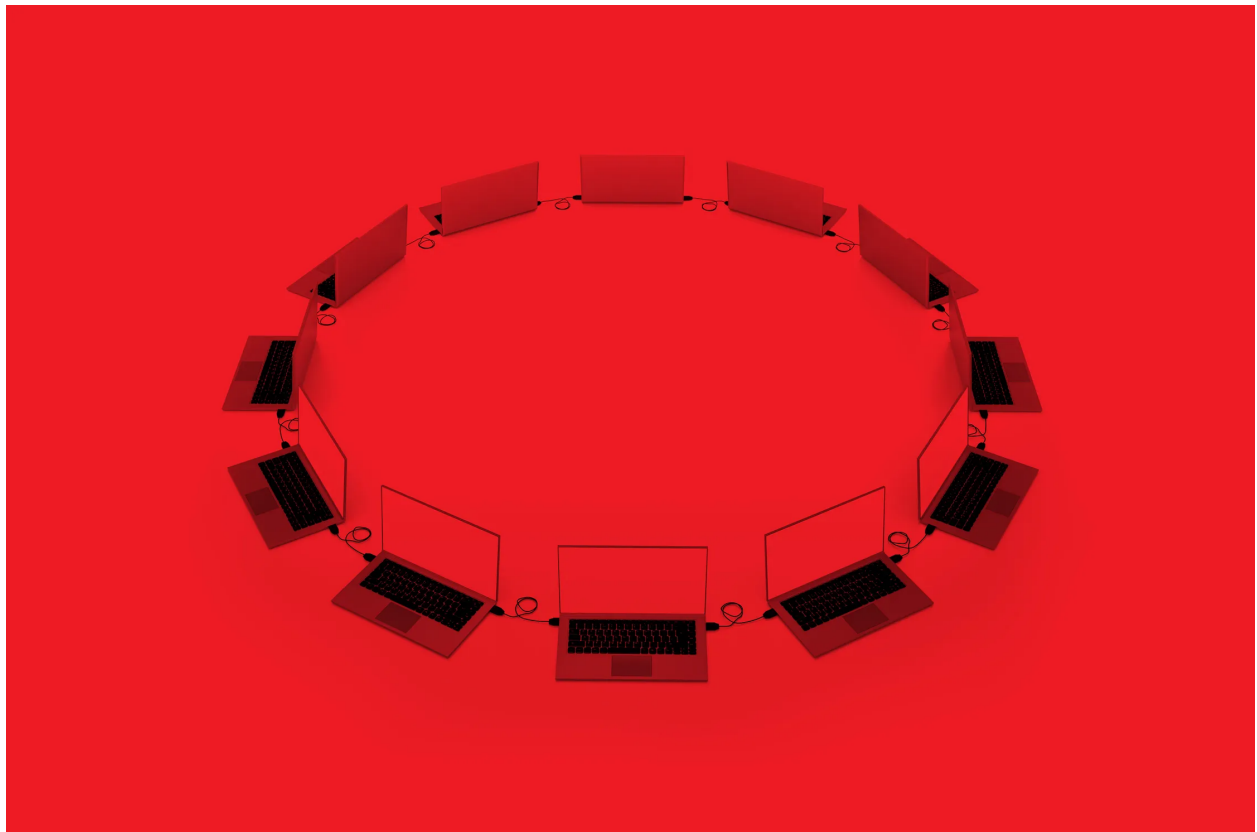


One of the Most Powerful DDoS Attacks Ever Hits a Crypto Platform

The onslaught was delivered through HTTPS, which puts more strain on a target, and it suggests that attackers are getting more powerful.



PHOTOGRAPH: GETTY IMAGES

A CRYPTOCURRENCY PLATFORM was recently on the receiving end of

one of the biggest distributed denial of service attacks ever recorded, after threat actors bombarded it with 15.3 million requests, the content-delivery network [Cloudflare](#) said.

Ars Technica

This story originally appeared on [Ars Technica](#), a trusted source for technology news, tech policy analysis, reviews, and more. Ars is owned by WIRED's parent company, Condé Nast.

[DDoS attacks](#) can be measured in several ways, including by the volume of data, the number of packets, or the number of requests sent each second. The current records are [3.4 terabits per second](#) for volumetric DDoS's—which attempt to consume all bandwidth available to the target—and [809 million packets per second](#), and [17.2 million requests per second](#). The latter two records measure the power of application-layer attacks, which attempt to exhaust the computing resources of a target's infrastructure.

