

OSINT Report

Anonymous Sudan

● Origin

The group emerged in mid-January 2023 in the form of a Telegram channel that presented itself as pro-Islamic hackers. The name was borrowed from the 2019 “Anonymous Sudan” hacking operation; the original Anonymous movement publicly distanced itself from the new group immediately after its emergence.[6]

● Attribution

Assessments by Truesec, Trustwave, Mandiant, and Microsoft indicate possible coordination or links between the group and the pro-Russian hacker environment, particularly Killnet. Microsoft tracks the Anonymous Sudan actor under the identifier Storm-1359 and notes likely links to Killnet and possible support from the Russian Federation. At the same time, the available open-source data is insufficient to conclusively confirm direct organizational subordination to or control by Killnet or Russian state structures.[3]

● Legal Status

On 16 October 2024, the U.S. Department of Justice unsealed a federal grand jury indictment against two Sudanese nationals (the Omer brothers) as the actual operators of the group. The documents classify it as a cybercriminal organization responsible for tens of thousands of DDoS attacks against critical infrastructure, corporate networks, and government institutions in the United States and worldwide. [9]



2. Ideology, Motivation, and Target Selection

2.1. The Group's Stated Ideology

It is based on the protection of the religious interests of Islam, while the selection of targets is justified by actions of the victim country that the group classifies as “anti-Muslim” (public burning of copies of the Quran, support for the State of Israel, participation in military operations against the ISIS group). This formulation is sufficiently broad to retrospectively justify the selection of virtually any target.

2.2. Geopolitical Aspect and Anti-Western Rhetoric

The available behavioral data support the stated ideological motivation only partially. The group systematically ignores documented cases of oppression of Muslim populations in countries that do not belong to the Western bloc, a circumstance that is not characteristic of an authentic religiously motivated movement. Instead, a consistent correlation can be observed between the list of the group's actual targets and the list of states providing support to Ukraine in the context of the Russo-Ukrainian War, namely: Sweden, the Netherlands, Australia, Germany, and, at a later stage, the banking systems of the United States and European Union countries.

1. The Swedish direction particularly clearly demonstrates the intersection of religious and geopolitical motives. The formal pretext for the attacks was Quran-burning demonstrations, but the campaign took place simultaneously with Sweden's NATO accession process. This in itself does not prove that NATO was the group's actual or sole motivation, but it demonstrates that the religious pretext overlapped with an ongoing geopolitical conflict.
2. Anonymous Sudan did not carry out any attacks against Ukraine itself. This may indicate a deliberate reluctance to create the appearance of being pro-Russian and a desire to maintain greater room for maneuver, without making openly pro-Russian positioning a central part of its public identity.
3. Israel requires separate consideration. Unlike the attacks on Sweden or the Netherlands, the religious-political justification here was much more direct: Anonymous Sudan referred to the Palestinian issue, the “occupation of Palestine,” and later participated in attacks timed to coincide with Quds Day. In May 2023, during the escalation in the Gaza Strip, Anonymous Sudan claimed that it had disabled a number of civilian rocket-alert applications (Red Alert, Cumta, Halamish, Evigilo) and attributed to itself a reduction in the effectiveness of Iron Dome interceptions that day. Open-source data from this period do not allow Iranian control of Anonymous Sudan to be conclusively established, but they demonstrate that the group may have operated in an informational and operational environment where Russian, Iranian, and anti-Israeli interests partially overlapped.

At the same time, it is important not to overstate Iran's role. The mere fact that Anonymous Sudan's anti-Israeli campaign coincided with Quds Day or that the group had contact with the Iranian hacktivist environment does not constitute evidence of coordination with the Iranian state. On the contrary, the available data primarily indicate an overlap of narratives, targets, and certain operational activities, while the question of direct coordination remains unresolved.

