Actividad 1: Investigación

Iker Ejido Martínez

Seguridad y Alta Disponibilidad

16/09/2024

Contenido

Resumen

El motivo del trabajo es el entendimiento y estudio de el vocabulario y la terminología de la Ciberseguridad, incluyendo en esto distintos tipos de ataques informáticos junto con sus definiciones, explicación y ejemplos.

El trabajo se desarrolla empezando con un glosario de los distintos términos a recordar de ciberseguridad, los cuales vienen definidos por mi propio conocimiento y por su definición técnica de acuerdo al **Glosario de términos de ciberseguridad: una guía de aproximación para el empresario** del Instituto Nacional de Ciberseguridad.

Después una pequeña aproximación a un caso personal de phishing.

Y por ultimo la clasificación y explicación de 4 conceptos relacionados a ataques informáticos: Phishing, Ransomware, WannaCry y Botnet.

Introducción

En la actualidad, la seguridad informática se enfrenta a desafíos cada vez más complejos, debido al creciente número de ciberataques y la sofisticación de las técnicas utilizadas por los delincuentes. Entre las amenazas más importantes destacan el **phishing**, el **ransomware** como **WannaCry**, los **ataques DDoS** y las **botnets**, que han demostrado tener un impacto significativo tanto en las infraestructuras tecnológicas como en la economía global.

El **phishing** es una técnica de ingeniería social que busca engañar a las personas para que revelen información sensible, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web fraudulentos. Por su parte, el **ransomware WannaCry** fue un ataque masivo que afectó a cientos de miles de organizaciones alrededor del mundo, encriptando archivos y exigiendo un rescate para restaurar el acceso, lo que puso de manifiesto la vulnerabilidad de sistemas críticos ante este tipo de ciber amenazas.

Los **ataques DDoS**, diseñados para interrumpir el funcionamiento de servicios en línea al inundarlos con tráfico masivo, son otra herramienta poderosa utilizada por los atacantes para generar caos o extorsionar a empresas. Estos ataques suelen apoyarse en **botnets**, redes de dispositivos comprometidos que, bajo el control de un atacante, realizan actividades maliciosas de forma coordinada y silenciosa, afectando no solo a empresas, sino también a usuarios comunes cuyos dispositivos son parte de estas redes.

Este trabajo explora en detalle estas amenazas cibernéticas, analizando su funcionamiento, objetivos y el impacto que tienen en el panorama actual de la seguridad informática. Además, se discuten ejemplos notables y las medidas de prevención y mitigación que se pueden tomar para protegerse de ellas. La investigación subraya la importancia de comprender estas técnicas para desarrollar estrategias efectivas de defensa y mantener la seguridad en un mundo cada vez más digital.

Glosario

1. **Puerta trasera:** error, fallo o punto débil de un programa o sistema mediante el cual un usuario o dispositivo puede acceder a nuestro sistema sin necesidad de credenciales y usuario.

   Definición Técnica:
   Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores, pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos. Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante. Por lo tanto, aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat.

   Sinónimo: Backdoor

2. **Spoofing**: tipo de ataque cibernético mediante el cual el atacante suplanta la identidad de una entidad (véase una página web o empresa), y mediante esta vulnera la privacidad de datos de los usuarios recopilándolos para su uso o venta.

   Definición Técnica:
   Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.
   De acuerdo a la tecnología utilizada se pueden diferenciar varios tipos de spoofing:

   - IP spoofing: consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
   - ARP spoofing: es la suplantación de identidad por falsificación de tabla ARP. ARP (Address Resolution Protocol) es un protocolo de nivel de red que relaciona una dirección MAC con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que se envíe a un usuario, será direccionado al atacante.
   - DNS spoofing: es una suplantación de identidad por nombre de dominio, la cual consiste en una relación falsa entre IP y nombre de dominio.
   - Web spoofing: con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos

facilitados, páginas que visita con frecuencia, perfil del usuario, etc. Los ataques de phishing son un tipo de Web spoofing.
- Mail spoofing: suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de spam.

