LIQUID
CLOUD & CYBER SECURITY

Threat Advisory Report

Anonymous Sudan Threat Actor Targets Kenyan Infrastructure

01 August 2023

Cyber Security Fusion Centre

At Liquid C2, we provide cutting-edge solutions to help our customers avoid cyber threats. With our SOC Services, we empower businesses with the latest in cyber security technology backed by proven expertise.

We are committed to delivering exceptional service and support to our customers, so you can focus on what matters most – growing your business. With the Liquid C2 Cyber Security Fusion Centre, you can trust that your cybersecurity is in good hands.

Contents

Introduction

In light of the ongoing attacks faced in Kenya, our Cyber Security Fusion Centre has made safeguarding our customers a top priority by closely monitoring the activities of the notorious group known as "Anonymous Sudan." This group has gained infamy for employing highly impactful Distributed Denial of Service (DDoS) tactics.

To proactively address this emerging threat, we have taken decisive actions to strengthen our monitoring capabilities. By leveraging Indicators of Compromise (IOCs) associated with the IP addresses used by "Anonymous Sudan" for their DDoS attacks, we have developed comprehensive use case dashboards and queries. These tools enable us to closely track and assess the situation effectively.

Our continuous monitoring approach empowers us to respond promptly to any potential threats and swiftly implement necessary countermeasures. The goal is to ensure the safety and security of our customers' critical infrastructures and valuable data. By staying vigilant and proactive, we strive to maintain a resilient defence against cyber threats posed by "Anonymous Sudan". The SOC created a dashboard to monitor the published IoC's.

Indicators of Compromise Dashboard

The Liquid C2's SOC has developed a comprehensive dashboard that oversees all Indicators of Compromise (IoC's) related to this threat. Our valued C2 SOC customers are provided with access to these dashboards.

The original hacktivist collective "Anonymous Sudan" emerged in 2019 during a period of political instability in Sudan. However, the current Anonymous Sudan group appears to be pro-Russian performing DDOS attacks against western countries.

Although not proved yet, it is widely believed that Anonymous Sudan is a sub-group of pro-Russian collective Killnet while claiming to be Sudanese actors.

This report sheds light on Anonymous Sudan's origins, operations, tactics, techniques, procedures, associated indicators of compromise and actions to avoid such attacks.

Attack on Kenya - Motive

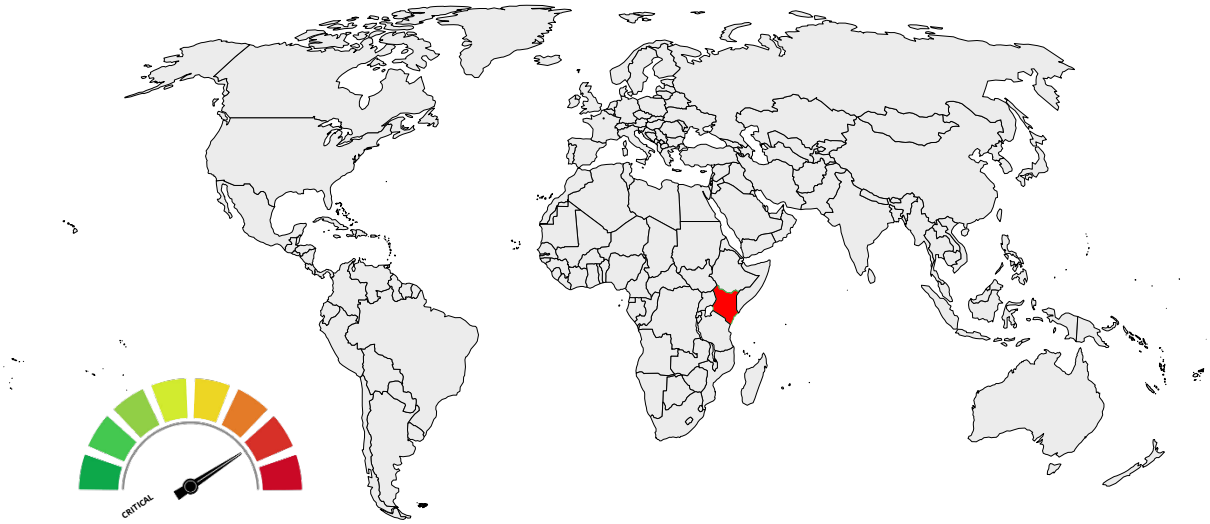
Recently, Anonymous Sudan launched DDOS attacks against several of Kenya's web services including universities with media websites, hospitals, Kenya Commercial Bank, Safaricom, and an eCitizen website which hosts several government services.

