Cloudflare ha anunciado que logró mitigar un ataque de denegación de servicio distribuido (DDoS) sin precedentes, que alcanzó un máximo de 3.8 terabits por segundo (Tbps) y duró 65 segundos.

> La compañía de seguridad e infraestructura web explicó que neutralizó *«más de cien ataques DDoS hiper-volumétricos de capas L3/4 durante el último mes, muchos de los cuales superaron los 2 mil millones de paquetes por segundo (Bpps) y los 3 terabits por segundo (Tbps)».*

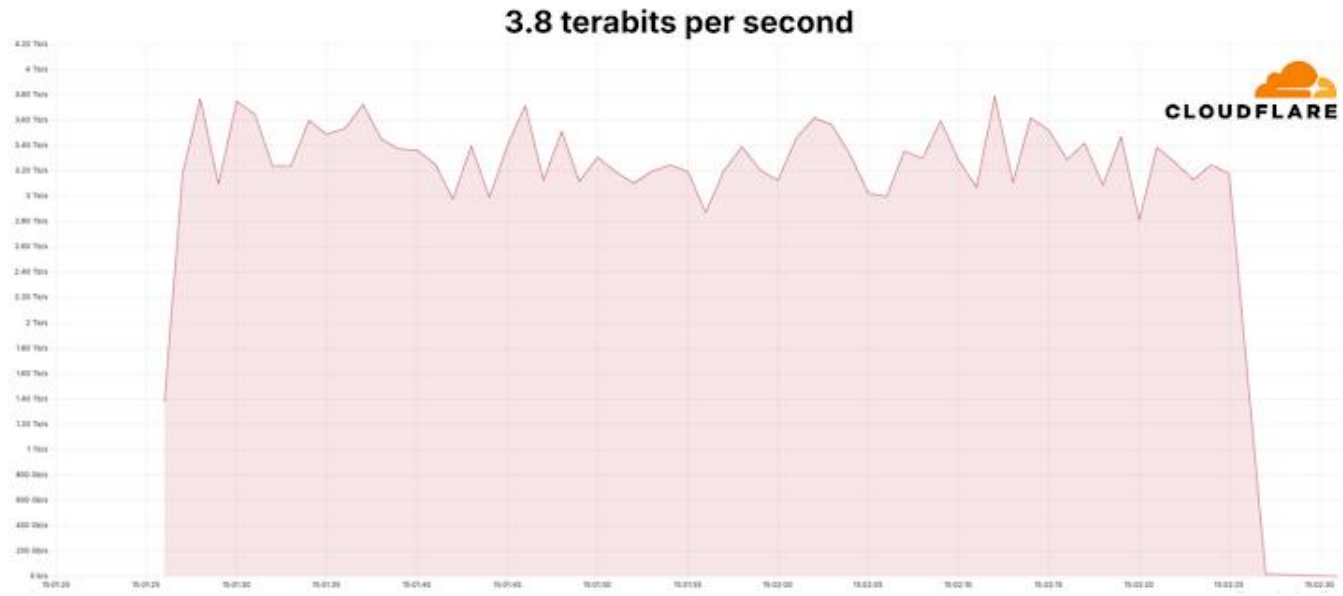
Estos ataques DDoS hiper-volumétricos de capas L3/4 comenzaron a principios de septiembre de 2024 y estaban dirigidos a varios clientes en sectores como los servicios financieros, Internet y telecomunicaciones. Hasta ahora, no se ha identificado a un actor de amenazas específico detrás de estas acciones.

El récord anterior del mayor ataque DDoS volumétrico fue en noviembre de 2021, alcanzando un pico de 3.47 Tbps, y afectó a un cliente no identificado de Microsoft Azure en Asia.

Los atacantes emplearon el protocolo UDP (User Datagram Protocol) en un puerto específico, con una oleada de paquetes que se originaron en países como Vietnam, Rusia, Brasil, España y Estados Unidos. Estos paquetes provinieron de dispositivos comprometidos como routers MikroTik, grabadoras de vídeo digitales (DVRs) y servidores web.

Cloudflare indicó que la alta tasa de transmisión de estos ataques probablemente proviene de una botnet masiva que incluye routers domésticos ASUS infectados, los cuales fueron explotados debido a una vulnerabilidad crítica descubierta recientemente (CVE-2024-3080, con una puntuación de 9.8 en el sistema CVSS).

De acuerdo con datos proporcionados por la firma de gestión de superficies de ataque Censys, más de 157,000 modelos de routers ASUS estaban potencialmente expuestos a la vulnerabilidad hasta el 21 de junio de 2024, y la mayoría de estos dispositivos se encuentran en Estados Unidos, Hong Kong y China.



El objetivo principal de la campaña, según Cloudflare, es saturar el ancho de banda de la red del objetivo, así como consumir los recursos de CPU, impidiendo que los usuarios legítimos puedan acceder al servicio.

> *«Para contrarrestar ataques con tasas de paquetes tan elevadas, es crucial poder inspeccionar y descartar los paquetes maliciosos utilizando la menor cantidad posible de ciclos de CPU, dejando suficiente capacidad para procesar los paquetes válidos»*, explicó la empresa.
>
> *«Muchos servicios en la nube no cuentan con la capacidad suficiente, y el uso de equipos locales tampoco es adecuado para defenderse de ataques DDoS de esta magnitud, ya que la saturación del ancho de banda puede bloquear los enlaces de Internet, mientras que la elevada tasa de paquetes puede colapsar los dispositivos en línea.»*

Los sectores bancario, financiero y los servicios públicos han sido blancos comunes de ataques DDoS, con un aumento del 55% en los últimos cuatro años, según NETSCOUT, una empresa de monitoreo de redes. Solo en la primera mitad de 2024, los ataques volumétricos crecieron un 30%.

