Ataques de denegación de servicio distribuido, Cómo evitarlos y cómo enfrentarlos

Mauricio Pacheco Manotas.
Universidad Piloto de Colombia – Especialización En seguridad informática
Bogotá D.C., Colombia
mauricio-pacheco@upc.edu.co

***Resumen*— En el presente escrito abordaremos los ataques de denegación de servicios, como se dan, y que podemos hacer para evitarlos, ayudando al lector a conocerlos y entender su funcionamiento, así como a la manera de ejecutar controles que permitan mitigar dichos ataques.**

Antes que nada, es importante mencionar que estos ataques son mucho más comunes de lo que normalmente se cree y sus víctimas más frecuentes son los sectores médicos, educativos, gubernamentales y financieros, este último sobre el cual nos centraremos en este escrito, lo que buscan dichos ataques es Causar un impacto económico o social a la organización o simplemente crear una cortina de humo para distraer al equipo de seguridad mientras se lleva a cabo un ataque más sofisticado.

En nuestro caso como entidad que se mueve en el sector económico hemos sido víctimas de intentos de ataques de este tipo tanto a nuestra plataforma web como a nuestros servicios de telefonía, los cuales se han hecho muy frecuentes y por lo cual se tiene conocimiento suficiente al respecto como para exponer técnicas de ataque y mitigación al respecto.

***Abstract*-- In this paper we will address denial of service attacks, how they occur, and what we can do to avoid them, helping the reader to learn about them and understand how they work, as well as how to execute controls that can mitigate such attacks.**

First of all, it is important to mention that these attacks are much more common than is normally believed and their most frequent victims are the medical, educational, governmental and financial sectors, the latter on which we will focus in this writing, what said said attacks is to Cause an economic or social impact to the organization or simply create a smoke screen to distract the security team while a more sophisticated attack is carried out.

In our case, as an entity that operates in the economic sector, we have been victims of attempted attacks of this type both on our web platform and on our telephone services, which have become very frequent and for which there is sufficient knowledge regarding to expose attack and mitigation techniques in this regard.

I. Introducción

El conocer cómo se originan, ejecutan, y multiplican estos ataques, así como los medios que pueden servir como origen de los mismos, permite tanto a personal de área de tecnología como a las organizaciones a estar prevenidos y ser precavidos en cuanto a que se expone y como se protege en la red. No es un secreto que actualmente y con el avance de la tecnología los ataques de todo tipo han aumentado de una manera abismal, bien sea por temas políticos, terroristas o a manera de protesta.

Antes de adentrarnos más en el tema de los ataques distribuidos de denegación de servicio, debemos comprender que no es solo una práctica que ejecuta uno o varios hackers, sino que también van ligados al grado de cuidado y conciencia sobre seguridad que tengan los usuarios en las organizaciones y en común en la vida, ya que generalmente son usados sin saberlo para realizar ataques como el que estamos tratando en este documento, el phishing es una puerta de entrada para ser parte de este ejército de atacantes, y es bien sabido que aún hoy con toda la información y advertencia acerca de esto, existen muchas personas que por inocencia, desconocimiento o simplemente por negligencia se dejan llevar por lo llamativo y caen fácilmente, dando así una ayuda a los atacantes a formar sus ejércitos o ser parte de botnets, con los que ejecutaran sus delitos.

Botnet. Es una red de equipos infectados que se pueden controlar a distancia y a los que se puede obligar a enviar spam, propagar malware o llevar a cabo un ataque DDoS, y todo sin la autorización del dueño del dispositivo. Estas no son un es un virus en sí mismo, sino una es una colección de dispositivos automáticos conectados. Los atacantes suelen utilizar sus botnets para lanzar ataques, detectar contraseñas confidenciales o distribuir ransomware. [1]

II. Que es un ataque DDoS

Para pensar en cómo protegernos primero debemos comprender a que nos enfrentamos, estos tienen como objetivo inhabilitar un servicio, servidor o sistema completo con el fin de bloquear el fin al que están destinados para los usuarios, y que son generados desde distintas maquinas o dispositivos coordinados que generan una gran cantidad de peticiones al objetivo.