In this case, religious rhetoric provides a good explanation for some specific campaigns but does not sufficiently explain the full range of targets, so it may have served not only as an ideological justification but also to provide the group with additional credibility and room to define its own political affiliation. At the same time, its affiliation with KillNet and the alignment of a significant portion of its targets with Russian geopolitical interests make the pro-Russian context a significant factor in assessing Anonymous Sudan's activities, although these factors alone do not prove direct Russian control over the group.

2.3. Financial Layer of Motivation

At the very beginning of the group's emergence, there were few signs of commercial motivation, with only a few advertising posts. However, within a year, the picture had changed completely: paid DDoS attacks on demand, ransom demands from victims (ranging from several thousand dollars to a demand for \$3 million from Scandinavian Airlines), and an offer to take down an internet service provider in a selected country for \$500 per hour. Thus, while in February 2023 the motivation appeared predominantly ideological, after March 2024 it shifted toward seeking financial incentives. [4]

2.4. What Does Not Fit the Group's Ideological Motivation

1. Inconsistent target selection that correlates with the Kremlin's geopolitics and, at the same time, with the geopolitical adversaries of Iran (which is an ally of the Russian Federation), rather than with the situation of Muslim communities around the world;
2. The emergence of a price list for services that has no connection to the religious narrative;
3. Willingness to attack targets that directly harm the civilian population (a hospital, an emergency alert service in Israel) — behavior that is poorly aligned with the image of fighters for justice but is well aligned with the logic of a mercenary.[14]
4. Both Reddit and PayPal were targeted, although neither has any connection to anti-Muslim activities.



3. Chronology of Activities

Date	Event
18 January 2023	Creation of the “Anonymous Sudan” Telegram channel; [6]
23 January 2023	Start of DDoS attacks on Swedish and Dutch targets under the pretext of protesting against the burning of the Quran. [2]
19 February 2023	Public affiliation with Killnet — reposting of screenshots in the Killnet channel. [7]
March 2023	Attacks on Australia, Germany, and the Netherlands; Trustwave begins monitoring. [3]
14 June 2023	Joint statement with Killnet and REvil on the “Darknet parliament” and a campaign against the banking systems of the United States and the EU. [4]
June 2023	Large-scale Storm-1359 DDoS campaign against Microsoft services; Microsoft officially linked the activity to Storm-1359. Anonymous Sudan demanded \$1 million to stop the attacks. [5]
July 2023	Attack on PayPal. [8]
October 2023	After 7 October — attack on Israel’s “Red Alert” warning system and The Jerusalem Post as part of the #OpIsrael campaign. [13]
November–December 2023	Attacks on OpenAI/ChatGPT. [8]
March 2024	The FBI, pursuant to a court warrant, seizes and disables key components of the DCAT tool (also known as Godzilla / Skynet / InfraShutdown); effective cessation of the group’s activity, although this was not publicly disclosed for another six months. [10]
16 October 2024	The U.S. Department of Justice unseals the indictment against Ahmed and Alaa Omer. [9]

4. Organizational Structure and External Links

4.1. General Structure

The core of the operation consists of two brothers with a clear division of roles, plus at least three unnamed accomplices who appear anonymously. The infrastructure footprint supports the assessment of substantial funding. As early as February 2023, Truesec identified a cluster of at least 61 paid servers rented from IBM/SoftLayer in Germany, with traffic additionally routed through open proxies to conceal its source. CyberCX later estimated the geographic distribution of the group’s supporting infrastructure at 1,720 autonomous systems across 132 countries — a scale that no small team could afford without external funding. Infrastructure of this level requires substantial financial resources, although the question of “whose money it is” remains open even after charges were brought against specific individuals. [1]

4.2. Leaders of the Group

Ahmed Salah Yousif Omer

Citizenship — Sudan, 22 years old at the time the charges were filed. Aliases: WilfordCEO, Zac, Soldi01. According to prosecutors, he performed the “public” function: launched attacks, handled communications on Telegram, and negotiated the price and payment for DDoS services with clients. He was also charged with three additional counts of damaging protected computers. The maximum penalty for the combined charges is life imprisonment, which is linked to the attack on the Israeli emergency alert system on 7 October 2023, classified as an attempt that could have resulted in loss of life. [12]

