Wie eine von Freiwilligen betriebene Waldbrandstätte in Portugal während der DDoS-Angriffe online blieb

2025-08-21

Joo Tomé

5 min gelesen

Am 31. Juli 2025, als Portugal den Höhepunkt einer weiteren intensiven Waldbrandsaison erreichte, erhielt Joo Pina, auch bekannt als Tomahock, eine automatisierte Warnung von Cloudflare. Sein freiwillig geführtes Projekt, fogos.pt, jetzt eine vertrauenswürdige Quelle für Waldbrandinformationen in Echtzeit für Millionen in ganz Portugal, wurde

angegriffen.

Einer der verschiedenen Warnungen, die fogos.pt im Zusammenhang mit dem DDoS-Angriff erhalten hat

Was 2015 als Late-Night-Nebenprojekt mit Freunden an einem Esstisch in Aveiro begann, hat sich zu einer kritischen öffentlichen Ressource entwickelt. Während der Waldbrände ist der Ort, an dem Feuerwehrleute, Journalisten, Bürger und sogar Regierungsbehörden verstehen, was vor Ort passiert. Im Laufe der Jahre hat sich fogos.pt vom Parsen von PDFs zu visuellen Karten zu einer voll ausgestatteten App und Website mit historischen Daten, Wetter-Overlays und mehr entwickelt. Es ist auch Teil des Projekts Galileo, der Initiative von Cloudflare, um gefährdete, aber

wichtige öffentliche Seiten kostenlos zu schützen.

Waldbrände sind nicht nur eine portugiesische Herausforderung. Sie sind häufig in Südeuropa (Spanien, Griechenland, derzeit auch in Alarmbereitschaft), Kalifornien, Australien, und in Kanada, das 2023 mit Rekordbränden konfrontiert warrecord-setting. In all diesen Fällen können verlässliche Informationen entscheidend sein, manchmal lebensrettende. Andere Organisationen, die ähnliche öffentliche Dienstleistungen anbieten, können sich auch für den Beitritt zu bewerben, um Schutz zu erhalten und starken Verkehr zu bewältigen.