La abreviatura DDoS significa Distributed Denial Of Service. Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a los recursos de red, como la infraestructura sobre la que se basa el sitio web de una empresa. El ataque DDoS enviará gran cantidad de solicitudes al recurso web atacado con el fin de superar la capacidad del sitio web para gestionar tantas solicitudes y evitar así que este funcione correctamente. [2]

La manera más común de realizar un ataque ddos es a través de una botnet, siendo este el ciber ataque más usual y eficaz por su facilidad y sencillez tecnológica. Los ataques DDoS son difíciles de detectar ya que a menudo utilizan conexiones normales e imitan el tráfico autorizado normal. Como resultado es altamente efectivo ya que normalmente los servidores objetivos confían por error en el tráfico y, por tanto, facilitan los ataques ejecutando la solicitud que en última instancia los inunda.

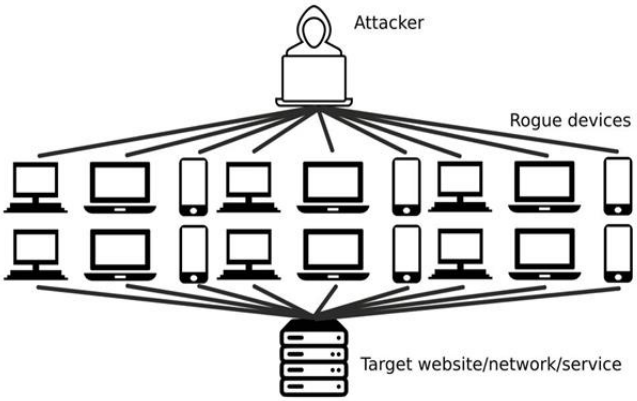

Figura 1. Ataque DDoS. Recuperado de https://www.bitdefenderperu.com/blog/que-son-los-ataques-ddos-y-por-que-son-tan-usados-en-las-ciberguerras/

Por que alguien ejecutaría un ataque DDos.
Existen innumerables razones para realizar estos ataques que como se ha mencionado anteriormente puede tener tintes políticos o terroristas, pero además estos pueden ir desde espionaje hasta guerra cibernética. Dentro de estos motivos más comunes se incluyen:

- Hacktivismo.
- Obtener una ventaja competitiva.
- Obtener ganancias financieras a través de extorsión, robo, etc.
- Causar daño a una marca/reputación.
- Lanzar un ataque de ransomware.
- Llevar a cabo una guerra cibernética.

Es importante saber que los ataques DDoS son ilegales en la mayoría de los países que tienen leyes de ciberdelincuencia. En Estados Unidos existe la Ley de Fraude y Abuso Informático (CFAA), mientras que en el Reino Unido, la Ley de Uso Indebido de Ordenadores cubre los ataques DDoS, así como una amplia gama de otros ciberdelitos.

III. Clasificación de ataques DDos

Estos tipos de ataque podemos clasificarlo en tipos según el nivel al que se realice.

A. Ataques a la capa de infraestructura

Los ataques a las capas 3 y 4, en general, están definidos como ataques a las capas de infraestructura. Y de paso sea dicho, son los ataques DDoS más comunes e incluyen técnicas como inundaciones sincronizadas (SYN) y otros ataques como inundaciones de paquetes de datagramas de usuario (UDP). Estos ataques, en general, tienen gran volumen y apuntan a sobrecargar la capacidad del servidor de la red o de la aplicación. Pero, afortunadamente, son un tipo de ataque que contiene firmas claras y son fáciles de detectar.

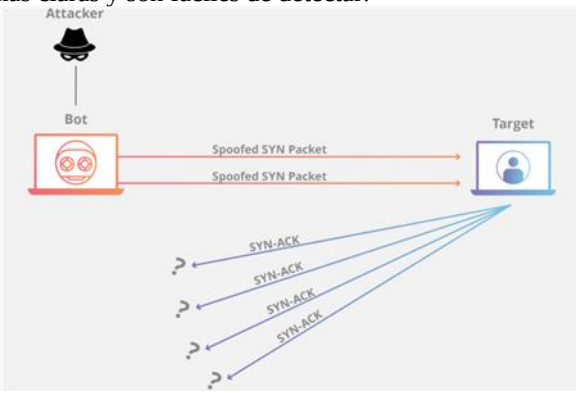

Figura 2. Ejemplo de ataque de protocolo. Recuperado de https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

B. Ataques a la capa de aplicación

Los ataques a las capas 6 y 7 se clasifican como ataques a las capas de aplicación. Mientras que estos ataques son menos comunes, tienden a ser más sofisticados. Estos ataques son, en general, más pequeños en volumen en comparación con los ataques a las capas de infraestructura, pero tienden a focalizarse en partes específicas y costosas de la aplicación e impiden que esté disponible a los usuarios reales. Por ejemplo, una inundación de requerimientos de HTTP a una página de inicio de sesión o a una búsqueda costosa de una API o incluso inundaciones Wordpress XML-RPC.