3. Kerberos: protocolo de seguridad que opera por debajo del sistema operativo.

   Definición Técnica:
   Protocolo de autenticación de red creado por el Instituto Protocolo de autenticación de red creado por el Instituto Tecnológico de Massachusetts (MIT), diseñado para proveer una autenticación fuerte para las aplicaciones cliente/servidor mediante el uso de la criptografía de clave secreta.

4. Log: Registro de eventos de actividad de usuarios, procesos, aplicaciones y sistema, en el cual se puede ver el uso completo de la unidad usada, así como sus inicios de sesión, registros ejecución de aplicaciones y más.

   Definición Técnica:
   Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio/ salida de sesión, tiempo de actividad o conexiones, entre otros. Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización.

5. Antivirus: software (o aplicación), dedicada a la protección del sistema y sus datos, que previene la ejecución de malware y detecta si este se está ejecutando en segundo plano.

   Definición Técnica:
   Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo.

   Sinónimo: Antimalware

6. Análisis de vulnerabilidades: documento o glosario en el que se especifican los fallos y debilidades del sistema para la prevención de ataques por esos medios (fallos, errores o exploits)

   Definición Técnica:
   Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

7. Zombie: elemento informático con conexión red infectado por malware, normalmente parte de una red con más de estos dispositivos, denominada botnet.

   Definición Técnica: Es el nombre que se da a los ordenadores controlados de manera remota por un ciberdelincuente al haber sido infectados por un malware. El atacante remoto generalmente utiliza el ordenador zombie para realizar actividades ilícitas a través de la Red, como el envío de comunicaciones electrónicas no deseadas, o la propagación de otro malware.
   Son sistemas zombie los ordenadores que forman parte de una botnet, a los que el bot master utiliza para realizar acciones coordinadas como ataques de denegación de servicio.

   Sinónimo: Bot

8. Zero-day: vulnerabilidad de día 0, esto quiere decir aquellos errores o exploits encontrados en el momento presente para el cual no hay medidas de seguridad ya que aún no se han usado o identificado.

   Definición Técnica:
   Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.

9. Spyware: malware que actúa en segundo plano y se dedica a recopilar información del sistema mediante los logs o una aplicación. Esto sin alterar el sistema o modificar archivos.

   Definición Técnica:
   Es un malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.
   El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.

   Sinónimo: Programa espía

10. Ataque de fuerza bruta: ataque de ciberseguridad para acceder a un sistema mediante la repetición de posibles contraseñas hasta poder acceder al sistema y averiguar las credenciales, se demora más que otros tipos de ataques dependiendo de la longitud y complejidad de las contraseñas.

Definición Técnica:
Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, tardan mucho tiempo en encontrar la combinación correcta (hablamos en ocasiones de miles años), por esta razón, la fuerza bruta suele combinarse con un ataque de diccionario.

11. Exploit: línea de comandos que al ser ejecutada provoca un fallo o error en el sistema produciendo acciones no deseadas y vulnerando el sistema.

    Definición Técnica:
    Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.
    Mediante la ejecución de exploit se suele perseguir:
    - el acceso a un sistema de forma ilegítima
    - obtención de permisos de administración en un sistema ya accedido
    - un ataque de denegación de servicio a un sistema

12. Fichero ejecutable: archivo que inicia o ejecuta un programa, ejecutando instrucciones (línea de comandos), bien para su instalación o ejecución.

    Definición Técnica:
    Archivo diseñado para inicializar un programa (instalación, ejecución, etc.) debido a que en su interior están las instrucciones precisas para poder ejecutar un software determinado.

¿Has recibido alguna vez un intento de phishing mediante correo electrónico de tipo spam? ¿por SMS?

Si, he recibido intentos de phishing mediante el correo electrónico, SMS, WhatsApp y en especial por Wallapop, donde estafadores, tratan de extraer tu información bancaria con la excusa de comprarte cualquier producto que hayas publicado.