El incremento en la frecuencia de los ataques DDoS, impulsado principalmente por actividades de hacktivistas que apuntan a organizaciones e industrias globales, también ha estado acompañado por el uso de DNS sobre HTTPS (DoH) para los comandos y controles (C2), con el fin de dificultar la detección.

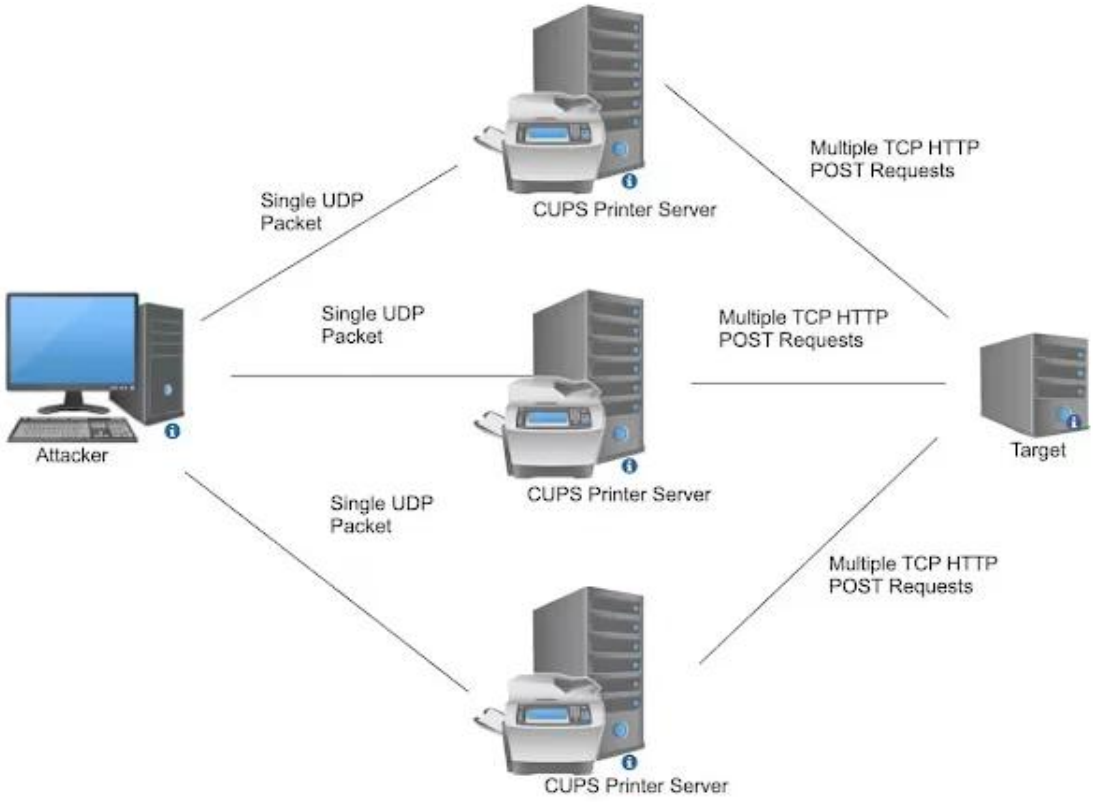
> *«La tendencia de utilizar una infraestructura distribuida de control y comando en botnets, aprovechando bots como nodos de control, complica aún más las tareas de defensa, ya que no solo hay que gestionar la actividad DDoS entrante, sino también la actividad saliente de los sistemas infectados que deben ser identificados y bloqueados»*, explicó NETSCOUT.

El avance ocurre luego de que Akamai revelara que las vulnerabilidades recientemente descubiertas en el Sistema de Impresión Común de UNIX (CUPS) en Linux podrían ser un vector efectivo para lanzar ataques DDoS, con un factor de amplificación de hasta 600 veces en solo segundos.

El análisis de la compañía determinó que más de 58,000 (34%) de los aproximadamente 198,000 dispositivos accesibles a través de internet podrían ser utilizados para llevar a cabo ataques DDoS.

> *«El problema se presenta cuando un atacante envía un paquete modificado que especifica la dirección de un objetivo como si fuera una impresora para agregar»*, explicaron los investigadores Larry Cashdollar, Kyle Lefton y Chad Seaman.

> *«Por cada paquete enviado, el servidor CUPS vulnerable generará una solicitud IPP/HTTP de mayor tamaño y parcialmente controlada por el atacante, dirigida al objetivo. Como resultado, no solo el objetivo se ve afectado, sino que también el servidor CUPS sufre, ya que el ataque consume su ancho de banda y recursos de CPU».*



Se estima que hay alrededor de 7,171 hosts que exponen servicios CUPS a través de TCP y que son vulnerables a la CVE-2024-47176, según Censys, aunque esta cifra podría ser inferior a la real, dado que *«parecen haber más servicios CUPS accesibles a través de UDP que de TCP».*

Se aconseja a las organizaciones desinstalar CUPS si la funcionalidad de impresión no es necesaria, y bloquear los puertos de servicio (UDP/631) si son accesibles desde la red pública.