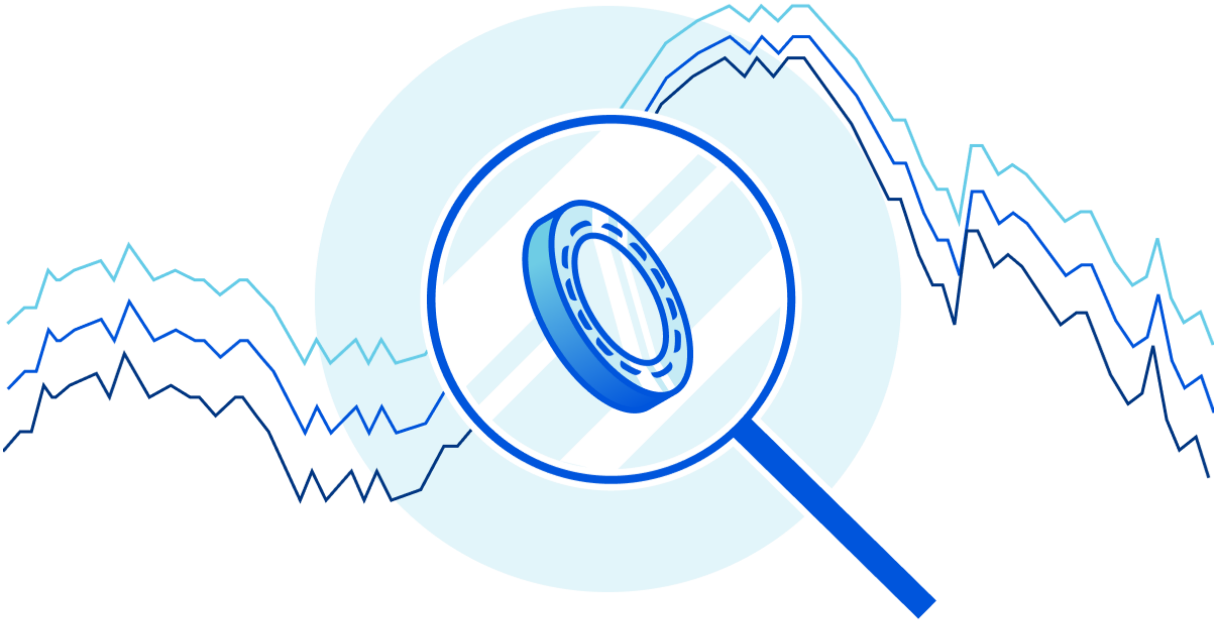
CLOUDFLARE The Cloudflare Blog

# Cloudflare blocks 15M rps HTTPS DDoS attack

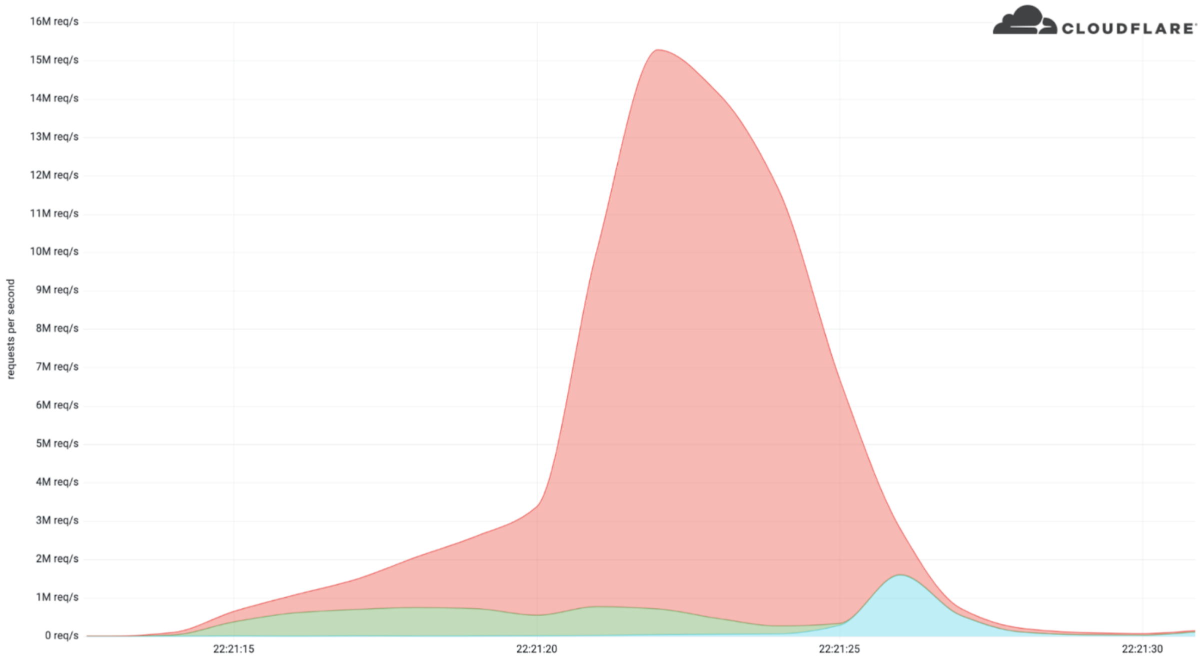


Earlier this month, Cloudflare's systems automatically detected and mitigated a 15.3 million request-per-second (rps) DDoS attack — one of the largest HTTPS DDoS attacks on record.

While this isn't the largest application-layer attack we've seen, it is the largest we've seen over HTTP**S**. HTTPS DDoS attacks are more expensive in terms of required computational resources because of the higher cost of establishing a secure TLS encrypted connection. Therefore it costs the attacker more to launch the attack, and for the