**Otras formas de malware**

**Ransomware**

El ransomware es uno de los tipos de malware más dañinos y temidos. Su objetivo es secuestrar archivos y exigir un rescate para devolver el acceso. Funciona así:

**Infección:** Se introduce en el sistema a través de correos electrónicos falsos, descargas maliciosas o vulnerabilidades en software.

**Cifrado de archivos:** Bloquea el acceso a documentos, imágenes y datos importantes mediante algoritmos de cifrado avanzados.

**Exigencia de pago:** Los atacantes piden un pago en criptomonedas a cambio de la clave para desbloquear los archivos.

**Ejemplo real:** WannaCry (2017), que afectó a hospitales, empresas y gobiernos en más de 150 países, causando pérdidas millonarias.

**Spyware**

El spyware es un software espía que se instala sin permiso y monitorea la actividad del usuario. Puede:

* Registrar las pulsaciones del teclado (keyloggers).
* Capturar contraseñas y datos bancarios.
* Activar la cámara o el micrófono sin que el usuario lo note.

**Ejemplo real:** Pegasus, un spyware usado para espiar a periodistas y políticos sin su consentimiento.

**Adware**

El adware es un software que muestra anuncios invasivos en los dispositivos del usuario. Aunque no siempre es peligroso, puede:

* Redirigir a sitios web maliciosos.
* Ralentizar el sistema y consumir recursos.
* Instalarse junto con otros programas sin que el usuario lo sepa.

**Ejemplo real:** Superfish, un adware preinstalado en algunas computadoras Lenovo que comprometía la seguridad de los usuarios.

**Términos asociados**

**Payload (carga útil del malware)**

El payload es la parte del malware encargada de ejecutar la acción maliciosa. Puede ser:

* Destructivo (borrar archivos).
* Espía (robar información).
* Permanente (crear puertas traseras para futuros ataques).

**Ejemplo:** Un virus que, al ejecutarse, borra toda la información del sistema.

**Botnets**

Una botnet es una red de dispositivos infectados (bots), controlados de forma remota por un atacante para lanzar ataques masivos. Se utilizan en:

* Ataques DDoS: Saturan servidores hasta colapsarlos.
* Spam masivo: Envío de correos fraudulentos.

**Ejemplo real:** Mirai Botnet, que atacó servidores en 2016 afectando servicios como Netflix y Twitter.

**Rootkits**

Los rootkits son programas que permiten el acceso encubierto a un sistema, ocultando la presencia del atacante. Pueden:

* Desactivar antivirus y sistemas de seguridad.
* Permitir el control remoto del dispositivo.

**Ejemplo real:** El rootkit de Sony (2005), que fue instalado en CD de música para evitar copias, pero dejó puertas traseras en los sistemas de los usuarios.

**Prevención y detección**

**Antivirus y antimalware**

* Escanean archivos en busca de amenazas conocidas.
* Detectan y eliminan virus, troyanos y spyware.
* Algunos incluyen protección en tiempo real para evitar infecciones.

**Firewalls**

* Actúan como una barrera entre el dispositivo e internet.
* Bloquean accesos no autorizados y tráfico malicioso.

**Buenas prácticas de seguridad**

* Mantener software y sistemas operativos actualizados.
* No descargar archivos o hacer clic en enlaces sospechosos.
* Realizar copias de seguridad periódicas en dispositivos externos o en la nube.
* Usar contraseñas seguras y autenticación en dos pasos.