July 24, 2024

Six-day, 14.7 Million RPS Web DDoS Attack Campaign Attributed to SN_BLACKMETA

Key Attack Insights:

- Web DDoS attack campaign lasted six days and peaked at 14.7 Million RPS
- Featured multiple attack waves amounting to a total of 100 hours of attack time
- Sustained an average of 4.5 million RPS
- Targeted a financial institution in the Middle East
- Averaged a 0.12% ratio of legitimate to malicious web requests
- Attributed by Radware to SN_BLACKMETA, a pro-Palestinian hacktivist with potential ties to Sudan that may operate from within Russia
- Possibly leveraged the InfraShutdown premium DDoS-for-hire service

This year has been marked by a record-breaking six-day attack campaign consisting of multiple four to 20-hour Web DDoS waves, amounting to a total of 100 hours of attack time and sustaining an average of 4.5 million RPS with a peak of 14.7 million RPS.

Figure 1: Ten waves of the Web DDoS attack campaign (source: Radware)

During the six days, a financial institution located in the Middle East was under attack 70% of the time. While under attack, the ratio of legitimate to malicious web requests was as low as 0.002% and averaged 0.12%. Radware's Web DDoS Protection Services stopped more than 1.25 trillion malicious web requests while leaving 1.5 billion legitimate web requests untouched.

	Wed	Thu	Fri	Sat (AM)	Sat (PM)	Sun (AM)	Sun (AM)	Sun (AM)	Mon (AM)	Mon (AM)	6 days
Duration [hours]	12.05	11.60	19.85	7.18	4.16	6.58	10.02	9.82	9.83	10.00	**101.09**
% time under attack	50.21%	48.33%	82.71%	59.83%	34.67%	54.83%	83.50%	81.83%	81.92%	83.33%	**70.20%**
Max RPS	5,528,829	14,652,566	13,538,520	13,558,301	3,048,283	5,285,425	10,196,679	5,571,367	9,717,985	7,416,667	**14,652,566**
Avg RPS	2,339,163	6,935,632	4,488,406	5,379,275	978,664	985,130	3,265,967	1,065,804	2,444,654	3,402,565	**4,408,825**
Received Req	101,402,734,075	289,978,805,092	321,100,614,286	139,484,602,358	14,719,117,639	23,416,544,333	117,836,106,031	37,708,179,334	86,785,229,407	122,356,266,667	**1,254,788,199,222**
Dropped Req	101,158,022,259	289,925,578,273	320,582,965,583	139,426,394,363	14,716,282,276	23,379,395,212	117,325,706,311	37,665,669,152	86,751,607,095	122,354,407,670	**1,253,286,028,194**
Passed Req	244,711,816	53,226,819	517,648,703	58,207,995	2,835,363	37,149,121	510,399,720	42,510,182	33,622,312	1,858,997	**1,502,171,028**
% legitimate	0.24%	0.02%	0.16%	0.04%	0.02%	0.16%	0.43%	0.11%	0.04%	0.002%	**0.12%**

Figure 2: Statistics of the ten-wave, six-day Web DDoS attack campaign (source: Radware)

Throughout the attack campaign, the attacker tried several times to overrun the customer's web applications but failed to impact the services. Ultimately, after six days and 100 hours of generating malicious web requests, the attacker moved on.

Attribution

A few days before the attack, an actor by the name of SN_BLACKMETA announced an attack campaign on its Telegram channel mentioning the financial institution. Based on the motivation, common traits with earlier threat groups and threats announced by the group, Radware's Cyber Threat Intelligence (CTI) attributes the attack campaign to the hacktivist threat group SN_BLACKMETA. CTI assumes that the infrastructure leveraged during the attack might be part of the InfraShutdown DDoS-for-hire service, a premium service with subscription fees that range from $500 for a week up to $2,500 for a month.

The Rise and Unfolding of SN_BLACKMETA

The digital age has brought about complex shifts in how conflicts surface and manifest. One such emerging player in the cyber warfare landscape is the Telegram channel "**SN_BLACKMETA**," established on November 14, 2023. The initial content on this channel set the tone for its future endeavors, featuring updates on cyberattacks targeting Israeli and Palestinian infrastructure, primarily through distributed denial of service (DDoS) attacks. These early posts laid a strong foundation for the group's operations and clearly indicated their ideological stance.

