



**| Flash |**

# Anonymous Sudan Increases Attack Tempo

F-2023-11-15a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Israel-Hamas War

**November 15, 2023**

**Scope Note:** ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on November 15, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

## | Flash | Anonymous Sudan Increases Attack Tempo

### › Key Findings

- Threat group Anonymous Sudan has increased its attack frequency throughout Q3 and Q4 2023, targeting a wide array of organizations—the majority of which are based in, or associated with, the United States, Europe, or Israel.
- The group specializes in distributed denial-of-service (DDoS) attacks, usually against user-facing services such as applications and webpages. Although the duration of downtime is usually short, there is a risk of operational disruption, reputational damage, or financial implications.
- Anonymous Sudan's recent increase in attack tempo is likely tied to the ongoing Israel-Hamas War and the perceived stances taken by Western entities. Throughout 2023, Anonymous Sudan has repeatedly pledged support for Gaza and threatened organizations perceived to hold a pro-Israel bias.
- The group is very likely to continue this increased tempo over the short to medium term, with a roughly even chance that the severity will increase as a result of obtaining additional resources or collaborating with other threat groups with aligned agendas.

## **Details**

ZeroFox Intelligence has observed an increased frequency of attacks associated with cyber threat group Anonymous Sudan (also tracked as Storm-1359) during Q3 and Q4 2023. Since approximately Q2 2023, the group has been primarily associated with disruptive DDoS attacks.<sup>1</sup> Anonymous Sudan is almost certainly politically and religiously motivated, with the majority of its victims being based in the United States, Europe, or Israel and often representative of values and activity likely perceived as associated with the West.

- The group claims to operate in the furthering of an Islamic agenda and in the interests of both Sudan and Gaza, though it has displayed techniques, tactics, and procedures (TTPs) that are indicative of logistical and ideological affiliations with Russia. This includes the use of messaging platform Telegram, which is often used by Russia-based cyber threat collectives. The group has also operated in affiliation with other Russian disruption and ransomware groups such as Killnet, Skynet, and REvil.<sup>2</sup>

Over several days beginning on November 8, 2023, the group targeted various services operated by American Artificial Intelligence (AI) company Open AI, such as Chat GPT and the company's Application Programming Interface (API), with periodic DDoS attacks.<sup>3,4</sup> Anonymous Sudan has since claimed responsibility by posting subsequent, inflammatory statements to its Telegram channel.<sup>5</sup> The group claimed to have targeted Open AI due to the company's perceived stance on the ongoing Israel-Hamas War, citing its "general biases toward Israel and against Palestine", the use of AI tools by Israeli intelligence agencies, and the fact that Open AI is an American entity.<sup>6</sup>

---

<sup>1</sup> [hXXps://www.cloudflare\[.\]com/learning/ddos/glossary/anonymous-sudan/](https://www.cloudflare.com/learning/ddos/glossary/anonymous-sudan/)

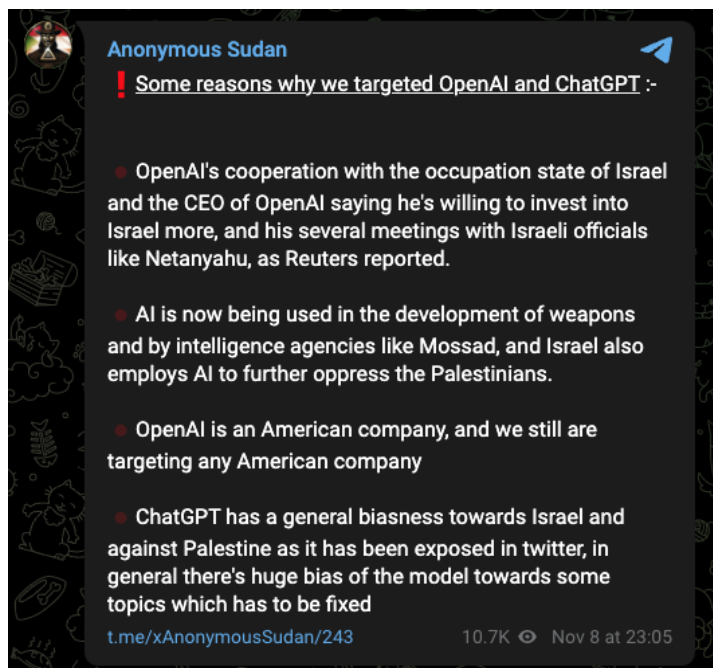
<sup>2</sup> [hXXps://cyberint\[.\]com/blog/research/anonymous-sudan-an-analysis/](https://cyberint[.]com/blog/research/anonymous-sudan-an-analysis/)