The group said it attacked Kenya because Kenya has been attempting to meddle in Sudanese affairs and released statements doubting the sovereignty of their government.

Summary of Attack

Targeted Attack Region: Kenya
Targeted Industries: The group has focused its attacks on the government and telecommunications sectors.
Attack Type: Anonymous Sudan employs sophisticated DDOS tactics leveraging public cloud server infrastructure to generate traffic and launch attack floods. They also utilise free and open proxy infrastructures to conceal and randomise the source of their attacks. The group primarily utilises application layer DDoS botnets, such as Skynet and Godzilla, but also possesses layer 4 capabilities.

Targeted attack country



Anonymous Sudan Previous Attacks

Before the attack on Kenya and since early 2023, Anonymous Sudan performed multiple attacks, mostly DDOS in nature, targeting several countries and industries. These targeted entities existed in the North Atlantic Treaty Organization (NATO) and European Union (EU) and were targeted via its #OpSweden and #OpDenmark campaigns and participated in the establishment of the #OpIndia campaign.

Between January and February, in response to Rasmus Paludan's actions Anonymous Sudan performed DDOS attacks on Nordic countries targeting mainly the Swedish healthcare sector. In May of this year the Scandinavian Airlines Services(SAS) was attacked, with the adversary demanding an amount of $3 million to stop the disruption on SAS services.

In March, Anonymous Sudan attacked French flag carrier Air France and stole data from the company. This attack was followed by several attacks on Australian companies.