Just days after its inception on November 18, 2023, SN_BLACKMETA announced a significant escalation in its cyber offensive. This proclamation was not just empty rhetoric, as it was immediately followed by a series of attacks on November 22 and 24, targeting websites in Israel, Canada and Saudi Arabia. The group's audacity and range of targets grew, leading to notable assaults on infrastructure such as the International Airport of Azrael and the Saudi Ministry of Defense on January 23 and 24, 2024.

The surge in activities continued into March 2024. During this period, SN_BLACKMETA executed multiple attacks including those on French infrastructure, Israel's Smart Shooter company, Israeli telecom companies and the Tel Aviv Stock Exchange. April saw no decline in their fervor; instead, they focused on UAE's digital infrastructure, Israeli scientific and technological websites, and a range of Western entities. By May and June 2024, the group had broadened its target range extensively, launching cyber campaigns against tech giants and highly visible organizations like Microsoft, Yahoo, Orange and the Internet Archive in addition to further UAE infrastructure.

Amidst this flurry of cyber activity, a pivotal figure emerged. In March 2024, the X user @Sn_darkmeta was created, proclaiming himself as the leader of SN_BLACKMETA. The self-styled "Great Leader DarkMeta" routinely began his posts with big declarations. They reposted images and summaries of the actions and attacks reported on the Telegram channel, crafting a persona that bolstered the group's visibility and ideological messaging.

Figure 3: Sn_darkmeta user profile on X (source: x.com)

The primary motivation driving SN_BLACKMETA's activities is a strong pro-Palestinian ideology. The group positions its attacks as retribution for perceived injustices against Palestinians and Muslims. Their targets typically include critical infrastructure such as banking systems, telecommunication services, government websites and major tech companies, all reflecting a strategy to disrupt entities viewed as complicit in or supportive of their adversaries.

Figure 4: Darkmeta announcing attacks targeting highly visible organizations on its SN_BLACKMETA channel (source: Telegram, Telegram)

SN_BLACKMETA is not shy about publicizing its successes. It regularly updates its audience, often providing screenshots and links to validate its claims. This transparency not only legitimizes its actions but also rallies support and garners attention from wider media channels. It openly

encourages the publicizing of its activities to amplify its cause, leveraging user complaints and third-party validations to substantiate the impact of its operations.

Interestingly, based on observed timestamps and activity patterns, it is plausible that the actors behind these attacks may be operating in a time zone close to Moscow Standard Time (MSK, UTC+3) or other Middle Eastern or Eastern European time zones (UTC+2 to UTC+4). Their operational hours, stretching from early morning to late evening, align well with typical active hours in these regions. Another compelling possibility, besides being located in the Moscow time zone, is that the group could be pro-Sudanese.

In the context of SN_BLACKMETA, the abbreviation “SN” could plausibly stand for “Sudan.” This interpretation aligns not only with the group’s activity patterns and time zones but also with the content and focus of their operations.

A deeper look at SN_BLACKMETA reveals striking similarities with Anonymous Sudan in terms of ideological motivations, attack methodologies, target selections and attack patterns. Both groups are driven primarily by pro-Palestinian sentiments, anti-Western stances and reactions to geopolitical developments involving Muslim countries. By disrupting high-impact infrastructures, they aim to create visibility for their causes and leverage their cyber capabilities effectively.

month	Anonymous Sudan	SN_BlackMeta
2023-01	40	0
2023-02	128	0
2023-03	106	0
2023-04	237	0
2023-05	99	0
2023-06	57	0
2023-07	60	0
2023-08	7	0
2023-09	1	0
2023-10	2	0
2023-11	1	0
2024-01	2	0
2024-03	0	1
2024-04	0	2
2024-05	0	21
2024-06	0	61

country	Anonymous Sudan	SN_BlackMeta
United States	98	42
United Arab Emirates	28	13
Israel	204	10
France	56	8
Sweden	94	5
Netherlands	27	4
Belgium	1	2

Figure 5: Number of attacks over time and targeted countries for Anonymous Sudan and SN_BLACKMETA

