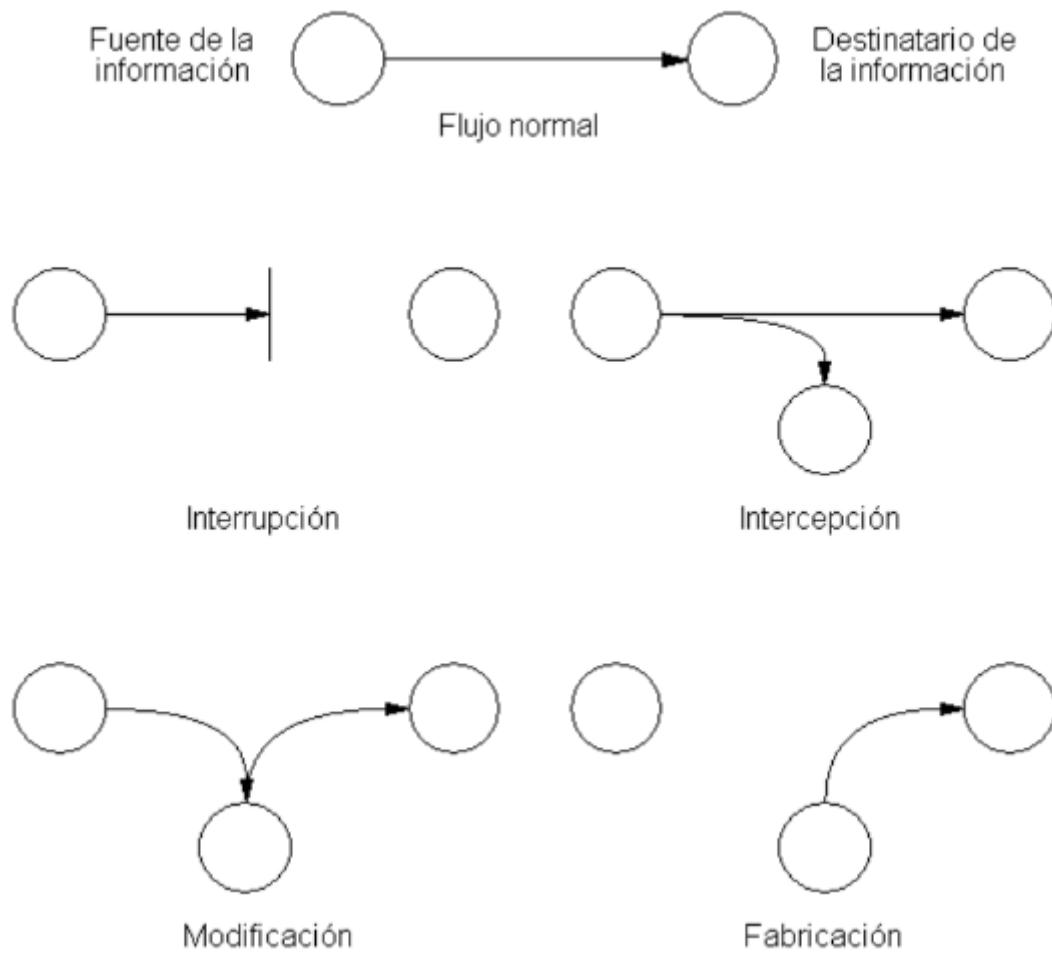


4.1. Tipos de ataques

- **Interrupción:** Destruir o dejar inutilizable los dispositivos.
- **Interceptación:** Acceder a recursos para los que no tiene autorización.
- **Modificación:** Acceder a los recursos y manipularlos.
- **Suplantación o fabricación:** Inserta objetos falsificados. Pueden ser:
 - Suplantación de identidad
 - Suplantación de una dirección web
 - Suplantación de una dirección IP



4.2. Ataques remotos

Se trata de un conjunto de técnicas utilizadas para intentar acceder a un sistema informático a distancia. Se suele utilizar software malicioso que aprovecha vulnerabilidades de seguridad de programas o del sistema operativo.