<sup>3</sup> [hXXps://status.openai\[.\]com/](https://status.openai[.]com/)

<sup>4</sup> [hXXps://status.openai\[.\]com/incidents/21vl32gvx3hb](https://status.openai[.]com/incidents/21vl32gvx3hb)

<sup>5</sup> [hXXps://t\[.\]me/s/xAnonymousSudan](https://t[.]me/s/xAnonymousSudan)

<sup>6</sup> [hXXps://t\[.\]me/xAnonymousSudan/243](https://t[.]me/xAnonymousSudan/243)



## Screenshot of post on the Anonymous Sudan Telegram Channel claiming responsibility for recent Open AI attacks

Source: X (formerly known as Twitter)

- The attack reportedly leveraged Skynet DDoS services, which had recently been updated at the request of Skynet's community—enabling support for attacks targeting network application layers.<sup>78</sup>
- Application layers are particularly vulnerable to DDoS attacks due to the presence of insecure application interfaces (APIs), the existence of known software vulnerabilities, and the challenges associated with identifying malicious traffic without affecting legitimate processes.

Anonymous Sudan often releases post-attack statements in public forums, which reveal either outright or subtly hints as to its recent target selections. The group has been associated with a host of prominent DDoS attacks in 2023 so far, the majority of which have taken place since September.

<sup>7</sup>

<sup>78</sup> <https://www.bleepingcomputer.com/news/security/openai-confirms-ddos-attacks-behind-ongoing-chatgpt-ou-tages/>

<sup>8</sup> <https://t.me/xSkynet/235>

- IT service management (ITSM) company Cloudflare, October 2023. A subsequent Telegram post did not directly reveal motivations but indirectly addressed Cloudflare's customers.<sup>9,10</sup>
- Instant messaging application Telegram, September 2023.<sup>11</sup> This was very likely a retaliatory attack following the suspension of Anonymous Sudan's channel, reportedly due to the group's use of bot accounts. Anonymous Sudan had moved its primary forum to X but has since begun posting regularly to Telegram again.<sup>12</sup>
  - Threat actors are increasingly using Telegram for liaising with the public and malicious transactions due to the end-to-end encryption offered in direct communications and the ability to host blogs and forums.
- Streaming service Netflix, September 2023. The attack was reportedly a response to the site's LGBTQ+ content.<sup>13</sup>
- Social media platform X, August 2023. The attack very likely aimed to bring attention to the ongoing war in Sudan, as well as exert pressure on Elon Musk to introduce the satellite internet technology Starlink into the region.<sup>14</sup>
- Scandinavian Airline (SAS), February 2023. The attack targeted the organization's website and mobile app and was reportedly in response to a public burning of a Qur'an by Swedish political activists.<sup>15</sup>

---

<sup>9</sup> [hXXps://t.me/xAnonymousSudan/260](https://t.me/xAnonymousSudan/260)

<sup>10</sup>

[hXXps://www.bleepingcomputer.com/news/technology/cloudflare-website-downed-by-ddos-attack-claimed-by-anonymous-sudan/](https://www.bleepingcomputer.com/news/technology/cloudflare-website-downed-by-ddos-attack-claimed-by-anonymous-sudan/)

<sup>11</sup> [hXXps://www.darkreading.com/attacks-breaches/anonymous-sudan-sets-sights-telegram-ddos-attack](https://www.darkreading.com/attacks-breaches/anonymous-sudan-sets-sights-telegram-ddos-attack)

<sup>12</sup> [hXXps://twitter.com/FalconFeedsio/status/1700338497645871466?s=20](https://twitter.com/FalconFeedsio/status/1700338497645871466?s=20)

<sup>13</sup> [hXXps://www.scmagazine.com/brief/netflix-impacted-by-anonymous-sudan-ddos-attack](https://www.scmagazine.com/brief/netflix-impacted-by-anonymous-sudan-ddos-attack)