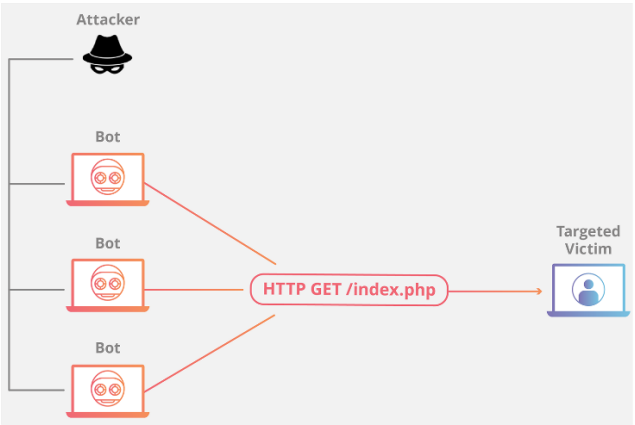

Figura 3. Ejemplo de ataque a la capa de aplicación. Recuperado de https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

IV. Técnicas de ataque

A. Inundación SYN

Esta técnica usa paquetes regulares y paquetes grandes, simultáneamente. Los paquetes regulares se encargan de agotar los recursos del servidor, mientras que los grandes saturan la red; es muy utilizada en los ataques DDoS.

B. Cortina de humo

Como su nombre lo dice este tipo de ataque se usa para desviar la atención de otro ataque que tiene como objetivo una

capa distinta, siendo ejecutado en otro vector de la red para ocasionar conflictos en reglas de seguridad automatizadas.

C. Ataque Multivectorial

Esta técnica es usada para realizar exploración de vulnerabilidades, es una acción de prueba y error, se realiza reconocimiento previo y da pistas a la construcción de futuros ataques; con este no se pretende solamente sacar el sitio del aire, sino que además buscan derribar el desempeño de los servicios, a través de una sobrecarga de los recursos existentes. En el ataque multi vector mas grande registrado se ha detectado el uso de 21 vectores distintos.

D. Ampliación y reflexión de tráfico

Esta técnica se volvió de las más usadas para realizar ataques a gran escala, se aprovecha de vulnerabilidades encontradas en protocolos ntp, no solo para reflexión sino también para propagación de ataques por medio de servidores reales que responden a esos protocolos, de esta manera no es necesario infectar miles de máquinas para ejecutar los ataques. También los ataques de reflexión usan tanto protocolos básicos de internet como los recursos disponibles de aplicaciones web para saturar un objetivo con datos no deseados.

E. Ataques volumétricos

Se usan maquinas zombies, infectadas generalmente a través de phishing; que posteriormente son usadas en ataques coordinados por hackers sin que el dueño del dispositivo lo sepa. El objetivo es saturar el ancho de banda del recurso objetivo.

F. Ataques a la capa 7

En este tipo de ataques múltiples comandos son enviados con el objetivo de disminuir la capacidad de procesamiento de los servidores, inhabilitando el uso de algunas aplicaciones. Son los servicios financieros y comercio electrónico los blancos más comunes de este vector de ataque. Dentro de estos tenemos Inundación HTTP, HTTP pipelining y Low-and-slow entre muchos otros.

G. Ataques de fragmentación

Esta técnica genera negación de los servicios mediante la saturación de la red, y es que intencionalmente fragmenta los paquetes, que no pueden ser montados en el destino, originando así la saturación del servicio. Ya cuando finalmente el paquete es cargado se impide el funcionamiento del host, otra manera de hacerlo es que se envían fragmentos incompletos o muy pequeños del paquete para obtener el mismo efecto.

V. Ataques DDoS Conocidos A nivel mundial

Desde que se conocieron este tipo de ataques los cuales han existido durante ya más de 20 años han sido muchos y se han efectuado diversos tipos de técnicas, que continúan afectando a las empresas siendo algo que nos permite conocer que sin importar cuan grande y cuanta seguridad se tenga nadie está exento de sufrir un intento de ataque.

DynDNS. Este tuvo lugar en octubre de 2016, uno de los servidores DNS más utilizados en Internet, sufrió un ataque dirigido que involucró a millones de direcciones IP relacionadas con la botnet Mirai. La mayoría de estas direcciones IP provenían de dispositivos IoT que no contaban con la suficiente protección. Como resultado de este ataque masivo, servicios como Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast y la red de PlayStation, entre muchos otros, se quedaron sin conexión ante la caída del servicio que redirigía a los usuarios hasta sus servidores.
Poco más de tres años después del ataque DynDNS, AWS observó un ataque de reflexión UDP de 2,3 Tbps que se cree que es el ataque DDoS más grande de la historia.