- **Inyección de Código:** Añade o borra información en sitios remotos
- **Escaneo de Puertos:** Averigua los puertos abiertos para atacar.
- **Denegación de Servicios (DoS):** Satura los recursos de un equipo o de una red para que deje de responder.

- **Escuchas de Red:** Captura e interpreta el tráfico de una red.
- **Spoofing:** Suplanta la identidad del usuario.
- **Fuerza Bruta:** Probar todas las combinaciones posibles de claves de un sistema.
- **Elevación de Privilegios:** El atacante se hace root o administrador para controlar más.

Ejemplos:

- [SQL Injection](#)

4.3. Botnets

Una botnet, o mejor dicho, una red de bots (también conocida como ejército zombi) es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, que quedan bajo control del atacante.

Usos

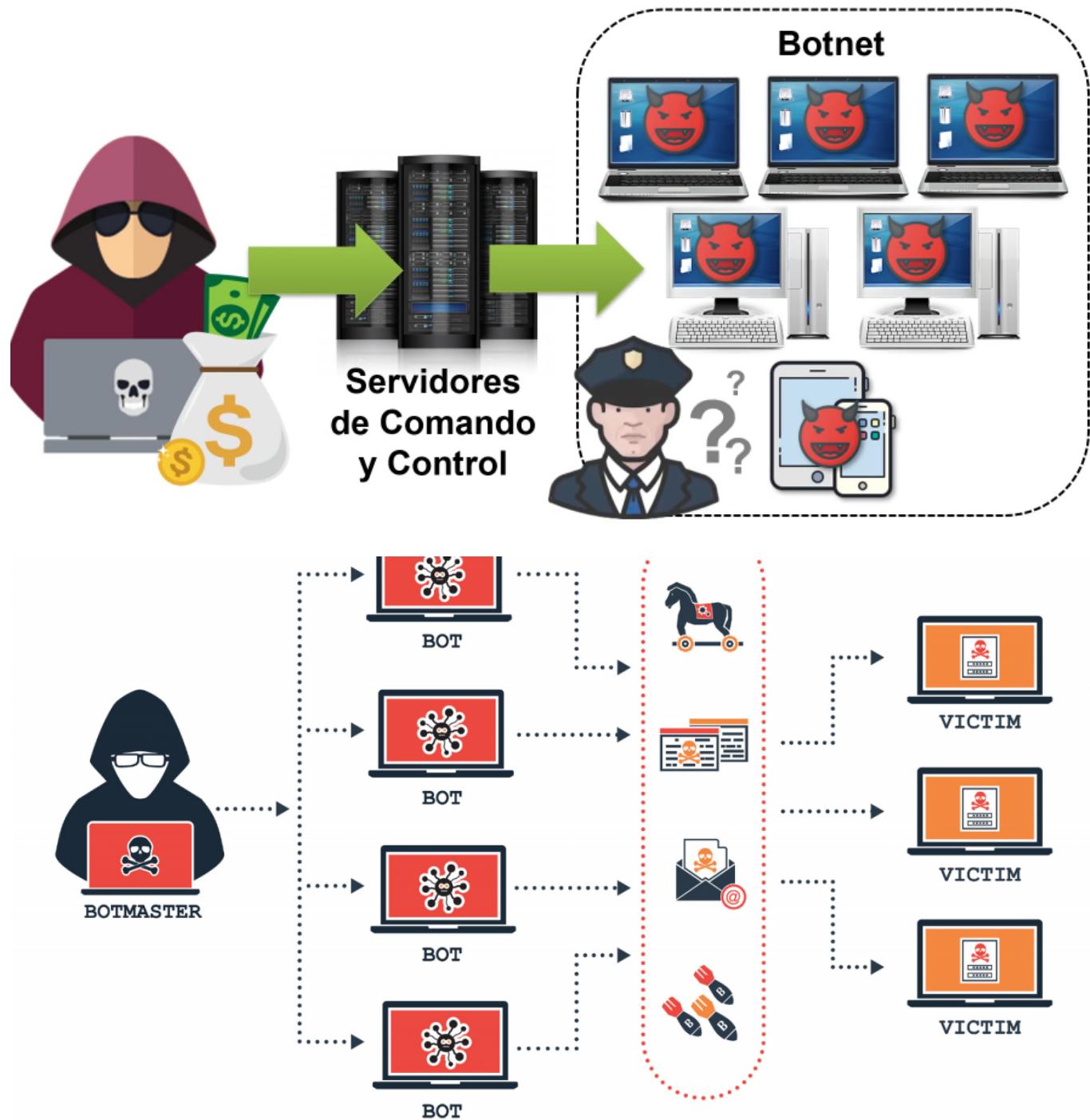
Al tomar el control de cientos o miles de equipos, las botnets se suelen utilizar para:

