February 28, 2024

InfraShutdown: Anonymous Sudan Partners With DDoS-for-Hire Operator

Background

Anonymous Sudan joined the global threat scene in January 2023 when they attacked Denmark and Sweden, claiming to be pro-Muslim hacktivists operating from Sudan. Some believe Anonymous Sudan to be a black flag operation run by the Russian government, while others believe they were originally pro-Islamic hacktivists operating from Sudan. In last year's Global Threat Analysis Report, we referred to Anonymous Sudan as the rebel with too many causes, claiming distributed denial of service (DDoS) attacks driven by religion (pro-Islamic), by politics (pro-Sudanese and pro-Russian) and financial gain (extortion DDoS and stresser advertisements). This random behavior became most prominent in the second half of 2023, during which the overall activity of Anonymous Sudan slowed considerably. Now, in 2024, Anonymous Sudan is back on the forefront with an announcement that cannot be ignored.

Anonymous Sudan still regularly made headlines in the second half of 2023 by targeting and disrupting high-profile online services. Microsoft, X, OpenAI and others became a target of Anonymous Sudan and suffered interruptions to some extent. When Anonymous Sudan first appeared on the stage, it was an unknown entity until it attacked a common enemy of the enigmatic Russian hacktivist group Killnet and was inaugurated in the Killnet cluster by former Killnet leader KillMilk. Leveraging the Killnet brand to lift itself out of anonymity (pun intended), Anonymous Sudan quickly became a force to reckon with.

In the first few months of 2023, Anonymous Sudan's primary tactic was Web DDoS attacks from public cloud servers, hiding attack sources behind and across thousands of HTTPS/SOCKS proxies. After the attacks on Denmark, Anonymous Sudan's IBM/SoftLayer Cloud servers were flagged for abuse and taken down. Anonymous Sudan continued its attacks after its servers were taken offline, most probably migrating their operations to a bulletproof[1] cloud provider. Attacks from Anonymous Sudan were characterized by Web DDoS attacks combined with alternating waves of UDP and SYN floods. Attacks originating from tens of thousands of unique

[1] Hosting services that offer anonymous secure dedicated servers, virtual private servers and domains, without restrictions on content and activities. Operators of bulletproof services ignore abuse and takedown requests.

source IP addresses and UDP traffic reaching up to 600 gigabits per second (Gbps) while HTTPS request floods reached in the several million requests per second (RPS).

In the second half of 2023, Anonymous Sudan leveraged the SKYNET/GODZILLA botnet to perform attacks against Microsoft, X and OpenAI (ChatGPT). In the posted claims on Telegram for the attacks, Anonymous Sudan added the footnote that these attacks were performed with the SKYNET botnet. The SKYNET/GODZILLA botnet rents its infrastructure for DDoS attacks and provides a combination of Web DDoS, volumetric attacks (UDP Frag and UDP Amplification), TCP SYN and SYN-ACK. Through the dstat Linux command[2], SKYNET/GODZILLA demonstrated 40Gbps for L4 TCP attacks and over 200Gbps for UDP attacks, while Web DDoS (HTTPS) attacks leveraging proxies had a potential of 15 million RPS.

