Tema: CIBERSEGURIDAD

ÍNDICE

1. Introducción a la Ciberseguridad

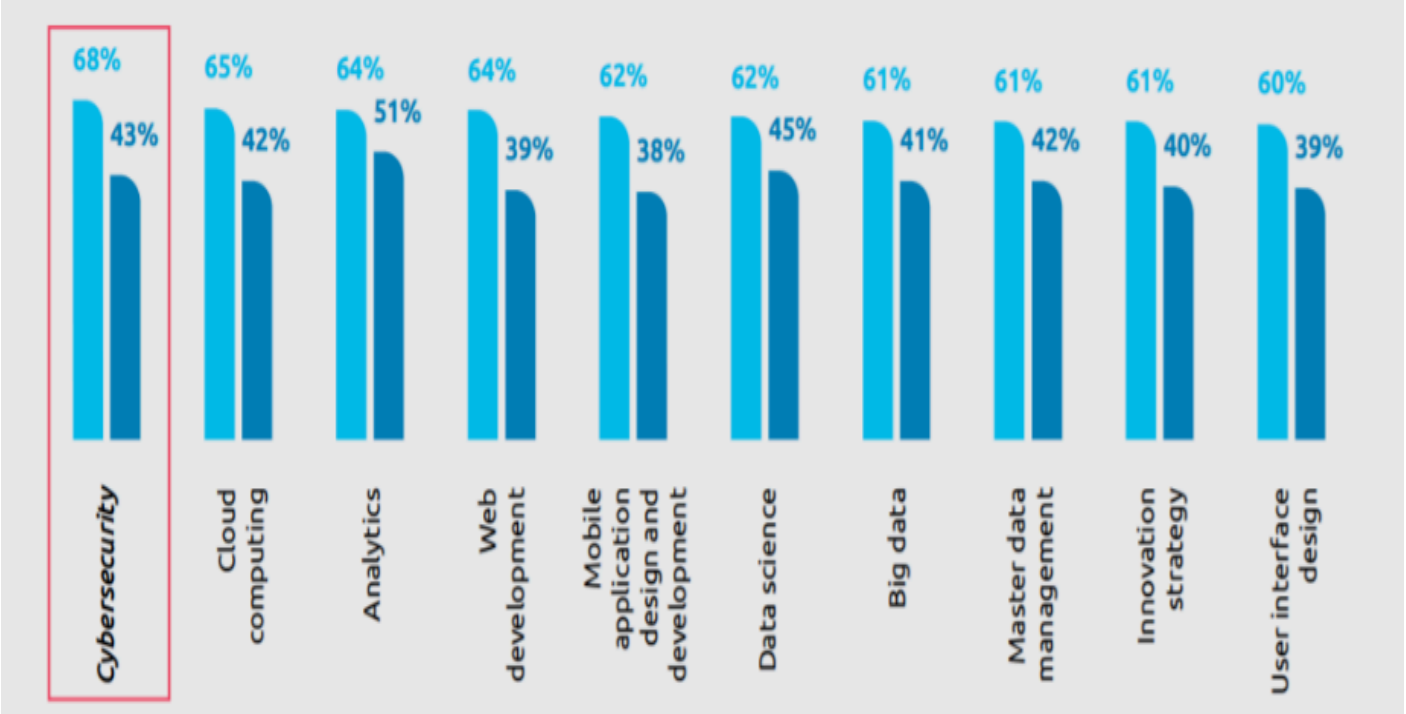
Definición

La ciberseguridad es la práctica de **DEFENDER**:

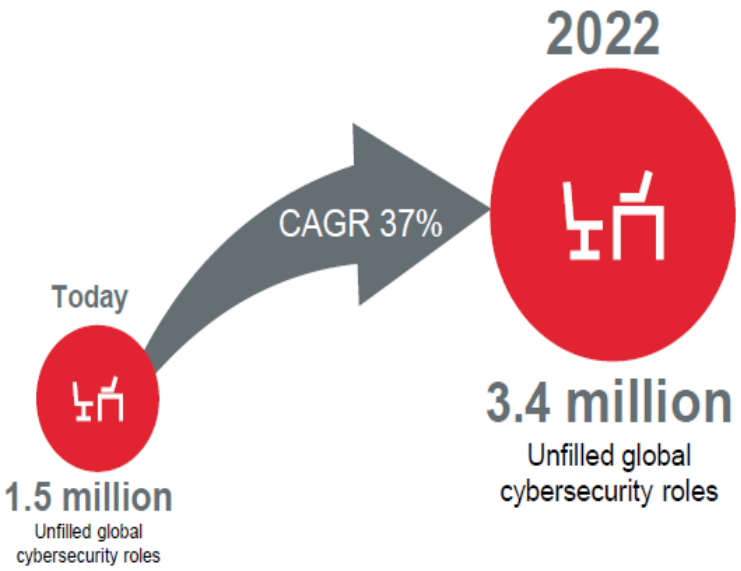
- las computadoras,
- los servidores,
- los dispositivos móviles,
- los sistemas electrónicos,
- las redes
- y los **datos** de ataques maliciosos.

- Software

El mercado de talento en **ciberseguridad** es el mercado de talento digital que presenta mayor GAP (diferencia) entre oferta (azul claro) y demanda (azul oscuro).



El déficit de talento en ciberseguridad, lejos de reducirse, seguirá creciendo durante los próximos años.


2022
CAGR 37%
Today
3.4 million
Unfilled global
cybersecurity roles
1.5 million
Unfilled global
cybersecurity roles


CYBER-
SECURITY
There is an urgent need for qualified cyber
defenders to strike back at the increase in
cybercrime.
600%
COVID-19 increased cybercrime by 600%.
87.5%
87.5% of all cybersecurity jobs remain open.
MÁS VÍDEOS
int o Diferentes puestos en
seguridad cibernética

Para 2022 la falta de profesionales en ciberseguridad superaría los 4 millones

COMPARTIR:

La industria IT se encuentra en alerta por la escasez de talento en un área donde cada vez más personas son requeridas, la de ciberseguridad. En 2020 se publicaron más de 166,000 búsquedas de analistas de seguridad y se espera que este sector crezca un 28% en la próxima

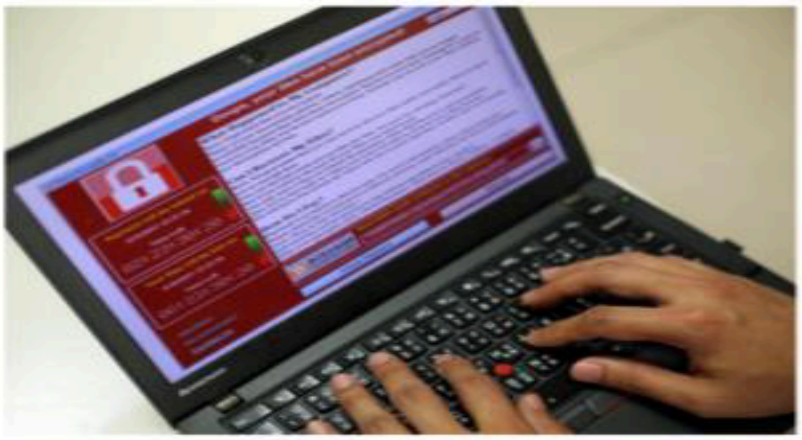
HERALDO Ocio y Cultura

TECNOLOGÍA

Las empresas de ciberseguridad buscan 'hackers': "Falta talento por todas partes"

El sector ofrece una profesión con mucha demanda, poca oferta y menos paro.

NOTICIA ACTUALIZADA 10/4/2021 A LAS 13:57
MARÍA TRASPADERNE



El sector de la ciberseguridad necesita profesionales. | EFE/EPA

"Cazamos donde podemos, levantando las piedras y buscando en el desierto si hace falta", josé Rosell tiene una empresa de 450 trabajadores y le cuesta encontrar empleados.