Alaa Salah Yusuuf Omer

Citizenship — Sudan, 27 years old. Technical developer: wrote software code, including the WebSocket API (WSAPI) architecture that Ahmed used to coordinate attack servers. According to investigators, he left his own name and the @alaaelrefaie account in comments in the source code — negligence that apparently significantly facilitated attribution by investigators. The maximum penalty for him is up to five years, which is significantly less than for his brother and reflects the difference in their roles: the developer of the tool versus the operator who directly monetized and used the tool against live targets. [11]

The status of the suspects following the March 2024 operation remained a separate issue from the seizure of the infrastructure. In March 2024, U.S. law enforcement authorities, pursuant to court warrants, seized and disabled key components of DCAT, but the charges against Ahmed and Alaa Omer were not publicly announced until 16 October 2024. The DOJ did not report in its press release that the brothers had been arrested in March 2024. [10]

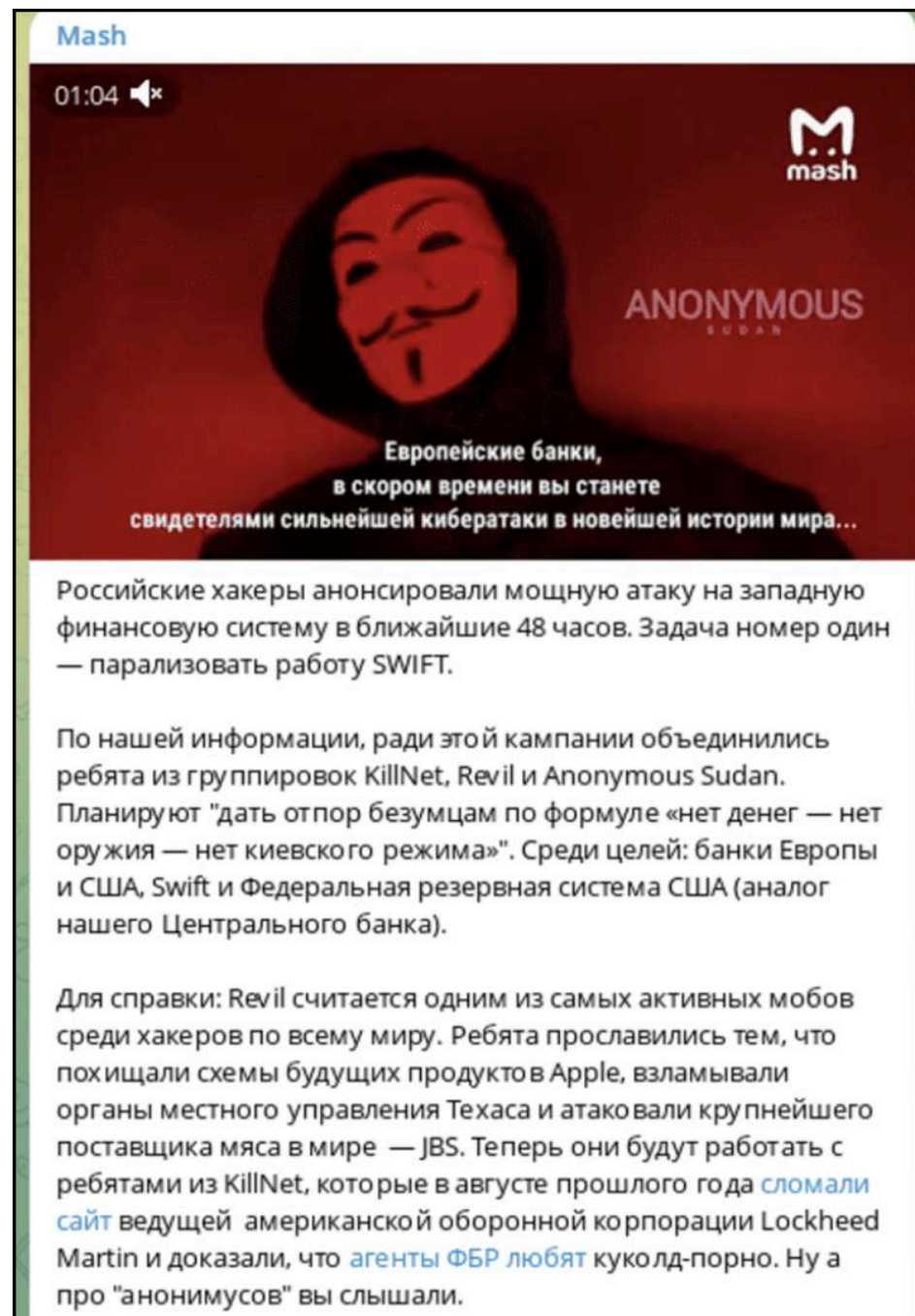
4.3. Links to KillNet and REvil

The most documented external link of Anonymous Sudan is its interaction with KillNet. It became apparent practically from the beginning of the group’s activities. Mandiant included Anonymous Sudan in its list of KillNet-associated channels and, as of July 2023, assessed it as an active KillNet affiliate. [17] According to Mandiant’s estimates, during the first half of 2023, Anonymous Sudan was responsible for 63% of all identified DDoS attacks claimed by KillNet and groups associated with it.



The link with REvil is of a different nature and is much better substantiated for a specific period than as an ongoing organizational interaction. On 14 June 2023, KillNet, Anonymous Sudan, and a group presenting itself as the revived REvil announced a joint campaign against the Western financial system, with European and American banks and the SWIFT network named as targets. The participants linked the campaign to ending Western military support for Ukraine.

The announcement of the alliance was distributed through the Telegram channels of KillNet and Anonymous Sudan, as well as the Russian media outlet Mash.



The campaign against SWIFT is the best example of how Anonymous Sudan may have operated as part of a broader coalition of pro-Russian hacktivist actors. At the same time, the affiliation with KillNet itself is not sufficient evidence of direct control or funding by Russian state structures. Anonymous Sudan's link to KillNet is more appropriately viewed as a strong indicator of its involvement in the pro-Russian hacktivist environment and operational interaction, rather than as evidence of state and operational control over the group.