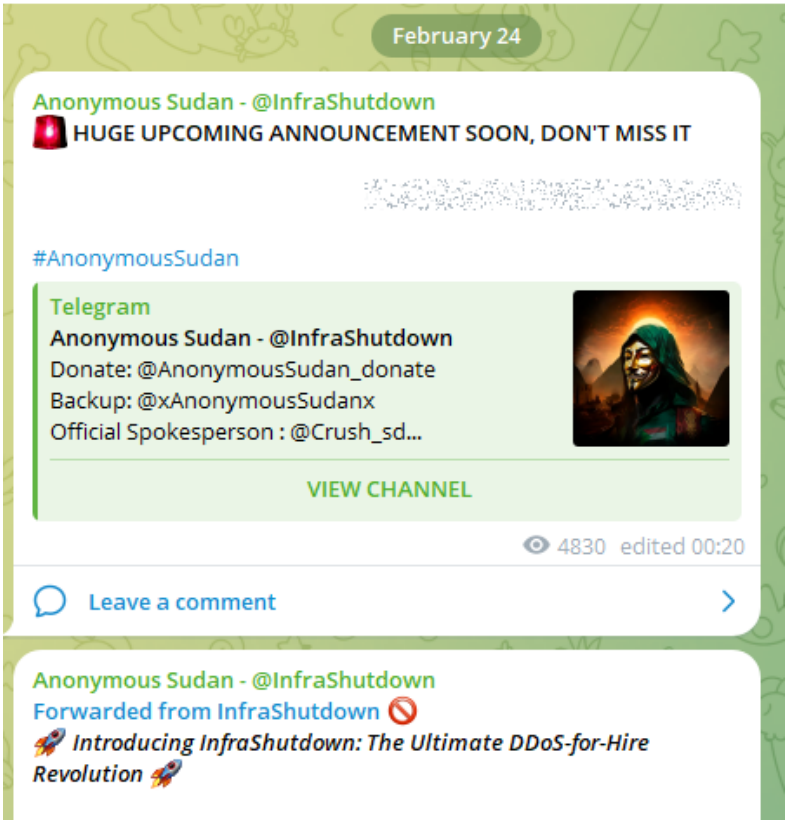
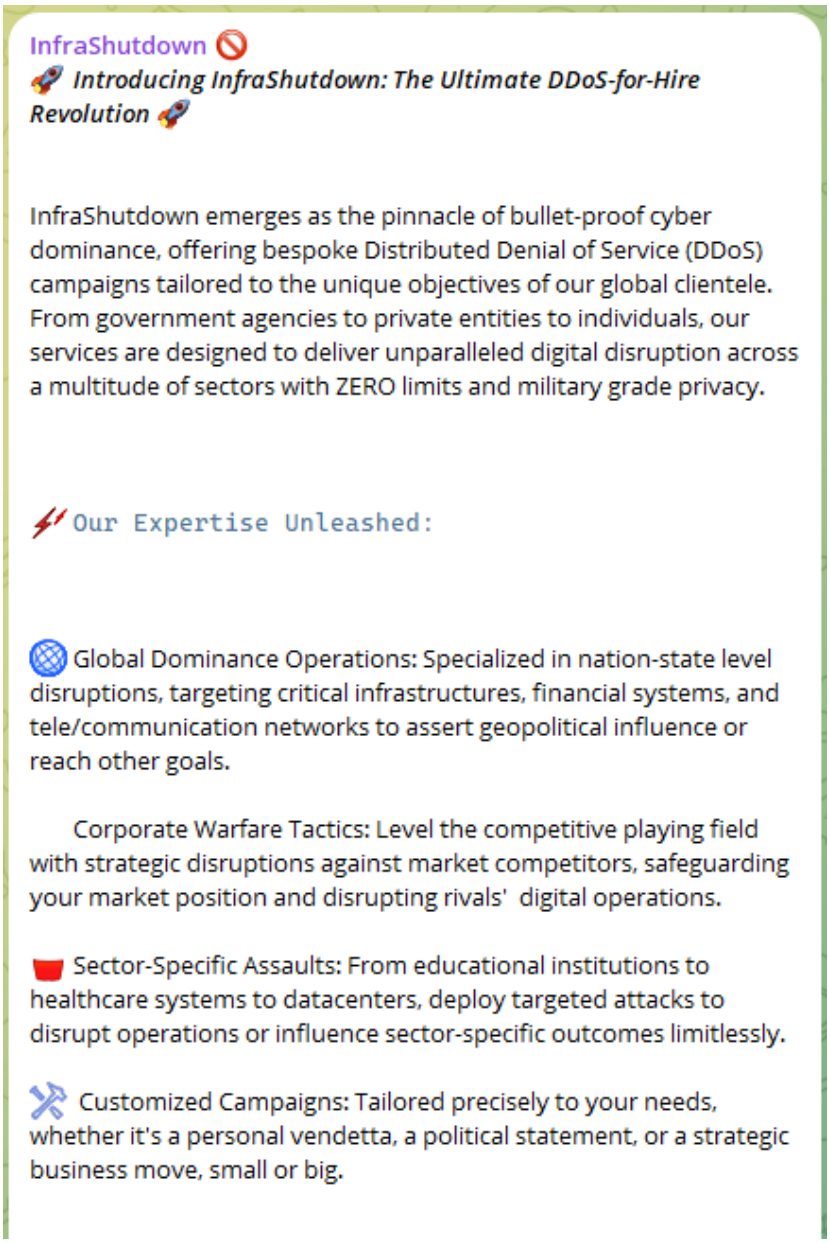