- Enviar spam o virus
- Realizar ataques de denegación de servicio distribuido (DDoS).
- Minería de criptomonedas
- Ataques de fuerza bruta



Para que un equipo forme parte de una botnet, primero es necesario que se **infecte** con algún tipo de **malware** que se comunica con un servidor remoto o con otros equipos infectados de la red. De esta forma, recibe instrucciones de quien controla la botnet, normalmente hackers y cibercriminales.

Servidores de comando y control



Ejemplos

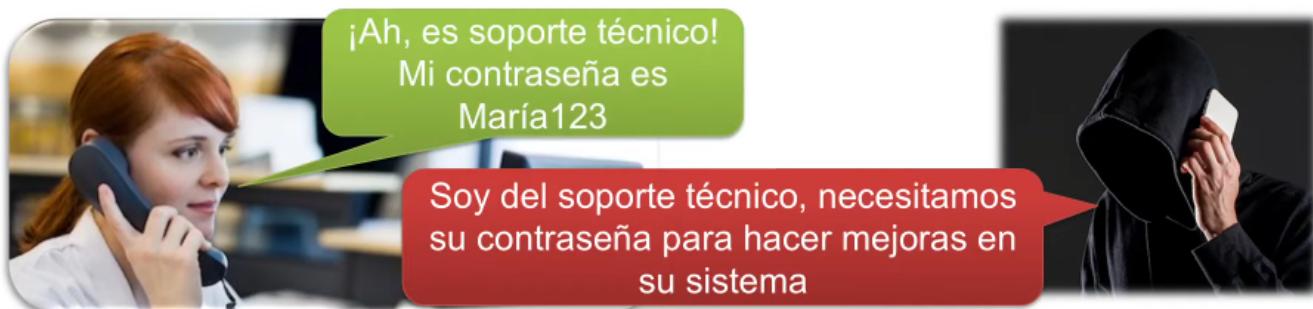
- Zeus
 - ✓ Troyano que se ejecuta en Windows.
 - ✓ Incorpora keylogger.
 - ✓ Roba información bancaria.
 - ✓ Usado para propagar CryptoLocker.



4.4. Ingeniería social

Los **eslabones** más **débiles** de cualquier cadena de seguridad son los seres humanos. La ingeniería social busca explotar este punto débil, apelando a la vanidad, la avaricia, la curiosidad, el altruismo o el respeto o temor a la autoridad de las personas, para conseguir que revele cierta información o que permita el acceso a un sistema informático.

