What is Anonymous Sudan?

Anonymous Sudan is a hacker group that has launched DDoS attacks against western organizations and governments. Learn how they operate and how to protect your organization from DDoS attacks.

Copy article link

What is Anonymous Sudan?

Anonymous Sudan is a hacker group that has participated in a variety of distributed denial-of-service (DDoS) attacks against targets in Sweden, Denmark, America, Australia, and other countries since early 2023. While the group claims to be based in Sudan and has been known to target so-called "anti-Muslim activity," its actual origins are unclear, with threat researchers identifying possible logistical and ideological links to Russia.

Anonymous Sudan has used public warnings and other forms of propaganda to attract widespread attention. With that said, the group is only the latest of many to employ DDoS attacks, and organizations can protect themselves following a standard set of DDoS mitigation best practices.

What are Anonymous Sudan's origins and goals?

As mentioned, Anonymous Sudan's origins and motives are so far unclear.

The group claims to be a group of Sudanese grassroots hacktivists who target countries and organizations engaging in self-described "anti-Muslim activity." Examples of such attacks include the following:

- Starting in February of 2023, Anonymous Sudan attacked a number of websites in Sweden and Denmark, purportedly in response to a Swedish and Danish far-right activist who publicly burned a copy of the Quran
- In April of 2023, the group attacked a number of Israeli websites, purportedly due to the Israeli military's activity in Palestine
- In July of 2023, the group attacked the fan-fiction website AO3, purportedly due to religious objections to the website's content

However, Anonymous Sudan has also collaborated with pro-Russian attack groups like Killnet to attack organizations for other reasons. Examples of such activity include the following:

- In March of 2023, Anonymous Sudan and Killnet attacked a series of Australian universities, hospitals, and airports
- In June of 2023, Anonymous Sudan, Killnet, and the attack group ReVIL threatened to attack critical banking infrastructure for reasons related to the Russia/Ukraine war

For these reasons — along with signals like the languages Anonymous Sudan communicates in and the attack infrastructure they have used — some threat researchers believe the group originates from or is supported by Russia.

Efforts to learn more about the group's origins and motives are still ongoing. At times, the purported reasons for Anonymous Sudan's attacks remain unclear, as was the case with their March 2024 attacks on the French government.

Note: While Anonymous Sudan shares a name with the longstanding attack group Anonymous, the latter claims to have no connections to the former.

What attack tactics does Anonymous Sudan employ?

Anonymous Sudan primarily uses DDoS attacks, which flood an organization's website and/or web infrastructure with floods of malicious traffic. Without proper protection in place, too much DDoS traffic can overwhelm a website's ability to respond to legitimate requests, leaving actual users unable to access it.

Anonymous Sudan has employed a variety of attack tactics since its emergence in early 2023. Several repeating patterns include these:

- **Launching HTTP attacks.** They have sent floods of HTTP traffic specifically designed to overwhelm targeted infrastructure

- **Using paid infrastructure.** Unlike many other attack groups, research indicates that Anonymous Sudan does not use a botnet of infected personal and IoT devices to conduct attacks. Rather, the group has used a cluster of rented servers — which can output more traffic than personal devices — to launch attacks. The fact that Anonymous Sudan has the financial resources to rent these servers is another reason some researchers believe the group are not the grassroots hacktivists they claim to be

- **Making threats via public announcements and propaganda.** Anonymous Sudan often threatens targets in advance of actual attacks, and sometimes makes threats that are never borne out. Likely reasons for doing so include gaining attention for their ideological motives and sowing uncertainty amongst potential targets

How can organizations protect themselves from DDoS attacks like those launched by Anonymous Sudan?

DDoS mitigation is the practice of protecting websites and web infrastructure from DDoS attacks. Organizations can help protect themselves from large DDoS attacks — including those launched by Anonymous Sudan — with best practices like these:

- **Use dedicated, always-on DDoS mitigation.** A DDoS mitigation service uses a large bandwidth capacity, continuous analysis of network traffic, and customizable policy changes to absorb DDoS traffic and prevent it from reaching a targeted infrastructure. Organizations should ensure they have DDoS protection for Layer 7 traffic, Layer 3 traffic, and DNS

- **Use a web application firewall (WAF).** A WAF uses customizable policies to filter, inspect, and block malicious HTTP traffic between web applications and the Internet

- **Configure rate limiting.** Rate limiting restricts volumes of network traffic over a specific time period, essentially preventing web servers from getting overwhelmed by requests from specific IP addresses

- **Cache content on a CDN.** A cache stores copies of requested content and serves them in place of an origin server. Caching resources on a content delivery network (CDN) can reduce the strain on an organization’s servers during a DDoS attack

- **Establish internal processes for responding to attacks.** This includes understanding existing security protection and capabilities, identifying unnecessary attack surfaces, analyzing logs to look for attack patterns, and having processes in place for where to look and what to do when an attack begins

Learn about DDoS mitigation strategies in more detail.

How Cloudflare can help

Cloudflare offers Layer 3-7 DDoS protection that helps organizations monitor, prevent, and mitigate attacks before they reach targeted applications, networks, and infrastructure. Cloudflare also offers a WAF, along with other critical services for secure application delivery.

Learn more about Cloudflare's application and network layer DDoS mitigation services. And if your organization is under an active attack, visit our Under Attack page for prompt diagnosis and support.

Getting Started

Free plans

For enterprises

Compare plans

Request a demo

Contact sales

About DDoS attacks

DDoS attacks

DDoS attack tools

DDoS glossary

Learning Center navigation