Ein Nebenprojekt, das zu einer nationalen Referenz wurde

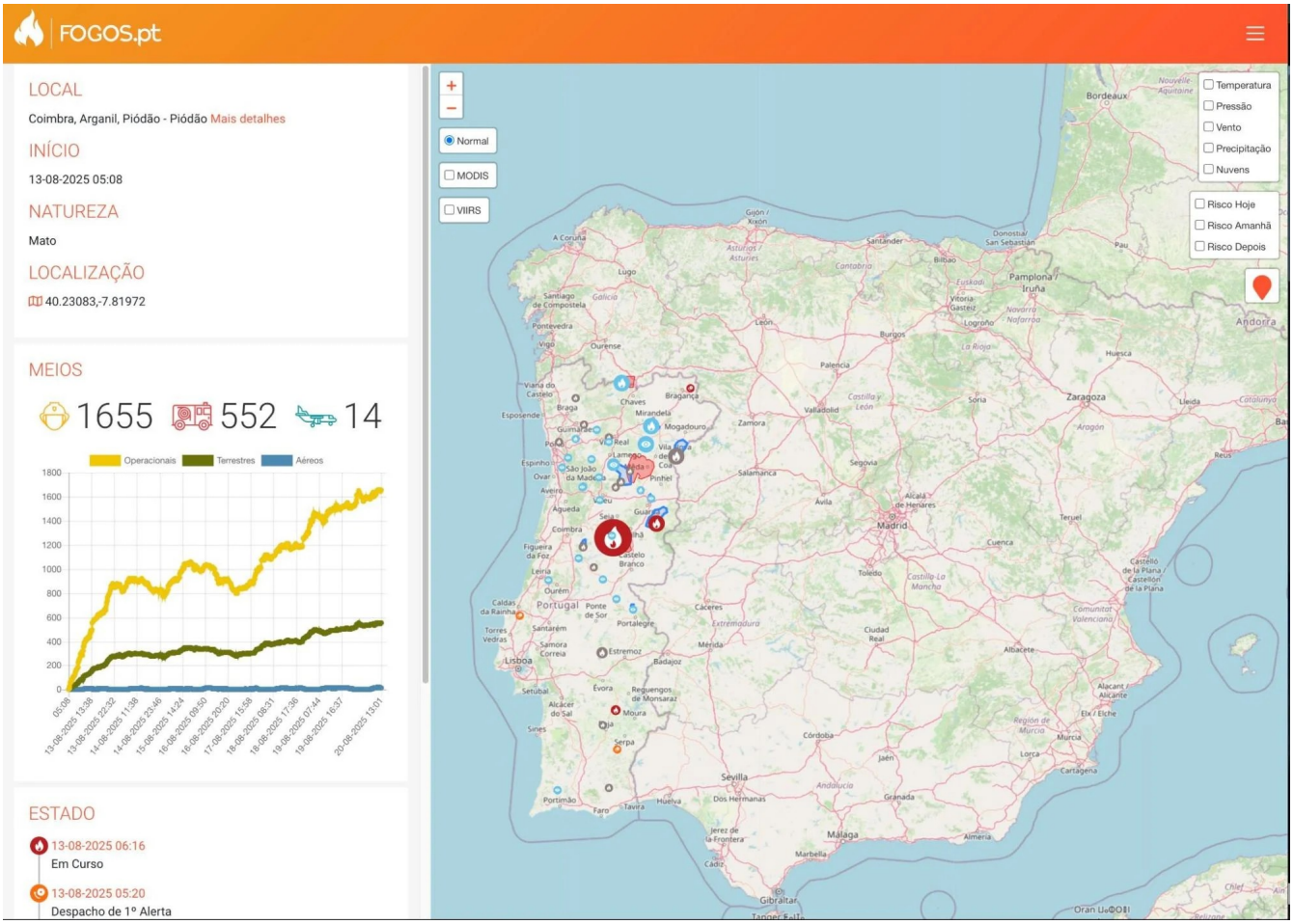
Fogos.pt begann mit einer einfachen Frage: Warum waren Branddaten nur in schwer lesbaren PDF-Dokumenten verfügbar? Joo und eine Gruppe von Freunden, darunter Freiwillige Feuerwehrleute, beschlossen, etwas Besseres zu bauen. Sie zogen die Daten, verlagerten die Brandberichte und visualisierten sie auf einer Karte.

Bald benutzten Tausende von Menschen es. Dann Zehntausende. Heute ist fogos.pt in die offizielle Kommunikation integriert, einschließlich Erwähnungen der portugiesischen Regierung in den sozialen Medien und direkte Links vom nationalen Waldbrandinformationsportal (SGIFR.gov.pt).

Im Jahr 2018 schloss sich fogos.pt formell mit VOST Portugal zusammen, einer digitalen Freiwilligenorganisation, die schon früh auch Teil unseres Projekts Galileo war - dessen Geschichte auch in einer früheren Fallstudie zu sehen war. Joo Pina ist auch Mitbegründer von VOSTPT. Gemeinsam erstellten sie ein ergänzendes Modell: fogos.pt liefert Daten und die Plattform; VOSTPT validiert und teilt es der Öffentlichkeit in Echtzeit in Notfällen mit.

Es ist eine Operation, die ausschließlich von Freiwilligen durchgeführt wird,

ohne Finanzierung, kein formelles Team - nur Leidenschaft und die Hilfe von Partnern.



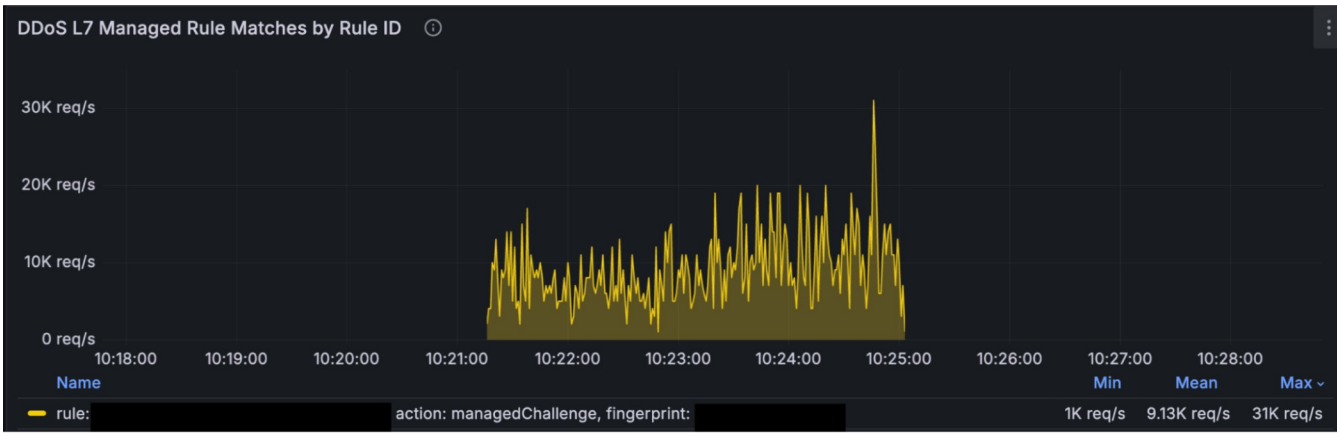
Homepage von fogos.pt am 20. August 2025, die einen großen Waldbrand in der Nähe von Pisdo in Zentralportugal hervorhebt.

In der Feuersaison unter Beschuss

Am 31. Juli und 1. August 2025 zielten zwei Distributed Denial of Service (DDoS) auf nebel.pt. Cloudflare erkannte und milderte beide Angriffe automatisch.

July 31 attack: • Duration: 7 minutes • Peak: 33,000 requests per second at 11:27 UTC • Bandwidth: 1.7 Gbps (Max) How the attack looks like in requests per second:

August 1 attack: • Duration: 5 minutes • Peak: 31,000 requests per second at 10:24 UTC • Bandwidth: 849 Mbps (Max) How the attack looks like in requests per second from our perspective:



By Cloudflare's standards, these were small. For comparison, last year we mitigated an attack exceeding 700,000 requests per second against a high-profile US election campaign site. But for an civic project like fogos.pt, even tens of thousands of requests per second — if unprotected — can be enough to take services offline at the worst possible time.

Attackers typically use three main methods for DDoS attacks:

- IoT devices: hacked cameras, routers, or smart gadgets sending traffic.
- Proxies: open or misconfigured servers, residential proxy networks, or anonymity tools that hide attackers' IPs.
- Cloud machines: compromised or rented servers from cloud providers.