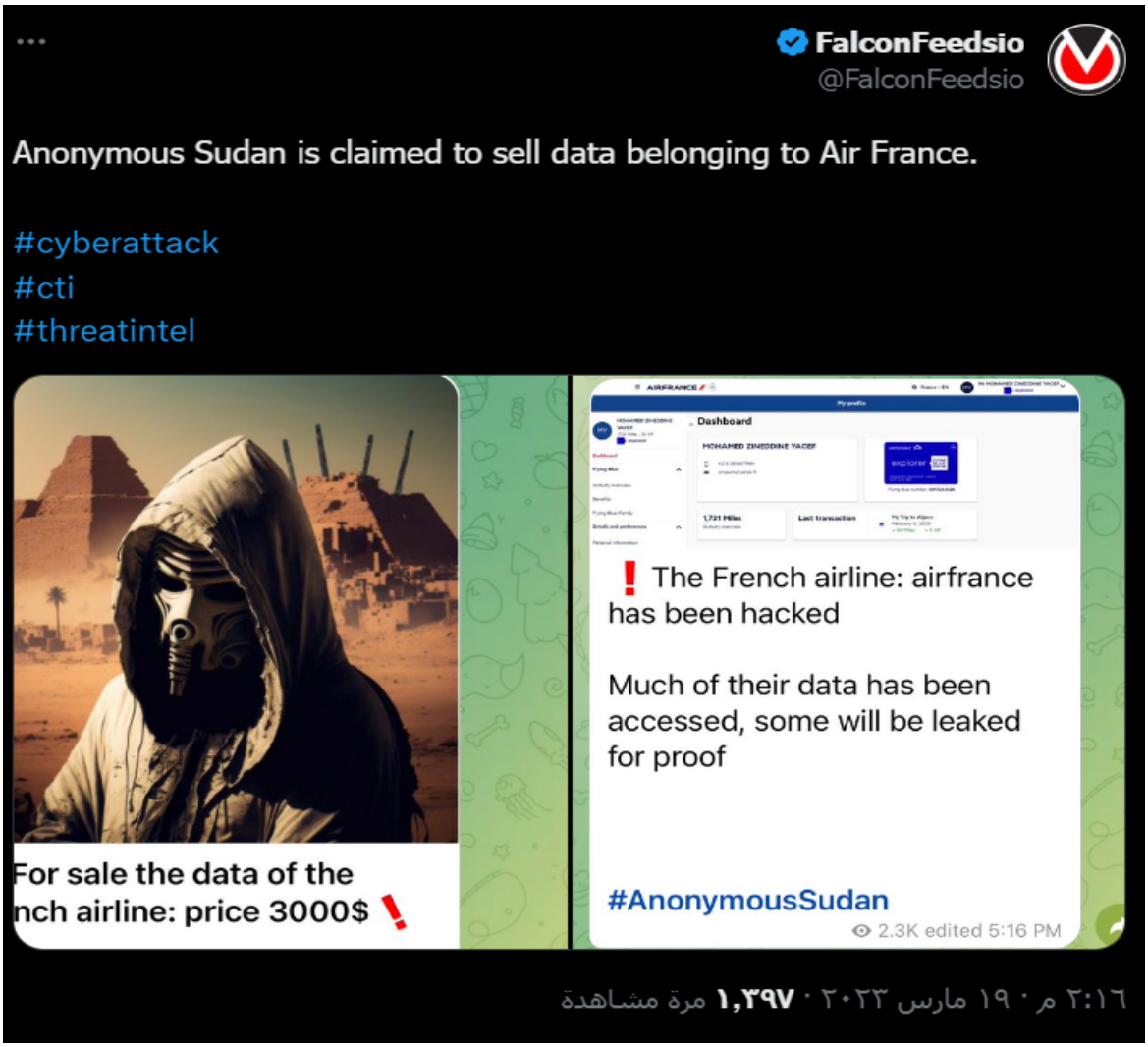


Figure 1: Air France Data Allegedly Sold by Anonymous Sudan

Several reports linked Anonymous Sudan with DDOS attacks on Benjamin Netanyahu's website and other Israeli organisations in April.

In May, the group claimed that they performed DDOS attacks on several UAE websites.

In June, Anonymous Sudan attacked Microsoft with DDOS traffic and caused temporary outage of Office 365 and Outlook. Microsoft identifies and tracks Anonymous Sudan as "Storm-1359."

According to Microsoft, Anonymous Sudan has been observed launching several types of layer-7 DDoS attack traffic:

- HTTP(S) flood attack – In this case, the attacker sends a high load (in the millions) of HTTP(S) requests that are well distributed across the globe from different source IPs. This causes the application backend to run out of compute resources (CPU and memory).

- Cache bypass – In this case, the attacker sends a series of queries against generated URLs that force the frontend layer to forward all the requests to the origin rather serving from cached contents.

- Slowloris – This attack is where the client opens a connection to a web server, requests a resource (e.g., an image), and then fails to acknowledge the download (or accepts it slowly). This forces the web server to keep the connection open and the requested resource in memory.
- Finally, in the same month, Anonymous Sudan launched a DDOS attack targeting the European Investment Bank with possible collaboration with Killnet and REvil.

