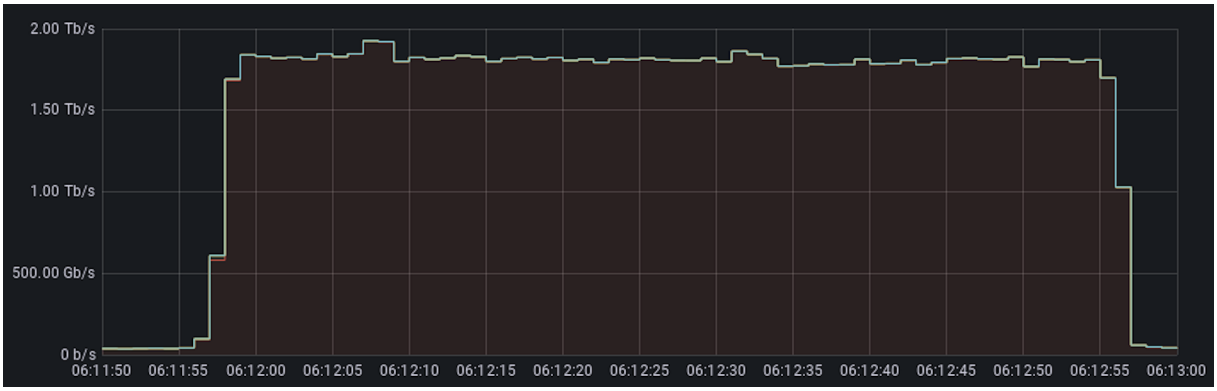
Cloudflare blocks an almost 2 Tbps multi-vector DDoS attack

13-11-2021

- 

Omer Yoachimik

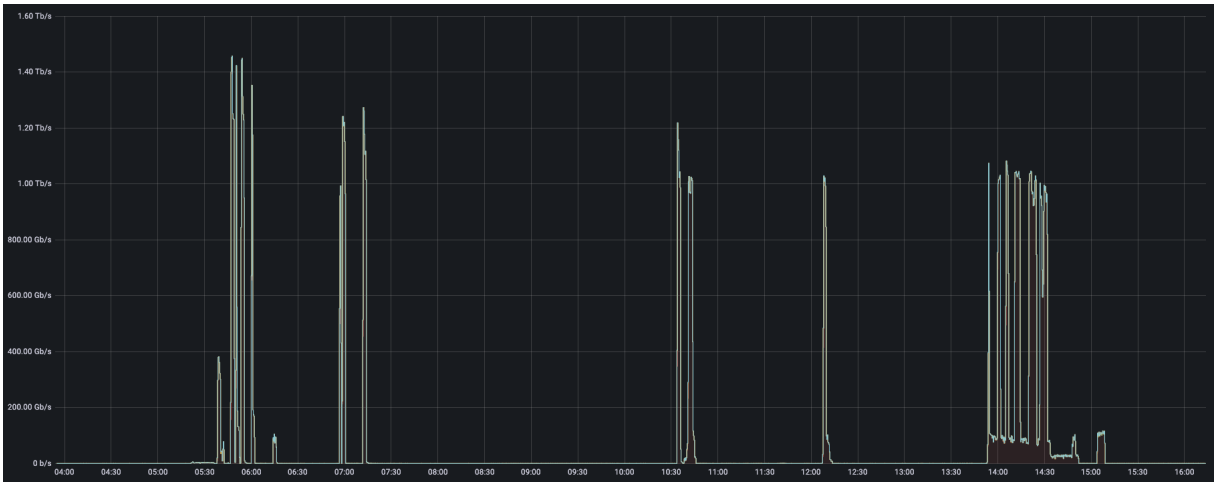
Earlier this week, Cloudflare automatically detected and mitigated a DDoS attack that peaked just below 2 Tbps — the largest we've seen to date. This was a multi-vector attack combining DNS amplification attacks and UDP floods. The entire attack lasted just one minute. The attack was launched from approximately 15,000 bots running a variant of the original Mirai code on IoT devices and unpatched GitLab instances.