The July 31 attack likely relied on open proxies, with much of the traffic

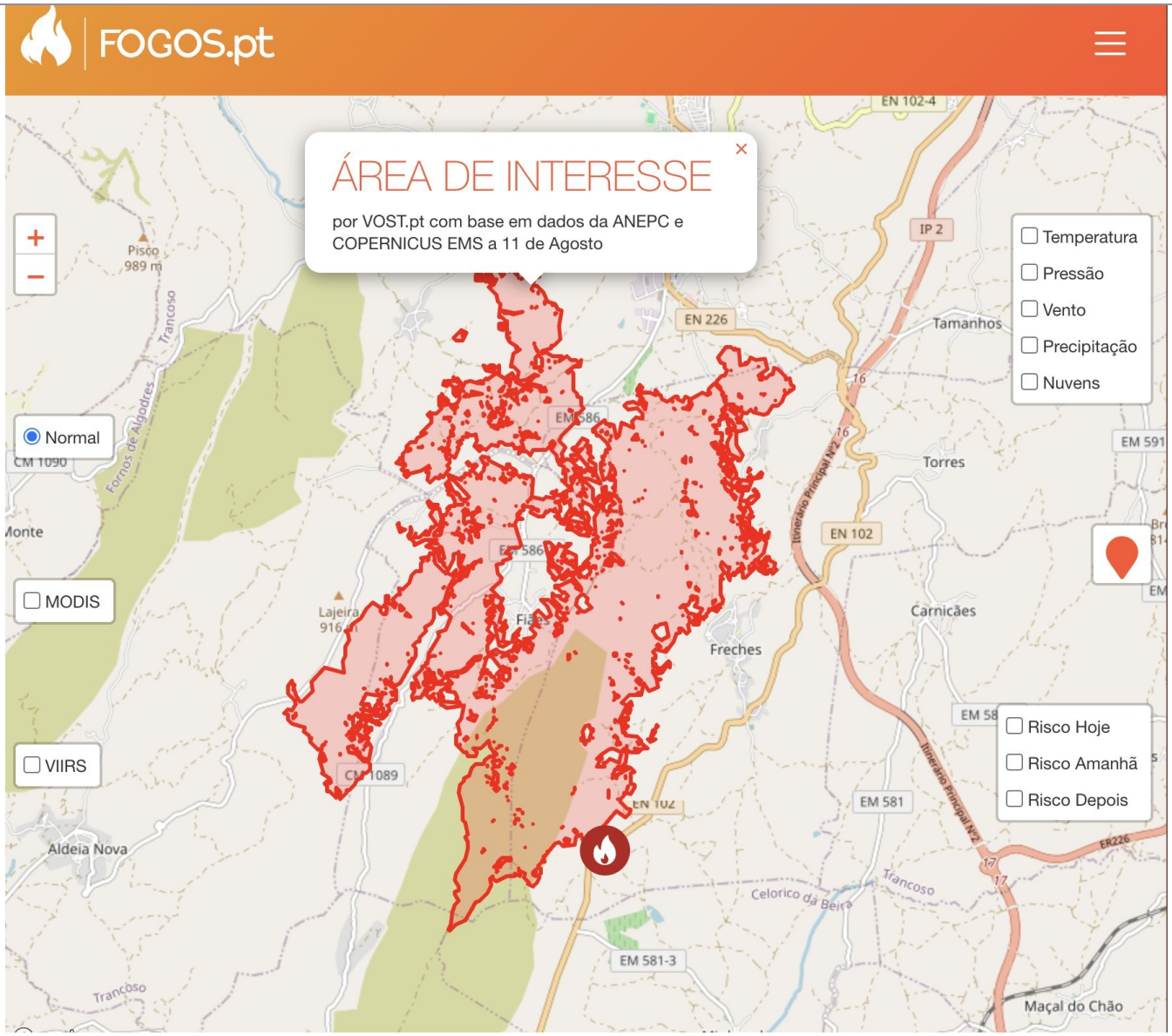
arriving unencrypted (a common sign of proxy-based attacks). The August 1 attack, in contrast, came largely from cloud machines, matching patterns we see from botnets that exploit cloud infrastructure.

These attacks were blocked without disruption. Cloudflare's autonomous mitigation systems kicked in, and email alerts were automatically sent to João and the team. No downtime, no manual intervention required.