Investiga y Explica

• Phishing

El **phishing** es una técnica de **ciberataque** diseñada para engañar a las personas y hacer que revelen información confidencial, como nombres de usuario, contraseñas, números de tarjetas de crédito o datos personales. Los atacantes suelen hacerse pasar por entidades legítimas o personas de confianza, como bancos, compañías de tecnología, o incluso contactos personales, utilizando distintos métodos para ganarse la confianza de la víctima y obtener la información que desean.

¿Cómo funciona el phishing?

El objetivo principal del phishing es que la víctima, convencida de estar interactuando con una entidad legítima, entregue voluntariamente información sensible. Los ataques de phishing suelen involucrar:

1. **Correos electrónicos falsificados** o mensajes diseñados para parecer auténticos.
2. **Enlaces o sitios web fraudulentos** que imitan a los legítimos.
3. **Solicitudes de información sensible** que parecen razonables o necesarias.
4. **Engaños o urgencias emocionales** para manipular a la víctima y hacer que actúe de forma impulsiva.

Principales tipos de phishing

El phishing se ha diversificado en diferentes formas según el vector de ataque, la técnica utilizada y los objetivos específicos. Aquí te presento los tipos más comunes:

1. Phishing tradicional (Email phishing)

Es el tipo más común de phishing y generalmente se lleva a cabo mediante **correos electrónicos** que aparentan ser de una empresa legítima, como bancos, redes sociales, servicios de correo o comercios electrónicos. Estos correos suelen incluir:

- Un mensaje urgente (por ejemplo, problemas con tu cuenta).
- Un enlace que redirige a una página falsa que parece real.
- Solicitud de credenciales o datos personales.

Ejemplo: Un correo que parece ser de tu banco, diciéndote que tu cuenta ha sido comprometida, y te pide que entres a un enlace para "verificar" tus datos.

2. Spear phishing

A diferencia del phishing tradicional, que es masivo y genérico, el **spear phishing** es más **personalizado y dirigido**. El atacante investiga a la víctima y crea un mensaje altamente específico, a menudo utilizando datos personales o profesionales que hacen que el engaño sea más creíble.

Ejemplo: Un correo que parece provenir de un compañero de trabajo o de tu jefe, solicitándote que descargues un archivo o transfieras dinero a una cuenta.

3. Whaling (Phishing dirigido a altos cargos)

El **whaling** es una variante del spear phishing, pero se centra en objetivos de **alto perfil** dentro de una organización, como ejecutivos o directores. Los atacantes intentan engañar a estas personas para obtener información valiosa o dinero.

Ejemplo: Un CEO recibe un correo que parece ser de un proveedor importante solicitando el pago urgente de una factura.

4. Vishing (Phishing por voz)

En el **vishing**, los atacantes utilizan llamadas telefónicas o mensajes de voz para engañar a la víctima. A menudo, fingen ser representantes de empresas, entidades gubernamentales o bancos y tratan de obtener información sensible a través de una conversación.

Ejemplo: Una llamada telefónica que parece provenir de tu banco, donde te dicen que han notado actividad sospechosa en tu cuenta y te piden información personal para verificarla.

5. Smishing (Phishing por SMS)

El **smishing** es una forma de phishing que se realiza a través de **mensajes SMS**. Los atacantes envían mensajes de texto que incluyen enlaces o solicitudes de información confidencial.

Ejemplo: Un SMS que parece provenir de una empresa de paquetería, diciendo que tienes un paquete en espera y necesitas ingresar tus datos en un enlace para recogerlo.

6. Pharming

El **pharming** es un tipo de ataque en el que los atacantes **redirigen el tráfico web** de un sitio legítimo a uno fraudulento sin que el usuario lo sepa. Esto puede hacerse manipulando los **servidores DNS** o infectando la computadora del usuario con malware.

Ejemplo: Intentas acceder a la página web de tu banco, pero el navegador te redirige a un sitio falso que parece idéntico. Sin saberlo, introduces tus credenciales en la página falsa.

7. Clone phishing

En este tipo de phishing, los atacantes crean una **copia exacta de un correo electrónico legítimo** que la víctima haya recibido previamente, pero modifican enlaces o archivos adjuntos para incluir contenido malicioso. Dado que la víctima reconoce el formato y el remitente del correo, es más probable que caiga en el engaño.