Figure 1: Pre-announcement and announcement of the InfraShutdown service (source: Telegram)

On February 24, 2024, Crush, the leader of Anonymous Sudan, announced a new DDoS service named “InfraShutdown,” labeling it as “the pinnacle of bullet-proof cyber dominance,”

[2] The dstat command in Linux provides statistics from system components such as network connections, IO devices, CPU, … Dstat servers office free L3/L4/L7 dstat statistics to DDoS-for-Hire operators to check the power of their booter or stresser services.

offering DDoS attack campaigns tailored to the needs of its global clientele with military-grade privacy. This supposedly new DDoS-for-hire service was described as “specialized in nation-state level disruptions, targeting critical infrastructures, financial system, and telecommunication networks” in an announcement forwarded by the @InfraShutdown Telegram channel that was created on February 24, 2024, coinciding with the date of the announcement.



InfraShutdown 🚫

🚀 ***Introducing InfraShutdown: The Ultimate DDoS-for-Hire Revolution*** 🚀

InfraShutdown emerges as the pinnacle of bullet-proof cyber dominance, offering bespoke Distributed Denial of Service (DDoS) campaigns tailored to the unique objectives of our global clientele. From government agencies to private entities to individuals, our services are designed to deliver unparalleled digital disruption across a multitude of sectors with ZERO limits and military grade privacy.

⚡ Our Expertise Unleashed:

🌐 Global Dominance Operations: Specialized in nation-state level disruptions, targeting critical infrastructures, financial systems, and tele/communication networks to assert geopolitical influence or reach other goals.

Corporate Warfare Tactics: Level the competitive playing field with strategic disruptions against market competitors, safeguarding your market position and disrupting rivals' digital operations.

🪣 Sector-Specific Assaults: From educational institutions to healthcare systems to datacenters, deploy targeted attacks to disrupt operations or influence sector-specific outcomes limitlessly.

🛠 Customized Campaigns: Tailored precisely to your needs, whether it's a personal vendetta, a political statement, or a strategic business move, small or big.

