baffin bay

by

2024 Retrospect

Observations from the past year's DDoS- and web application attack landscape

Executive summary

- Threat actors continued to leverage the wide selection of **DDoS-for-hire-tools** available on digital marketplaces and social media. These criminal services are an attractive choice for low-skill, entry-level actors looking to commit cyber offences.

- 2024 saw closer **operational- and strategic partnerships** form between activist hacker groups (hacktivists) and state-sponsored actors, whose alignment in attack-motivations and ideological convictions were fuelled by politics and world events.

- The so called **"silent stream"** of DDoS-attacks continued to dominate our mitigation efforts, which involves consistent and forceful flows of malicious activity that remain unattributed to a specific actor or motive.

- Unprotected web applications are vulnerable towards both denial-of-service disruptions and intrusion attempts that risk compromising sensitive information. Last year, targeted CVE-attacks and the proliferation of 3rd-party integrations in web applications contributed to a **rising number of data breaches.**

- DDoS- and web application attacks remain accessible and impactful attack vectors that appeal to a variety of different threat actors. **Adequate protection** is the only way to avoid incurring costs and reputational damage caused by unwanted downtime or breach events.

1. Introduction

This report highlights a selection of key events, trends and observations[1] from the DDoS- and web application attack landscape in 2024. In addition to intelligence collected from external sources, Threat Protection's internal metrics are used to enrich the analysis on how cyber threats manifested themselves on a customer facing-level. Moving on to a new year with new cyber security challenges ahead, a forecasting outlook on what we can expect from 2025 is provided as a concluding remark.

Five key developments

Increase in attack volumes and complexity

The past year saw an increase in both intensity and complexity among DDoS attacks, meaning that not only did attack volumes grow, but so did the threat actors' capabilities. One key indication of this development is that large, hyper-volumetric attacks are becoming more frequent. Threat actors also demonstrated a growing appetite for launching multiple attack vectors simultaneously to complicate mitigation efforts. This can be achieved for instance through targeting the application layer of a web service while launching a large TCP flood on the network level.

Most targeted sector

The financial sector stands out as the most targeted industry category. The level of attacks against the sector has seen a steady surge since 2021 and culminated in 2024[2]. According to several reports, banking and financial services were subject to a

[1] This report does not cover an all-encompassing, globally comprehensive examination of DDoS- and web application attacks in 2024. Rather, it offers a curated, digestible version of events and trends that are pertinent to Threat Protection and its scope of operations.

[2] Cloudflare DDoS Threat Report 2024 Q3, Imperva 2024 DDoS Threat Landscape Review, Radware H1 DDoS Threat Review, among others.

third of all global attack traffic during 2024. Adding to the problem, media is quick to pick up on incidents where web services that cater to large customer bases experience unwanted downtime. Banks in particular are often scrutinized in the media when their services are inaccessible due to DDoS attacks. People tend to get nervous when they cannot access their personal accounts or conduct transactions, and financial services are nowadays considered critical infrastructure in many jurisdictions. These factors, in combination with potential monetary gain to be made, make financial entities profoundly attractive targets for cyber threat actors.

DDoS-for-hire services

2024 saw a continued high-availability in DDoS-for-hire services, offered by hacker groups on criminal marketplaces and social media channels. This proliferation may come as no surprise, given how lucrative the Crime-as-a-Service-model[1] has proven itself. Yet it introduces a more pronounced financial dimension to many DDoS campaigns that stem from ideological convictions, thrill-seeking or revenge. Hacker groups who auction their infrastructure[2] can, aside from monetary profits, bolster their image through sustained marketing efforts and customer testimonies.

DDoS-suppliers may offer various types of bundles with different price points and guarantees of impact, sometimes promising the ability to take down or bypass specific ISP:s or cybersecurity providers. One example is the InfraShutdown/Godzilla botnet-service operated by the notorious hacktivist group Anonymous Sudan. For 500 USD per hour, they vowed to cripple whole country ISP:s. The group did in fact deliver on such promises with examples from Armenia and Bahrain, who suffered severe

[1] CaaS (Crime-as-a-Service) is a phenomenon where experienced cyber criminals develop and re-sell tools or services to less experienced threat actors, allowing them to carry out cyber attacks despite limited knowledge.

[2] Most commonly, this infrastructure consists of botnets in combination with misconfigured or vulnerable proxy- or amplification servers

internet outages following DDoS attacks launched by Anonymous Sudan.

Effects of geopolitics

Geopolitical tensions have served as key catalysts for numerous threat actors, most notably hacktivists and state sponsored-groups. For hacktivists, DDoS attacks on both network- and application layers are often their tool of choice, and world events influence how these groups select targets, form alliances and justify their actions. In 2024, the multiple wars fought across the Middle-East introduced new hacktivist collectives and consolidated a distinguished battleground for cyber warfare operations. A concrete example, that also affected Threat Protection's customer base, was the spike in DDoS-traffic towards Swedish web entities following its NATO accession in March. These developments have led to growing concerns and increased awareness among organizations on how world events may trigger politically motivated cyber attacks towards their online resources.

