Abstract – This document provides a analysis of the hacktivist group known as Anonymous Sudan. The analysis delves into various aspects of the group's activities, including their origins, motivations, methods, and the implications of their actions. It offers a qualitative unpacking of the group's operations, highlighting key findings and patterns in their behavior.

The insights gained from this analysis are useful for cyber security experts, IT professionals, and law enforcement agencies. Understanding the modus operandi of Anonymous Sudan equips these stakeholders with the knowledge to anticipate potential attacks, strengthen their defenses, and develop effective countermeasures against similar hacktivist threats

I. Group’s specifics and motivation behind

Anonymous Sudan is a hacktivist group that has gained notoriety for its series of distributed denial-of-service (DDoS) attacks on various global targets. The group presents a unique blend of political and religious motivations, leveraging digital tools to advance its causes and create disruptions. They have targeted organizations associated with infrastructure and key services, including in government and private sectors.

The group has been active since January 2023, making consistent headlines around the world since then, prioritizing Sweden, the Netherlands, and Denmark, Israel, UAE, France, and Australia. In terms of recent activities, cyberattack on Chad telecommunications provider Sudachad. They have also targeted the ChatGPT over an OpenAI employee's support for Israel.

However, there is a significant debate about the true origins and affiliations of Anonymous Sudan. The theory of the use of the Russian language by them, as seen from the perspective of all Western countries, clearly indicates the true origins of this language (or rather, the intellectual development).

The group likely recruits new members through online platforms, leveraging the influence of other groups, offering financial incentives, and possibly implementing a pre-selection process to ensure a certain level of skill among recruits to maintain operational security and effectiveness unlike the broader Anonymous collective, which is known for welcoming anyone regardless of skill level. The group often recruits new members through online platforms, hacker forums and social media channels, Telegram. These platforms allow them to reach a wide audience of potential recruits who are interested in cybersecurity, hacking, and activism.

Anonymous Sudan claims to be motivated by both political and religious beliefs. For instance, they have cited geopolitical events that they perceive as anti-Muslim as the catalyst for their actions. They have targeted Swedish and Danish organizations and critical infrastructure in response to burning a copy of the Quran in Sweden.

II. Operational Tactics

The group primarily uses DDoS attacks, employing a combination of Web DDoS attacks and alternating UDP/SYN floods to disrupt services. They also compromise email accounts. The group often follows through in attacking targets they have publicly threatened, and the detrimental impact of these attacks is often demonstrated using reachability tools. They also often retrospectively take credit for unrelated service outages.

The group uses standard DDoS-For-Hire services and botnet rentals, breaking from the traditional hacktivist mentality and capabilities and behaving more like an advanced persistent threat (APT) group. They leverage public cloud server infrastructure to generate traffic and attack floods. The group's attacks originate from tens of thousands of unique source IP addresses with UDP traffic reaching up to 100 Gbps.

Before launching an attack, Anonymous Sudan often threatens targets in advance. This is typically done through public posts on social media or other online platforms, where they announce their intentions and the reasons behind their actions. This approach not only serves as a warning to the intended target but also helps to generate publicity for the group's cause and actions.

Anonymous Sudan employs a variety of tools and methods to launch DDoS attacks:

- **High Bandwidth Attacks**: They use large byte-size packets and/or large amounts of network traffic to increase TCP attacks; the maximum observed attack bandwidth and throughput were 284 Gbps and 57 Mpps
- **UDP Floods**: This involves a combination of various UDP reflectors/amplifiers to overwhelm the target.
- **UDP Reflection/Amplification Vectors**: Specific vectors like DNS and SSDP are used to magnify the attack traffic.
- **Web DDoS Attacks**: These attacks disrupt web services by overwhelming the target with a flood of internet traffic.
- **SYN Floods**: This type of attack exploits the TCP handshake process to consume resources on the target server.

- **Public Cloud Server Infrastructure**: Group leverages cloud services to generate traffic and attack floods, which provides them with a layer of anonymity and makes it difficult to pinpoint the source of the attacks.