5. Attack Tactics, Techniques, and Methods

5.1. Infrastructure Model

One of the characteristic features of Anonymous Sudan was the use of rented server and cloud infrastructure in combination with open proxies. In February 2023, Truesec and its partners identified a cluster of at least 61 paid IBM/SoftLayer servers in Germany that were used in the attack infrastructure. Microsoft later described Storm-1359 as an actor that used VPS, rented cloud infrastructure, open proxies, and DDoS tools. [1]

According to materials from the U.S. investigation, the Skynet tool used by Anonymous Sudan was effectively a Distributed Cloud Attack Tool (DCAT), consisting of a command-and-control server, a set of cloud servers, and an array of open proxies through which DDoS traffic was transmitted to the target. This architecture made it possible to distribute traffic sources and made it more difficult to block the attack solely by individual IP addresses. [11]

The use of paid and scalable infrastructure indicates that the group had continuous access to the financial resources necessary to sustain its operations, but the source of funding could not be established.

5.2. Approximate Operational Cycle

1. The target is usually a country or organization that can be linked either to an “anti-Muslim” narrative or to support for Ukraine or Israel.
2. A public threat statement is posted on the Telegram channel, often accompanied by political rhetoric.
3. An L7 attack (application layer) is launched through the group’s own DCAT tool — the group’s proprietary development, which was also sold to third parties as a DDoS service. [10]
4. Evidence is published, for example, screenshots from services such as check-host.net, which in themselves are not reliable confirmation of an actual outage but work well as media content.
5. Where there is a commercial interest, a ransom is demanded to stop the attack or prevent the dissemination of stolen data (from \$3,500 to \$3 million in the case of Scandinavian Airlines; separately, an offer of a package to take down an internet service provider in a selected country for \$500 per hour). [14]
6. The group moves on to the next target, often without a pause. It was precisely this ability to conduct several parallel campaigns and rapidly switch between targets that created the impression for Microsoft and other victims of a much larger adversary than a team of two to five people.

5.3. Technical Repertoire (According to Microsoft)

Microsoft, which tracked the group under the identifier Storm-1359, documented three main types of L7 DDoS attacks used against Outlook.com, OneDrive, and the Azure portal [5] in June 2023:

- HTTP(S) flood - millions of requests and SSL/TLS handshakes distributed worldwide, designed to exhaust computational resources (CPU, memory) on the application side rather than network bandwidth.ня обчислювальних ресурсів (CPU, пам'ять) на боці застосунку, а не мережевого каналу.



- Cache bypass - deliberately generated URLs that force the infrastructure to bypass the CDN cache and direct each request straight to the origin server, thereby overloading the very component that the CDN is supposed to protect.
- Slowloris - a “slow exhaustion” attack: the client opens a connection, requests a resource, and either does not acknowledge the download at all or acknowledges it extremely slowly, forcing the server to keep the connection open and consume memory until the pool of available connections is exhausted.

5.4 MITRE ATT&CK Analysis

Technique	Name	Sub-technique / Comment
T1498	Network Denial of Service	T1498.001 (Direct Network Flood), T1498.002 (Reflection Amplification) — saturation of the network with high-volume traffic
T1499	Endpoint Denial of Service	T1499.002 (Service Exhaustion Flood) — exhaustion of application resources without necessarily saturating the network; Slowloris and Cache bypass also fall under this category
T1583.003	Acquire Infrastructure: Virtual Private Server	Renting VPS and cloud resources to conduct attacks
T1090	Proxy	Use of open proxies to conceal the source of traffic
T1657	Financial Theft	DDoS extortion and selling attacks as a service (applicable more to the business model than to a specific technique)

5.5. Monetization as Part of the Tactics

Over time, the group’s business model acquired the same tactical significance as the technical attack techniques themselves. Publicly documented financial demands include a demand for \$1 million to stop attacks on Microsoft, as well as other amounts related to the commercial use of DDoS infrastructure. The existence of a price list and the sale of DDoS services support the existence of a commercial model but do not constitute evidence of the absence of state funding. Theoretically, commercial activity, self-financing, and external support can exist in parallel.

In March 2024, the FBI and the district prosecutor’s office executed a warrant to seize key elements of this infrastructure — attack management and launch servers, command relay servers, and accounts containing the source code of DDoS tools. Instead of countering traffic on the victims’ side, which the group had learned to bypass, law enforcement agencies eliminated the infrastructure layer itself, the restoration of which requires significant time and financial resources. [10]

6. Technical Capability: Claimed Image and Confirmed Capabilities

6.1. Claimed Image

The claimed image of Anonymous Sudan as a technologically advanced group capable of competing on equal terms with state cyber units does not fully correspond to what can be reconstructed from open sources. At the same time, the group demonstrated high practical effectiveness: over approximately one year of activity, Microsoft Azure, Outlook, ChatGPT, X, and PayPal services were subjected to attacks. CrowdStrike specifically noted the scale of the results achieved relative to the number of group members, which, according to the most substantiated estimates, can be placed at between two and five individuals. [8]

At the same time, there are grounds to suggest that the group possessed its own technical expertise rather than merely the ability to use ready-made services. In particular, Anonymous Sudan developed its own DDoS tool, DCAT, also known as Godzilla, Skynet, or InfraShutdown. According to the indictment, the code for this tool was directly developed by Alaa Salah. This indicates the presence of at least some members with sufficient skills to develop specialized software.

6.2. Confirmed Capabilities

However, the technical complexity of the attacks themselves does not provide grounds for assessing the group as a highly skilled cyber operator. As early as 2023, Trustwave assessed its level of technical proficiency as low to medium. Anonymous Sudan's main tactics largely overlapped with Killnet's approaches and involved the use of large-scale L7 attacks, including HTTP floods, cache bypass, and Slowloris. Such attacks do not require the exploitation of zero-day vulnerabilities, sophisticated intrusion into the victim's infrastructure, or prolonged persistence within its network.

Anonymous Sudan's key advantage was not the uniqueness of the methods used, but the ability to scale them. According to available estimates, the group used more than 61 servers in commercial data centers and a proxy network distributed across at least 132 countries. Such infrastructure significantly increases the power of even relatively simple L7 attacks. Accordingly, the ability to disrupt the operations of Microsoft or other major technology companies does not in itself indicate that the attackers possessed technologies at the level of state cyber units. [15]

Thus, Anonymous Sudan is more appropriately viewed as a small but well-organized and well-resourced group capable of effectively scaling relatively simple DDoS operations. Its main advantages were access to substantial infrastructure, funding, and the ability to concentrate resources on individual targets. This is also important for assessing the group's vulnerabilities: its capabilities largely depend on access to servers, proxies, and other infrastructure resources. Financial and infrastructure links, rather than the search for more sophisticated technical vulnerabilities, therefore represent one of the most promising areas for countering such an operator.

7. Limitations and Vulnerabilities

- Dependence on a small number of people. The entire operation was literally sustained by two brothers plus several unnamed accomplices. The arrest of the two key figures in March 2024 effectively stopped the group's activity — this is an unusually resilient structure for a group that allegedly had state support; state cyber units usually withstand the arrest of individual operators without a complete cessation of activity.
- Centralized and expensive infrastructure. Relying on rented commercial servers instead of a distributed botnet is a double-edged sword: it provides stability and power but creates a single point of failure. When the FBI seized key servers and accounts containing source code in March 2024, the group apparently had no quick way to restore operations. [10]
- Internal inconsistency of the narrative. Poorly concealed motivation, with selective disregard for actual cases of oppression of Muslims outside the Western context and an almost complete overlap of targets with the geopolitical map. From a reputational perspective, the group's stated ideology is vulnerable to any careful analytical investigation.

Conclusion

If the trajectory from January 2023 to March 2024 is traced, a fairly consistent arc emerges: a religious-hacktivist debut, alignment with the pro-Russian information cluster, expansion of its own technical and infrastructure base, commercialization, a strike against the infrastructure and key operators, and a period of inactivity that coincides perfectly with the timing of the brothers' arrest, although the arrest itself was not publicly reported for another six months.

This is not the trajectory of a typical state cyber unit (which, after the failure of one project, usually relaunches under a new name or simply continues operating with new personnel), nor is it the trajectory of a purely ideological movement (which rarely moves so consistently toward price lists and extortion). They attempted to find a niche in which they could resonate with a particular audience, gain access to partnerships, test their technology against high-profile targets for publicity, and then directly monetize the recognition and infrastructure they had built.

The logic of the business model suggests a shift toward an increasingly explicit DDoS-for-hire service with an increasingly thin ideological cover, similar to how Killnet itself increasingly behaved over time as a group of cyber mercenaries rather than ideological "patriots."

8. Assessment of Significance and Threat Level

Over a year of activity, Anonymous Sudan demonstrated that a small group can create a significant impact without using technologies at the level of state cyber units. Its capability was based primarily on a combination of access to paid server and proxy infrastructure, the ability to scale DDoS attacks, and the active use of publicity to amplify the effect of its operations. Confirmed targets included major technology companies, U.S. government institutions, financial and healthcare organizations, as well as transportation infrastructure. The U.S. investigation estimated the total damage caused by the attacks at more than \$10 million. This estimate reflects documented economic losses and does not include potential indirect costs, including reputational consequences or expenses for additional security measures. [16]

The geopolitical context of the group's activities is also of particular significance. At the initial stage, Anonymous Sudan consistently used religious and anti-Western rhetoric to justify its target selection. At the same time, the subsequent geography and nature of the attacks demonstrated a noticeable overlap with the broader anti-Western and pro-Russian hacktivist environment, and the group publicly interacted with Killnet. This is not sufficient grounds to conclude that the group was directly controlled by Russian state structures, but it allows Anonymous Sudan to be viewed as an actor whose activities overlap with the objectives of Russian groups. [4]

Conclusion

Thus, Anonymous Sudan is more appropriately characterized not as a high-tech cyber operator capable of competing with state structures in terms of technical sophistication, but as a small and organized group that effectively scaled relatively accessible DDoS technologies. Its strength lay in the combination of infrastructure, financial resources, organizational coordination, and media impact. It was this combination that made it possible to turn a technically relatively simple tool into an operationally significant means of pressure.

At the same time, the commercialization of DDoS infrastructure and extortion for financial gain demonstrate that Anonymous Sudan's activities cannot be explained exclusively by political or religious motivation. Its operations simultaneously reflect a hacktivist narrative, geopolitical context, and financial interest. It is the combination of these components, rather than any single ideological motivation, that best explains the group's operational model.

9. Recommendations for Countermeasures

- L7 protection at the application layer. Enabling and fine-tuning services such as Azure WAF or equivalents, with dedicated rules for HTTP flood signatures; configuring bot protection and request rate limiting at the level of individual endpoints rather than only the entire domain.
- Geographic and infrastructure filtering. Since the group's attack infrastructure has historically been concentrated among several commercial hosting providers and open proxies, traffic from known ranges previously identified in reports by Truesec, CyberCX, and Microsoft should be monitored and, where necessary, temporarily restricted, without relying entirely on country-based geoblocking.
- Monitoring and early identification of spikes. Automated alerts for anomalous traffic spikes before they develop into a full-scale service outage.
- Channel redundancy and geographically distributed architecture for critical services, particularly in sectors that have already attracted the group's attention: healthcare, government registries, and financial services.
- Extortion response protocol. Do not negotiate or pay ransom (as this validates the viability of the business model and finances further attacks), but thoroughly document all demands and communications for subsequent transfer to law enforcement — such details formed the basis of the 2024 indictment.

List of Sources

1. <https://www.truesec.com/hub/report/anonymous-sudan-threat-intelligence-report>
2. <https://www.truesec.com/hub/blog/hacktivists-target-denmark-in-simultaneous-attacks>
3. <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/>
4. <https://www.avertium.com/resources/threat-reports/an-update-on-pro-russia-threat-actor-killnet>
5. <https://www.microsoft.com/en-us/msrc/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks>
6. <https://thecyberwire.com/stories/19e7d683bdd34891b42158c8c6d3a52e/anonymous-sudans-questionable-provenance>
7. <https://cyberscoop.com/anonymous-sudan-killnet-russia-onlyfans/>
8. <https://www.crowdstrike.com/en-us/blog/anonymous-sudan-hackivist-group-ddos-indictment/>
9. <https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals>
10. <https://krebsonsecurity.com/2024/10/sudanese-brothers-arrested-in-anonsudan-takedown/>
11. <https://flashpoint.io/blog/usa-vs-ahmed-salah-yousif-omer-alaa-salah-yusuuf-omer/>
12. <https://sudantribune.com/article292154/>
13. <https://www.jpost.com/international/article-825144>
14. <https://www.cbsnews.com/news/2-sudanese-nationals-charged-cyber-attack-for-hire-gang/>
15. <https://www.securityweek.com/anonymous-sudan-ddos-service-disrupted-members-charged-by-us/>
16. <https://therecord.media/anonymous-sudan-brothers-charged-ddos-attacks-hospital-critical-infrastructure>
17. <https://cloud.google.com/blog/topics/threat-intelligence/killnet-new-capabilities-older-tactics>