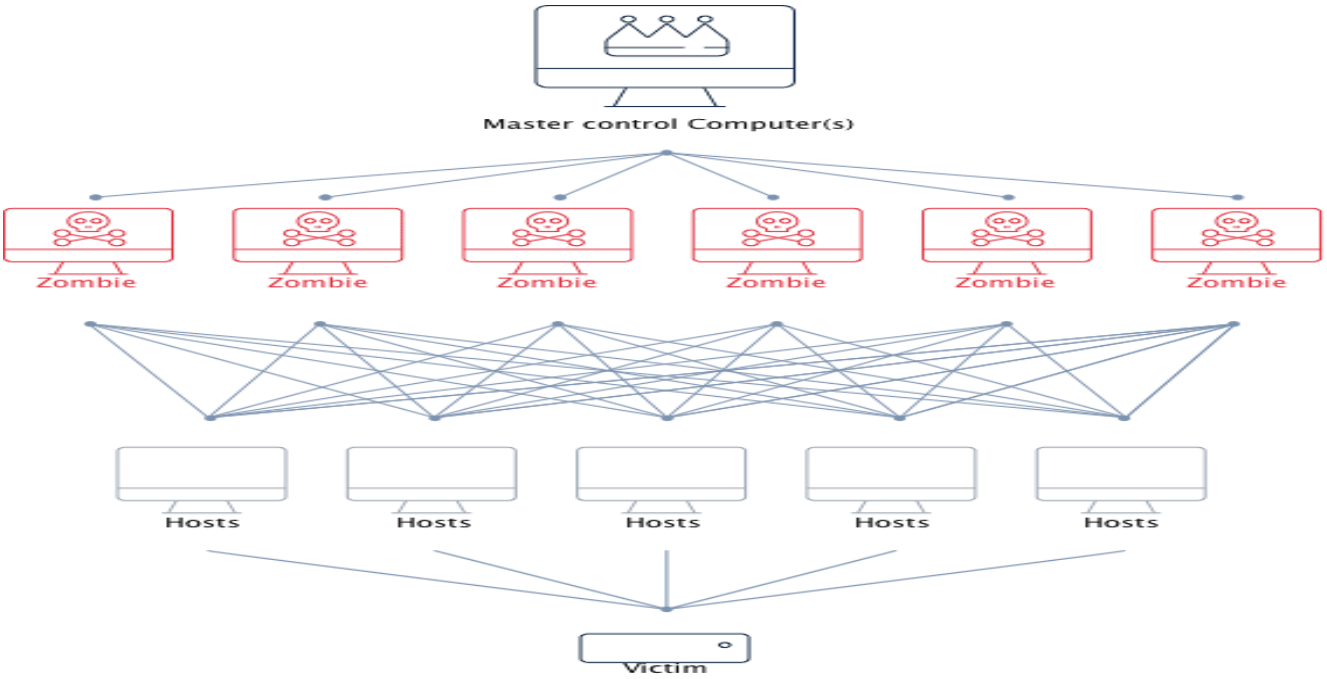
Ataques Ddos

Ataques Ddos es la denegación de servicio distribuido o DDoS por sus siglas en inglés Distributed Denial of Service. Muchas veces son llevados a cabo por bots, sistemas infectados cuyo propietario muchas veces desconoce que sus dispositivos forman parte de esta red maliciosa. Este tipo de ataque consiste en un grupo de sistemas comprometidos (también conocidos como "ordenadores zombie") que atacan a un solo objetivo para causar una denegación de servicios a los usuarios que sí son legítimos



Algunas medidas de protección son:

- Ubicar el servidor web en una zona desmilitarizada evitando que un intruso pueda acceder a la red interna si vulnera el servidor web.
- Implementar un sistema de detección y prevención de intrusiones que monitorice las conexiones y nos alerta si detecta intentos de acceso no autorizados.
- Utilizar un dispositivo o software como un UTM que permite gestionar de manera unificada la mayoría de ciberamenazas que pueden afectar a una empresa.

Las diferencias entre DoS y DDoS son que os ataques DoS sólo necesitan un ordenador y una conexión a Internet para abrumar el ancho de banda y recursos de un objetivo mientras que el ataque DDoS usa muchos dispositivos y varias conexiones de Internet desde distintas direcciones

Tipos de ataques DDoS:

- Consumo de recursos computacionales, como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, por ejemplo información de rutas de encaminamiento.
- Alteración de información de estado, como interrupción de sesiones TCP.
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, para que no puedan comunicarse adecuadamente.