Ejemplo: Recibes un correo que parece ser una actualización de un pedido en línea que hiciste, pero en lugar del enlace original de seguimiento, te redirige a un sitio web falso.

8. Phishing en redes sociales

Los ataques de phishing también ocurren a través de **plataformas de redes sociales**. Los atacantes pueden hacerse pasar por amigos, familiares o contactos profesionales de la víctima para solicitar información personal o redirigir a enlaces fraudulentos.

Ejemplo: Un mensaje de un amigo en Facebook que parece estar en apuros y te pide que transfieras dinero o hagas clic en un enlace.

9. Business Email Compromise (BEC)

En el **BEC**, los atacantes se infiltran en el sistema de correo electrónico de una empresa o se hacen pasar por un ejecutivo o proveedor para engañar a los empleados para que realicen transferencias de dinero o revelen información confidencial.

Ejemplo: Un empleado de finanzas recibe un correo electrónico que parece ser del director financiero, solicitando una transferencia urgente de fondos a una cuenta de terceros.

10. Phishing en motores de búsqueda

Este tipo de phishing ocurre cuando los atacantes crean **sitios web falsos** que aparecen en los resultados de búsqueda de los motores de búsqueda. Las víctimas pueden ingresar a estos sitios pensando que son legítimos y terminar entregando información sensible.

Ejemplo: Al buscar en Google cómo renovar tu pasaporte, haces clic en un sitio web falso que se parece al oficial y terminas ingresando tus datos personales.

Tácticas comunes en phishing

Los atacantes de phishing utilizan ciertas tácticas psicológicas para manipular a las víctimas:

1. **Urgencia**: Correos que indican que algo requiere acción inmediata (por ejemplo, "Tu cuenta será suspendida si no actúas en las próximas 24 horas").
2. **Miedo**: Amenazas de pérdida de acceso, multas o cargos si no actúas.
3. **Confianza**: Mensajes que imitan a fuentes confiables como bancos o instituciones gubernamentales.
4. **Curiosidad**: Correos intrigantes que invitan a la víctima a hacer clic en enlaces (por ejemplo, "Has ganado un premio").

Prevención del phishing

Para protegerte contra el phishing, sigue estos consejos:

- **No hagas clic en enlaces sospechosos**: Siempre verifica la URL manualmente.
- **Desconfía de solicitudes urgentes de información**.

- **Habilita autenticación de dos factores** en tus cuentas.
- **Verifica la autenticidad del remitente** antes de actuar.
- **Mantén tu software actualizado** para protegerte contra malware.

• WannaCry

¿Qué es WannaCry?

WannaCry es un tipo de **ransomware**: un software malicioso que cifra (bloquea) los archivos del sistema infectado y solicita un **rescate** en **bitcoins** para liberar los datos. Una vez que el sistema está infectado, los archivos quedan inaccesibles, y la víctima ve una pantalla que le pide pagar un rescate en un plazo determinado para obtener una clave de desencriptación. Si el rescate no es pagado a tiempo, los archivos pueden perderse permanentemente.

El ataque de WannaCry en 2017 fue tan efectivo debido a su capacidad de **propagación autónoma** a través de una vulnerabilidad en los sistemas Windows, lo que permitió que el malware se extendiera como un gusano sin intervención humana.

¿Cómo funciona WannaCry?

1. **Infección inicial**: El malware infectaba a la máquina aprovechando la vulnerabilidad EternalBlue para ejecutar código malicioso a través del protocolo SMB.
2. **Cifrado de archivos**: Una vez dentro del sistema, WannaCry **cifraba** una gran cantidad de tipos de archivos importantes (documentos, imágenes, videos, bases de datos, etc.) utilizando un algoritmo de cifrado fuerte como **AES** o **RSA**, lo que hacía prácticamente imposible acceder a ellos sin una clave de descifrado.
3. **Mensaje de rescate**: El malware mostraba un mensaje de rescate, solicitando a las víctimas pagar una cantidad en **bitcoins** (generalmente alrededor de $300 a $600) a cambio de la clave de descifrado. El mensaje también incluía una advertencia de que el monto del rescate se duplicaría si no se pagaba en un plazo determinado, y que los archivos podrían ser eliminados permanentemente si el pago no se realizaba.
4. **Propagación**: WannaCry se diferenciaba de otros tipos de ransomware porque tenía la capacidad de **propagarse automáticamente** a otras computadoras en la red, lo que lo hacía extremadamente peligroso en redes empresariales. Utilizaba el exploit EternalBlue para infectar rápidamente

otros sistemas vulnerables sin necesidad de intervención humana, comportándose como un gusano.