III. Target profile

The group's operational patterns and the sectors they target suggest a strategic approach to their hacktivism, aiming to cause disruption and draw attention to their causes. Here are some key points profiling the victims.

Time Period of Activity – the group has been most active in February and April, with a significant number of attacks occurring during these months.

Targeted Countries and Sectors

- Most mentioned countries: Sweden, Israel, United States, Netherlands, Denmark, Australia, France, Germany, United Arab Emirates (UAE), Iran
- Israel has been a major target, with over 70 attacks, accounting for more than 20% of the total victims, particularly during the "OpIsrael" campaign
- Scandinavian entities, including Scandinavian Airlines (SAS), were targeted following an anti-Islam protest by Rasmus Paludan who burned a copy of the Quran.
- Critical sectors targeted include finance, aviation, healthcare, and government entities

Publicity and Community Engagement

Anonymous Sudan craves publicity and public recognition, actively engaging with their audience and involving followers in target selection

A. *Affected companies*

Top of the companies that have been affected include:

- The tech giant Microsoft
- The airline Air France
- The online payment system PayPal
- The financial services corporation American Express
- The web infrastructure and website security company Cloudflare experienced a DDoS attack that took down its website for a few minutes
- The government-owned airline based in Dubai Flydubai
- The news agency Associated Press (AP)

B. *Industries*

- **Transportation**: reservation systems, customer databases, and other networked systems.
- **Government**: public-facing websites, email systems, and other network infrastructure.
- **Education**: student information systems, online learning platforms, and email systems.
- **Healthcare**: electronic health record systems, appointment scheduling systems, and other networked medical devices.
- **Finance**: online banking systems, customer databases, and email systems.
- **Manufacturing**: industrial control systems, supply chain management systems, and other networked systems.
- **Technology**: public-facing websites, customer databases, and cloud services.

C. *Overall Impact*

- **Disruption of Services**: The group's primary method of attack is DDoS, which can disrupt services across various sectors, including finance, aviation, healthcare, and government entities. This can lead to significant service interruptions, affecting both businesses and consumers
- **Economic Impact**: The cost of mitigating DDoS attacks can be substantial. This includes the cost of additional bandwidth, hardware, and software to mitigate attacks, as well as potential revenue loss due to service disruptions
- **Public Perception and Trust**: The publicity generated by these attacks can affect public perception and trust in the targeted entities and the country's ability to protect against cyber threats
- **Resource Allocation**: Responding to and mitigating these attacks requires significant resources, which can divert resources away from other critical areas
- **Potential for Escalation**: There is a risk that the group could escalate its tactics over time, potentially moving beyond DDoS attacks to more destructive or disruptive forms of cyberattacks
- **Political Impact**: The group's attacks are often politically motivated, which can exacerbate existing tensions and conflicts

D. *Impact [Transportation Industry]*

- **Service Disruption**: Attacks can lead to the disruption of critical services such as flight operations, ticketing, and customer service, causing inconvenience to passengers and potential safety concerns.
- **Economic Losses**: Airlines and other transportation entities may suffer economic losses due to service downtime, the cost of mitigating the attacks, and potential compensation to affected customers.
- **Reputational Damage**: Repeated attacks can damage the reputation of the targeted companies, leading to a loss of customer trust and potentially affecting future business.
- **Operational Strain**: Responding to and recovering from DDoS attacks can strain the operational capabilities of the targeted entities, requiring significant resources and potentially diverting attention from other critical tasks

E. *Impact [Goverment Industry]*

- **Disruption of Public Services**: Government websites and online services can be taken offline, affecting citizens' access to important information and services
- **Economic Costs**: The financial impact includes the cost of mitigating the attacks and potential loss of productivity due to service downtime
- **Undermining Public Confidence**: Repeated attacks can erode public trust in the government's ability to secure its digital infrastructure
- **Strain on Resources**: Government agencies may need to allocate significant resources to respond to and recover from these attacks, which could otherwise be used for public services.

