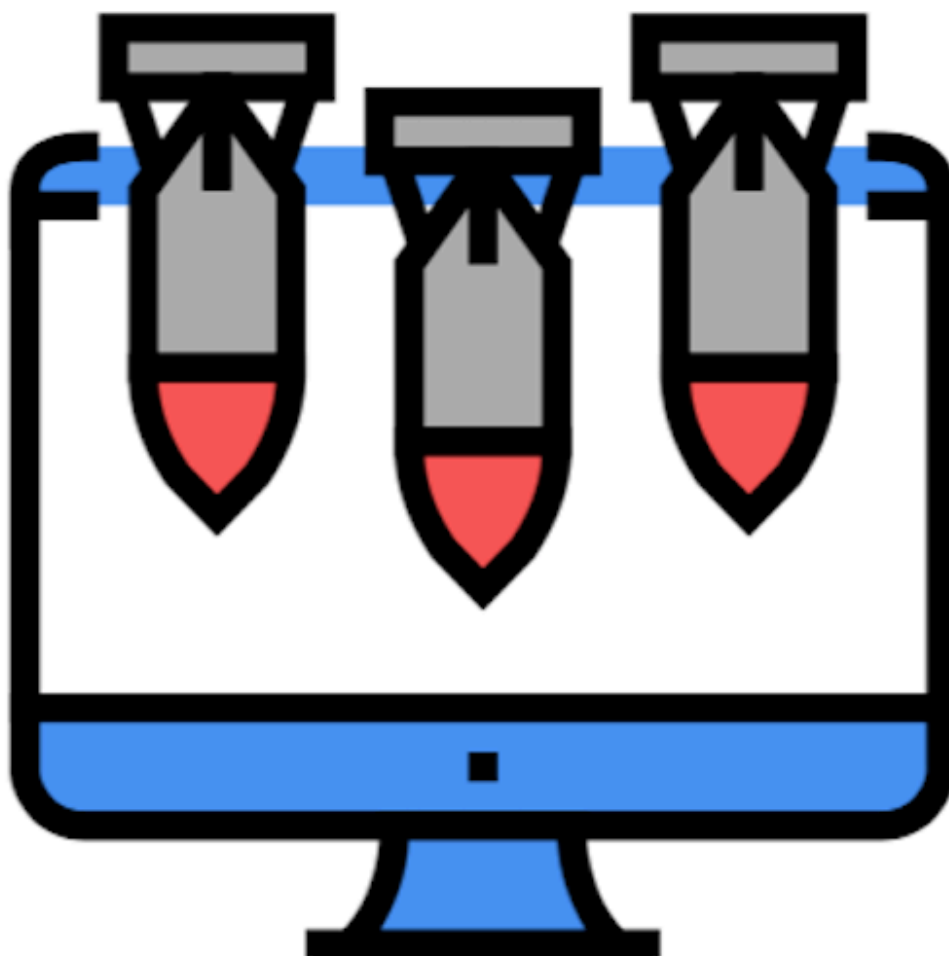


KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS

Published: 2025-05-20 · Archived: 2026-04-05 16:14:47 UTC

KrebsOnSecurity last week was hit by a near record distributed denial-of-service (DDoS) attack that clocked in at more than 6.3 terabits of data per second (a terabit is one trillion bits of data). The brief attack appears to have been a test run for a massive new Internet of Things (IoT) botnet capable of launching crippling digital assaults that few web destinations can withstand. Read on for more about the botnet, the attack, and the apparent creator of this global menace.



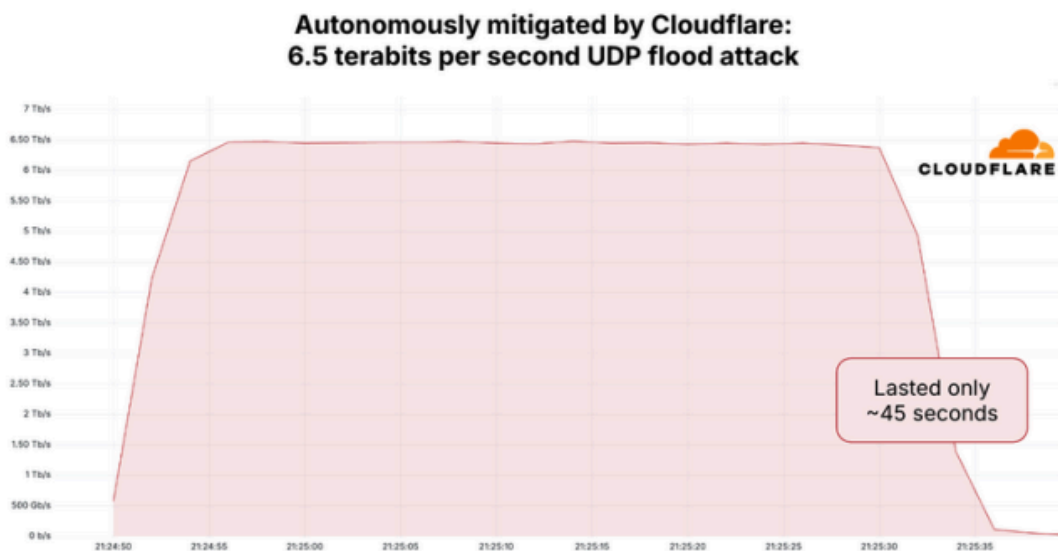
For reference, the 6.3 Tbps attack last week was ten times the size of the assault launched against this site in 2016 by the **Mirai** IoT botnet, which [held KrebsOnSecurity offline for nearly four days](#). The 2016 assault was so large that **Akamai** – which was providing pro-bono DDoS protection for KrebsOnSecurity at the time — asked me to leave their service because the attack was causing problems for their paying customers.

