TIPOS DE ATAQUES INFORMATICOS

**Phishing:** Phishing se refiere a la obtención de datos personales realizada de manera ilícita. Phishing proviene de la palabra en ingles Fishing que significa pescar, por lo tanto Phishing se refiere a pescar información. Regularmente clonando un sitio web y por medio de Ingeniería Social convencer a nuestra victima a iniciar sesión en la web clonada creyendo que es la página real.  
Regularmente se utiliza para obtener información Bancaria y/o de sesiones a redes sociales.

**Trashing:** Se trata de la acción de recolectar información a partir de material desechado, generalmente con el fin de obtener datos que sirvan  para cometer delitos.  
Como ejemplo: Un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema..."nada se destruye, todo se transforma".

**Keyloggers y Stealers:** Estos programas están encaminados al aspecto financiero, la suplantación de personalidad y el espionaje. Los Keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para realizar operaciones fraudulentas como son pagos desde cuentas de banco o tarjetas de crédito. La mayoría de estos sistemas son usados para recopilar contraseñas de acceso, espiar conversaciones de chat u otros fines. Los Stealers también roban información privada pero sola la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados y si tienen contraseñas recordadas, por ejemplo en los navegadores web la descifran.

**Botnets:** Son redes de computadoras infectadas, también llamadas “zombis”, que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de spam o para lanzar ataques contra organizaciones. En una Botnet cada computadora infectada por el malware se logue en un canal de IRC u otro sistema de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente. Las botnets también pueden ser usadas para actualizar el malware en los sistemas infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad.

**Spyware:** Son creados para recopilar información sobre las actividades realizadas por un usuario, obteniendo datos sobre los sitios web que visita, direcciones de email a las que después se envía spam. La mayoría de los programas son instalados como troyanos. Otros programas spyware recogen la información mediante cookies de terceros o barras de herramientas instaladas en navegadores web. Generalmente se presentan como programas que muestran publicidad o ventanas emergentes (pop-up) que son aceptadas de forma involuntaria, afectando los sistemas del usuario.

**Backdoor o Puerta Trasera:** Es un método para eludir los procedimientos habituales de autenticación al conectarse en una computadora. Una vez que el sistema ha sido comprometido, puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro de los atacantes. Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, permaneciendo ocultos ante posibles inspecciones, utilizando troyanos, gusanos u otros métodos.