Considering the number of attacks claimed per month by Anonymous Sudan and SN_BLACKMETA (see Figure 5), it becomes apparent that the slowing number of claimed attacks by Anonymous Sudan coincides with an uptick in attack claims by SN_ BLACKMETA, the ending of the former separated by a single month with the initial start of the latter. When comparing the

most targeted countries by both hacktivists, the top targeted countries by SN_ BLACKMETA were also top targets for Anonymous Sudan. Moreover, all of the attacks claimed by SN_ BLACKMETA were in countries that were also previously targeted by Anonymous Sudan. When comparing the countries targeted by Anonymous Sudan, almost 70% of the countries Anonymous Sudan attacked were also targeted by SN_ BLACKMETA.

Based on an analysis of the language, style, attack methods and shared ideological motivations, it is reasonably likely that messages on both the SN_BLACKMETA and Anonymous Sudan channels could have been posted by the same individuals or closely collaborating individuals. The shared characteristics in style and content strongly suggest a coordinated effort or at least a significant overlap in the operational and strategic direction of both groups.

The Telegram channel Anonymous Sudan, according to TGStat.ru, was created from within Russia and its initial language was set to Russian. While most posts by Anonymous Sudan were in Arabic and English, initial posts also contained Russian. The SN_BLACKMETA Telegram channel has no geography or language listed, however the X account profile in Figure 6 shows it was created in Staraya Russa, a town in Novgorod Oblast, Russia. Although SN_BLACKMETA posts some announcements to its Telegram channel in three languages (English, Arabic and Russian), other posts are just in English and Arabic (see Figure 4).

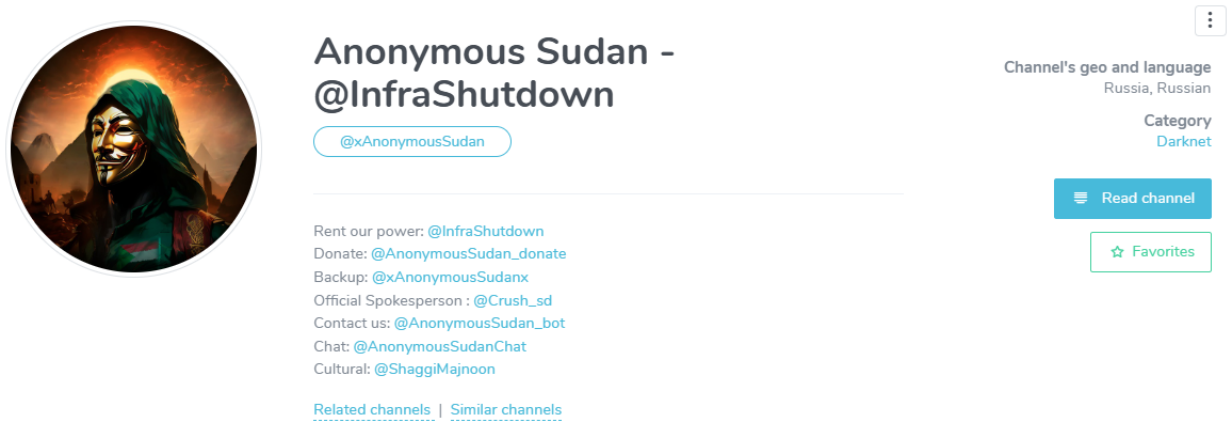

Figure 6: Properties of the Anonymous Sudan Telegram channel (source: TGStat)

The motivations for a hacktivist group like SN_BLACKMETA to target organizations in the UAE can be drawn from a combination of political and ideological alignment with the Palestinian cause, opposition to UAE's normalization with Israel, and broader regional political dynamics. High-profile attacks on prominent UAE organizations provide significant opportunities for these groups to increase their reputational influence and visibility.

Moreover, SN_BLACKMETA mentions collaborations with other hacktivist groups, such as Killnet, Ghosts of Palestine and subsets of the broader Anonymous collective. These alliances enhance

their capabilities and extend the reach of their operations. By marketing tools and services like DDoS-for-hire, malware, and cyberattack training, they have adopted a structured approach to expanding their influence and operational capacity.