Ejemplos de ataques DDoS

- El ataque de MafiaBoy. El 7 de Febrero de 2000, Michael Demon Calce, que en Internet era conocido como MafiaBoy, lanzó un ataque DDoS contra Yahoo!lo que provoco que el sitio dejara de funcionar durante una hora entera. El fin del ataque era obtener credibilidad en Internet para él y para su grupo de ciberamigos que era TNT. MafiaBoy continuó con los ataques deteniendo completamente los servidores de eBay, CNN, Amazon y Dell.com.
- Ciberataques de julio de 2009. Estos ataques DDoS afectaron sitios web de noticias, finanzas y de los gobiernos tanto de Estados Unidos como de Corea del Sur. Según las estimaciones de varias empresas de seguridad, se creó un ejército de alrededor de 50.000 ordenadores zombies ubicados en Corea del Sur. Hubo tres ataques consecutivos: uno el 4 de julio, día de Independencia en Estados Unidos, donde se vieron afectadas las páginas de la Casa Blanca y el Pentágono; otro el 7 de julio, el cual afectó únicamente a sitios gubernamentales de Corea del Sur; y finalmente el 9 de julio, donde se vieron afectados sitios web de ambos países.

Botnet

Una botnet, o una red de bots (que también se conoce como ejército zombi) es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición de un hacker. Al tomar el control de los equipos, las botnets se suelen utilizar para enviar spam o virus, para robar información personal o para realizar ataques de denegación de servicio distribuido (DDoS).

Algunos síntomas pueden ser que el equipo funcione lento, que actúe de forma extraña, que muestre mensajes de error o que su ventilador comience a funcionar de repente mientras está inactivo. Todos estos son síntomas de que alguien puede estar utilizando su equipo de forma remota como parte de una red de bots.
Para quitar un equipo de una red botnet, se debe de desinstalar el software malicioso que lo controla. Para esto lo mejor es realizar un análisis antivirus de su equipo, que debería localizar el malware botnet y eliminarlo.

Se pude evitar de las siguientes formas:

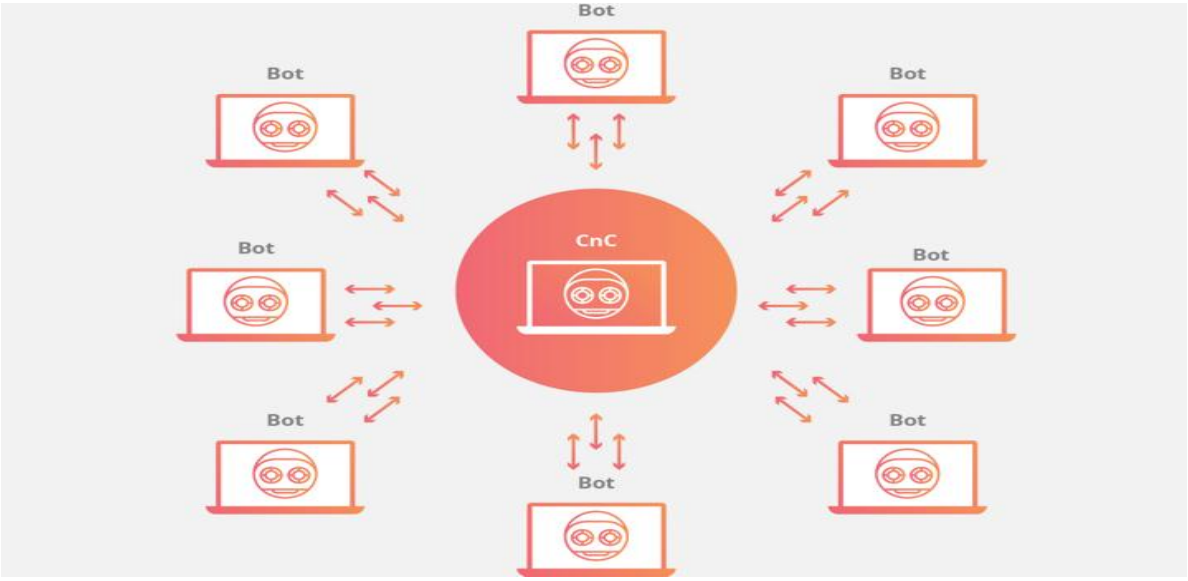
- Tener instalado en el equipo un software antivirus potente y de confianza
- Configurar el software para que se actualice automáticamente
- Tener mucho cuidado con dónde hace clic, qué descarga o qué archivos abre

En los sistemas Windows y macOS la forma más habitual de expansión de los "bots" es la distribución de software ilícito. Este tipo de software suele contener malware que una vez ejecutado el programa pueda escanear su red de área local, disco duro.