Factores que contribuyeron a la propagación de WannaCry

1. **Sistemas no actualizados**: Muchos sistemas en el mundo, particularmente en entornos empresariales y gubernamentales, no habían aplicado el parche de seguridad emitido por Microsoft. Esto se debió a diversos factores, incluyendo:
    - Falta de conocimiento o gestión de parches.
    - Uso de versiones antiguas y no soportadas de Windows (como Windows XP).
    - Infraestructuras críticas con políticas de actualización lenta.
2. **Redes empresariales interconectadas**: WannaCry se aprovechó de redes empresariales mal configuradas donde los sistemas compartían conexiones directas entre ellos, lo que facilitó su expansión.
3. **Uso de SMB**: El protocolo **SMB** estaba activado en muchas organizaciones y entornos, lo que permitió que WannaCry se propagara más fácilmente entre los equipos.

Impacto global de WannaCry

WannaCry afectó a **más de 230,000 computadoras en 150 países** en cuestión de días, lo que provocó interrupciones masivas en empresas, hospitales, infraestructuras críticas y gobiernos.

Prevención contra ransomware como WannaCry

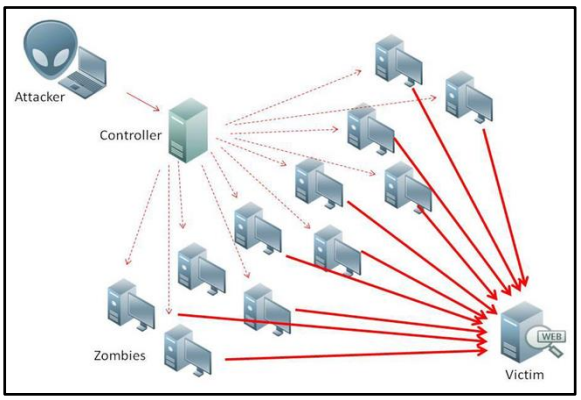
Para protegerse contra ransomware como WannaCry, es esencial seguir varias prácticas de ciberseguridad:

1. **Actualizaciones y parches**: Mantener el sistema operativo y el software actualizado con los últimos parches de seguridad es la mejor defensa contra ataques que aprovechan vulnerabilidades conocidas.
2. **Copias de seguridad regulares**: Tener **copias de seguridad frecuentes** y almacenarlas fuera de línea o en lugares seguros es fundamental. Si tus archivos se ven comprometidos, puedes restaurarlos desde la copia de seguridad sin pagar el rescate.
3. **Segmentación de redes**: Dividir la red en segmentos más pequeños limita la propagación de malware en caso de una infección.
4. **Desactivar SMB si no es necesario**: Si no es esencial para la operación de la empresa, desactivar el protocolo **SMB** puede prevenir futuras explotaciones de este tipo.
5. **Antivirus y firewalls**: Usar **software antivirus actualizado** y configurar adecuadamente **firewalls** para bloquear el tráfico no deseado puede detener el ransomware antes de que infecte el sistema.
6. **Concienciación de los empleados**: Capacitar a los empleados sobre las tácticas comunes de ataque, como los correos electrónicos de phishing,

ayuda a reducir el riesgo de que los usuarios hagan clic en enlaces maliciosos o descarguen archivos peligrosos.