Since the Mirai attack, KrebsOnSecurity.com has been behind the protection of **Project Shield**, a free DDoS defense service that **Google** provides to websites offering news, human rights, and election-related content.

Google Security Engineer **Damian Menscher** told KrebsOnSecurity the May 12 attack was the largest Google has ever handled. In terms of sheer size, it is second only to a very similar attack that **Cloudflare** mitigated and [wrote about in April](#).

After comparing notes with Cloudflare, Menscher said the botnet that launched both attacks bears the fingerprints of **Aisuru**, a digital siege machine that first surfaced less than a year ago. Menscher said the attack on KrebsOnSecurity lasted less than a minute, hurling [large UDP data packets](#) at random ports *at a rate of approximately 585 million data packets per second*.

“It was the type of attack normally designed to overwhelm network links,” Menscher said, referring to the throughput connections between and among various Internet service providers (ISPs). “For most companies, this size of attack would kill them.”



A graph depicting the 6.5 Tbps attack mitigated by Cloudflare in April 2025. Image: Cloudflare.

The Aisuru botnet comprises a globally-dispersed collection of hacked IoT devices, including routers, digital video recorders and other systems that are commandeered via default passwords or software vulnerabilities. As [documented](#) by researchers at **QiAnXin XLab**, the botnet was first identified in an August 2024 attack on a large gaming platform.

Aisuru reportedly went quiet after that exposure, only to reappear in November with even more firepower and software exploits. In a [January 2025 report](#), XLab found the new and improved Aisuru (a.k.a. “**Airashi**”) had incorporated a previously unknown zero-day vulnerability in Cambium Networks cnPilot routers.