En otros entornos como UNIX, GNU/Linux o BSD la forma más habitual es por telnet o SSH por medio del sistema prueba-error: probando usuarios comunes y contraseñas al azar contra todas las IPs que se pueda de forma sistemática o bien mediante ataques a bugs muy conocidos, que los administradores pueden haber dejado sin enmendar.

El funcionamiento una botnet que envía spam sigue los siguientes pasos

1.El operador de la botnet manda el malware a los usuarios.
2.Los PC entran en el IRC o se usa otro medio de comunicación.
3.El Spammer le compra acceso al operador de la Botnet.
4.El Spammer manda instrucciones vía un servidor de IRC u otro canal a los PC infectados causando que éstos envíen Spam al los servidores de correo.



Las Botnets normalmente usan servicios gratuitos de DNS para IP's dinámicas para apuntar a un subdominio al cual el creador puede conectarse en caso que le cierren el servidor de IRC. En la mayoría de lso casos es suficiente avisar a estos proveedores para que cancelen su cuenta y así desarticular la Botnet

La estructura de servidores de la botnet tiene vulnerabilidades inherentes a su arquitectura. Como puede ser que se encuentre el servidor de IRC y el canal, se tiene acceso a la botnet completa, con lo cual al servidor de IRC lo soluciona cerrarando el canal

Otras veces los bots están configurados con un dominio, el cual puede cambiar fácilmente de IP para guiar al botnet al servidor.

El control de la botnet es normalmente a través del IRC, aunque en las nuevas versiones el control es mediante HTTP, por lo que la detección de estas redes es más compleja y las redes de empresas son más vulnerables porque el tráfico de IRC queda bloqueado.

Algunos botnet crean una red p2p descentralizada entre las víctimas que utilizan una comunicación cifrada y para que el dueño pueda controlarlas libremente. Como no tienen un servidor central la eliminación es más difícil.

Se usan para

- Enviar masivamente correos ‘spam’ con los que se pretende infectar otros equipos y servidores
- Ataques de denegación de servicio (DDoS), la red de equipos infectados, pueden saturar los servidores informáticos con millones de consultas y solicitudes con los que provocar un colapso y la caída del servicio.
- Robo de credenciales, todo el control de los datos que se encuentren en un equipo infectado pueden ser usados por el atacante
- Envío masivo de publicidad que aparece en la pantalla y que impide el correcto funcionamiento del navegador. En ocasiones, las botnets también llevan consigo la función de acceder a los banners publicitarios por lo que podrías estar accediendo a servicios de pago sin poder controlarlo.
- Robo de bitcoins. Las redes de botnets pueden alterar el funcionamiento de los sistemas de pago con Bitcoin ya que se integran en la cadena y pueden realizar operaciones con cargo a tus cuentas.
- Reclutamiento de otros equipos. Una vez que el dispositivo está infectado, entra a formar parte de una red de botnets cuyo objetivo es seguir expandiéndose reclutando nuevos ordenadores zombis.

- Ataques a dispositivos Internet. Se aprovechan de la falta de seguridad en los objetos conectados para crear una red de objetos y dispositivos zombi con los que controlar su funcionamiento y solicitudes.

Consejos para protegerse de las botnets

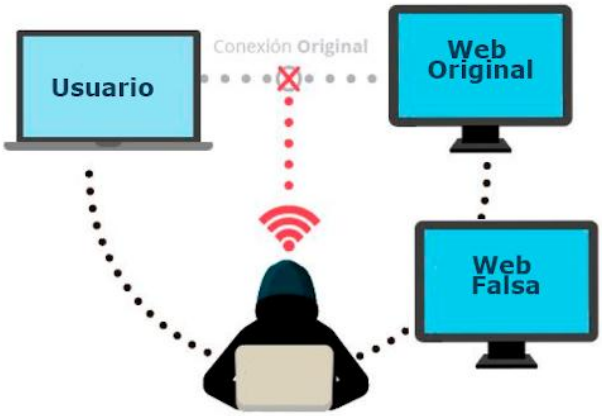
1. Cambiar regularmente las contraseñas de tus cuentas e incluso del acceso a tu router.
2. Evitar acceder a sitios con poca seguridad
3. Tener actualizado el sistema operativo y los antivirus
4. Evita realizar descargas P2P o vía Torrent
5. No acceder a enlaces que te remitan desde correo electrónico o a través de redes sociales sin tener la seguridad de la fiabilidad del remitente y la seguridad de que este te lo ha enviado.