The role of Project Galileo: traffic surges

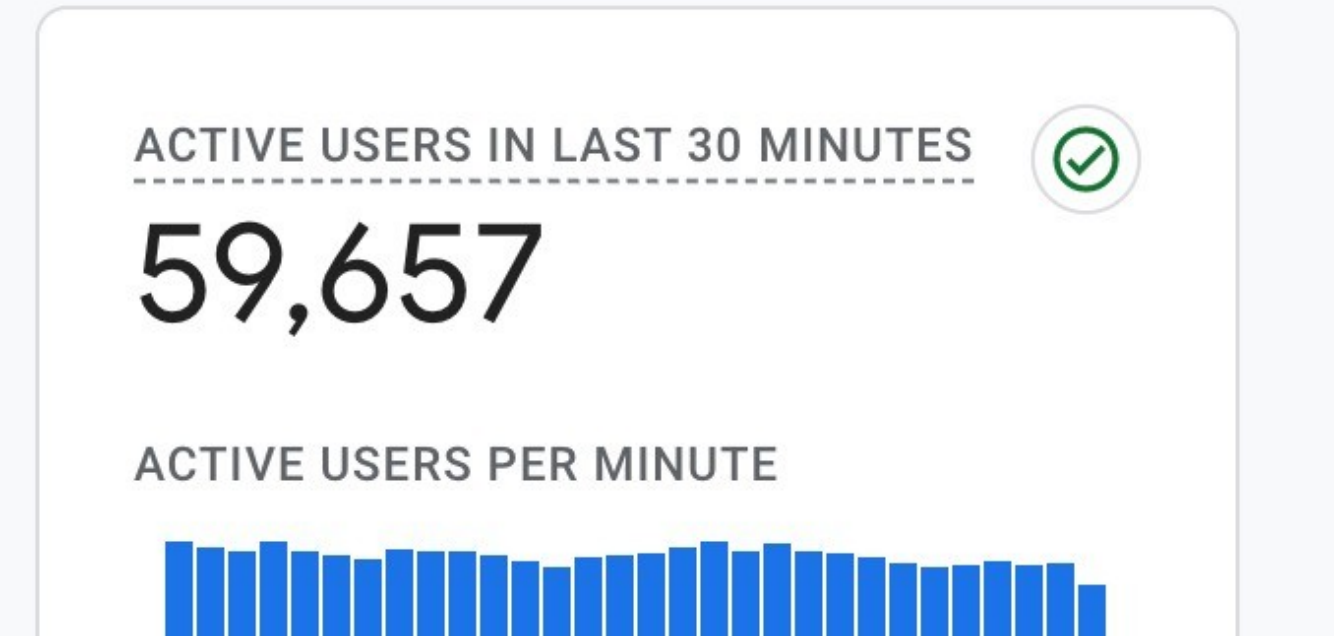
Fogos.pt has used Cloudflare's free services since the beginning, starting with DNS and gradually expanding to DDoS mitigation, caching, rate limiting, and more. The site joined Project Galileo, which protects journalists, human rights defenders, and public service projects, to get stronger, upgraded features and service at no cost.

> *"Without Cloudflare, the site would have gone down many times during fire season," says João Pina. "We use almost every product — but protection against attacks is critical."*