GitHub. Para este ataque que aconteció en el año 2018, se enviaron paquetes a 1,35 Tbps saturando de esta manera los servidores de la plataforma de desarrollo colaborativo. Resulta curioso que utilizaron la propia memoria caché de los servidores de GitHub para amplificar la potencia de ataque, el tráfico de la plataforma se multiplicó por 51.000. A pesar de eso el servicio solo estuvo caído durante 5 minutos.

Ataque de VoIP.ms en 2021. En septiembre de 2021, el proveedor canadiense de VoIP, VoIP.ms fue víctima de un intento de extorsión de 4,2 millones de dólares en el cual a través de un ataque DDoS. Durante este tiempo se estuvo atacando el sitio y se exigía el pago del dinero para detener el ataque, los autores de la amenaza detrás del ataque se hicieron pasar por la banda de ransomware REvil. La empresa victima de este hecho tardó casi dos semanas en actualizar su infraestructura y restablecer el servicio a sus clientes.

Ataque de Yandex en 2021. También en 2021, la red de bots Mēris batió el récord de mayor número de peticiones por segundo (RPS) cuando se llevó a cabo un ataque a la empresa rusa de Internet Yandex cuando utilizo 21,8 millones de RPS. Para el ataque usaron una técnica conocida como «HTTP pipelining», en la que los bots emiten flujos de peticiones HTTP sin esperar a que se complete cada una.[3]

Para el segundo trimestre del año 2022 el principal desencadenante de los ataques de DDoS en el mundo fueron los motivos políticos, en el cual fueron blanco de ataques los sitios web de la autoridad del puerto de Londres y la autoridad de aeropuertos de Israel, fueron también víctimas de ataques DDoS sitios web de los gobiernos de Rumania y Republica checa; en Italia también fueron víctimas sitios como el del senado de ese país y el instituto nacional de salud. Para este último se utilizó una técnica conocida como HTTP lenta. Así mismo en medio del conflicto entre Rusia y ucrania, se han presentado una gran cantidad de ataques DDoS como el que recibió el servicio postal ucraniano el 22 de abril del presente año, los sitios web del gobierno de estonia también cayeron ante estos ataques de denegación de servicio distribuidos, pues estuvieron fuera de línea por al menos un par de días, a su vez múltiples sitios rusos como NashStore, el RosDorBank servicios del desarrollador de software empresarial ruso 1C, fueron víctimas de dichos ataques por parte de activistas pro-ucranianos. [4]

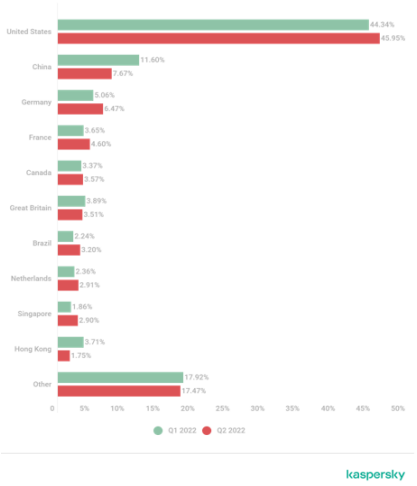

Figura. 4. Geografía de ataques DDoS. Recuperado de https://securelist.com/ddos-attacks-in-q2-2022/107025/?reseller=sea_GlobalFBPosts_awarn_ona_smm

VI. Como saber si somos o estamos siendo víctimas de un ataque DDos.

Si bien no existe forma de detectar un ataque DDoS, hay varias señales, algunas muy visibles, que nos permiten saber o tener indicios de cuando estamos siendo víctimas de un ataque de DDoS, que van desde lentitud en el procesamiento hasta la lentitud en la navegación.

A. Latencia excesiva

Esta es una de las formas más comunes para saber o sospechar que estamos siendo víctimas de un ataque, puesto que los navegadores de los usuarios y los servidores responde de una manera lenta y no convencional, se evidencia mucho retardo en la carga y en la navegación.

B. Tiempo de demora

Verificando el uso de la cpu, el tiempo que este puede demorar en dar servicio y las cargas de tráfico en la red, siempre que se evidencie que hay un consumo excesivo, que no suele ser usual, podríamos dudar de que estamos siendo víctimas de un ataque que está reflejando tráfico sospechoso.