Cloudflare's recent DDoS mitigation peaked at 15.3 million requests per second. While short of the record, the attack may have been more powerful, because it was delivered through HTTPS requests rather than the HTTP requests used in the record. Because HTTPS requests are much more compute-intensive, this new attack had the potential to put much more strain on the target.

The resources required to deliver the HTTPS request flood were also greater, indicating that DDoSers are growing increasingly powerful. Cloudflare said that the [botnet](#) responsible, comprising about 6,000 bots, has delivered payloads as high as 10 million requests per second. The attack originated from 112 countries, with about 15 percent of the firepower from Indonesia, followed by Russia, Brazil, India, Colombia,

and the United States.

“Within those countries, the attack originated from over 1,300 different networks,” Cloudflare researchers Omer Yoachimik and Julien Desgats wrote. They said that the flood of traffic mainly came from data centers, as DDoSers move away from residential network ISPs to cloud computing ISPs. Top data center networks involved included the German provider Hetzner Online (Autonomous System Number 24940), Azteca Comunicaciones Colombia (ASN 262186), and OVH in France (ASN 16276). Other sources included home and small office routers.



“In this case, the attacker was using compromised servers on cloud hosting providers, some of which appear to be running Java-based applications. This is notable because of the recent discovery of a vulnerability (CVE-2022-21449) that can be used for authentication bypass in a wide range of Java-based applications,” Patrick Donahue, Cloudflare's VP of product, wrote in an email. “We also saw a significant number of MikroTik routers used in the attack, likely exploiting the same vulnerability that the Meris botnet did.”

The attack lasted about 15 seconds. Cloudflare mitigated it using systems in its network of data centers that automatically detect traffic spikes and quickly filter out the sources. Cloudflare didn't identify the target except to say that it operated a crypto launchpad, a platform used to help fund decentralized finance projects.

The numbers underscore the arms race between attackers and defenders as each attempts to outdo the other. It won't be surprising if a new record is set in the coming months.

This story originally appeared on Ars Technica.

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- This startup wants to [watch your brain](#)
- The artful, subdued translations of [modern pop](#)
- Netflix doesn't need a [password-sharing crackdown](#)
- How to revamp your workflow with [block scheduling](#)
- [The end of astronauts](#)—and the rise of robots
-  Explore AI like never before with [our new database](#)
- ✨ Optimize your home life with our Gear team's best picks, from [robot vacuums](#) to [affordable mattresses](#) to [smart speakers](#)

Dan Goodin is IT Security Editor at Ars Technica



TOPICS ARS TECHNICA CLOUDFLARE DDOS BOTNETS CRYPTOCURRENCY

MORE FROM WIRED

North Korea Hacked Him. So He Took Down Its Internet

Disappointed with the lack of US response to the Hermit Kingdom's attacks against US security researchers, one hacker took matters into his own hands.

ANDY GREENBERG

The Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site

They thought their payments were untraceable. They couldn't have been more wrong. The untold story of the case that shredded the myth of Bitcoin's anonymity.

ANDY GREENBERG

Ice Cream Machine Hackers Sue McDonald's for \$900 Million

Kytch alleges that the Golden Arches crushed its business—and left soft serve customers out in the cold.

ANDY GREENBERG

‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

LILY HAY NEWMAN

You Need a Password Manager. Here Are the Best Ones

Keep your logins locked down with our favorite apps for PC, Mac, Android, iPhone, and web browsers.

SCOTT GILBERTSON

The McDonald's Ice Cream Machine Hacking Saga Has a New Twist

The cold war between a startup and a soft-serve machine manufacturer is heating up, thanks to a newly released trove of internal emails.

ANDY GREENBERG

Amazon's Dark Secret: It Has Failed to Protect Your Data

Voyeurs. Sabotaged accounts. Backdoor schemes. For years, the retail giant has handled your information less carefully than it handles your packages.

WILL EVANS

Apple's Killing the Password. Here's Everything You Need to Know

With iOS 16 and macOS Ventura, Apple is introducing passkeys—a more convenient and secure alternative to passwords.

MATT BURGESS

One year for
~~\$29.99~~ \$10
Get WIRED

SUBSCRIBE