• DDoS

Un **ataque DDoS** (**Ataque Distribuido de Denegación de Servicio**) es un tipo de ataque cibernético en el que múltiples sistemas distribuidos (como computadoras, servidores o dispositivos conectados) son utilizados para **sobrecargar un servidor, servicio o red**, de modo que quede **inhabilitado para responder a solicitudes legítimas**. El objetivo de este ataque es interrumpir el servicio de un sitio web, aplicación o infraestructura, haciendo que no esté disponible para los usuarios.



¿Cómo funciona un ataque DDoS?

El ataque DDoS se basa en enviar una **gran cantidad de tráfico malicioso** o solicitudes simultáneas a la víctima (generalmente un servidor web o servicio en línea) desde múltiples puntos, con el fin de saturar sus recursos y provocar que deje de funcionar. El término "distribuido" hace referencia a que el ataque proviene de **múltiples ubicaciones** al mismo tiempo, generalmente aprovechando una red de **dispositivos infectados**, conocidos como una **botnet**.

Los ataques DDoS suelen utilizar varios dispositivos comprometidos, como:

- Computadoras.
- Servidores.
- **IoT** (Internet de las cosas), como cámaras de seguridad, routers, impresoras inteligentes, etc.

Estos dispositivos, sin el conocimiento de sus propietarios, son infectados con malware que los convierte en **bots** que, al ser controlados de forma remota por los atacantes, envían solicitudes simultáneas al objetivo.

Objetivos de un ataque DDoS

Los ataques DDoS tienen diferentes objetivos, dependiendo del atacante:

1. **Interrupción del servicio**: El objetivo más común es **interrumpir el servicio** de una empresa, gobierno o individuo, afectando su operatividad y causando pérdidas económicas o de reputación.
2. **Daño a la competencia**: Los competidores maliciosos podrían utilizar DDoS para hacer que un sitio o servicio quede fuera de línea, afectando a sus competidores.
3. **Extorsión**: Los atacantes pueden exigir un **pago de rescate** a cambio de detener el ataque.

4. **Activismo político**: Algunos ataques DDoS son llevados a cabo por grupos de activistas que quieren **protestar contra gobiernos o corporaciones**.
5. **Demostración de poder**: Hackers o grupos de cibercriminales a veces realizan ataques DDoS simplemente para **mostrar su capacidad técnica** o como un acto de vandalismo.

Tipos de ataques DDoS

Existen varios tipos de ataques DDoS, clasificados según la forma en que afectan los recursos del sistema:

1. Ataques de volumen

Estos ataques buscan saturar el ancho de banda de la víctima inundando la red con un gran número de paquetes o solicitudes.

- **Flood de UDP (User Datagram Protocol)**: Inunda el servidor con paquetes UDP, lo que provoca que el servidor tenga que procesar cada paquete, aunque no haya datos útiles en ellos. Esto agota los recursos de la red.

Ejemplo: Enviar millones de paquetes UDP vacíos a un servidor web para saturar su capacidad de respuesta.

- **Flood de ICMP (Ping Flood)**: Se envían grandes cantidades de mensajes ICMP (ping) al servidor con el objetivo de consumir los recursos del sistema.

Ejemplo: Enviar pings en masa a un servidor para saturar su capacidad de procesamiento.

- **DNS Amplification**: Un tipo de ataque DDoS que utiliza servidores DNS para amplificar la cantidad de tráfico enviado a la víctima. Se envían solicitudes a servidores DNS con la dirección IP de la víctima falsificada, de modo que el servidor envíe respuestas mucho más grandes a la víctima.

Ejemplo: El atacante envía una pequeña solicitud de DNS, pero la respuesta es varias veces mayor, lo que sobrecarga al objetivo.

2. Ataques de protocolo

Este tipo de ataques agotan los recursos del servidor objetivo o los equipos de red intermediarios, como routers y firewalls, al explotar fallos o debilidades en los protocolos de red.

- **SYN Flood**: En este ataque, el atacante envía múltiples solicitudes **SYN** (parte del protocolo TCP) al servidor, pero nunca completa el "handshake" o proceso de conexión TCP. Esto provoca que el servidor mantenga abiertas muchas conexiones incompletas, agotando sus recursos.