Por Economía Digital
13 abril 2021
a las 06:55

Desde hace años los expertos en ciberseguridad vienen alertando de la **falta de trabajadores cualificados en ciberseguridad**. Un déficit cuyas consecuencias, reales y potenciales, se han agravado durante el último año.

El confinamiento y la pandemia han provocado la **migración a internet de gran parte de la actividad económica y social**, como también ha paralizado numerosos negocios y sectores enteros.

Como consecuencia, **la digitalización y el crecimiento de la actividad online** derivada del ecommerce, el teletrabajo, la telemedicina y la educación a distancia; de la transformación de empresas, industrias, negocios y administración, y de un mayor consumo de entretenimiento online, entre otros, **ha incrementado la demanda de personal cualificado en ciberseguridad**.

Las empresas necesitan más que nunca “digital workers” ciberseguros.

Expertos que sepan desenvolverse con soltura y ofrecer soluciones ciberseguras en un entorno virtual.

2. Hacker versus cibercriminal/ciberdelincuente/cracker.

- **Hacker**

  Informar, paliar sobre problemas encontrados en un sistema (**MUY BIEN PAGADO**).

- **Ciberdelincuente**

  Sacar partido (ilegalmente) de dichos fallos.

Motivación de un **ciberdelincuente**:

- ➢ Superación
- ➢ Beneficio económico
- ➢ Ideología

➢ **Venganza**

Cómo actúan:

- ➢ **Malware**
- ➢ Robo de credenciales
- ➢ Chantaje y extorsión
- ➢ Ataques de denegación de servicio

3. Tipos de ataques

- **Interrupción**

  Se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.

- **Intercepción**:
  Se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.

- **Modificación**

  Se trata de modificar la información sin autorización alguna.

- **Fabricación**

  Se crean productos, tales como páginas web o tarjetas magnéticas falsas.
  Ejemplo:

  Alcasec, hacker

Clasificación por nivel de daño de los ataques:

Nivel	Clasificación	Nivel	Clasificación
Crítico	APT / Ciberterrorismo	Medio	Contenido abusive
Muy alto	Código dañino		Obtención de información
	Intrusión		Intento de intrusion
	Disponibilidad		Fraude
Alto	Contenido abusivo	Bajo	Vulnerabilidad
	Código dañino		Intrusión sin privilegios
	Intrusión		Otros
	Compromiso de la información		

Fuente: INCIBE-CERT

4. Malware

El Malware es el software que tiene **objetivos** maliciosos. Por ejemplo:

- Borrado de información
- Robo de información
- Denegación de servicio
- Control remoto
- Etc.

Se suele clasificar por su capacidad de propagación. Las tres grandes familias son:

- Virus
- Troyanos
- Gusanos

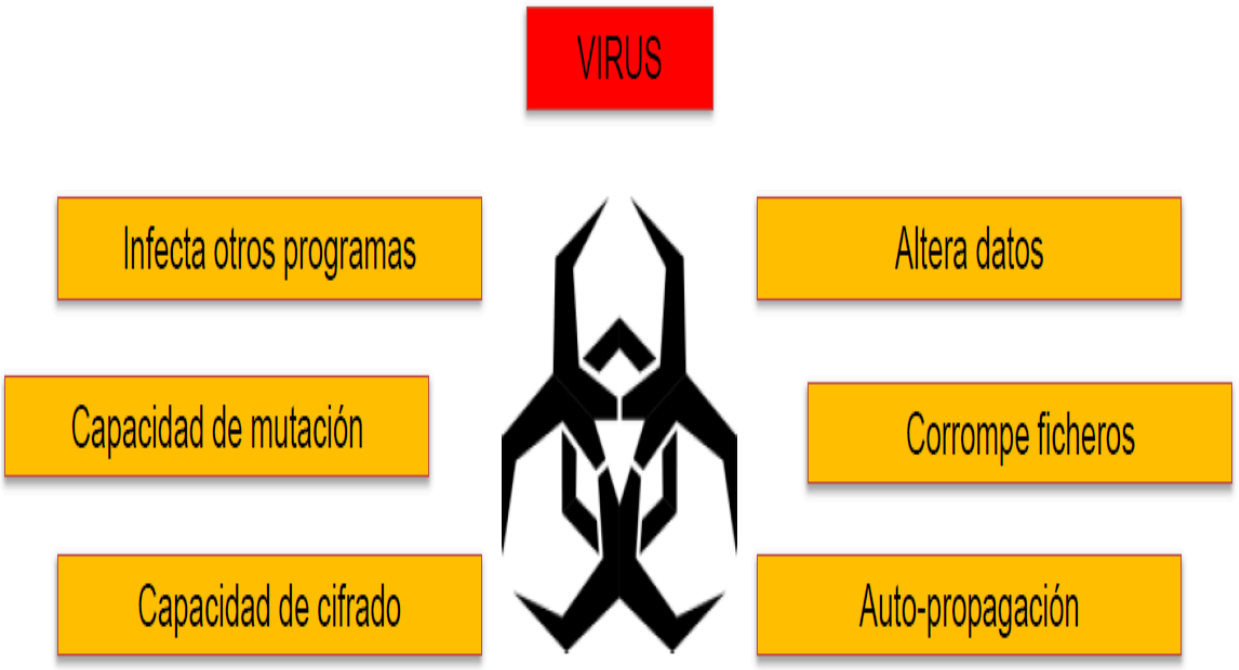
- Virus

El virus es un tipo específico de malware.

Es común llamar “virus” al malware, pero en realidad es solo un subconjunto.

Su nombre viene por su parecido a los virus reales (infección y propagación).

Para su propagación **necesitan** que cierta **interacción** por parte del **usuario**.



- **Gusanos**

Los gusanos (habitualmente llamados worms) son programas maliciosos que se **propagan** por la red de forma automática.

Los gusanos se transmiten explotando vulnerabilidades de los sistemas sin que el usuario tenga que interactuar con ellos de ninguna manera.

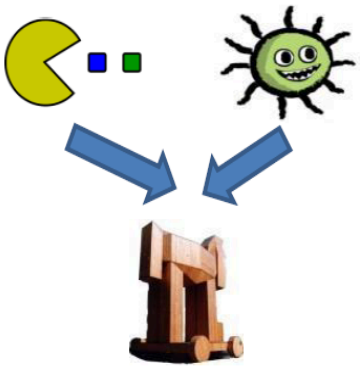
Este tipo de malware es habitual en teléfonos, ya que este tipo de dispositivo conectado es idóneo para una propagación rápida.

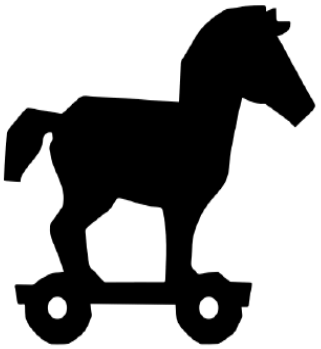
Un gusano muy famoso, **Stuxnet**, es un malware supuestamente desarrollado por Israel y Estados Unidos diseñado para infectar infraestructuras críticas que infectó a 60.000 equipos en Irán.

- **Troyanos**

Un troyano o caballo de Troya es un programa malicioso (malware) que se presenta al usuario como un programa aparentemente inofensivo.

El término proviene de la Odisea de Homero.