Ejemplo

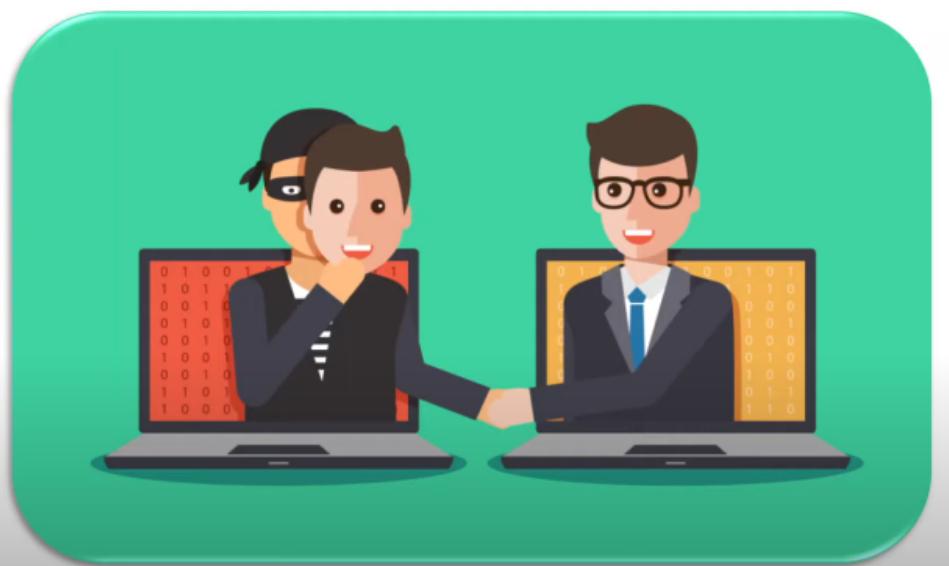


Hay una serie de técnicas de ingeniería social que los ladrones utilizan. Incluyen:

- Cebos (ofrecerle algo que desea para conseguir que descargue un archivo malicioso),
- Phishing (un correo electrónico fraudulento para que comparta información personal)
- Pretextos (hacerse pasar por otra persona con el fin de obtener acceso a información privilegiada)
- Scareware (engañarle para que crea que su equipo está infectado con malware y luego ofrecer una solución que infecta el ordenador).

Componentes psicológicos

- Autoridad
- Intimidación
- Consenso
- Escasez
- Urgencia
- Familiaridad
- Confianza



Autoridad

• Autoridad

- Intimidación
- Consenso
- Escasez
- Urgencia
- Familiaridad
- Confianza

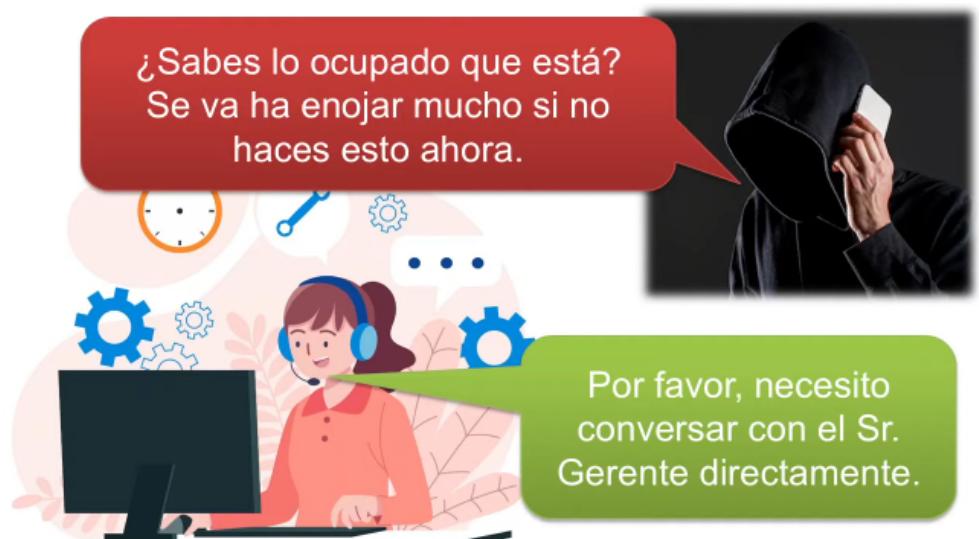
Autoridad: Las personas escuchan y respetan a alguien que transmite un aire de autoridad. Y los atacantes se aprovechan de este mecanismo psicológico.



Intimidación

- Autoridad
- **Intimidación**
- Consenso
- Escasez
- Urgencia
- Familiaridad
- Confianza

¿Sabes lo ocupado que está?
Se va ha enojar mucho si no
haces esto ahora.