DDoS attack peaking just below 2 Tbps

Network-layer DDoS attacks increased by 44%

Last quarter, we saw multiple terabit-strong DDoS attacks and this attack continues this trend of increased attack intensity. Another key finding from our Q3 DDoS Trends report was that network-layer DDoS attacks actually increased by 44% quarter-over-quarter. While the fourth quarter is not over yet, we have, again, seen multiple terabit-strong attacks that targeted Cloudflare customers.

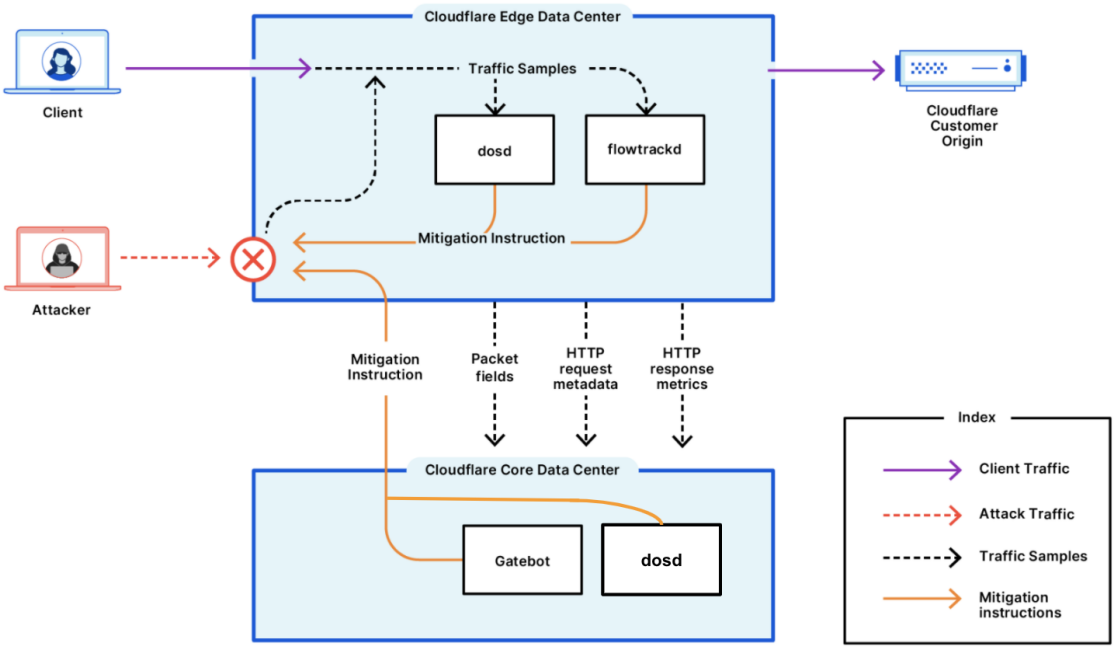


DDoS attacks peaking at 1-1.4 Tbps

How did Cloudflare mitigate this attack?

To begin with, our systems constantly analyze traffic samples “out-of-path” which allows us to asynchronously detect DDoS attacks without causing latency or impacting performance. Once the attack traffic was detected (within sub-seconds), our systems generated a real-time signature that surgically matched against the attack patterns to mitigate the attack without impacting legitimate traffic.

Once generated, the fingerprint is propagated as an ephemeral mitigation rule to the most optimal location in the Cloudflare edge for cost-efficient mitigation. In this specific case, as with most L3/4 DDoS attacks, the rule was pushed in-line into the Linux kernel eXpress Data Path (XDP) to drop the attack packet at wirespeed.



A conceptual diagram of Cloudflare's DDoS protection systems

Read more about Cloudflare's DDoS Protection systems.

Helping build a better Internet

Cloudflare's mission is to help build a better Internet — one that is secure, faster, and more reliable for everyone. The DDoS team's vision is derived from this mission: our goal is to make the impact of DDoS attacks a thing of the past. Whether it's the Meris botnet that launched some of the largest HTTP DDoS attacks on record, the recent attacks on VoIP providers or this Mirai-variant that's DDoSing Internet properties, Cloudflare's network automatically detects and mitigates DDoS attacks. Cloudflare provides a secure, reliable, performant, and customizable platform for Internet properties of all types.

For more information about Cloudflare's DDoS protection, reach out to us or have a go with a hands-on evaluation of Cloudflare's Free plan here.