Amazon dijo que su servicio AWS Shield, mitigó el ataque DDoS más grande jamás registrado, de 2.3 Tbps a mediados de febrero de este año.

El incidente fue revelado en AWS Shield Threat Landscape, un informe que detalla los ataques web mitigados por el servicio de protección AWS Shield de Amazon.

El informe no identificó al cliente objetivo de AWS, pero dijo que el ataque se llevó a cabo utilizando servidores web CLDAP secuestrados y causó tres días de *«amenaza elevada»* para su personal de AWS Shield.

CLDAP (Protocolo Ligero de Acceso a Directorios sin Conexión) es una alternativa al antiguo protocolo LDAP, y se utilizar para conectarse, buscar y modificar directorios compartidos en Internet.

Se ha abusado del protocolo para ataques DDoS desde finales de 2016, y se sabe que los servidores CLDAP amplifican el tráfico DDoS entre 56 y 70 veces su tamaño inicial, lo que lo convierte en un protocolo muy solicitado y una opción común proporcionada por los servicios DDoS de alquiler.

El récord anterior para el mayor ataque DDoS registrado fue de 1.7 Tbps, mitigado por NETSCOUT Arbor en marzo de 2018.

Antes de eso, el mayor ataque DDoS jamás registrado fue de 1.3 Tbps que golpeó a GitHub, un mes antes, en febrero de 2018.

Los ataques Netscout y GitHub DDoS abusaron de los servidores Memcached expuestos a Internet para alcanzar anchos de banda masivos.

Durante los ataques de 2018, Memcached era un nuevo vector de ataque DDoS, y muchos grupos de hackers y servicios DDoS de alquiler se apresuraron a abusar de más de 100,000 servidores Memcached para crear problemas en Internet.

Sin embargo, los ataques masivos DDoS se han convertido en una rareza, principalmente porque los proveedores de servicios de Internet (ISP), las redes de entrega de contenido (CDN) y otros jugadores importantes de Internet, trabajan juntos para proteger los sistemas vulnerables de Memcached.

Actualmente, la mayoría de los ataques DDoS por lo general alcanzan su punto máximo en el rango de 500 Gbps, por lo que la noticia del ataque de AWS de 2.3 Tbps fue una sorpresa para la industria.

Por ejemplo, en su informe trimestral para el primer trimestre de 2020, el servicio de mitigación DDoS, Link11, informó que el mayor ataque DDoS que mitigó fue de 406 Gbps. En su informe DDoS del primer trimestre de 2020, Cloudflare dijo que el mayor ataque DDoS que mitigó fue de poco más de 550 Gbps.

Por otro lado, Akamai informó hoy que mitigó un ataque DDoS de 1.44 Tbps en la primera semana de junio de 2020.

Cloudflare informó que el 92% de los ataques DDoS que mitigó en el primer trimestre de 2020 tenían menos de 10 Gbps y que el 47% eran aún más pequeños, de menos de 500 Mbps.