Por favor, necesito
conversar con el Sr.
Gerente directamente.

Consenso

- Autoridad
- Intimidación
- **Consenso**
- Escasez
- Urgencia
- Familiaridad
- Confianza

Consenso o prueba social: mecanismo psicológico por el cual tendemos a acomodarnos a la opinión mayoritaria.



Escasez

- Autoridad
- Intimidación
- Consenso
- **Escasez**
- Urgencia
- Familiaridad
- Confianza

Escasez: El atacante Hace creer a las personas que si no actúan rápidamente, perderán una oportunidad.



Urgencia

- Autoridad
- Intimidación
- Consenso
- Escasez
- **Urgencia**
- Familiaridad
- Confianza



Familiaridad

- Autoridad
- Intimidación
- Consenso
- Escasez
- Urgencia
- **Familiaridad**
- Confianza

Familiaridad o agrado: El atacante utiliza la familiaridad o el agrado de otras personas para obtener información confidencial o que realicen ciertas actividades.



Confianza

- Autoridad
- Intimidación
- Consenso
- Escasez
- Urgencia
- Familiaridad
- **Confianza**

Confianza: El atacante se aprovecha la confianza de las personas para obtener información confidencial o pedir que realicen ciertas actividades.

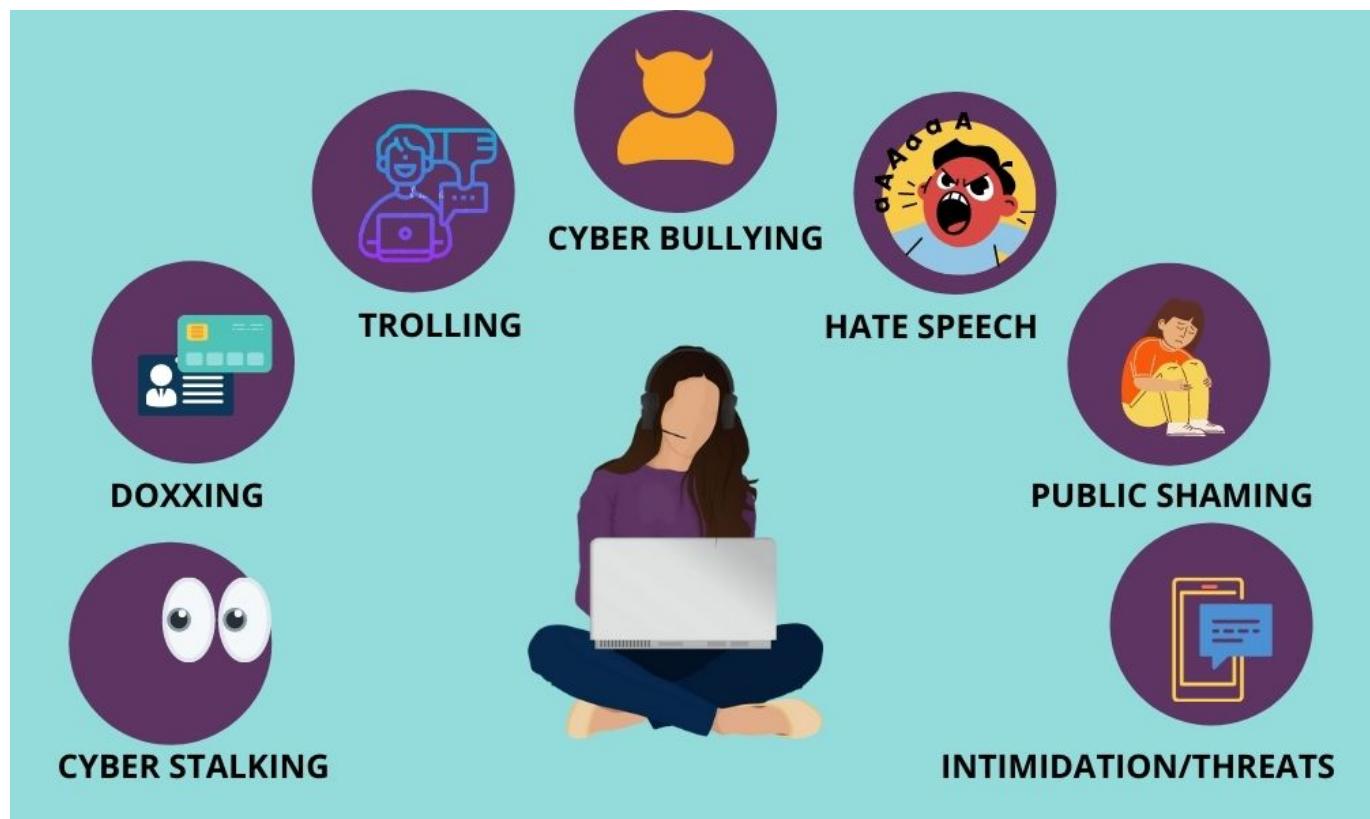


¿Cómo defendernos?

- Educación y capacitación a los usuarios
- Políticas de seguridad sin excepciones