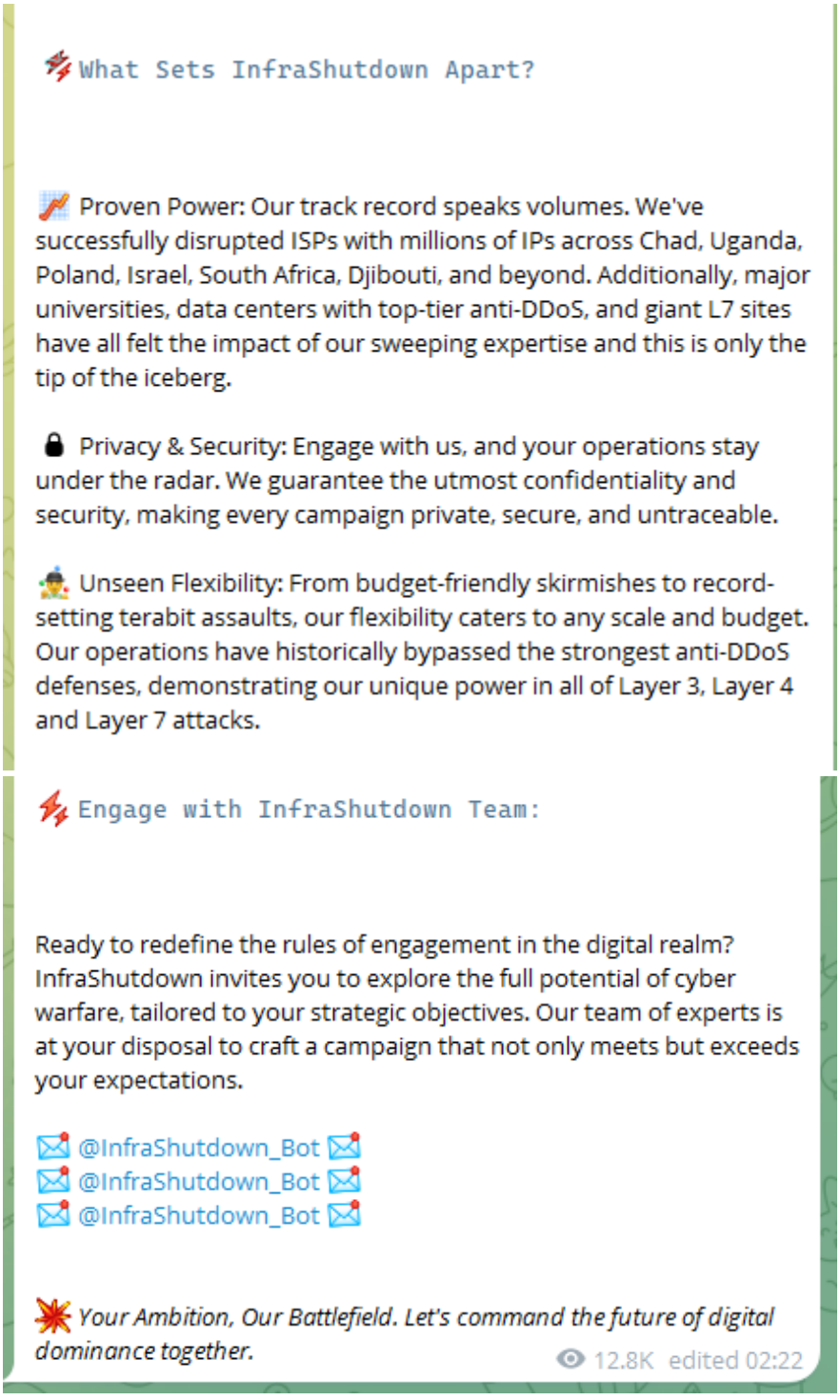


Figure 2: InfraShutdown service announcement (source: Telegram)

An Exclusive Service

New subscribers are asked to provide visual proof of their crypto balance. No proof, no admittance. Typical booter and stresser services are very lenient in their terms for users to subscribe and openly advertise their (cheap) prices on Telegram. It looks like InfraShutdown is attempting to create an exclusive offering, targeting a market with very specific needs and a requirement for more serious attack power.

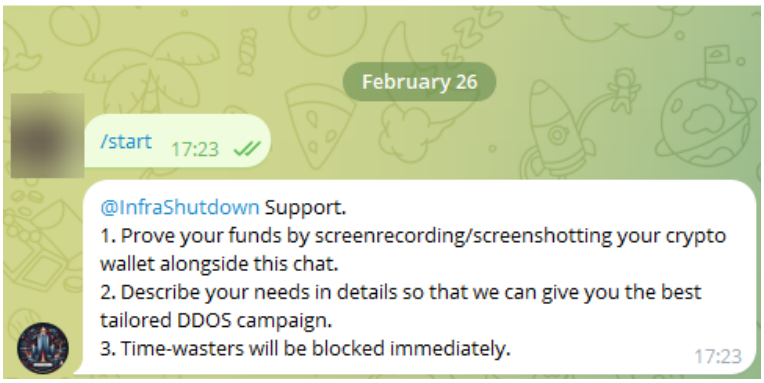


Figure 3: Requirement to provide visual proof of funds in a crypto wallet to join the service (source: Telegram)