Ejemplo: Enviar miles de solicitudes de conexión TCP sin completar el proceso, haciendo que el servidor se quede sin recursos para manejar nuevas solicitudes.

- **ACK Flood**: Es similar al SYN Flood, pero en este caso, el atacante envía un flujo masivo de paquetes **ACK** (paquetes de confirmación), abrumando al servidor y consumiendo su capacidad de procesamiento.
- **Fragmentación de IP**: Se envían paquetes de datos fragmentados que deben ser reensamblados por el servidor objetivo. El servidor se ve

abrumado al intentar recomponer los paquetes, lo que consume sus recursos.

3. Ataques a la capa de aplicación (L7)

Estos ataques están dirigidos a las aplicaciones o servicios que corren sobre el servidor, como **servidores web, bases de datos o servicios de DNS**. Estos ataques suelen ser más complejos y difíciles de detectar porque parecen tráfico legítimo.

- **HTTP Flood**: El atacante envía múltiples solicitudes HTTP al servidor web objetivo, saturando sus recursos. A menudo, se envían solicitudes GET o POST que parecen legítimas, lo que hace que el servidor tenga que procesarlas todas.

Ejemplo: Enviar millones de solicitudes para cargar una página específica de un sitio web, lo que agota la capacidad del servidor de responder a usuarios reales.

- **Slowloris**: Este ataque envía solicitudes HTTP muy lentas al servidor web, manteniendo abiertas muchas conexiones sin completarlas, lo que agota los recursos de conexión del servidor.

Ejemplo: Enviar solicitudes HTTP a un servidor, pero de manera tan lenta que el servidor sigue esperando a que se complete la solicitud, hasta que queda saturado.

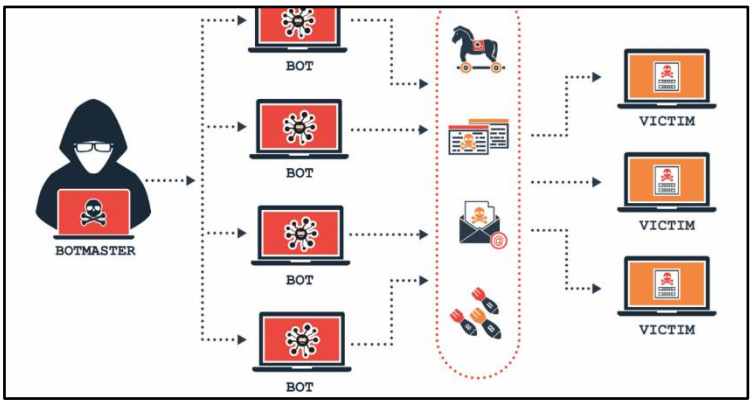
Consecuencias de un ataque DDoS

- **Pérdidas económicas**: Las empresas pueden perder millones de dólares debido a la interrupción de sus servicios. El tiempo de inactividad de un sitio web o servicio crítico puede afectar gravemente las operaciones diarias y las ventas.
- **Daño a la reputación**: Las empresas pueden sufrir **daños a su imagen** y perder la confianza de sus clientes si no pueden garantizar la disponibilidad de sus servicios.
- **Costos de recuperación**: Restaurar los servicios, mitigar futuros ataques y revisar las infraestructuras de seguridad puede ser costoso.
- **Impacto social y político**: Los ataques a infraestructuras gubernamentales o servicios públicos pueden causar caos, como ocurrió en Estonia o en ataques a sistemas de votación.

Prevención y mitigación de ataques DDoS

1. **Ancho de banda redundante**: Tener una infraestructura con ancho de banda suficiente puede ayudar a mitigar los ataques de volumen, ya que puede absorber parte del tráfico malicioso.
2. **CDN (Content Delivery Networks)**: Las redes de distribución de contenido pueden ayudar a distribuir el tráfico en múltiples servidores alrededor del mundo, lo que reduce la carga sobre un solo servidor.
3. **Sistemas de mitigación DDoS**: Existen servicios especializados en **mitigar ataques DDoS**, como Cloudflare o AWS Shield, que filtran el tráfico malicioso antes.

