Killnet and AnonymousSudan DDoS attack Australian university websites, and threaten more attacks — here's what to do about it

2023-03-29

Patrick R. Donahue

Ben Munroe

3 min read

This post is also available in 简体中文, Français, Deutsch, 日本語, 한국어, Español and 繁體中文.

Over the past 24 hours, Cloudflare has observed HTTP DDoS attacks targeting university websites in Australia. Universities were the first of several groups publicly targeted by the pro-Russian hacker group Killnet and their affiliate AnonymousSudan, as revealed in a recent Telegram post. The threat actors

called for additional attacks against 8 universities, 10 airports, and 8 hospital websites in Australia beginning on Tuesday, March 28.

Killnet is a loosely formed group of individuals who collaborate via Telegram. Their Telegram channels provide a space for pro-Russian sympathizers to volunteer their expertise by participating in cyberattacks against western interests.

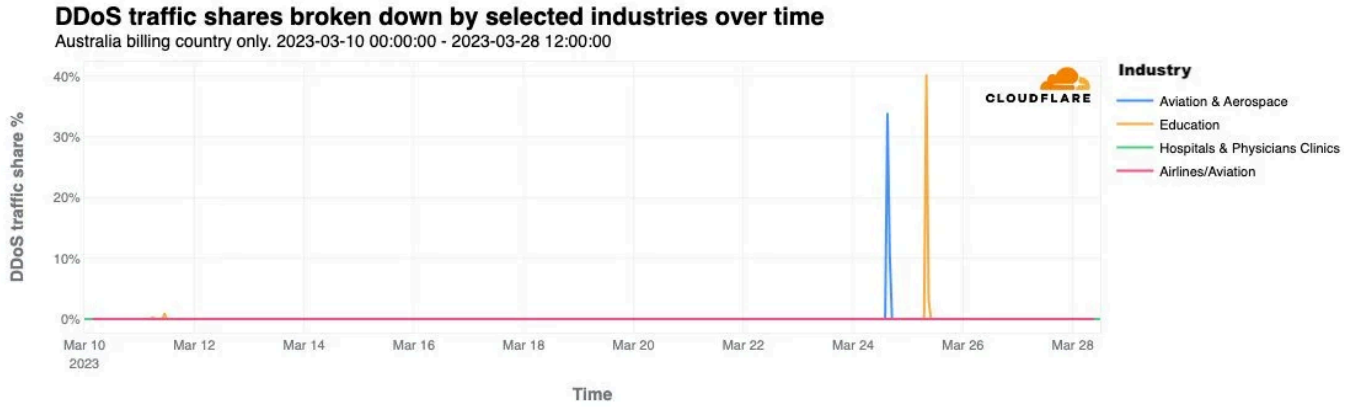

Figure: % of traffic constituting DDoS attacks for organizations in Australia

This is not the first time Cloudflare has reported on Killnet activity. On February 2, 2023 we noted in a blog that a pro-Russian hacktivist group — claiming to be part of Killnet — was targeting multiple healthcare organizations in the US. In October 2022, Killnet called to attack US airport websites, and attacked the US Treasury the following month.

As seen with past attacks from this group, these most recent attacks do not seem to be originating from a single botnet, and the attack methods and sources seem to vary, suggesting the involvement of multiple individual threat actors with varying degrees of skill.

DDoS (Distributed Denial of Service) attacks often make headlines due to their ability to disrupt critical services. Cloudflare recently announced that it had blocked the largest attack to date, which peaked at 71 million requests per second (rps) and was 54% higher than the previous record attack from June 2022.

DDoS attacks are designed to overwhelm networks with massive amounts of malicious traffic, and when executed correctly, can disrupt service or take networks offline. The size, sophistication, and frequency of attacks have been increasing over the past months.

What is Killnet and AnonymousSudan?

Killnet is not a traditional hacking group: it does not have membership, it does not have tools or infrastructure, and it does not operate for financial gain. Instead, Killnet is a space for pro-Russian "hacktivist" sympathizers to volunteer their expertise by participating in cyberattacks against western interests. This collaboration happens entirely in the open via Telegram, where anyone is welcome to join.

Killnet was formed shortly after (and likely in response to) the IT Army of Ukraine, and it emulates their tactics. Most days, administrators of the Killnet telegram channel will put out a call for volunteers to attack some particular target. Participants share many different tools and techniques for launching successful attacks, and inexperienced individuals are often coached on how to launch cyber attacks by those who are more experienced.