4.5. Ciberacoso

El ciberacoso puede ser el tipo de ataque en línea más pernicioso, ya que los acosadores, que suelen **ocultarse** tras personalidades falsas, tienden a aprovecharse de las **inseguridades** o **debilidades** personales de la víctima para humillarla y causarle daños **psicológicos**.



El ciberacoso suele consistir en:

- El envío de mensajes amenazantes.
- La publicación de fotografías o vídeos humillantes de la víctima en redes sociales.

En ocasiones, incluso se crean páginas web sobre la víctima. Como a menudo vemos en los periódicos, el efecto del ciberacoso puede ser devastador y, en ocasiones, incluso mortal.

¿De dónde proviene el ciberacoso?

El ciberacoso lo practica la misma gente indeseable que acosa en la vida real. Personas que quieren **abusar de su poder** y elevar su **status** en las redes sociales **denigrando** y **humillando** a otros, especialmente si consideran que la otra persona es más débil o creen que puede representar una amenaza.



Los ciberacosadores pueden:

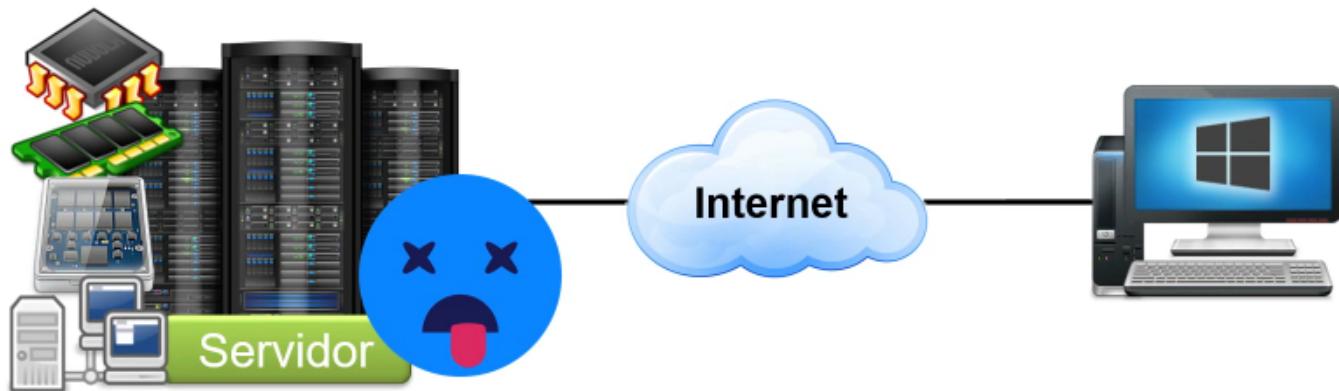
- Realizar publicaciones anónimas
- Esconderse tras identidades falsas
- Utilizar su identidad real sabiendo que no se van a enfrentar cara a cara con sus víctimas.

