3. Malware

Se trata de un programa malicioso, potencialmente peligroso. Tiene la capacidad de hacer daño a un equipo y posibilidad de propagación.

Los **ciberataques** combinan habitualmente varios tipos.

3.1. Tipos de malware más conocidos

Enlace: los 8 virus más famosos de todos los tiempos.

https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

Virus

Programa que se instala en el ordenador sin el conocimiento del usuario Finalidad de propagarse a otros equipos. Puede provocar desde pequeñas bromas hasta la destrucción total de discos duros.

Gusano

Tipo de virus cuya finalidad es la de multiplicarse e infectar una red de ordenadores.

Las consecuencias no suelen implicar la destrucción de archivos pero sí ralentizan el funcionamiento.

Troyano

Código malicioso que **se oculta dentro de un archivo** inofensivo y útil o llamativo para el usuario. Requieren la intervención de sus víctimas para propagarse.

Existen una gran variedad de troyanos, en función de sus acciones y utilidades:

- **Downloader** (descarga otros programas maliciosos)
- **Clicker** (busca beneficio económico a través de clicks en publicidad)
- **Keylogger** (registra las actividades que se realizan en el sistema)
- **Backdoor** (abre puertos en el sistema)
- **Bot** (controla el equipo de forma remota), etc.

Spyware

Programa que se instala en el ordenador sin conocimiento del usuario con la finalidad de recopilar información sobre el usuario para enviarla a servidores de Internet gestionados por compañías de publicidad.

Adware

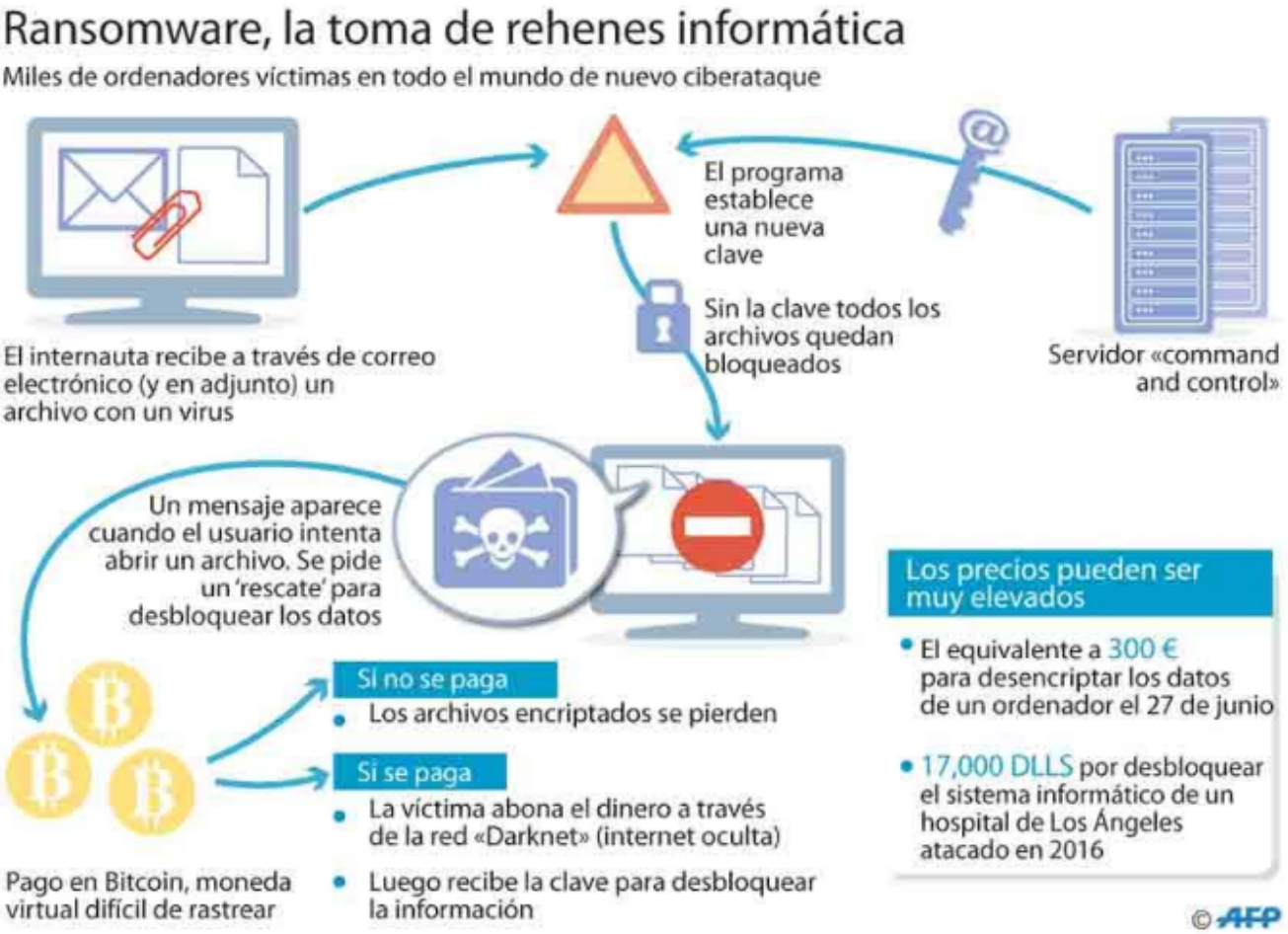
Software que se esconde en los anuncios de Internet. Tras acceder los equipos y dispositivos, este malware roba la información de las empresas y usuarios.