victim to mitigate it. We've seen very large attacks in the past over (unencrypted) HTTP, but this attack stands out because of the resources it required at its scale.

The attack, lasting less than 15 seconds, targeted a Cloudflare customer on the Professional (Pro) plan operating a crypto launchpad. Crypto launchpads are used to surface Decentralized Finance projects to potential investors. The attack was launched by a botnet that we've been observing — we've already seen large attacks as high as 10M rps matching the same attack fingerprint.

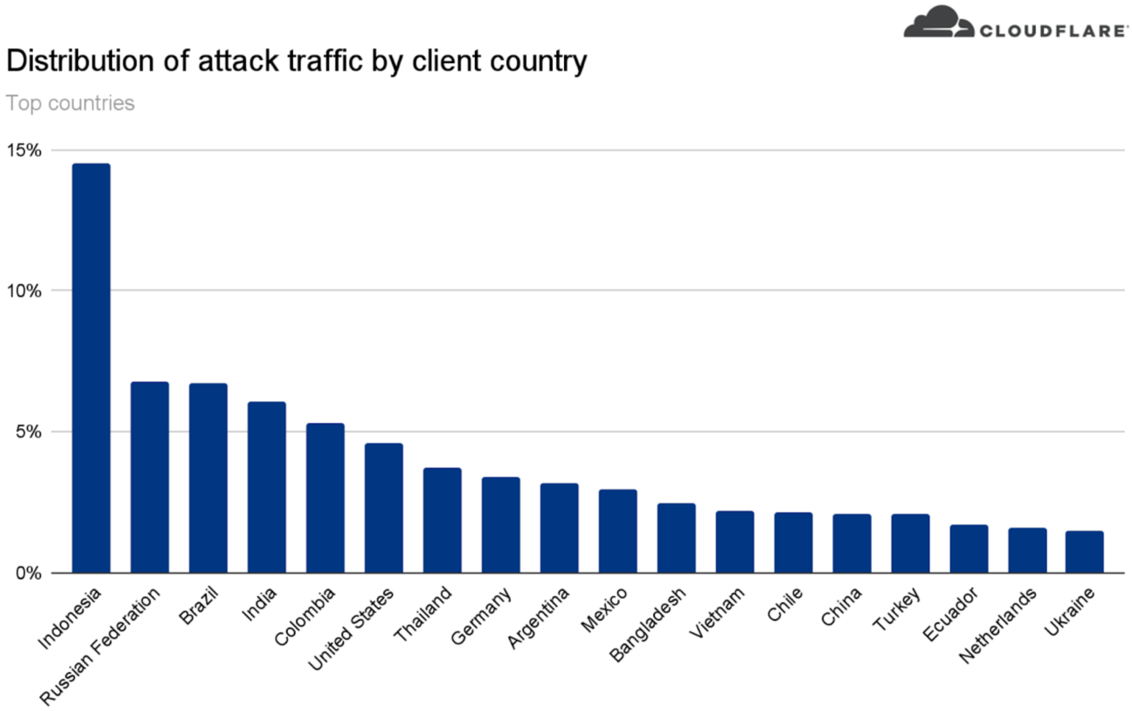
Cloudflare customers are protected against this botnet and do not need to take any action.