Muchos de ellos dicen o publican cosas en línea que jamás se atreverían a decir en la vida real.

4.6 DDoS: denegación de servicio distribuido

Los ataques de denegación de servicio (DoS) **bloquean** sitios web o redes completas **saturándolos con tráfico**.

- Causa que un servicio o recurso sea inaccesible a usuarios legítimos.
- El atacante sobrecarga diferentes tipos de recursos como CPU, memoria, almacenamiento o recursos de la red.



¿cómo se ven afectados los usuarios?

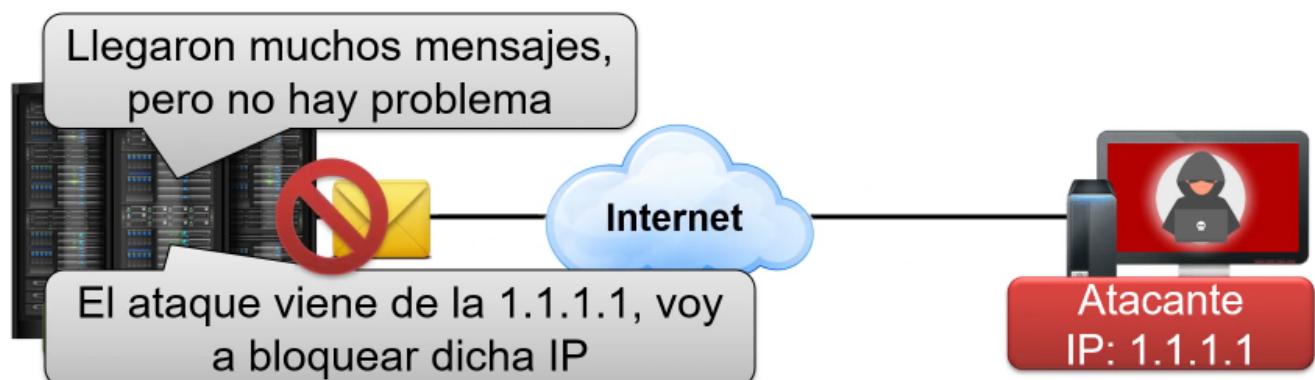
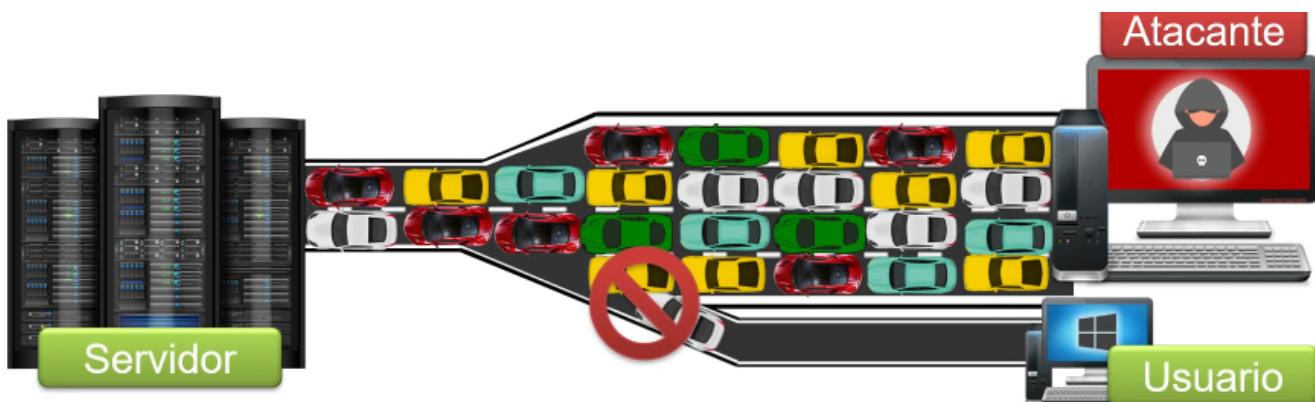
Dado que tanto el objetivo como los equipos utilizados en la botnet son víctimas, los usuarios individuales reciben daños colaterales en el ataque, ya sus equipos se ralentizan y fallan mientras se encuentran bajo el control del hacker.