Ransomware

El **ransomware** es un tipo de malware que toma a sus archivos como rehenes.

Lanzado en septiembre de 2013, **CryptoLocker** se extendió a través de archivos adjuntos de correo electrónico y cifró los archivos del usuario para que no pudieran acceder a ellos.

Luego, los piratas informáticos envian supuestamente una clave de descifrado a cambio de una suma de dinero.

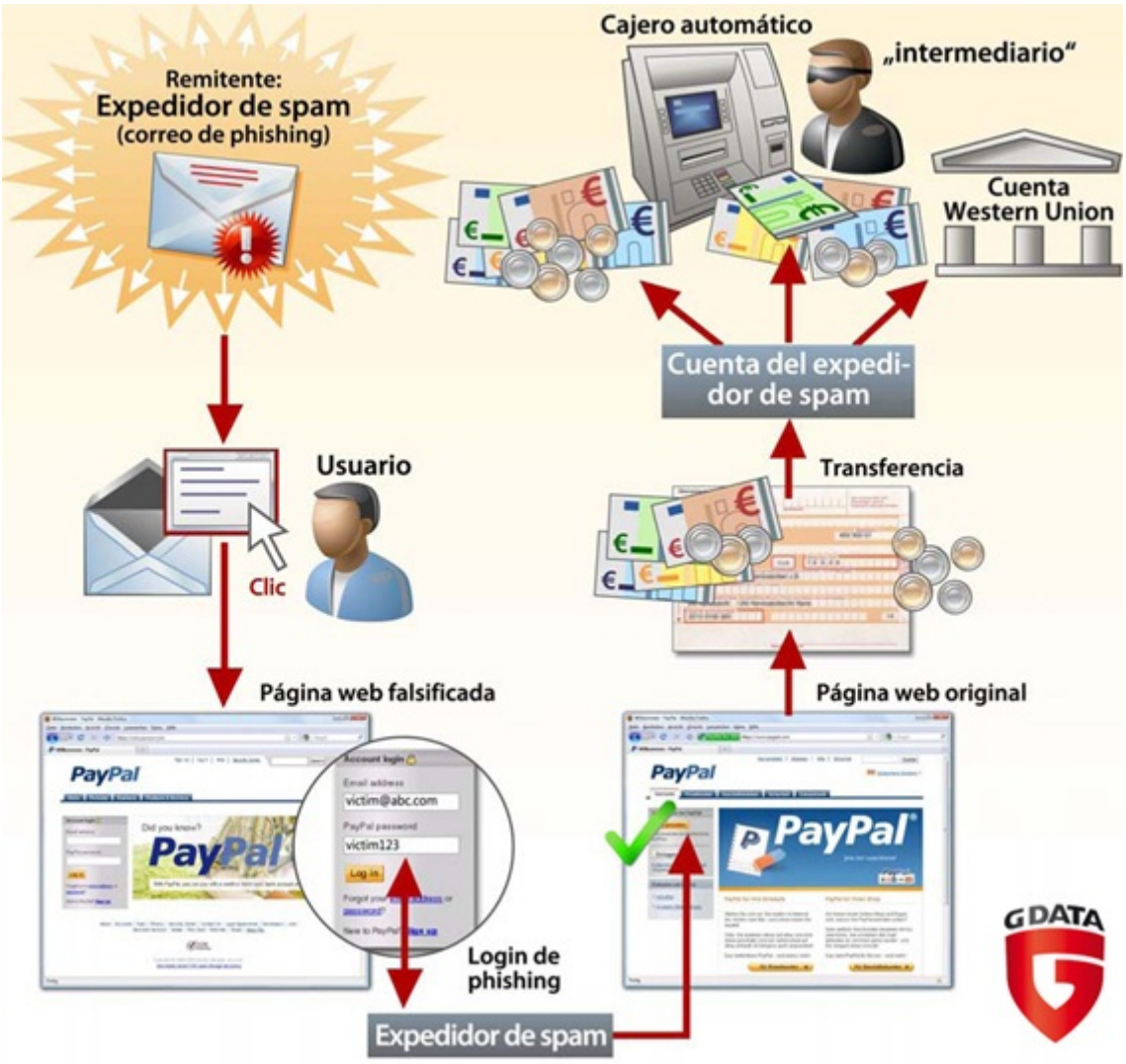


3.2. Otras amenazas malware

Phishing

Es un tipo de fraude ejecutado a través de un **correo electrónico** en el que se solicita la actualización de los datos personales (usualmente vinculados a cuentas u otros instrumentos financieros).

Aparece un **enlace** para que se haga clic de acceso a una página falsa que tendrá prácticamente la **misma apariencia** de la página de la institución simulada.



Pharming

Se instala un código malicioso introducido premeditadamente que permite **redireccionar** un nombre de dominio a otra máquina diferente.

Si el usuario ha sido redireccionado, cuando introduzca el nombre de dominio ingresará a una página 'web' falsa (en apariencia similar a la que deseaba ingresar) permitiéndole al estafador obtener todos los datos personales del cliente.

Finalidad:

- Obtener datos bancarios
- Cometer delitos económicos

Spam

Envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico existente. Su finalidad en general suele ser la de vender productos.

Hoax

Mensajes de correo distribuidos en cadena, cuyo objetivo es realizar engaños masivos. Por ejemplo:

- Historias solidarias inventadas
- Mensajes que traen mala suerte
- Alertas falsas sobre virus