



Existen varios tipos de malware o “software malicioso” y cada uno realiza una acción diferente.

**Virus**

Afectan los archivos dejándolos inutilizables. Los virus fueron el primer tipo de malware que apareció, para evitarlos y eliminarlos se crearon los antivirus.

**Keyloggers**

Registra la actividad del teclado y la envía al atacante, quien roba contraseñas e información personal, con fines de extorsión.

**Troyano**

Es un programa que se hace pasar por otro. Una vez que el usuario lo instala por error, permite que un tercero tome el control de su computadora. Normalmente un troyano se utiliza para instalar otro malware de control como keyloggers, puertas traseras o para ejecutar exploits.

**Backdoor**

También conocidos como puertas traseras, son códigos introducidos en los programas para lograr un control remoto de los mismos.

**Exploits**

Son programas que “explotan” los fallos o debilidades de los programas, como errores de codificación o bugs.

**Worms**

Reciben el nombre de gusanos informáticos, ya que se expanden por los archivos de la computadora, afectando el rendimiento e imposibilitando el trabajo. Se caracterizan por extenderse a través de email, memorias USB, discos duros externos y cualquier dispositivo de almacenamiento.

**Spyware**

Es un programa que recopila datos, sin consentimiento del usuario, y generalmente se esconden dentro de publicidad y actualizaciones. Un keylogger puede ser un tipo particular de spyware.

**Adware**

Muestra ventanas de publicidad al usuario. Por lo general no provoca ningún daño al sistema ni a los datos de éste, pero dificulta el trabajo por las constantes interrupciones.

**Rootkit**

Otorga al atacante permisos como si fuera el usuario administrador de la PC víctima. Normalmente se esconden bajo la apariencia de programas inofensivos, como los de oficina, para no ser detectados. Un rootkit normalmente se utiliza por medio de un exploit o un troyano.

**Rogue /
Scareware**

Mejor conocidos como “falsos antivirus”. Son aplicaciones que se instalan en el sistema y muestran avisos falsos, de compra de un software que supuestamente sirve para desinfectar el equipo. Generalmente son muy difíciles de desinstalar y suelen causar fallas en el rendimiento.

**Ransomware**

Uno de los más usados actualmente. Cifra la información del equipo de la víctima por completo, bloquea la computadora y solicita un pago para arreglarla.

Recuerda que para contrarrestar todas las amenazas que no son virus, necesitas un antimalware.