



Brief

Anonymous Sudan Announces Return in Telegram Group

B-2025-03-10a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Threat Groups, Hacktivism, DDoS

March 10, 2025

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 March 10, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Anonymous Sudan Announces Return in Telegram Group

Key Findings

- In January 2025, ZeroFox observed a new Telegram channel claiming to be associated with the hacktivist collective Anonymous Sudan. According to posts made in the channel, the collective has resumed operations under the name “Anonymous Sudan Second Battalion”.
- Statements posted in the channel indicate the resurgence is very likely motivated by an intent to inflict punitive retribution against institutions perceived by the collective as opposed to the political policies of the Russian Federation, Palestinians, and Sudan.
- During January, the collective claimed to have conducted a number of distributed denial-of-service (DDoS) attacks targeting entities located in African nations (primarily Uganda and Libya).
- There is a likely chance that the new Telegram channel is reflective of a legitimate Anonymous Sudan resurgence. In such a case, there is a roughly even chance that the collective will resume the targeting of U.S., Europe, and Israel-based entities in the short to medium term.

In January 2025, ZeroFox observed a new Telegram channel claiming to be associated with the hacktivist collective Anonymous Sudan. According to posts made in the channel, the collective has resumed operations under the name Anonymous Sudan Second Battalion and has already conducted a series of attacks. Statements posted in the channel indicate there is a very likely chance that the resurgence is motivated by an intent to inflict punitive retribution against institutions perceived by the collective as opposed to the political policies of the Russian Federation, Palestinians, and Sudan.

Anonymous Sudan (also tracked as Storm-1359) is a hacktivist group that is almost certainly politically and religiously motivated, and has a history of conducting DDoS attacks against perceived opposition entities. Historically, the majority of the collective's victims have been located in the United States, Europe, or Israel and are often representative of values and activity perceived as associated with the West.

- Anonymous Sudan has historically targeted organizations perceived as displaying support for Israel's role in the Israel-Hamas conflict. In 2024, the collective conducted attacks against organizations such as artificial intelligence (AI) company Open AI, citing its "general biases toward Israel and against Palestine."¹²
- The collective has also conducted attacks against high-profile organizations that are perceived as holding opposing ideological views, including Netflix and Scandinavian Airlines.³⁴
- While claiming to operate in furtherance of an Islamic agenda and in the interests of both Sudan and Gaza, Anonymous Sudan has displayed tactics, techniques, and procedures (TTPs) that are indicative of logistical and ideological affiliations with Russia. This includes the use of messaging platform Telegram, which is often utilized 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.⁵

¹ [hXXps://status.openai\[.\]com/](https://status.openai.com/)

² [hXXps://status.openai\[.\]com/incidents/2lv132gvx3hb](https://status.openai.com/incidents/2lv132gvx3hb)

³ [hXXps://www.scmagazine\[.\]com/brief/netflix-impacted-by-anonymous-sudan-ddos-attack](https://www.scmagazine.com/brief/netflix-impacted-by-anonymous-sudan-ddos-attack)

⁴

[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/)

⁵ [hXXps://cyberint\[.\]com/blog/research/anonymous-sudan-an-analysis/](https://cyberint.com/blog/research/anonymous-sudan-an-analysis/)

- In 2024, Anonymous Sudan revealed in a Telegram post that it had been using "infrashutdown," a DDoS-for-hire service, while confirming its intention to continue using this service for future attacks. The group also claims to have previously leveraged SkyNet DDoS services.⁶

Anonymous Sudan seemingly ceased activity in October 2024, following the reported disruption and indictment of key members referred to as the "Sudanese Brothers" by law enforcement (LE) entities.⁷ The group's existing Telegram channel was also disabled.

- Shortly following the group's recent resurgence announcement, pro-Palestine threat actor group "LulzSec Black" announced an alliance with Anonymous Sudan; this alliance claims to "strengthen online Islamic unity and collaborative cyber efforts."⁸
- ZeroFox also observed mentions of Anonymous Sudan's return in the Telegram channels of several other hacktivist collectives, most of which seemingly prioritize the targeting of Israel-based entities.

Anonymous Sudan claims to have conducted at least 12 DDoS attacks between January 2 and January 17, 2025. All of the alleged listed targets are located in African nations (primarily Uganda and Libya), which the group accuses of having a "disgraceful stance against the Sudanese cause".

