acciones que se ejecuta al cabo de un tiempo de haber infectado la máquina(días o semanas). La autoreproducción es su principal característica.

RANSOMWARE. Identifica a un tipo de software que, una vez que ha conseguido instalarse en el ordenador de la víctima, encripta todos los archivos de datos(documentos, fotos, videos). Utiliza una clave que el usuario desconoce, de forma que este no puede descryptar los ficheros. Entonces presenta un mensaje de secuestro pidiendo una cantidad de dinero a cambio de proporcionar la clave al usuario.

PHISHING Se le llama así por su parecido con el acto de pescar. Se lanza un “anzuelo”(normalmente vía correo electrónico) que contiene un enlace a una página que imita a una legítima y en la que se piden datos privados del usuario. Ejemplo: piden el número de PIN de la cuenta bancaria. Esto ha llevado a que les vacíen la cuenta a algunas personas.

SPYWARE Como su nombre lo indica, el **spyware** es un malware, que, una vez instalado en la computadora del usuario, se dedica a espiar con intención de sacar – o robar- datos como las contraseñas y otros datos como las claves bancarias para poder realizar operaciones bancarias on line. Como los espías literales es sigiloso y el usuario no se da cuenta de que está instalado.

ANTIVIRUS

Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de virus y/o software malicioso en sistemas informáticos.

Un antivirus debe cumplir con ciertos requisitos para ser considerado efectivo y eficiente: constante actualización, protección permanente y una completa base de datos de programas malignos.

Algunos antivirus populares son: *Norton, Avast, McAfee, Kaspersky y Panda Security.*