C. Monitorear el tráfico

Realizando un monitoreo del tráfico web en nuestra red podemos darnos una idea de cómo actúa y cuál es el tráfico recurrente y que puede ser confiable, así con base en estos registros se pueden detectar datos de conexiones sospechosas o picos de tráfico no usual en la red, para esto es posible apoyarnos en programas y/o servicios que realicen dicho monitoreo y nos puedan brindar la mayor información posible sobre el tráfico de red.

D. Identificación de usuarios sospechosos

Otro indicador que nos daría señales de que algo anómalo está pasando en nuestra red es cuando tenemos ciertos intentos de conexión recurrentes en determinados lapsos de tiempo por parte de usuarios desconocidos y aunque estos tiempos suelen ser muy cortos y no se refleje un mal funcionamiento, es un indicio de que están realizando intentos por atacarnos.

VII. Como protegernos de los ataques DDos.

La preparación es la clave para enfrentar y corregir oportunamente un ataque, se debe tener una estrategia de defensa clara para intentar detectar, prevenir y reducir estos ataques, como usuarios debemos revisar la configuración de nuestros routers y firewalls para detectar IP´s inválidas o falsas, que provengan de posibles atacantes. Normalmente, nuestro Proveedor de Servicios de Internet (ISP) se encarga de que nuestro router esté al día con esta configuración.

Por otro lado, las empresas que proveen estos servicios, deben proteger tanto su red, como toda su infraestructura para poder evitar que estos ataques puedan afectar al desempeño de su trabajo y como consecuencia derivada de ello, a sus clientes. Si una empresa se ve afectada por un ataque de denegación de servicio (DoS) perderá la confianza de sus clientes y descartarán la contratación de sus servicios.

Las posibilidades de ser objetivo de un grupo de hacktivistas, como usuario doméstico, son escasas. Sin embargo, el mayor riesgo aquí es que sus dispositivos se infecten con malware, se alisten en botnets y se utilicen para atacar a otros objetivos.

Así también los departamentos de TI deberían saber cuáles son sus cuellos de botella. Una organización TI bien preparada debería identificar las partes de la red más propensas a ser atacadas por DDoS, como el ancho de banda a internet, firewalls, prevención de intrusiones (IPS), balanceador de cargas o servidores. Más aún, las TI necesitan monitorizar de cerca estos potenciales puntos de fallo, y evaluar si actualizar u optimizar su rendimiento y resistencia.

Para protegernos o intentar protegernos de estos ataques tenemos algunas recomendaciones que podemos aplicar en nuestro entorno cibernético, como lo son:

A. Configuración del firewall

Una de las barreras que podemos utilizar es la de configurar correctamente un firewall. De esta manera podremos monitorizar el tráfico entrante y definir diferentes pautas para decidir qué puede entrar y qué no, estos dispositivos van a ser los encargados de decidir qué conexiones se aceptan y cuáles no.

B. Mantener nuestros equipos seguros

Un método adecuado para evitar que nuestros equipos se vean afectados o que caigan en manos de hackers mediante las famosas botnets es mantenerlos completamente actualizados puesto que pueden surgir vulnerabilidades que los delincuentes pueden usar para distribuir sus ataques, también el contar con un buen sistema de antivirus puede ayudar a protegernos contra virus o malware que nos podrían llevar a convertir en miembros de redes zombi

C. Herramientas específicas

Con esto nos referimos al uso de herramientas que puedan controlar y monitorizar nuestro tráfico yendo más allá de las funciones que podría realizar un firewall, De esta forma podrán

alertar de posibles anomalías e incluso bloquear tráfico que pueda ser malicioso, afortunadamente hoy en día contamos con muchos equipos o programas de este tipo que pueden ayudarnos a mejorar la seguridad de nuestra red

D. Prevención ante las primeras señales

Siempre que nos encontremos con una pista o un síntoma debemos actuar prontamente para intentar bloquear el ataque, esto es importante para la seguridad de nuestra red y puede prevenir que suceda algo más que un ataque DDos.

E. Reducir la superficie expuesta

Una técnica primordial o esencial para protegernos es minimizar el espacio de área que puede ser atacada, y así limitar las opciones a los atacantes, entre menos servicios, puertos o aplicaciones vean el acceso a internet, cerrar accesos o restringirlos minimiza los puntos de ataque, haciendo así que al momento de ser víctimas de algún ataque podamos centrar nuestros esfuerzos en proteger puntos específicos.