NOT FORKING AROUND

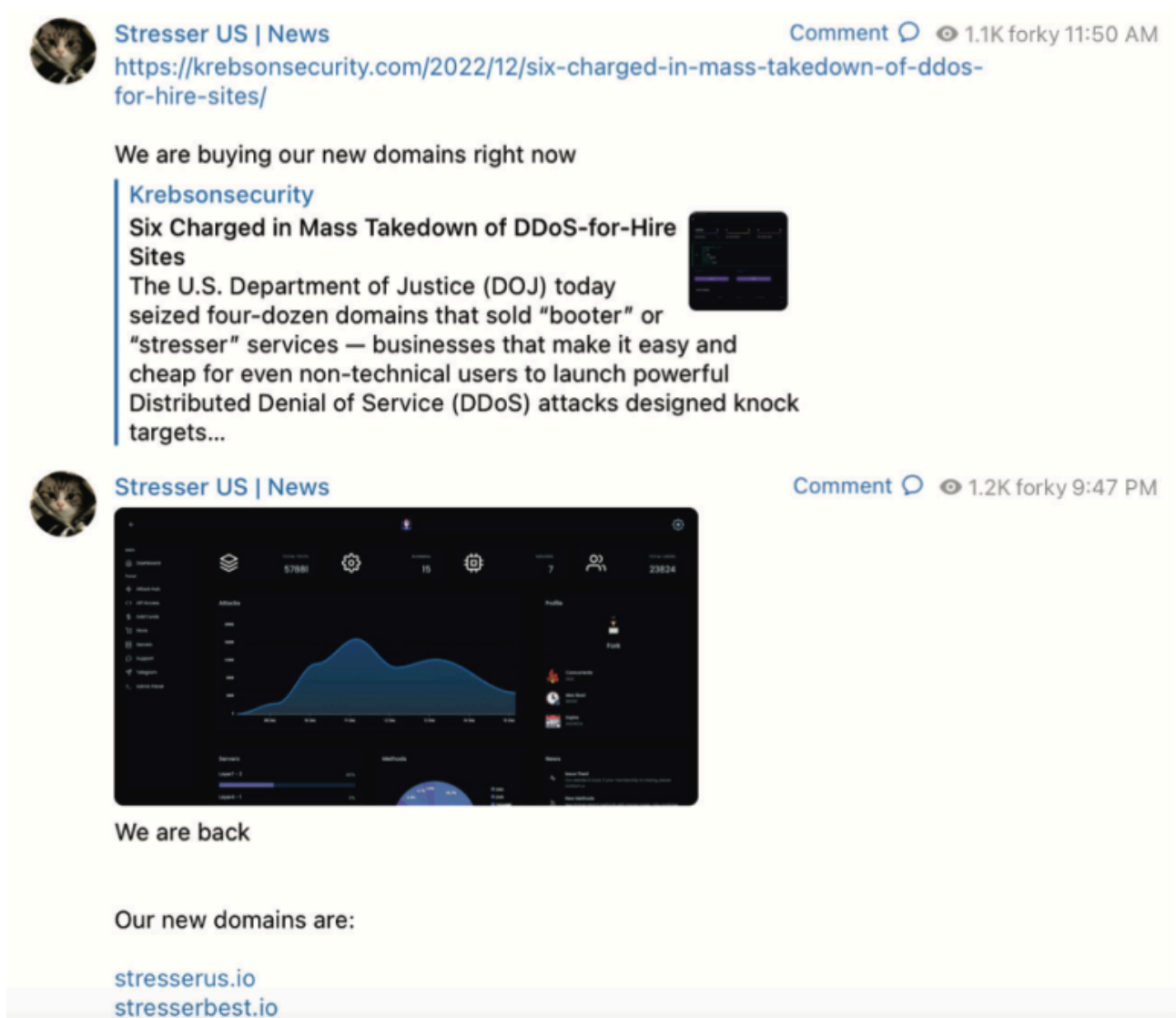
The people behind the Aisuru botnet have been peddling access to their DDoS machine in public **Telegram** chat channels that are closely monitored by multiple security firms. In August 2024, the botnet was rented out in subscription tiers ranging from \$150 per day to \$600 per week, offering attacks of up to two terabits per second.

“You may not attack any measurement walls, healthcare facilities, schools or government sites,” read a notice posted on Telegram by the Aisuru botnet owners in August 2024.

Interested parties were told to contact the Telegram handle “@yfork” to purchase a subscription. The account @yfork previously used the nickname “Forky,” an identity that has been posting to public DDoS-focused Telegram channels since 2021.

According to the FBI, Forky’s DDoS-for-hire domains have been seized in multiple law enforcement operations over the years. Last year, Forky said on Telegram he was selling the domain **stresser[.]best**, which saw its servers seized by the FBI in 2022 as part of an ongoing international law enforcement effort aimed at diminishing the supply of and demand for DDoS-for-hire services.

“The operator of this service, who calls himself ‘Forky,’ operates a Telegram channel to advertise features and communicate with current and prospective DDoS customers,” reads [an FBI seizure warrant](#) (PDF) issued for stresser[.]best. The FBI warrant stated that on the same day the seizures were announced, Forky posted [a link to a story on this blog](#) that detailed the domain seizure operation, adding the comment, “We are buying our new domains right now.”



A screenshot from the FBI’s seizure warrant for Forky’s DDoS-for-hire domains shows Forky announcing the resurrection of their service at new domains.

Approximately ten hours later, Forky posted again, including a screenshot of the stresser[.]best user dashboard, instructing customers to use their saved passwords for the old website on the new one.

A review of Forky’s posts to public Telegram channels — as indexed by the cyber intelligence firms **Unit 221B** and **Flashpoint** — reveals a 21-year-old individual who claims to reside in Brazil [full disclosure: Flashpoint is currently an advertiser on this blog].

Since late 2022, Forky’s posts have frequently promoted a DDoS mitigation company and ISP that he operates called **botshield[.]jio**. The Botshield website is connected to a business entity registered in the United Kingdom called [Botshield LTD](#), which lists a 21-year-old woman from Sao Paulo, Brazil as the director. Internet routing records indicate Botshield ([AS213613](#)) currently controls several hundred Internet addresses that were allocated to the company earlier this year.

Domaintools.com reports that botshield[.]jio was registered in July 2022 to a **Kaike Southier Leite** in Sao Paulo. A [LinkedIn profile](#) by the same name says this individual is a network specialist from Brazil who works in “the planning and implementation of robust network infrastructures, with a focus on security, DDoS mitigation, colocation and cloud server services.”

MEET FORKY



Image: Jaclyn Vernace / Shutterstock.com.