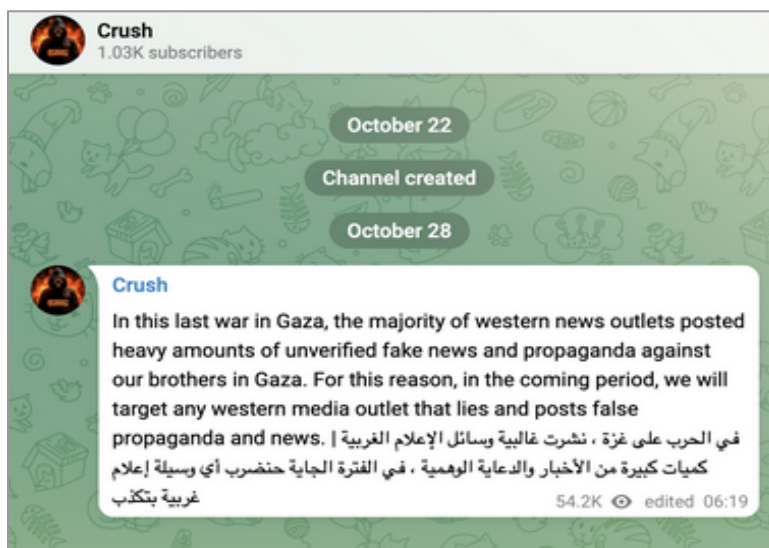
<sup>14</sup> [hXXps://www.scmagazine.com/brief/anonymous-sudan-targets-x](https://www.scmagazine.com/brief/anonymous-sudan-targets-x)

<sup>15</sup>

[hXXps://www.reuters.com/business/aerospace-defense/airline-sas-suffers-cyber-attack-customer-info-leaked-2023-02-14/](https://www.reuters.com/business/aerospace-defense/airline-sas-suffers-cyber-attack-customer-info-leaked-2023-02-14/)

- Other organizations targeted in 2023 include large technology companies such as Microsoft and Apple, as well as organizations that host objectionable or controversial content, such as Reddit, OnlyFans, and Tumblr.<sup>1617</sup>

Anonymous Sudan has also been associated with attacks targeting aspects of the Israeli government, which have likely increased since the start of the ongoing Israeli-Hamas War. Alongside the Russia-Ukraine conflict, this likely contributed to the first publication of Rules of Engagement for civilian hackers involved in conflicts by The International Committee of the Red Cross (ICRC) on October 4, 2023.<sup>1819</sup> Anonymous Sudan and associated collectives such as Killnet have suggested that there will not be adherence to these rules.<sup>20</sup>



**Screenshot of post on the Anonymous Sudan Telegram Channel warning of targeting of Western media outlets**

Source: CyberInt

<sup>16</sup>

[hXXps://www.hivepro\[.\]com/wp-content/uploads/2023/06/STORM-1359-DDoS-triggered-outage-of-Microsoft-Services\\_TA2023269.pdf](https://www.hivepro[.]com/wp-content/uploads/2023/06/STORM-1359-DDoS-triggered-outage-of-Microsoft-Services_TA2023269.pdf)

<sup>17</sup>

[hXXps://techround\[.\]co\[.\]uk/news/anonymous-sudan-targets-twitter-x-in-cyber-attack-to-pressure-elon-musk-over-starlink-launch/](https://techround[.]co[.]uk/news/anonymous-sudan-targets-twitter-x-in-cyber-attack-to-pressure-elon-musk-over-starlink-launch/)

<sup>18</sup> [hXXps://www.politico\[.\]eu/article/israel-hamas-war-hackers-cyberattacks/](https://www.politico[.]eu/article/israel-hamas-war-hackers-cyberattacks/)

<sup>19</sup>

[hXXps://blogs.icrc\[.\]org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-the-m/](https://blogs.icrc[.]org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-the-m/)

<sup>20</sup> [hXXps://www.bbc\[.\]co\[.\]uk/news/technology-66998064](https://www.bbc[.]co[.]uk/news/technology-66998064)

There is a roughly even chance that Anonymous Sudan will continue an increased attack tempo over the coming months. Victims are unlikely to be from any specific country or industry but will very likely be primarily based in Western countries, associated with controversial media content, or theological in nature. The intent of such attacks is likely the undermining of the West and discrediting of prominent, associated organizations.

Victim organizations will very likely be targeted with DDoS attacks that will seek to deny the service of applications and websites. While these attacks will likely be of a relatively low sophistication, they could cause significant short to medium-term disruption, financial loss, and reputational damage. There is a roughly even chance that the severity and sophistication of attacks will increase as a result of obtaining additional resources and collaborating with other threat groups with aligned agendas.

## **| Recommendations**

- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new Anonymous Sudan developments.
- Configure the ZeroFox Intelligence Platform to monitor for current mentions of your organization on Anonymous Sudan's Telegram channels.
- Beware of spikes in traffic, suspicious emails, and/or unauthorized access to the active directory.
- Leverage trusted and comprehensive DDoS mitigation tools and services.

## **| Appendix A: Traffic Light Protocol for Information Dissemination**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## **| Appendix B: ZeroFox Intelligence Probability Scale**

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |