# **Actividad 1.3. Técnicas de ataque más usuales**

Wuke Zhang

2-ASIR

**Malware**: Es un software malicioso diseñado para infiltrarse y dañar sistemas o robar información. Los ejemplos incluyen virus, troyanos y ransomware, que pueden bloquear tus archivos y pedirte un rescate.

**Ingeniería social**: Los atacantes manipulan a las personas para que revelen información confidencial. Ejemplo: hacerte creer que un correo es de tu banco y pedirte que ingreses tu contraseña.

**Scam**: Son fraudes que buscan engañar a las personas para que entreguen dinero o información. Pueden ser correos, mensajes o llamadas que simulan ofertas irresistibles o falsas emergencias.

**Spam**: Mensajes no solicitados, generalmente publicitarios, que saturan tu bandeja de entrada. Aunque molesto, el spam puede ocultar peligros como enlaces a malware o phishing.

**Sniffing**: Los hackers interceptan datos que viajan por la red, como contraseñas o información personal. Esto es peligroso en redes Wi-Fi públicas.

**Spoofing**: El atacante falsifica su identidad para hacerse pasar por alguien confiable. Puede ocurrir en correos, llamadas o incluso direcciones web, redirigiéndote a sitios falsos​.

**Pharming**: Similar al phishing, pero aquí los atacantes manipulan el DNS para redirigirte a sitios falsos sin que te des cuenta. Un ejemplo sería que creas estar en el sitio de tu banco cuando en realidad es uno falso​.

**Phishing**: El más común. Recibes correos o mensajes falsos que parecen legítimos, tratando de engañarte para que entregues información personal, como tus credenciales.

**Password Cracking**: Los atacantes usan software especializado para descifrar contraseñas mediante técnicas como fuerza bruta, probando múltiples combinaciones hasta dar con la correcta.

**Botnet**: Es una red de computadoras infectadas (bots) que los atacantes controlan de forma remota para realizar actividades como ataques DDoS, sin que los dueños de las computadoras lo sepan.

**Denegación de Servicio (DoS)**: Este ataque satura un servidor o red con tráfico masivo, haciendo que los usuarios legítimos no puedan acceder. Los ataques DDoS son aún más potentes, ya que usan múltiples dispositivos para llevarlo a cabo​.

En adicción de casos populares conocemos al del hacker conocido como **Alcasec**, cuyo verdadero nombre es José Luis Huertas, llevó a cabo diversos tipos de ataques cibernéticos que involucran varias técnicas avanzadas, algunas de las cuales se mencionan a continuación:

1. **Suplantación de identidad (Spoofing)**: Alcasec se hizo pasar por figuras públicas, como Paolo Vasile, logrando realizar operaciones financieras en su nombre. Esto es un claro ejemplo de spoofing, donde falsificó la identidad digital de otra persona para acceder a recursos y ejecutar transacciones.
2. **Intrusiones en bases de datos (Hacking)**: Penetró sistemas altamente sensibles, como los de la **Dirección General de Tráfico (DGT)**, donde expidió carnés de conducir legítimos que ojalá me hubiera llegado a mí. También logró entrar en el sistema de la **Policía Nacional** y el **Punto Neutro Judicial**, que alberga información confidencial de causas judiciales en España, incluidas las de la Audiencia Nacional y el Tribunal Supremo. Esto apunta a ataques basados en la explotación de vulnerabilidades de software y sistemas de seguridad.

Además otro caso es el del burger king donde dejo vulnerable las máquinas para que dejarán gratis las hamburguesas, otro caso que me hubiera gustado vivirlo.

1. **Revelación de secretos y tráfico de datos (Pharming)**: Alcasec creó un buscador de datos llamado **Udyat**, que agregaba información obtenida de distintas instituciones (como la Policía y el Consejo General del Poder Judicial). Este "Google de datos" estaba destinado a vender información a organizaciones criminales, lo que califica como un ataque de **pharming**, donde las víctimas son redirigidas a sitios falsos o bases de datos robadas sin su conocimiento.
2. **Smishing**: Participó en campañas de **smishing**, un tipo de ataque en el que se envían mensajes SMS haciéndose pasar por entidades legítimas (como bancos) para robar información confidencial o dinero de los usuarios, un ejemplo de ingeniería social.