Promotion

Through its Telegram channel @xAnonymousSudan, which reaches over 55,000 subscribers as of February 28, 2024, Anonymous Sudan promotes the new service through advertisements and by claiming denial of service attacks against highly visible and public targets. Note that the original @AnonymousSudan channel reached over 120,000 subscribers before it got banned, forcing the group to start anew with an alternative channel named @xAnonymousSudan.

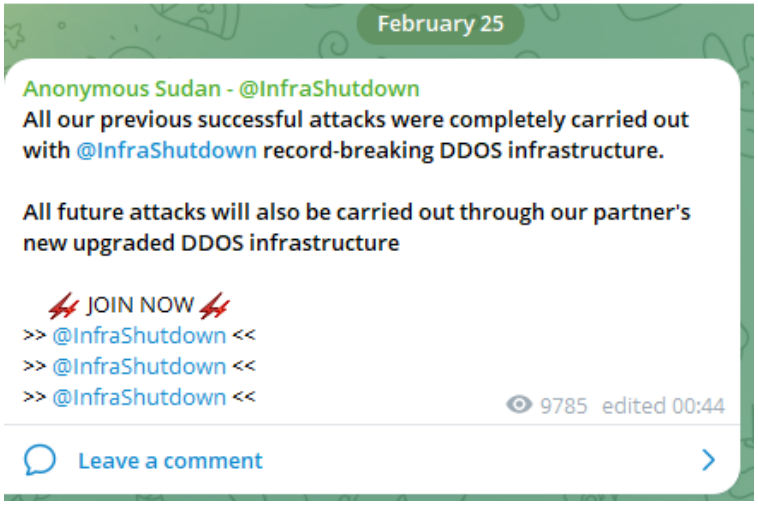


Figure 4: Advertising the services of InfraShutdown on its Telegram channel (source: Telegram)

On several occasions, Anonymous Sudan invites journalists to get in touch to receive early notifications of future attacks, describing the potential relation as a “cooperation.”

Figure 5: Inviting journalists to get in touch to receive early notification of future attacks (source: Telegram)

On other occasions, Anonymous Sudan was seen publishing positive “customer” reviews following InfraShutdown campaigns.

Figure 6: Positive feedback from a happy InfraShutdown “client”

In the days leading up to and following the announcement, Anonymous Sudan claimed attacks on several highly visible targets in multiple countries that were followed by proofs of impact based on messages in social media and industry-accepted sources that monitor network reachability and availability.

Figure 7: Advertising the services of InfraShutdown on its Telegram channel (source: Telegram)

In the last couple of days, several entities have reported disruptions after Anonymous Sudan claimed DDoS attack campaigns targeting them, including a hospital in North America, a university in the United Kingdom, two mobile providers in Israel, two satellite communication providers in the United Arab Emirates, a mobile provider in Egypt and several Israelian universities.

Reasons for Concern

Given the track record of Anonymous Sudan, this announcement should not be ignored, and InfraShutdown could become a serious threat to the infrastructure of nations and organizations. It is still unclear whether the new service is an evolution of the SKYNET/GODZILLA service or a breakup from the former, introducing the underground to a new potent DDoS-for-hire service that provides improved attack vectors and an increased capacity. As such, we might be looking at claimed multi-terabit-per-second volumetric attacks, Layer 4 attacks and high-scale RPS Web DDoS attacks. The new service differentiates itself by a high level of exclusivity for joining, compared to SKYNET/GODZILLA or other publicly available booter and stresser services. It is unclear at the time of writing if InfraShutdown is a partnership, cooperation or operation by Anonymous Sudan.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.