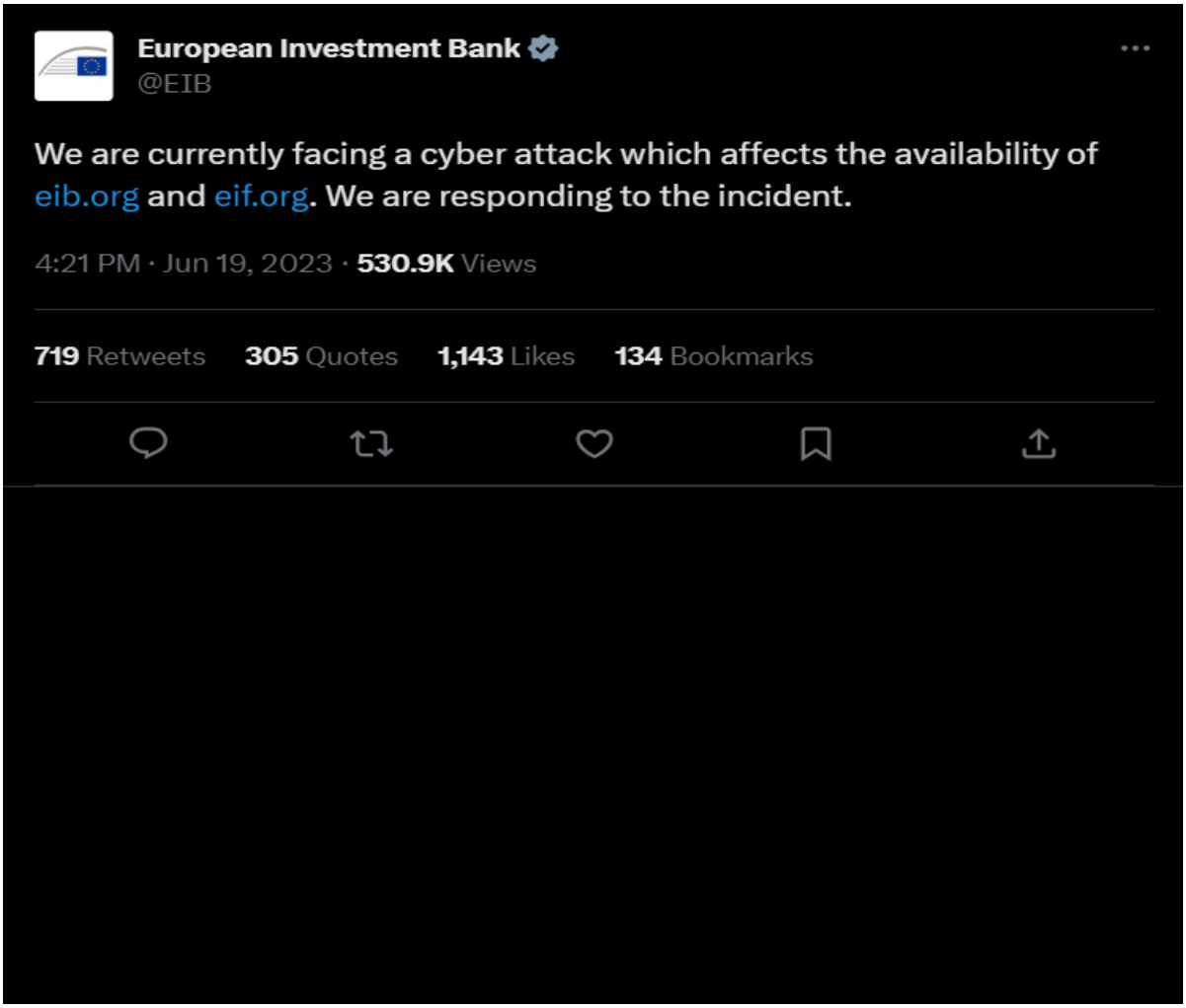


Figure 2: European Investment Bank Confirms Attack in June 2023

Threat Actor Details

DDoS Attacks and Security Breaches: "Anonymous Sudan" has emerged as a highly active threat, engaging in DDoS attacks and successfully breaching the security of various public and government entities. These actions are raising concerns about the potential impact on the affected organizations and their data security.

Identity and Motivation: "Anonymous Sudan" identifies itself as a hacktivist collective hailing from Sudan. While their actions are purportedly motivated by political causes, the specific objectives behind their attacks remain undisclosed to the public.

Association with Killnet: Notably, "Anonymous Sudan" is known to collaborate with a larger cyber-attack group called Killnet. This association suggests the possibility of shared objectives or collaboration between the two groups.

Support from Russian Hacktivists: Disturbingly, "Anonymous Sudan" has gained support from prominent Russian hacktivists who have actively endorsed and promoted the group through various channels on Telegram. This backing has likely bolstered the visibility and reach of the Sudanese group.

Discrepancies in Connection: Despite "Anonymous Sudan" claiming affiliation with the well-known "Anonymous" collective, a representative from the original "Anonymous" collective has publicly denied any association or connection with them. This revelation raises important questions regarding the true nature and independence of the Sudanese group's activities.

Group Details

NAME	ORIGIN	PAST VICTIMS	TARGET SECTORS
ANONYMOUS SUDAN	Believed to be a sub-group of Pro Russian hactivist group KillNet - Claims to be from Sudan **MOTIVATION** Political and Religious issues **ASSOCIATIONS** Infinity Hackers Group, Killnet, Anonymous Russia, MistNet, UserSec	Africa, US, Europe, India, Israel, UAE	Aviation, Education, Finance, Government, Healthcare

Impact of DDoS Attacks

Service Disruption: DDoS attacks overload the targeted infrastructure, such as servers, routers, and firewalls, with a massive volume of malicious traffic. This overload causes services to slow down, become unresponsive, or crash altogether, leading to widespread service disruption and rendering the infrastructure unusable for legitimate users.

Degraded Performance: Even if the infrastructure does not completely fail, DDoS attacks can degrade its performance significantly. The infrastructure might struggle to handle legitimate traffic alongside the attack traffic, resulting in increased response times and reduced efficiency.