Spoofing

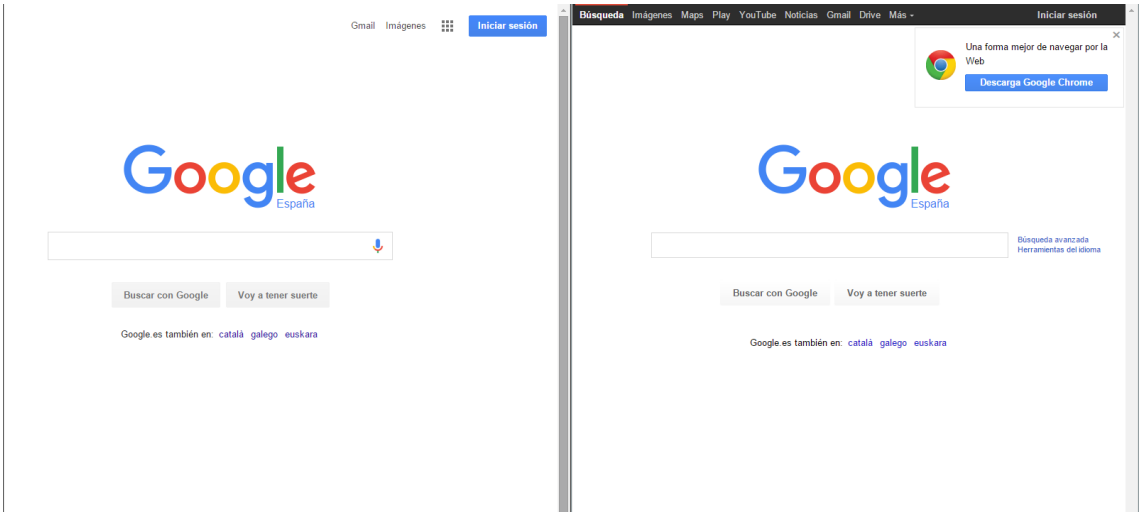
El spoofing es el uso de técnicas de suplantación de identidad . , Con el objetivo de obtener información privada o para conseguir acceder a páginas con una credencial falsa.
Ejemplos son el IP spoofing, el ARP spoofing, DNS spoofing, Web spoofing o email spoofing.
Tipos de spoofing

Cualquiera de las tecnologías de red actual es susceptible de ser utilizada para tal fin. Una clasificación según la fuente del ataque sería

- Suplantación de dirección IP
  Los ciberdelincuentes utilizan la dirección IP de la víctima para enviar paquetes de datos TCP/IP o UDP/IP. Con este sistema pueden atravesar protecciones Fireworks, al basearse en conceder acceso a una red a aquellas IP de confianza y rechazan el resto.
  Este tipo de suplantación es muy utilizada en los ataques de DDoS, porque la dirección suplantada es quien recibe la respuesta al envío de paquetes. Se puede hacer una DDoS enviando muchos paquetes desde una IP robada, que acabará colapsado con las respuestas recibidas o bien usurpando diferentes IP que envían paquetes para sobrecargar el servidor.