AnonymousSudan is another nontraditional hacking group similar to Killnet who is ostensibly composed of Sudanese "hacktivists". The two groups have recently begun collaborating to attack various western interests.

Attackers, including from these groups, are becoming more audacious in the size and scale of the organizations they are targeting. What this means for businesses, especially those with limited cyber resources, is an increasing threat level against vulnerable networks.

Organizations of all sizes need to be prepared for the eventuality of a significant DDoS attack against their networks. Detection and mitigation of attacks should ideally be automated as much as possible, because relying solely on humans to mitigate in real time puts attackers in the driver's seat.

How should I protect my organization against DDoS?

Cloudflare customers are protected against DDoS attacks; our systems have been automatically detecting and mitigating the attack. Our team continues to monitor the situation and will deploy countermeasures as needed.

As an additional step of precaution, customers in the Education, Travel, and Healthcare industries are advised to follow the below recommendations.

1. Ensure all other DDoS Managed Rules are set to default settings (High sensitivity level and mitigation actions).
2. Enterprise customers with Advanced DDoS should consider enabling Adaptive DDoS Protection.
3. Deploy firewall rules and rate-limiting rules to enforce a combined positive and negative security model. Reduce the traffic allowed to your website based on your known usage.
4. Turn on Bot Fight Mode or the equivalent level (SBFM, Enterprise Bot Management) available to you.
5. Ensure your origin is not exposed to the public Internet, i.e., only enable access to Cloudflare IP addresses.
6. Enable caching as much as possible to reduce the strain on your origin servers, and when using Workers, avoid overwhelming your origin server with more subrequests than necessary
7. Enable DDoS alerting.

As easy as it has become for the attackers to launch DDoS attacks, we want to make sure that it is even easier - and free - for defenders of organizations of all sizes to protect themselves against DDoS attacks of all types. We've been providing unmetered and unlimited DDoS protection for free to all of our

customers since 2017. Cloudflare's mission is to help build a better Internet. A better Internet is one that is more secure, faster, and reliable for everyone - even in the face of DDoS attacks.

If you'd like to learn more about key DDoS trends, download the Cloudflare DDoS Threat Report for quarterly insights.

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Discuss on X

Discuss on Hacker News

Discuss on Reddit

Attacks Australia

Follow on X

Patrick R. Donahue | @prdonahue
Ben Munroe | @munrolo
Cloudflare | @cloudflare

RELATED POSTS

October 02, 2024 10:30 PM

How Cloudflare auto-mitigated world record 3.8 Tbps DDoS attack

Over the past couple of weeks, Cloudflare's DDoS protection systems have automatically and successfully mitigated multiple hyper-volumetric L3/4 DDoS attacks exceeding 3 billion packets per second (Bpps). Our systems also automatically mitigated multiple attacks exceeding 3 terabits per second (Tbps), with the largest ones exceeding 3.65 Tbps. The scale of these attacks is unprecedented....

By Manish Arora, Shawn Bohrer, Omer Yoachimik, Cody Doucette, Alex Forster, Nick Wood

DDoS, Attacks, Trends, Security

September 27, 2024 10:30 PM

Network trends and natural language: Cloudflare Radar's new Data Explorer & AI Assistant

The Cloudflare Radar Data Explorer provides a simple Web-based interface to build more complex API queries, including comparisons and filters, and visualize the results. The accompanying AI Assistant translates a user's natural language statements or questions into the appropriate Radar API calls....

By David Belson, Sabina Zejnilovic

Birthday Week, Internet Quality, Attacks, Internet Traffic, Insights, Cloudflare Radar, Trends

July 09, 2024 10:30 PM

DDoS threat report for 2024 Q2

Welcome to the 18th edition of the Cloudflare DDoS Threat Report. Released quarterly, these reports provide an in-depth analysis of the DDoS threat landscape as observed

across the Cloudflare network. This edition focuses on the second quarter of 2024...

By Omer Yoachimik, Jorge Pacheco

DDoS Reports, Cloudflare Radar, Attacks, DNS Flood, Trends, SYN Flood, Ransom Attacks

July 09, 2024 1:22 AM

French elections: political cyber attacks and Internet traffic shifts

Check the dynamics of the 2024 French legislative elections, the surprising election results' impact on Internet traffic changes, and the cyber attacks targeting political parties...

By João Tomé

Elections, Cloudflare Radar, France, Internet Traffic, Trends, Election Security, DDoS, Attacks