Resource Exhaustion: DDoS attacks consume various resources within the infrastructure, such as network bandwidth, CPU, memory, and disk space. The sustained resource consumption can strain the infrastructure and potentially cause exhaustion, affecting the overall stability and availability of services.

User Disruptions: Affected websites experience a range of user-related issues, such as slow loading times, timeouts, and error messages. These discrepancies create a frustrating user experience, erode trust, and diminish the credibility of the targeted organisation.

Recommendations

To effectively mitigate the impact of DDoS attacks, a combination of proactive measures and responsive strategies is essential:

Robust DDoS Protection Solutions: Implementing robust DDoS protection solutions is crucial to detect and block malicious traffic before it reaches the website's infrastructure. Utilize dedicated DDoS mitigation services and hardware to bolster the website's defences effectively e.g. Cloudflare.

Scalable Infrastructure: Create a scalable and distributed infrastructure capable of handling increased traffic during peak times and DDoS attacks. Incorporate Content Delivery Networks (CDNs) and load balancers to efficiently distribute traffic and reduce strain on the website's resources.

Anomaly Detection: Deploy intrusion detection systems (IDS) and anomaly detection mechanisms to swiftly identify unusual traffic patterns that may indicate a potential DDoS attack. Real-time monitoring enables a rapid response and effective mitigation.

Traffic Filtering: Set up traffic filtering rules to distinguish legitimate users from malicious traffic. Utilise IP blacklists, whitelists, and rate limiting to manage incoming requests effectively and ensure the website remains accessible to legitimate users.

Comprehensive Incident Response Plan: Develop a comprehensive incident response plan that clearly outlines roles, responsibilities, and the specific steps to be taken in the event of a DDoS attack. Regularly test and update the plan to adapt to evolving threats effectively.

Cloud-Based Solutions: Consider migrating critical services to reputable cloud service providers that offer built-in DDoS protection capabilities. Cloud-based solutions can efficiently distribute traffic and provide additional layers of security to counter DDoS attacks.

Collaboration and Reporting: Foster cooperation with internet service providers (ISPs) and other relevant organizations to share information about ongoing attacks and malicious IP addresses. Collaborative efforts can enhance the collective response against DDoS attacks, while reporting incidents to relevant authorities aids in tracking down and prosecuting attackers.

How Liquid C2 can help.

Liquid C2 offers SOC services and DDOS solutions like Cloudflare

1. 24/7 Monitoring and Alerting: Liquid C2 operates round-the-clock, continuously monitoring network and application traffic for signs of DDoS attacks. When an attack is detected, the SOC immediately generates alerts to initiate the incident response process.

2. DDoS Protection and Mitigation: Cloudflare provides robust DDoS protection services. It's global network absorbs and filters incoming traffic, identifying and mitigating DDoS attacks close to their source. This prevents malicious traffic from reaching the organization's infrastructure, ensuring service availability.

Potential MITRE ATT&CK TTP's

TA0043 Reconnaissance	TA0042 Resource Development	T1526 Cloud Service Discovery
T1589 Gather Victim Identity Information	T1110 Brute Force	T1498 Network Denial of Service
T1498.001 Direct Network Flood	T1498.002 Reflection Amplification	T1491.002 external defacement
T1583 Acquire Infrastructure	T1190 Exploit Public-Facing Application	T1590 Gather Victim Network Information

Indicators of Compromise (IOCs)

The SOC established a watchlist to monitor communication attempts from the IoC's related to this threat'. Our recommendations include promptly blocking the identified IoC's on relevant security controls and conducting thorough system investigations to mitigate potential threats and strengthen overall security defences.

Please use the below link to accesses the list of IOCs:

https://github.com/securityscorecard/SSC-Threat-Intel-IoCs/blob/master/KillNet-DDoS-Blocklist/ipblocklist.txt

References and Proof Concept

- https://flashpoint.io/blog/anonymous-sudan-ddos-timeline/
- https://www.truesec.com/hub/blog/what-is-anonymous-sudan
- https://www.jpost.com/international/internationalrussia-ukraine-war/article-749702
- https://techcabal.com/2023/07/27/pro-sudan-hackers-attack-digital-services-in-kenya/
- https://flashpoint.io/blog/anonymous-sudan-ddos-timeline/
- https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/