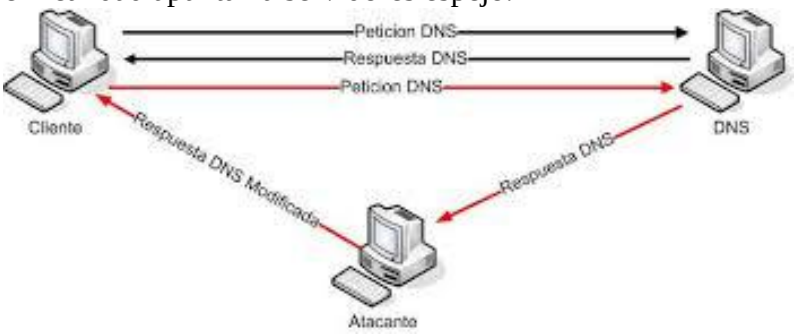


- E-mail spoofing
  El atacante utilizará la dirección de correo para solicitar información confidencial, para hacer spam o para enviar de forma masiva cadenas de bulos. De la misma manera, una cuenta de correos puede ser robada y utilizada para enviar cualquiera de sus correos malintencionados. Esta suplantación se denomina *phishing* y se usa sobre todo para hacerse pasar por entidades bancarias y solicitar de alguna manera las claves de acceso a la cuenta corriente.
- Suplantación web
  A diferencia del *phishing*, con este tipo de spoofing no se pretende imitar exactamente una web. En este caso, los atacantes hacen una intermediación entre el atacado y las páginas web que pretende visitar. De esta forma podrán monitorear su actividad, tener un registro de sus visitas, acceder a sus contraseñas y sus datos personales.



- Suplantación de DNS

  Consiste en acceder a los servidores de nombres de dominio de la víctima, y modificar sus direcciones IP para redirigirlas a servidores maliciosos. Además de ser otra forma de registrar los movimientos de la víctima, el mayor peligro es que puede burlar las conexiones cifradas ya que en realidad apuntan a servidores espejo.



- Suplantación de ARP

  El atacante ha logrado introducirse dentro de una red privaday podrá modificar las tablas ARP, asociando su MAC a la red de la víctima. De esta forma podrá interponerse entre los puntos de esa red controlando el flujo de datos.

Cómo detectar el spoofing

- La suplantación de correo electrónico es la forma más usada y detectable. El contenido de los e-mails nos debe hacer sospechar, porque intentará saber las contraseñas o datos personales. Además, suele ser de dudosa procedencia y su contenido es en esencia una estafa. Un síntoma claro de que una cuenta de correo ha sido intervenida y está siendo usada para enviar spam es cuando se reciben mensajes informando de que ciertos correos no pueden ser entregados. Los filtros antispam pueden colarse algunos correos indeseados que han utilizado una cuenta con buena reputación. Por tanto, hay que estar alerta y, en general, no seguir ningún tipo de enlace desde un correo.

  Por otro lado, se deben activar protocolos de verificación SPF, para evitar que envíen e-mails desde una cuenta suplantada. El dominio tendrá que autorizar al servidor de correo SMTP para enviar o, en su caso, para recibir un correo.
- Una de las maneras de comprobar el web spoofing es asegurarse de que la URL es correcta, y no se redirige a otras direcciones. Tambien podemos desactivar un JavaScript del navegador en los momentos en los que haya que exponer datos importantes. O contar con un software antivirus y un detector de malware, que puedan ofrecer protección en tiempo real
- Detectar otro tipo de suplantación como las de IP o DNS habría que fijarse en funcionamientos anómalos. Detectar si aumentan los tiempos de envío de paquetes, si notamos una navegación ralentizada o si las webs tienen un comportamiento diferente al usual. Una recomendación es configurar filtros en el router para controlar el acceso y el tráfico de paquete.

Ejemplos de casos de Soofing

- Uno de los casos más famosos de Spoofing es el de Pokémon GO, que permitía a los entrenadores cambiar su ubicación a través del GPS para así recoger Pokémon sin moverse de casa.

- Robarte la cuenta de WhatsApp Y a partir de tomar el control de tu WhatsApp, ya tendrían vía libre para infectar a todos tus contactos a través de un mensaje enviado por tu propia cuenta. El hacker de se hace con la cuenta de una persona que te tiene a ti como contacto, te engaña haciendo pensar que es uno de ellos, y logra registrar tu número en otro móvil para robarte tu cuenta de WhatsApp. Y ahora, a por todos los que tienes en tu listado. Por ello, la propia WhatsApp recomienda activar la Verificación en 2 pasos, que se hace así:

  1- Abre WhatsApp.
  2- Entra en Ajustes.
  3- Dentro de ajustes busca Cuenta
  4- Aquí veras entre las opciones una llamada Verificación en dos pasos
  5- Dale a Activar.

  Cuando habilites esta función, opcionalmente podrás introducir tu dirección de correo electrónico. Esta dirección de correo le permite a WhatsApp enviarte un enlace con el que podrás desactivar la verificación en dos pasos, en caso de que olvides tu PIN de seis dígitos, y así proteger tu cuenta. Ten en cuenta que WhatsApp no verifica esta dirección de correo electrónico para confirmar su validez, por lo que se recomienda que introduzcas una dirección de correo electrónico válida para que no se te niegue el acceso a tu cuenta si olvidas tu PIN.