

5.4.2. Busca la explicación de cada uno de los malware vistos arriba. Una pregunta del examen será definir algunos de ellos.

- **Adware**
Programa que automáticamente muestra u ofrece publicidad no deseada o engañosa.
- **Bloqueador**
Malware que de forma lógica bloquea la conexión del ordenador a distintos dispositivos periféricos.
- **Bomba lógica**
Parte de un código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.
- **Broma (Joke)**
Programa inofensivo que simula las acciones de un virus informático en nuestro ordenador.
- **Bulo (Hoax)**
Mensaje distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real.
- **Capturador de pulsaciones (Keylogger)**
Software que graba toda la información que se introduce usando el teclado.
- **Clicker**
Malware con el objetivo de que el usuario haga clic.
- **Criptovirus (Ransomware)**
Malware que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.
- **Descargador (Downloader)**
Malware cuya función es descargar otros malware.
- **Espía (Spyware)**
Malware que recopila información de una computadora y después transmite esta información a una entidad externa.
- **Exploit.**
Malware que explota vulnerabilidades de un sistema.
- **Herramienta de fraude**
Malware que intenta engañarte para obtener beneficio económico.
- **Instalador (Dropper)**
Un dropper es un software diseñado para instalar algún tipo de malware en el sistema operativo donde ha sido ejecutado.
- **Ladrón de contraseñas (PWStealer)**

Malware con el propósito de obtener de forma fraudulenta información confidencial del propietario.

- **Marcador (Dialer)**
Malware que marca un número de teléfono de tarificación especial usando el módem, estos NTA son números cuyo coste es superior al de una llamada nacional.
- **Puerta trasera (Backdoor)**
Malware diseñado para dar a los usuarios maliciosos el control de un equipo infectado.
- **Rootkit**
Herramientas que esconden los procesos y archivos que permiten a un intruso mantener el acceso a un sistema
- **Secuestrador del navegador (browser hijacker)**
Malware que realiza cambios en el navegador (Lanzando popups, modificando la página de inicio o de búsqueda predeterminada, etcétera.) sin consentimiento del usuario.