Los motivos que llevan a un hacker a organizar un ataque DDoS suelen ser:

- El beneficio económico
- La venganza
- El deseo de ser un "troll"

El ataque hace que se cierre el sitio web y que sus servicios en línea dejen de estar disponibles para los usuarios, que suelen perder la paciencia y la confianza en la empresa, terminando por buscar otras opciones empresariales alternativas. Además de la consecuente **pérdida de ingresos**, esto produce un daño importante en la **reputación** de la organización.

Denegación de servicios DoS



DDoS (DoS distribuido)

- ✓ Superan el problema de bloqueo de IP ya que el ataque provienen de diferentes fuentes.
- ✓ Es difícil distinguir qué direcciones IP son de usuarios legítimos.

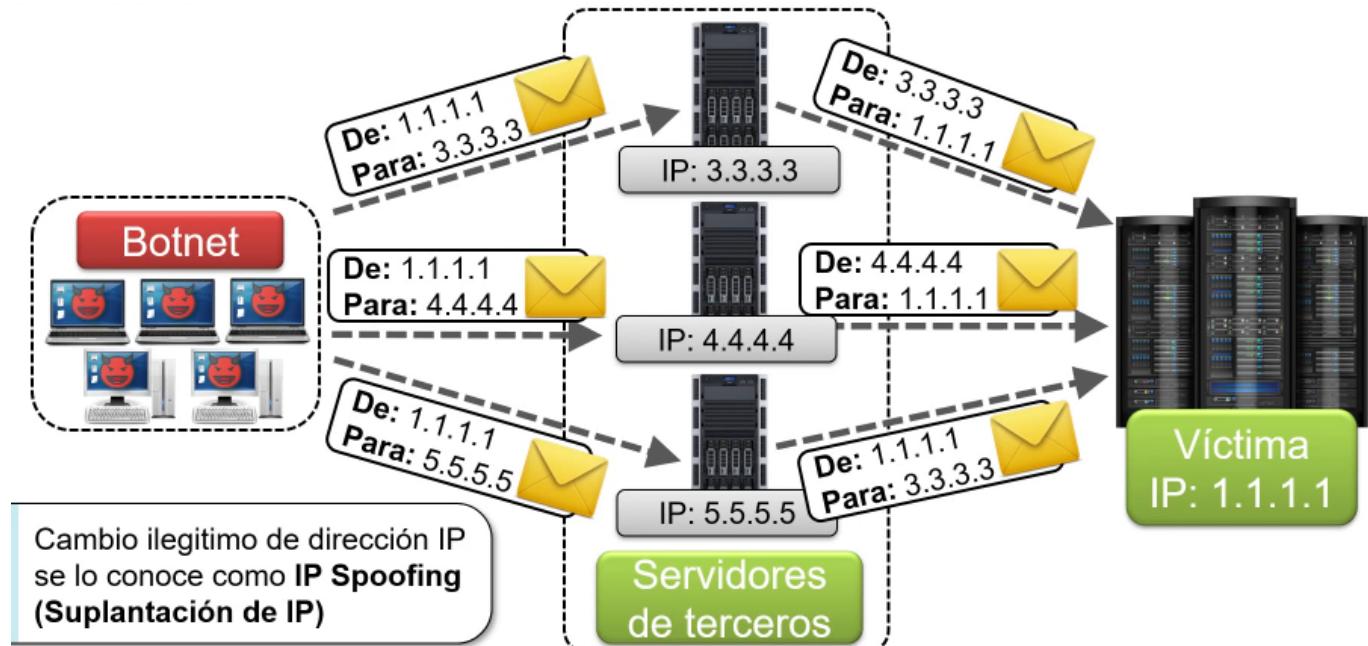
¡No sé cuál es la IP del usuario legítimo!



Ataques de reflexión y amplificación



Ataques de reflexión



Ataque de amplificación

Ping