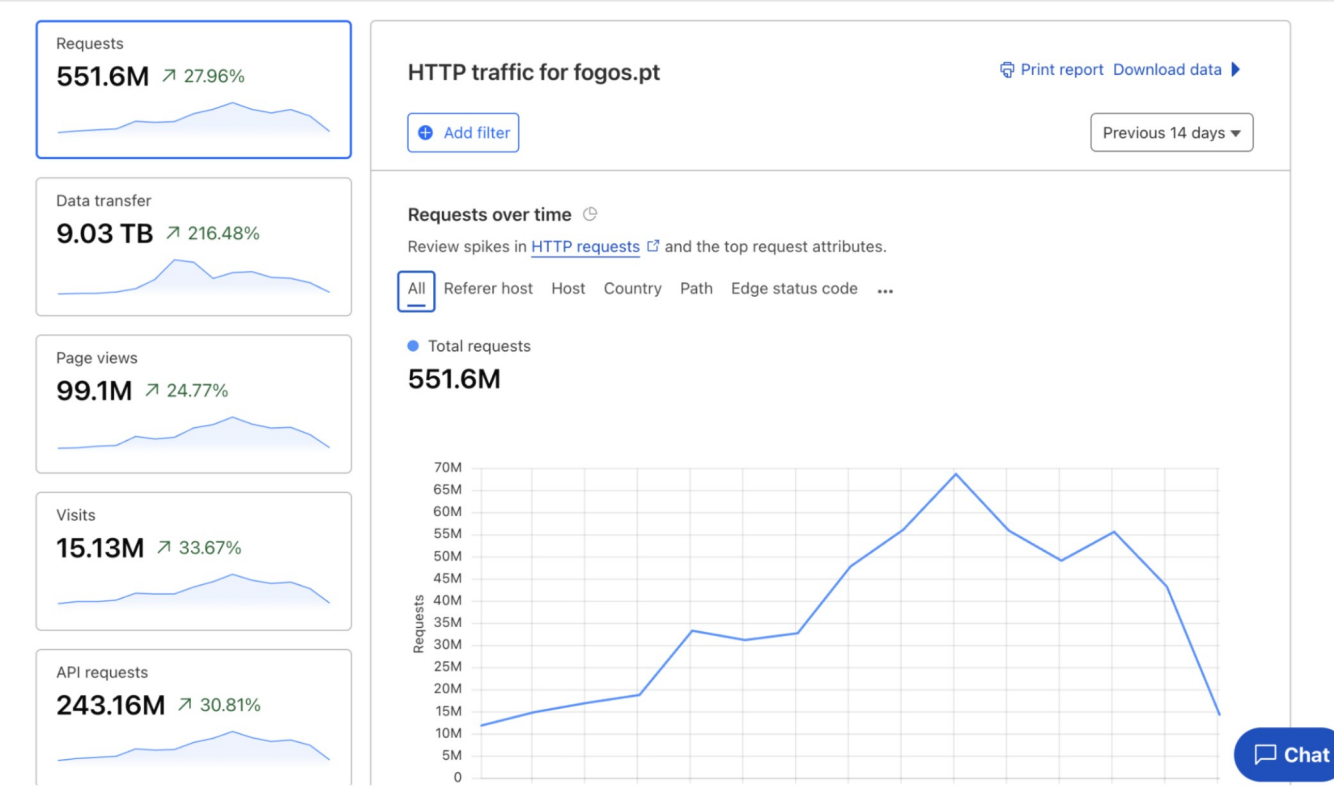


August 11, 2025, detail the area of interest of a wildfire in central Portugal.

Traffic to fogos.pt surges when wildfires hit the news or get mentioned by authorities. These spikes can bring tens of thousands of visitors per day. And as attention grows, so does the risk. Attacks can be used to silence or disrupt critical services, or simply as distractions for more malicious activity. In August 2025, the site often had close to 60,000 people browsing at the same time, with around 40,000 being the norm across the web and app services.



In just two weeks (with an August 15 peak of almost 70 million requests), fogos.pt handled over 550 million requests (more than 25 million per day) 9 TB of data transfer, nearly 100 million page views, 15 million visits, and 240 million API calls. A massive load for a volunteer-run project, as the next screenshot from the fogos.pt team shows:



In a time when timely wildfire updates can mean the difference between safety and danger, keeping the site online is essential.

Built by community, supported by allies

Fogos.pt is a reminder of what's possible when public service meets technology, and why we launched Project Galileo: to protect the digital infrastructure that keeps people informed and safe. Built with no formal funding or full-time team, it runs on volunteers, partners, and a shared sense of purpose, an authenticity that João Pina believes is why it works, and why it matters.

And while this story is about Portugal, wildfires are a global challenge. Other organizations providing critical public services can also apply to join Project Galileo and receive this protection.

From a dinner-table idea by an engineer to critical national infrastructure, fogos.pt shows the Internet at its best. Cloudflare is proud to help protect it.

Discuss on Hacker News

Project Galileo DDoS Trends Radar Consumer Services Portugal

Follow on X

João Tomé | @emot
Cloudflare | @cloudflare

RELATED POSTS

August 14, 2025 11:03 PM

MadeYouReset: An HTTP/2 vulnerability thwarted by Rapid Reset mitigations

A new HTTP/2 denial-of-service (DoS) vulnerability called MadeYouReset was recently disclosed by security researchers. Cloudflare HTTP DDoS mitigation, already protects from MadeYouReset....

By Alex Forster, Noah Maxwell Kennedy, Lucas Pardue, Evan Rittenhouse

Security, Vulnerabilities, Attacks, DDoS

July 22, 2025 2:00 PM

Shutdown season: the Q2 2025 Internet disruption summary

In Q2 2025, we observed Internet disruptions around the world resulting from government-directed shutdowns, power outages, cable damage, a cyberattack, and technical problems....

By David Belson

Radar, Internet Shutdown, Internet Traffic, Consumer Services

July 15, 2025 2:00 PM

Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report

June was the busiest month for DDoS attacks in 2025 Q2, accounting for nearly 38% of all observed activity....

By Omer Yoachimik, Jorge Pacheco

DDoS Reports, DDoS, Connectivity Cloud, DDoS Alerts, Radar, Internet Traffic

July 01, 2025 11:00 AM

From Googlebot to GPTBot: who's crawling your site in 2025

From May 2024 to May 2025, crawler traffic rose 18%, with GPTBot growing 305% and Googlebot 96%....

By João Tomé, Jorge Pacheco, Carlos Azevedo

Pay Per Crawl, AI, Radar, AI Bots, Bots