Los ataques de denegación de servicio distribuido (DDoS) que aprovechan una nueva técnica de amplificación llamada TCP Middlebox Reflection, se han detectado por primera vez en la naturaleza, seis meses después de que se presentara en teoría el nuevo mecanismo de ataque.

> *«El ataque abusa de los cortafuegos vulnerables y los sistemas de filtrado de contenido para reflejar y amplificar el tráfico TCP a una máquina víctima, creando un poderoso ataque DDoS»,* dijeron los investigadores de Akamai.

> *«Este tipo de ataque reduce peligrosamente el listón de los ataques DDoS, ya que el atacante necesita tan solo 1/75 (en algunos casos) de la cantidad de ancho de banda desde un punto de vista volumétrico»,* agregaron los investigadores.

Una denegación de servicio reflexiva distribuida (DRDoS) es una forma de ataque de denegación de servicio distribuido (DDoS) que se basa en servidores UDP de acceso público y factores de amplificación de ancho de banda (BAF) para abrumar el sistema de una víctima con un gran volumen de respuestas UDP.

En este tipo de ataques, el adversario envía una avalancha de solicitudes DNS o NTP que contienen una dirección IP de origen falsificada al activo objetivo, lo que hace que el servidor de destino entregue las respuestas al host que reside en la dirección falsificada de una forma amplificada que agota el ancho de banda al objetivo emitido.

Este desarrollo se produce luego de un estudio académico publicado en agosto de 2021 sobre un nuevo vector de ataque que explota las vulnerabilidades en la implementación del protocolo TCP en los middleboxes y la infraestructura de censura para llevar a cabo ataques de amplificación de denegación de servicio (DoS) reflejados contra objetivos.

Aunque los ataques de amplificación DoS han abusado tradicionalmente de los vectores de

reflexión UDP, debido a la naturaleza sin conexión del protocolo, la técnica de ataque no convencional aprovecha el incumplimiento de TCP en cajas intermedias, como las herramientas de inspección profunda de paquetes (DPI) para realizar ataques de amplificación reflexiva basados en TCP.

Al parecer, la primera ola de campañas de ataque *«perceptibles»* que aprovecharon la técnica ocurrió alrededor del 17 de febrero, golpeando a los clientes de Akamai en las industrias de banca, viajes, juegos, medios y alojamiento web con grandes cantidades de tráfico que alcanzaron un máximo de 11 Gbps en 1.5 millones de paquetes por segundo (Mpps).

«Se ha visto que el vector se usa solo y como parte de campañas de múltiples vectores, con el tamaño de los ataques aumentando lentamente», dijo Chad Seaman, líder del equipo de investigación de inteligencia de seguridad (SIRT) de Akamai.

La idea central con la reflexión basada en TCP es aprovechar los middleboxes que se utilizan para hacer cumplir las leyes de censura y políticas de filtrado de contenido empresarial mediante el envío de paquetes TCP especialmente diseñados para desencadenar una respuesta volumétrica.

De hecho, en uno de los ataques observados por la empresa de seguridad en la nube, un solo paquete SYN con una carga útil de 33 bytes desencadenó una respuesta de 2156 bytes, logrando efectivamente un factor de amplificación de 65x (6533%).

> *«La conclusión principal es que el nuevo vector está comenzando a ver abuso en el mundo real en la naturaleza. Por lo general, esta es una señal de que es probable que siga un abuso más generalizado de un vector en particular a medida que crece el conocimiento y la popularidad en el panorama DDoS y más atacantes comienzan a crear herramientas para aprovechar el nuevo vector»,* dijo Seaman.

> *«Los defensores deben ser conscientes de que hemos pasado de la teoría a la práctica, y deben revisar sus estrategias defensivas de acuerdo con este nuevo vector, que pronto verán en el mundo real»,* agregó Seaman.