To understand the roots of SN_BLACKMETA's potential Sudanese ties, one needs to dive into the current conflict in Sudan. The war is fundamentally a struggle over power involving former President Omar al-Bashir, who in his later years sought to coup-proof his regime by empowering the Janjaweed as the Rapid Support Forces (RSF), a paramilitary force. This conflict erupted between the Sudanese Armed Forces (SAF) and the RSF on April 15, 2023, in Khartoum, the capital of Sudan. The ongoing conflict has severely exacerbated the economic crisis in Sudan, leading to widespread unemployment, devaluation of the Sudanese pound, and looting and damage to infrastructure. It has left the population with dwindling access to goods, services and cash. A UN report alleged that the UAE is supporting the RSF in their war against the Sudanese Armed Forces. This allegation was denied by the UAE but would explain the alternate motivations behind SN_BLACKMETA's attacks against UAE organizations.

Infrashutdown, the Premium DDoS-for-Hire Service

On February 24, 2024, Crush, the leader of Anonymous Sudan, announced a new DDoS service named "InfraShutdown." Crush labeled it as "the pinnacle of bullet-proof cyber dominance," 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. Radware Cyber Threat Intelligence (CTI) published a detailed advisory about the InfraShutdown service on February 28, 2024.

On its Telegram channel, Anonymous Sudan promoted this new service through advertisements and by claiming denial of service attacks against highly visible and public targets.

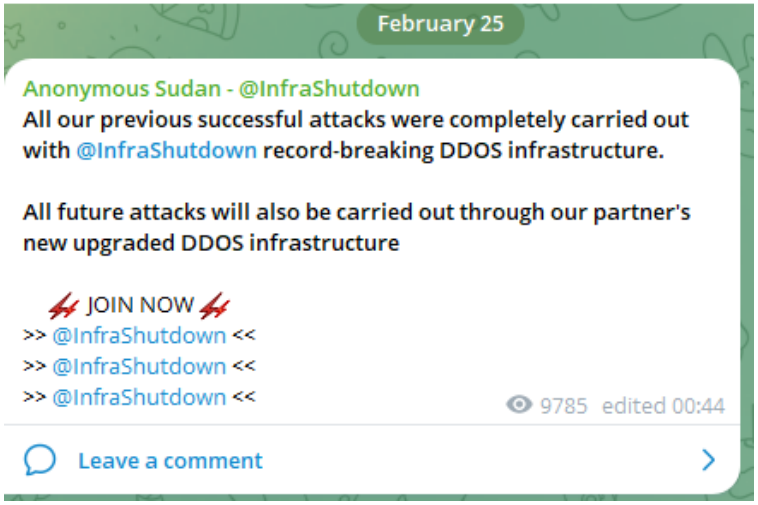

Figure 7: Anonymous Sudan advertises the services of InfraShutdown on its Telegram channel (source: Telegram)

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

In February, Radware CTI assessed that "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."

If the actors behind SN_BLACKMETA are in any way related to or support Anonymous Sudan, the premium InfraShutdown service is highly likely to be the origin of the 14.7 million RPS, 100-hour attack campaign mentioned at the beginning of this document.

Reasons for Concern

SN_BLACKMETA is a rising cyber threat, potentially located in Russia, fueled by a strong ideological stance and a strategic approach to cyber warfare. Their operations reveal a methodical expansion of targets, sophisticated public relations tactics, probable collaborations with other cyber groups, and a very likely connection to Sudan. As they continue to evolve, understanding their motivations, operational patterns and affiliations is crucial for cybersecurity efforts worldwide.

Recommendations

Mitigating attack campaigns that last several days—and sustain an average of 4.5 million RPS across 100 hours with a peak of 14.7 million RPS—requires a capable Web DDoS mitigation infrastructure with adequate capacity.

Rate limiting is not a solution for the sophistication and intensity of such attacks, considering the ratio of legitimate to malicious web requests averaged 0.12% for 70% of the time over six days. To keep the business going during the assaults, the mitigation solution had to be able to sustain the attack and differentiate 1.5 billion legitimate web requests from 1.25 trillion malicious web requests.

An inability to meet both requirements while protecting against the new, intense and sophisticated Web DDoS from hacktivists could have severe consequences for businesses across the globe.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises 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

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing 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.