**Malware**

**Gusano**

Los gusanos se duplican a sí mismos para dañar una red en concreto pasando de un ordenador a otro. Para esto, el gusano no necesita que un usuario lo ejecute. Su objetivo es dañar a la mayor cantidad de usuarios.

**Virus**

Tienen que ser ejecutados por otras personas para que se pongan en funcionamiento. Buscan infectar software dentro del ordenador.

**Mostrar publicidad**

**Spyware**

Buscan controlar la actividad en la web de los usuarios sin que estos lo sepan, con el objetivo de enviar esta información a agencias de publicidad. Se suelen instalar mediante troyanos, cookies, y con las barras de herramientas de los navegadores.

**Adware**

Muestran publicidad de forma intrusiva a los usuarios mediante ventanas o pestañas emergentes para ganar beneficios.

**Hijacking**

Realizan cambios en las configuraciones del navegador web para modificar la página de inicio o redireccionar los resultados hacia los anuncios que deseen.

**Suplantación de identidad**

**Phishing**

Se trata de obtener información de forma ilegal mediante engaños de forma no presencial.

**Malware para robar información**

**Keyloggers**

Analizan y registran las pulsaciones sobre el teclado de forma que esta información se envíe a través de internet. De esta forma se puede conseguir la contraseña del objetivo sin su consentimiento.

**Stealers**

Roba la información previamente guardada en el equipo. Se usa mucho para robar información privada del usuario.

**Dialers**

Se usan para realizar llamadas con un coste adicional por medio del módem del ordenador. Se usan para conseguir dinero de forma fraudulenta, por medio de llamadas con un coste muy alto.

**Ransomware**

Son programas que bloquean el ordenador, e impiden que se desbloquee hasta que consigue su objetivo. Estos programas cifran los archivos más importantes, para que no puedan ser usados por nadie. Después, solicitan un rescate para obtener la contraseña que permita recuperar los archivos. Un ejemplo de esto es el WannaCry.

**Ataques distribuidos DDos**

El programa niega el acceso a unos servicios o recursos a los que normalmente se puede acceder con normalidad. Esto se hace agotando los recursos o colapsando el ancho de banda, haciendo que el servidor sea incapaz de diferenciar entre las peticiones legítimas y el malware. Esto se logra por medio de multitud de conexiones simultáneas, el envío de paquetes alterados o el uso de botnets (ordenadores infectados por troyanos).

**Internos**

Pueden ser accidentales

**Externos**

Siempre son intencionales

**Amenazas APT**

Son programas que intentan robar información a corporaciones o empresas. Requieren de un largo periodo de preparación, gran motivación, una gran inversión económica, y los beneficios suelen ser exponenciales al tiempo e inversión realizados. Para defenderse de este tipo de ataques, es necesaria la existencia de una defensa en profundidad.

**Objetivos y consecuencias**

**Formas de ataque**

**Ataques a contraseñas**

Por medio de las contraseñas son capaces de acceder a nuestras cuentas y conseguir información, así como hacerse pasar por ti. Estos pueden ser de fuerza bruta (a base de ensayo y error), o por diccionario (utilizan un software que hace diferentes comprobaciones de forma automática). Para protegerte, es conveniente el uso de contraseñas robustas y una autentificación múltiple.

**Ataques por ingeniería social**

Se basan en manipular o engañar al usuario para que de su información y ganar así acceso a sus dispositivos. Ejemplos: Phishing, Vishing, y Smishing (nos envían un mensaje suplantando una identidad legítima, este mensaje tiene un carácter de urgencia que nos impide usar el sentido común), Bainting (Dejar una unidad infectada en la entrada de la empresa o en lugares de gran afluencia, también mediante falsos concursos online), Shoulder Surfing (se acercan y miran lo que hace el usuario con el dispositivo, o buscan alguna forma de compartir la cuenta), Dumpsert Diving (utilizan la información sobre el usuario para poder usarla en otros tipos de ataques), Spam (enviar masivamente mensajes sin ser solicitados), y Fraudes Online.

**Ataques a conexiones**

Atacan a la propia red para interponerse entre nosotros y los servicios web con el objetivo de robar y monitorizar nuestros datos. Los hay de los siguientes tipos: Redes Trampa (por medio de software y hardware se crea una red idéntica o muy similar a la usada por el usuario, y esperan a que el usuario se conecte a esta por accidente), Spoofing (suplantan la identidad de un usuario para tener acceso a la información de este), Ataques a Cookies (se roba la información que contiene una cookie evitando que pase por el protocolo HTTPS//:), Inyección SQL (se insertan líneas maliciosas de código SQL en la aplicación web para obtener acceso a los datos de la base de datos de la aplicación), Escaneo de Puertos (analizan los puertos conectados a una red para ver los protocolos de seguridad con los que cuentan), Man in the Middle (monitorizan las actividades online de redes infectadas al situarse entre el servidor y el usuario), Sniffing (escuchan todo lo que ocurre en una red).

**Seguridad en redes inalámbricas**

**WIFI**

En la seguridad se tienen que tener en cuenta la configuración del router y el cifrado de la red inalámbrica. Para acceder a redes públicas, que son más vulnerables, asegúrate de que usen el protocolo HTTPS://, usa una VPN, evita que sea una red inalámbrica abierta, deshabilita cualquier proceso de sincronización, y no inicies sesión.

**Organismos para la seguridad informática**

OSI (Oficina de Seguridad del Internauta), Incibe (Instituto Nacional de Ciberseguridad), y AEPD (Agencia española de protección de datos). Ante una ciberestafa, acudir al INCIBE-CERT (Centro de Respuesta a Incidentes de Seguridad del INCIBE).