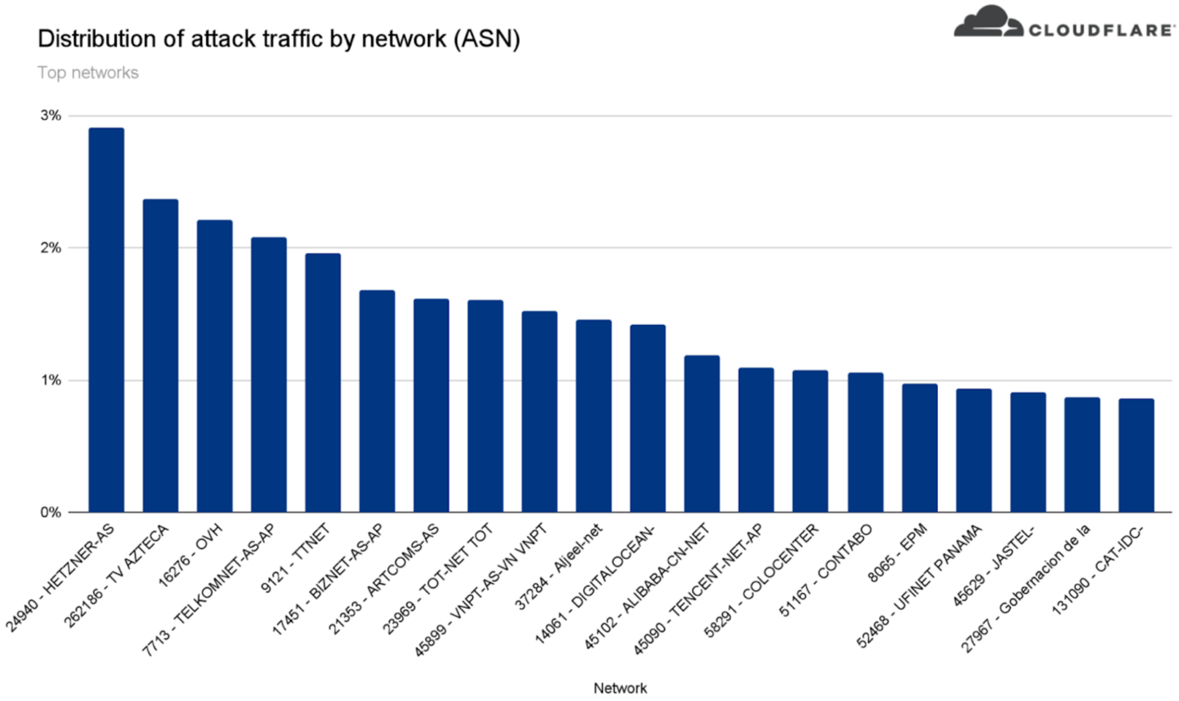
## The attack

What's interesting is that the attack mostly came from data centers. A change from residential network Internet Service Providers (ISPs) to cloud compute ISPs.

This attack was launched from a botnet of approximately 6,000 unique bots. It originated from 112 countries around the world. Almost 15% of the attack traffic originated from Indonesia, followed by Russia, Brazil, India, Colombia, and the United States.



Within those countries, the attack originated from over 1,300 different networks. The top networks included the German provider Hetzner Online GmbH (Autonomous System Number 24940), Azteca Comunicaciones Colombia (ASN 262186), OVH in France (ASN 16276), as well as other cloud providers.



### How this attack was automatically detected and mitigated

To defend organizations against DDoS attacks, we built and operate software-defined systems that run autonomously. They automatically detect and mitigate DDoS attacks across our entire network — and just as in this case, the attack was automatically detected and mitigated without any human intervention.

Our system starts by sampling traffic asynchronously; it then analyzes the samples and applies mitigations when needed.

### Sampling

Initially, traffic is routed through the Internet via BGP Anycast to the nearest Cloudflare data centers that are located in over 270 cities around the world. Once the traffic reaches our data center, our DDoS systems sample it asynchronously allowing for out-of-path analysis of traffic without introducing latency penalties.

### Analysis and mitigation

The analysis is done using data streaming algorithms. HTTP request samples are compared to conditional fingerprints, and multiple real-time signatures are created based on dynamic masking of various request fields and metadata. Each time another request matches one of the signatures, a counter is increased. When the activation threshold is reached for a given signature, a mitigation rule is compiled and pushed inline. The mitigation rule includes the real-time signature and the mitigation action, e.g. block.

Cloudflare customers can also customize the settings of the DDoS protection systems by tweaking the HTTP DDoS Managed Rules.

You can read more about our autonomous DDoS protection systems and how they work in our deep-dive technical blog post.

## Helping build a better Internet

At Cloudflare, everything we do is guided by our mission to help build a better Internet. 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. The level of protection that we offer is unmetered and unlimited — It is not bounded by the size of the attack, the number of the attacks, or the duration of the attacks. This is especially important these days because as we've recently seen, attacks are getting larger and more frequent.

Not using Cloudflare yet? Start now with our Free and Pro plans to protect your websites, or contact us for comprehensive DDoS protection for your entire network using Magic Transit.