VIII. MITIGAR UN ATAQUE DDOS

El problema en este caso radica en que tenemos que diferenciar entre el trafico normal o adecuado y el trafico que efectivamente es de un ataque, lo cual no resulta tan fácil como podría pensarse pues entre mas sofisticado sea el ataque más complicado será realizar esta distinción, sin contar que el ataque pueda adaptarse para superar las barreras establecidas previamente. Si establecemos una defensa por capas podemos pensar en:

A. Enrutamiento de agujeros negros

Pensando en una propuesta rápida se puede ejecutar esta opción en la que todo el trafico sea dirigido a una ruta nula, sin embargo, si se realiza un filtrado de esta manera y sin restricciones tanto el trafico bueno como el anómalo irán a ella y se excluirán de la red, lo que no lo hace viable puesto que el ataque consigue su objetivo de hacer inaccesible la red.

B. Limitación de velocidad

Otra opción en la que podemos pensar es en limitar el acceso o cantidad de solicitudes en cierto lapso de tiempo a nuestro servidor, con esto podemos disminuir en algo el objetivo del ataque, pero es muy posible que si es un ataque muy complejo se requiera de más medidas para mitigarlo.

C. Firewall de aplicaciones (WAF)

Esta medida es una ayuda para contrarrestar un ataque a las aplicaciones o servicios web ya que al igual que un firewall común, puede proteger nuestras aplicaciones de trafico malintencionado, pero para que tenga un adecuado funcionamiento debe estar bien configurado y con reglas de tráfico bien establecidas.

D. Red Anycast

Con esta medida lo que se busca es que el ataque se distribuya en toda la red hasta que se absorba el ataque y pueda ser administrado positivamente, el éxito de esta depende de las características que tenga dicha red como por ejemplo un ancho de banda de gran tamaño. [5]

IX. CONCLUSIÓN

Para finalizar podemos afirmar que los ataques DDoS serán parte de la estrategia a considerar en los próximos años por ser una de las amenazas silenciosas que pueden comprometer tu negocio de forma inesperada y masiva. Y aunque en un ataque DDos, la consecuencia más grave para una empresa es la pérdida de seguridad y confianza por parte de los usuarios. La razón es que la disponibilidad del sitio web es fundamental para obtener una buena experiencia por parte de los potenciales clientes para una compañía. Así, cuando los usuarios no pueden acceder al sitio web su experiencia de uso resulta muy negativa.

Entonces si piensa que su organización, por ser pequeña, es irrelevante para ser una víctima interesante para un hacker, piénselo de nuevo. Cualquier organización es una posible víctima y la mayoría de nosotros somos vulnerables a los ataques DDoS. Tanto si se trata de una empresa global, una agencia gubernamental o una pyme, todas ellas están dentro de la lista de objetivos de los ciberdelincuentes actuales. Incluso las empresas más seguras, con una gran inversión de recursos y expertos en seguridad han sido víctimas de estas amenazas.

Como hemos visto existen tanas formas de realizar un ataque de DDoS, algunas más complejas que otras; y que para hacer frente a estas amenazas una vez se hayan materializado en nuestra contra es primordial que contemos con una buena estrategía anti-DDoS, ya también existen compañías especializadas y dedicadas a este proceso de combatir o proteger a sitios de estos ataques.

REFERENCIAS

[1] Internet – Botnet – Online. Disponible en https://www.pandasecurity.com/es/security-info/botnet/

[2] Internet - Qué son los ataques DDos – Online. Disponible en https://www.kaspersky.es/resource-center/threats/ddos-attacks

[3] Internet - Ejemplos de ataques DDoS – Online. Disponible en https://www.avast.com/es-es/c-ddos

[4] Internet – Ataques DDoS en el Segundo trimester de 2022 – Online. Disponible en https://securelist.com/ddos-attacks-in-q2-2022/107025/?reseller=sea_GlobalFBPosts_awarn_ona_smm

[5] Internet - ¿Qué es un ataque DDoS? – Online. Disponible en https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

Autor.

Mauricio Pacheco Manotas, nacido en Sabanalarga, Atlántico en 1988, es graduado en Ingeniería de Sistemas en la universidad Simón Bolívar, cursa actualmente la especialización en Seguridad de la información en la universidad Piloto de Colombia y se desempeña como Ingeniero de infraestructura para la empresa tipo Fintech de origen argentino Solventa, así mismo como coordinador de sistemas para la compañía Hospimedics S.A