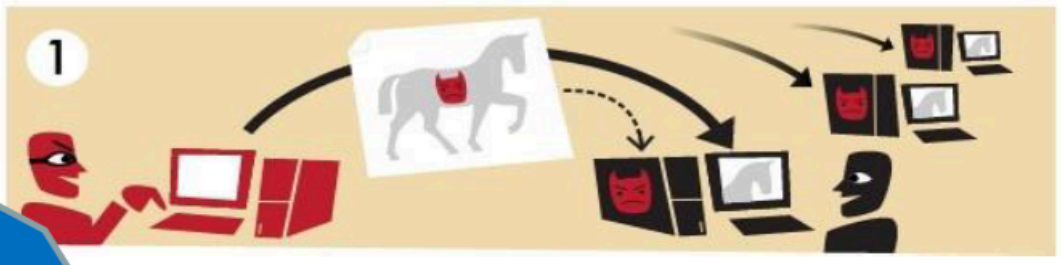
5. Botnets.

Una botnet es una red de ordenadores infectados controlados por un ciberdelincuente.

Los ordenadores infectados obedecerán a las órdenes del ciberdelincuente, de forma que éste dispone de un “ejército” de ordenadores listos para realizar operaciones maliciosas en Internet en cualquier momento.

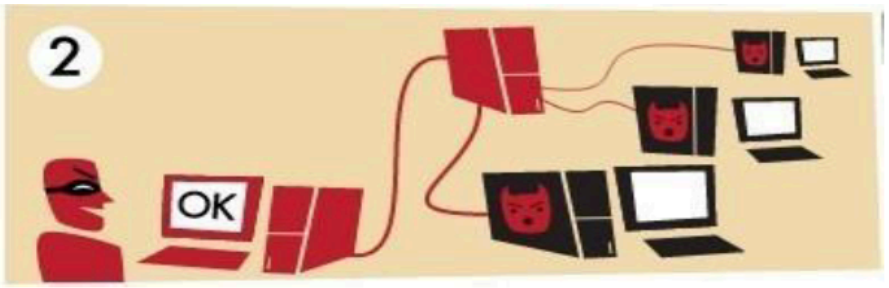
Ciclo de vida de una BOTNET:


1
2
OK
3
$
4



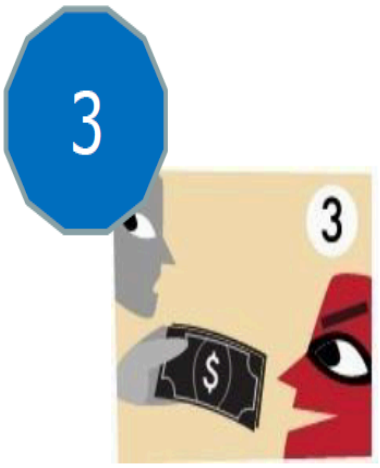
1

Infección: el atacante infecta ordenadores personales de usuarios por medio de troyanos.



2

El atacante forma así una red de miles de ordenadores controlados por un servidor *Command and Control*.

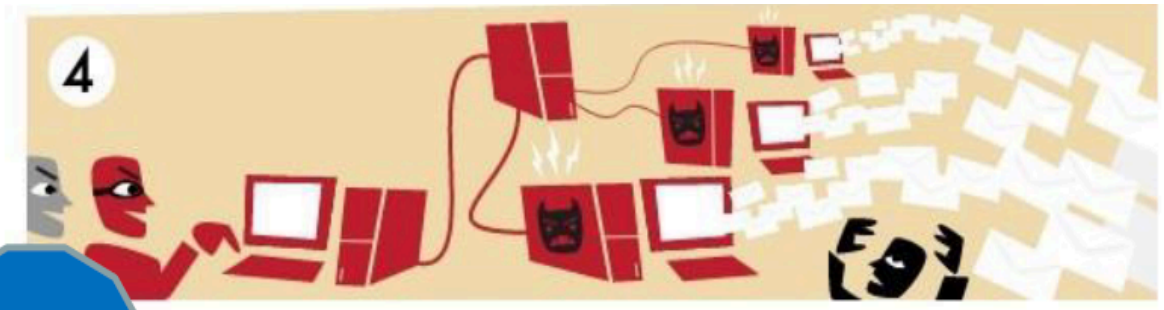


Una tercera parte malintencionada compra acceso a la botnet para realizar acciones maliciosas, como por ejemplo:

- Ataques de denegación de servicio distribuidos (DDoS)
- Envío de Spam
- Fraude de clicks

También podemos utilizar la herramienta AntiBotnet de Protege tu empresa para proteger nuestra red de posibles amenazas:

https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet



4

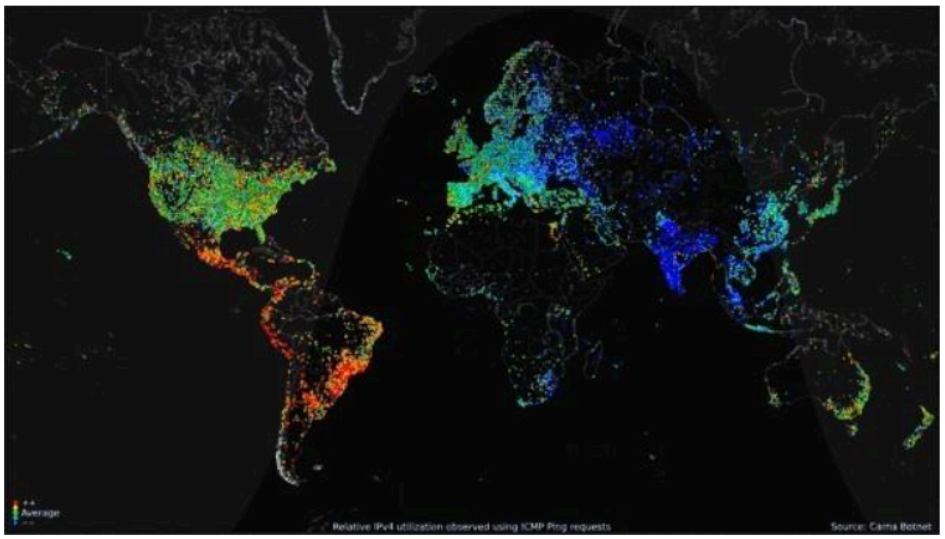
Se lanza el ataque distribuido. En este ejemplo, se utiliza la botnet para enviar millones de correos publicitarios.

Ejemplos:

- Carna Botnet:

BOTNET

CARNA



Carna Botnet fue una red de 420.000 dispositivos infectados.

- ZeroAccess botnet
  - La botnet ZeroAccess fue una botnet especializada en minería de bitcoin y click fraudulento.
  - Desde su creación, se han minado 18.119.425 Bitcoins.
  - El número máximo de Bitcoins que se pueden minar en tota es de 21 millones, por lo que nos estamos aproximando al límite.
  - Se estima que entre 3 y 4 millones de Bitcoins se han perdido para siempre.

BOTNET ZeroAccess (minado de Bitcoins)

El bitcoin es una moneda electrónica creada en 2009. La generación ("minería") de bitcoins necesita potencia computacional, algo que se puede conseguir con una red de ordenadores distribuidos.

6. Ciberataques más frecuentes.

a. Phishing

Ataque que consiste en recabar datos personales de usuarios con el fin de suplantar su identidad.

¡¡¡Más del 80 % de ataques informáticos empiezan con un phising !!!