- **Security Implications**: If government networks are perceived as vulnerable, it could embolden other malicious actors to launch further attacks

F. Impact [Education Industry]

- **Disruption of Educational Services**: DDoS attacks can disrupt the availability of online educational resources, including websites, learning management systems, and virtual classrooms.
- **Economic Costs**: The financial impact includes the cost of mitigating the attacks and potential loss of productivity due to service downtime.
- **Undermining Public Confidence**: Repeated attacks can erode the trust of staff, families, and students in the institution's ability to secure its digital infrastructure.
- **Strain on Resources**: Educational institutions may need to allocate significant resources to respond to and recover from these attacks.
- **Security Implications**: If educational networks are perceived as vulnerable, it could embolden other malicious actors to launch further attacks.

G. Impact [Healthcare Industry]

- **Disruption of Critical Services**: DDoS attacks can disrupt the availability of essential healthcare services, such as electronic health records, telemedicine, and online patient portals. This can impede the delivery of patient care and affect critical healthcare operations
- **Compromised Patient Safety**: If healthcare systems are disrupted, patient safety can be jeopardized, as access to medical information and timely patient care is critical
- **Economic Costs**: Healthcare institutions may face substantial costs related to mitigating the attacks, recovering services, and potential legal liabilities if patient data is compromised
- **Loss of Confidentiality**: Cyberattacks can expose sensitive patient information, leading to privacy breaches and potential identity theft or fraud
- **Reputational Damage**: Repeated attacks can damage the reputation of healthcare providers, leading to a loss of trust among patients and the public
- **Resource Diversion**: Responding to and recovering from DDoS attacks can require significant resources, diverting attention from patient care and other essential services

H. Impact [Finance Industry]

- **Disruption of Financial Services**: Attacks can disrupt the availability of online banking, payment processing, and other financial services, affecting both businesses and consumers
- **Economic Costs**: Financial institutions may face substantial costs related to mitigating the attacks, recovering services, and potential legal liabilities if customer data is compromised
- **Loss of Customer Trust**: Repeated attacks can damage the reputation of financial institutions, leading to a loss of trust among customers and potentially affecting future business
- **Resource Diversion**: Responding to and recovering from DDoS attacks can require significant resources, diverting attention from other essential services
- **Security Implications**: DDoS attacks can serve as a cover for more damaging cyber activities such as infiltration of systems and exfiltration of data, putting extra strain on already limited resources

I. Impact [Manufacturing Industry]

- **Disruption of Operations**: DDoS attacks can disrupt the availability of essential manufacturing services, such as production control systems, supply chain management, and customer service portals
- **Economic Costs**: Manufacturing entities may face substantial costs related to mitigating the attacks, recovering services, and potential loss of productivity due to service downtime
- **Loss of Intellectual Property**: Many attacks in the manufacturing sector include theft of intellectual property, which can lead to a loss of market share or the eventual demise of the manufacturer victimized in the attack
- **Reputational Damage**: Repeated attacks can damage the reputation of manufacturing companies, leading to a loss of trust among customers and potentially affecting future business
- **Resource Diversion**: Responding to and recovering from DDoS attacks can require significant resources, diverting attention from production and other essential services

J. Impact [Techonology Industry]

- **Disruption of Services**: DDoS attacks can take down websites and online services, affecting the availability of digital products and services
- **Economic Costs**: Companies may face substantial costs related to mitigating the attacks, recovering services, and potential loss of revenue due to service downtime
- **Reputational Damage**: Repeated attacks can damage the reputation of technology companies, leading to a loss of trust among customers and potentially affecting future business
- **Resource Diversion**: Responding to and recovering from DDoS attacks can require significant resources, diverting attention from innovation and other essential services
- **Security Implications**: DDoS attacks can serve as a cover for more damaging cyber activities such as infiltration of systems and exfiltration of data