- Anonymous Sudan's recently claimed victims include Libya's Ministry of Foreign Affairs, where critical systems and official websites were allegedly compromised.
- The collective also claims to have conducted "espionage attacks" focused on stealing sensitive data in order to disrupt Libya's support of military operations.
- None of Anonymous Sudan's recently announced attacks have targeted entities in the United States, Europe, Israel, or any other regions historically aligned with the collective's targeting patterns. There is a likely chance that this is due in part to an intent to avoid further disruption by Western LE entities, as well as to prioritize seeking retribution against those perceived as being politically opposed to Sudan.

⁶ [hXXps://t\[.\]me/xSkynet/235](https://t.me/xSkynet/235)

⁷

[hXXps://www.justice\[.\]gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals](https://www.justice[.]gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals)

⁸ [hXXps://t\[.\]me/+5tOXpaGX8o8xNDc8](https://t.me/+5tOXpaGX8o8xNDc8)

Anonymous Sudan²

• We successfully targeted several Libyan institutions involved in supporting militias in Sudan through a series of precise and calculated operations. Additionally, we executed a long-range espionage attack, skillfully penetrating systems to collect sensitive data and disrupt their activities supporting militias. These operations are part of a broader series of undisclosed missions, with many previous successful actions remaining confidential. Together, these efforts represent a strategic blow aimed at protecting Sudan and enhancing its stability.

• استهدفنا بنجاح العديد من المؤسسات الليبية المتورطة في دعم الميليشيات بالسودان، من خلال سلسلة من العمليات الدقيقة والمدروسة، كما نفذنا هجوماً تجسسياً طويل المدى، اخترقنا خلاله الأنظمة بمهارة فائقة لجمع بيانات حساسة وتعطيل أنشطتهم الداعمة للميليشيات، هذه العمليات تُعد جزءاً من سلسلة أوسع من المهام التي لن يتم الإفصاح عنها، بما في ذلك العديد من العمليات السابقة التي ظلت سرية، تمثل جهودنا مجتمعة ضربة استراتيجية تهدف لحماية السودان وتعزيز استقراره.

#AnonymousSudan

Anonymous Sudan announcing attack on Libyan institutions

Source: Telegram

▼ Immediate Consequences | النتائج المباشرة:

1. Paralysis of Security Operations | شلل العمليات الأمنية
2. Disruption of Critical Public Services | تعطل الخدمات العامة الحيوية
3. Complete Breakdown of Internal Coordination and Emergency Response | انهيار تام في التنسيق الداخلي والاستجابة للطوارئ

🔍 Evidence of Action | أدلة العملية:

- <https://check-host.net/check-report/224e0e3dk524>
- <https://check-host.net/check-report/224e0d5ekfec>
- <https://check-host.net/check-report/224e0b7dk105>
- <https://check-host.net/check-report/224e0b5ake98>

! A Clear Message | رسالة واضحة:

Libya is biased towards the militias and its position towards the Sudanese conflict is shameful. We demand an immediate end to Libya's role in empowering these forces, and a review of its immoral positions towards the Sudanese struggle. Any continuation of this bias will be met with consequences.

! ليبيا منحازة للميليشيات وموقفها مخزي تجاه الصراع السوداني، نطالب بوقف فوري لدور ليبيا في تمكين هذه القوى، وإعادة النظر في مواقفها غير الأخلاقية تجاه كفاح السودان، أي استمرار في هذا الانحياز سيواجه بعواقب.

Anonymous Sudan demands Libya stop empowering militia

Source: Telegram

There is a likely chance that the new Telegram channel is reflective of a legitimate Anonymous Sudan resurgence—particularly given the inclusion of check-host links. However, no further attack claims have been observed within the Telegram channel since January, which is likely indicative of the collective either lacking the resources to maintain a steady attack tempo or being cautious about its target selection. There is also an unlikely chance that the resurgence is a hoax, with the Second Battalion either not being representative of a hacktivist collective or having minimal association with Anonymous Sudan. If the collective is indeed a return of Anonymous Sudan, there is a roughly even chance that it will resume the targeting of U.S., Europe, and Israeli-based entities in the short to medium term.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED 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.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER 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. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR 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%