b. ***Arp-Spoofing***

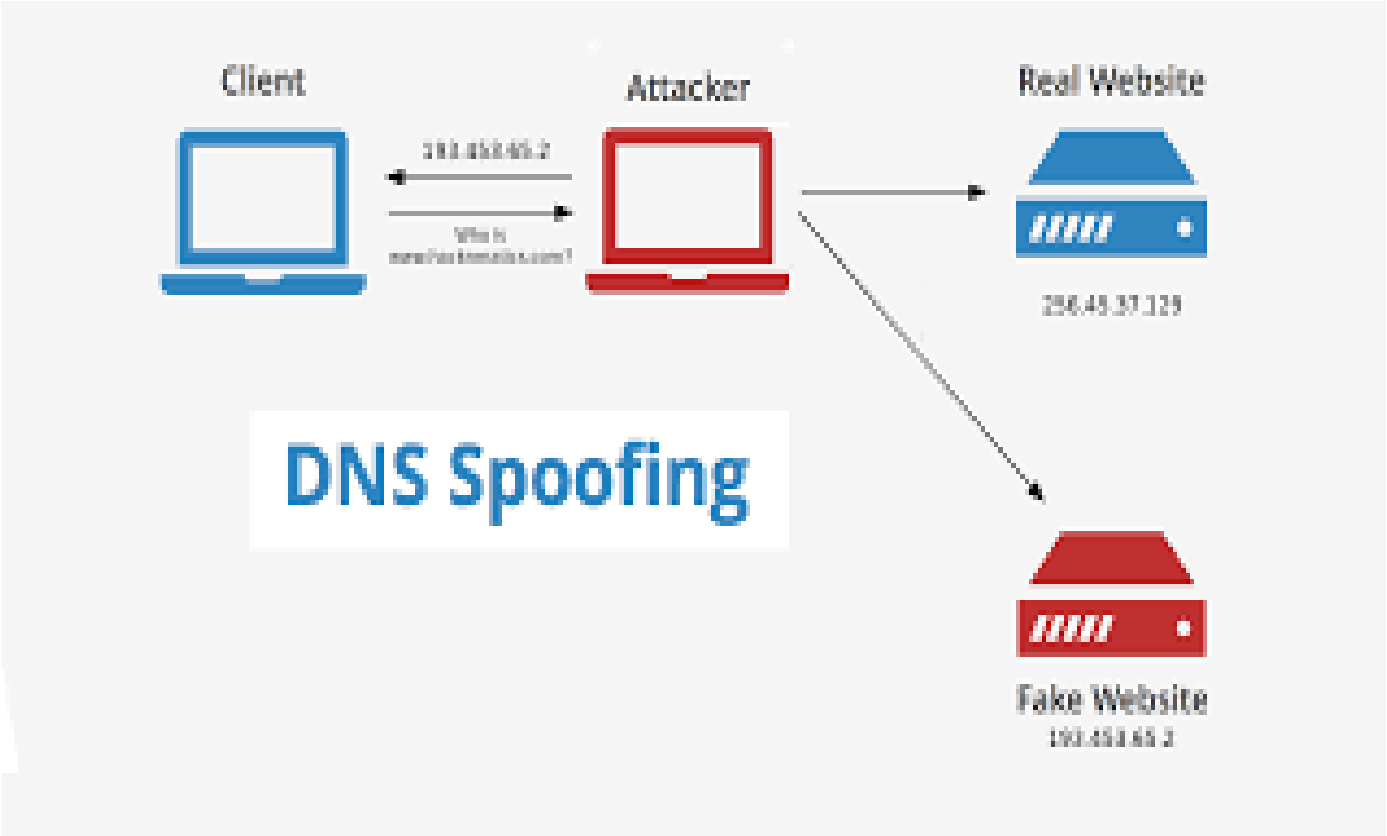
Los datos obtenidos de un sistema son utilizados en otro.

- Práctica arp-dns-spoofing (enlace)

c. ***IPSpoofing***

La IP atacante se oculta detrás de otra para mandar tramas TCP/IP mientras su propia Dirección permanece invisible en la red.

d. ***DNS-Spoofing***.



El atacante "*envenena*" el caché del servidor DNS y este resuelve los nombres con IPs erróneas.

e. ***WebSpoofing***

Consiste en Crear sitios web ficticios **haciéndose pasar** por verdaderos, auténticos u oficiales**.** El usuario cree acceder al sitio web verdadero y de confianza.

f. LOS ATAQUES DDOS

Seguro que has leído y escuchado muchas veces hablar sobre los ataques DDoS y DoS o también llamados **ataques de denegación de servicio**. Pero **¿sabes realmente lo que son?** A priori, parece un término muy técnico, pero este ciberataque es muy sencillo de comprender.

Además, son de los más utilizados por los ciberdelincuentes para desestabilizar nuestros sistemas informáticos. En el siguiente artículo te explicamos en qué consisten, sus diferencias y lo más importante, cómo deshacernos de estos o, por lo menos, mitigar el daño.

¿DDos, DoS o ataque de denegación de servicio?

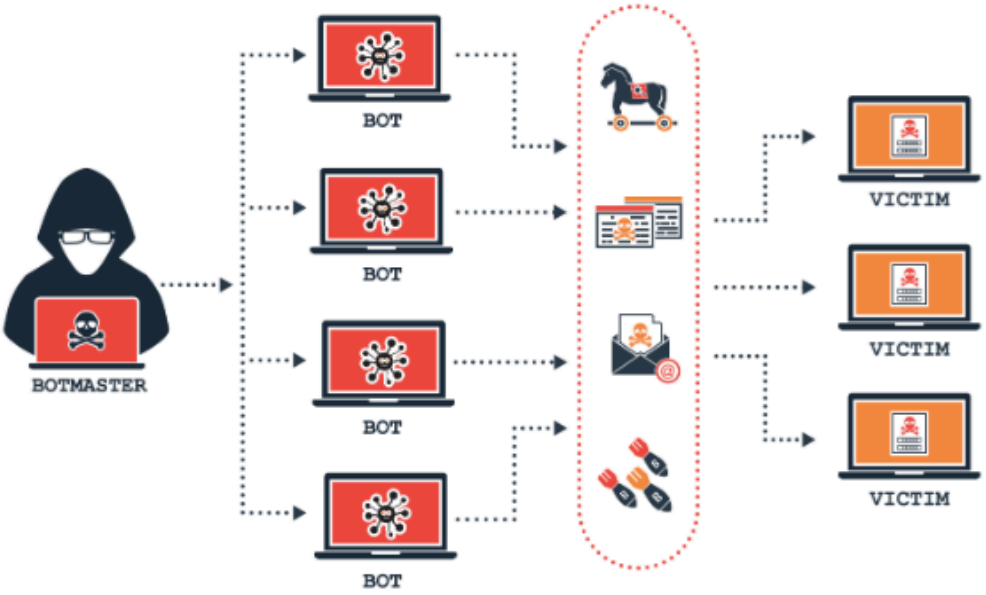
Como definición general de **ataque de denegación de servicio**, sería ese ataque que tiene como objetivo inhabilitar el uso de un sistema, una aplicación o un servidor. Así, se bloquea el servicio para el que está destinado. Como sabemos, los servidores web poseen la capacidad de resolver un número **determinado** de peticiones o conexiones de usuarios de forma simultánea. En caso de superar este número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta.

DDos y DoS

Existen dos técnicas de este tipo de ciberataques: la denegación de servicios **DoS (Denial of Service)** y la denegación de servicio distribuido o **DDoS (Distributed Denial Of Service):**

- En los ataques **DoS** se genera una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP. Se consume así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones. En ese momento, se ha materializado la denegación de servicio.
- Para los ataques **DDoS**, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio. Un ataque DDoS es más difícil de detectar. El número de peticiones proviene desde diferentes IP’s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en ataques **DoS**.

Los ordenadores que realizan los ataques **DDoS** son reclutados mediante la infección de un **virus** o **malware**, convirtiéndose así en **bots**, capaces de ser controlados de forma remota por un ciberdelincuente. Un conjunto de bots, es decir, de ordenadores infectados, forman una **botnet**. Obviamente, esta red tiene mayor capacidad para derribar servidores que un ataque realizado por sólo una máquina, como sería en el caso de los ataques **DoS.**



7. **dfdff**