In his posts to public Telegram chat channels, Forky has hardly attempted to conceal his whereabouts or identity. In countless chat conversations indexed by Unit 221B, Forky could be seen talking about everyday life in Brazil, often remarking on the extremely low or high prices in Brazil for a range of goods, from computer and networking gear to narcotics and food.

Reached via Telegram, Forky claimed he was “not involved in this type of illegal actions for years now,” and that the project had been taken over by other unspecified developers. Forky initially told KrebsOnSecurity he had been out of the botnet scene for years, only to concede this wasn’t true when presented with public posts on Telegram from late last year that clearly showed otherwise.

Forky denied being involved in the attack on KrebsOnSecurity, but acknowledged that he helped to develop and market the Aisuru botnet. Forky claims he is now merely a staff member for the Aisuru botnet team, and that he stopped running the botnet roughly two months ago after starting a family. Forky also said the woman named as director of Botshield is related to him.

Forky offered equivocal, evasive responses to a number of questions about the Aisuru botnet and his business endeavors. But on one point he was crystal clear:

“I have zero fear about you, the FBI, or Interpol,” Forky said, asserting that he is now almost entirely focused on their hosting business — Botshield.

Forky declined to discuss the makeup of his ISP’s clientele, or to clarify whether Botshield was more of a hosting provider or a DDoS mitigation firm. However, Forky has posted on Telegram about Botshield successfully mitigating large DDoS attacks launched against other DDoS-for-hire services.

DomainTools finds the same Sao Paulo street address in the registration records for botshield[.]io was used to register several other domains, including **cant-mitigate[.]jus**. The email address in the WHOIS records for that domain is forkcontato@gmail.com, which DomainTools says was used to register the domain for the now-defunct DDoS-for-hire service **stresser[.]jus**, one of the domains seized in [the FBI’s 2023 crackdown](#).

On May 8, 2023, the **U.S. Department of Justice** [announced](#) the seizure of stresser[.]jus, along with a dozen other domains offering DDoS services. The DOJ said ten of the 13 domains were reincarnations of services that were seized during a [prior sweep in December](#), which targeted 48 top stresser services (also known as “booters”).

Forky claimed he could find out who attacked my site with Aisuru. But when pressed a day later on the question, Forky said he’d come up empty-handed.

“I tried to ask around, all the big guys are not retarded enough to attack you,” Forky explained in an interview on Telegram. “I didn’t have anything to do with it. But you are welcome to write the story and try to put the blame on me.”

THE GHOST OF MIRAI

The 6.3 Tbps attack last week caused no visible disruption to this site, in part because it was so brief — lasting approximately 45 seconds. DDoS attacks of such magnitude and brevity typically are produced when botnet operators wish to test or demonstrate their firepower for the benefit of potential buyers. Indeed, Google’s

Menscher said it is likely that both the May 12 attack and the slightly larger 6.5 Tbps attack against Cloudflare last month were simply tests of the same botnet's capabilities.

In many ways, the threat posed by the Aisuru/Airashi botnet is reminiscent of Mirai, an innovative IoT malware strain that emerged in the summer of 2016 and successfully out-competed virtually all other IoT malware strains in existence at the time.

As first revealed by KrebsOnSecurity in January 2017, the Mirai authors were [two U.S. men who co-ran a DDoS mitigation service](#) — even as they were selling far more lucrative DDoS-for-hire services using the most powerful botnet on the planet.

Less than a week after the Mirai botnet was used in a days-long DDoS against KrebsOnSecurity, the Mirai authors [published the source code to their botnet](#) so that they would not be the only ones in possession of it in the event of their arrest by federal investigators.

Ironically, the leaking of the Mirai source is precisely what led to the eventual unmasking and arrest of the Mirai authors, who went on to serve probation sentences that [required them to consult with FBI investigators on DDoS investigations](#). But that leak also rapidly led to the creation of dozens of Mirai botnet clones, many of which were harnessed to fuel their own powerful DDoS-for-hire services.

Menscher told KrebsOnSecurity that as counterintuitive as it may sound, the Internet as a whole would probably be better off if the source code for Aisuru became public knowledge. After all, he said, the people behind Aisuru are in constant competition with other IoT botnet operators who are all striving to commandeer a finite number of vulnerable IoT devices globally.

Such a development would almost certainly cause a proliferation of Aisuru botnet clones, he said, but at least then the overall firepower from each individual botnet would be greatly diminished — or at least within range of the mitigation capabilities of most DDoS protection providers.

Barring a source code leak, Menscher said, it would be nice if someone published the full list of software exploits being used by the Aisuru operators to grow their botnet so quickly.

“Part of the reason Mirai was so dangerous was that it effectively took out competing botnets,” he said. “This attack somehow managed to compromise all these boxes that nobody else knows about. Ideally, we’d want to see that fragmented out, so that no [individual botnet operator] controls too much.”

Source: <https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/>