- Botnet



Una **botnet** es una red de dispositivos informáticos que han sido **infectados con malware** y son controlados de manera remota por un atacante (generalmente llamado **botmaster**) sin el conocimiento de sus propietarios. Estos dispositivos comprometidos, también llamados **bots** o **zombies**, son utilizados para llevar a cabo diversas actividades maliciosas, como **ataques DDoS**, envío masivo de **spam**, robo de datos, minería de criptomonedas o espionaje. Una botnet puede incluir miles, cientos de miles o incluso millones de dispositivos.

¿Cómo funcionan las botnets?

1. **Infección**: Para que un dispositivo sea parte de una botnet, primero debe ser **infectado con malware**. Esto puede ocurrir a través de:
    - **Phishing**: Correos electrónicos maliciosos con enlaces o archivos adjuntos infectados.
    - **Exploits**: Vulnerabilidades en el software o sistema operativo que permiten la instalación de malware.
    - **Descargas de software no seguro**: Al instalar programas o archivos de fuentes no confiables que contienen el malware.
    - **Dispositivos IoT mal configurados**: Muchos dispositivos conectados a Internet, como cámaras de seguridad, routers o impresoras inteligentes, son vulnerables debido a configuraciones de seguridad débiles.
2. **Conexión al servidor de control**: Una vez que el dispositivo ha sido infectado, se conecta a un **servidor de comando y control (C&C)**, desde el cual el atacante puede enviar instrucciones a todos los dispositivos comprometidos de la botnet.
3. **Acciones maliciosas**: El botmaster envía órdenes a los bots para ejecutar acciones maliciosas de manera coordinada. Dado que los dispositivos comprometidos pertenecen a diferentes usuarios y están dispersos por todo el mundo, los ataques pueden ser masivos y difíciles de rastrear.
4. **Propagación**: Muchas botnets están diseñadas para **auto-propagarse**, infectando otros dispositivos vulnerables en la red y aumentando el tamaño de la botnet.

Estructura de una botnet

Existen dos tipos principales de arquitectura en las botnets:

1. **Botnets centralizadas**: En este modelo, todos los bots se conectan a un **servidor central de comando y control (C&C)**, desde el cual el botmaster envía las instrucciones. Sin embargo, este tipo de botnet es más vulnerable, ya que, si se localiza y desactiva el servidor C&C, la botnet puede quedar inutilizada.
2. **Botnets descentralizadas (peer-to-peer)**: En este tipo de botnet, no hay un servidor central, sino que los bots se comunican entre sí para coordinar los ataques o las acciones maliciosas. Este modelo es mucho más difícil de desmantelar, ya que no depende de un único punto de control.

Ejemplos notables de botnets

1. Mirai

La botnet **Mirai** es una de las más famosas en la historia. Fue descubierta en 2016 y estaba compuesta principalmente por **dispositivos IoT** como cámaras de seguridad y routers mal configurados. Mirai se utilizó en varios ataques DDoS masivos, incluyendo el ataque contra **Dyn**, un proveedor de servicios DNS, que provocó la caída de servicios populares como **Twitter, Netflix, Amazon y GitHub**. Mirai aprovechó dispositivos IoT vulnerables utilizando contraseñas predeterminadas.

Prevención y mitigación de botnets

1. **Actualizar y parchear software**: Mantener los sistemas operativos, aplicaciones y firmware actualizados con los últimos parches de seguridad es crucial para evitar que los atacantes exploten vulnerabilidades conocidas.
2. **Seguridad en dispositivos IoT**: Cambiar las contraseñas predeterminadas y asegurar los dispositivos IoT es esencial, ya que estos dispositivos son objetivos fáciles para los botmasters.
3. **Software antivirus y antimalware**: Utilizar soluciones de seguridad confiables y mantenerlas actualizadas ayuda a detectar y eliminar malware que podría convertir un dispositivo en parte de una botnet.
4. **Detección y bloqueo de tráfico anómalo**: Implementar herramientas de monitoreo de red que detecten comportamientos inusuales puede ayudar a identificar y bloquear la actividad de botnets.