A concrete example, that also affected Threat Protection's customer base, was the spike in DDoS-traffic towards Swedish web entities following its NATO accession in March.

Web application attacks

To round up, what characterized the threat landscape of web application attacks in the past year? While DDoS attacks continue to represent one of the most common attack vectors used against web applications, they are also subject to less noisy attacks in the form of intrusion attempts. Two noteworthy trends from 2024 are the growth in targeted CVE attacks and the proliferation of 3rd-party integrations in web applications, both of which contributed to the rising number of data breaches.

According to a report from Verizon[1], web applications represent the most common entry vector for unauthorized data breaches, where CVEs and third-party vulnerabilities were increasingly exploited to reach these applications (the exploitation of vulnerabilities surged with 180% from the previous year!). These types of insidious attacks are primarily conducted by ransomware groups and other extortionist threat actors with financial incentives.

2. Threat Protection Attack Metrics

The following section outlines a selection of trends that emerged from Threat Protection's datasets.

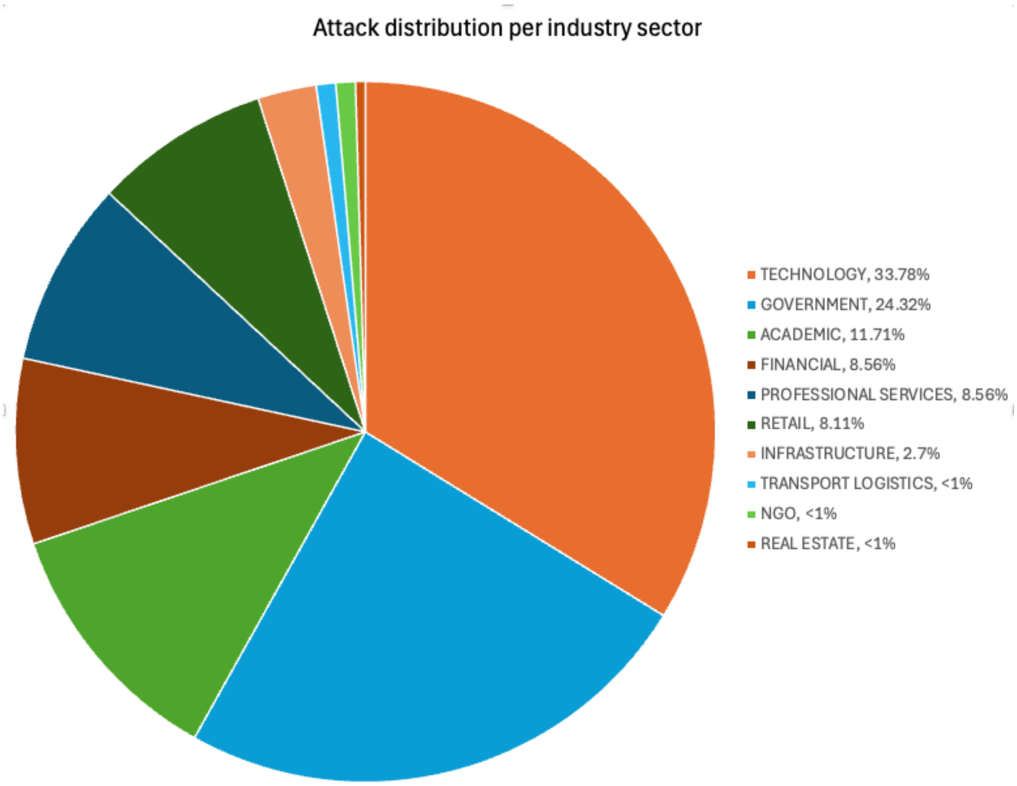
Threat Protection gathers and aggregates attack data towards its customer base, which allows for unique insights on how malicious activity manifested itself in the previous year. For starters, the vast majority of attacks we mitigated belong to the so called "silent stream" category. This stream is not labeled silent because it lacks impact or visibility, but rather due to its anonymous nature, which in turn complicates efforts to make any meaningful inferences about adversary identity or attack motivation. Even so, the category is significant in terms of its visibility in our attack statistics.

The average DDoS attack in 2024 lasted for 15.4 minutes

Top targeted industry

The technology sector was the most targeted industry category last year, receiving one third (34%) of all incoming DDoS attacks. The government sector followed in second place with 24% of the attack distribution, with academia 12% placing third.

[1] Verizon 2024 Data Breach Investigations Report

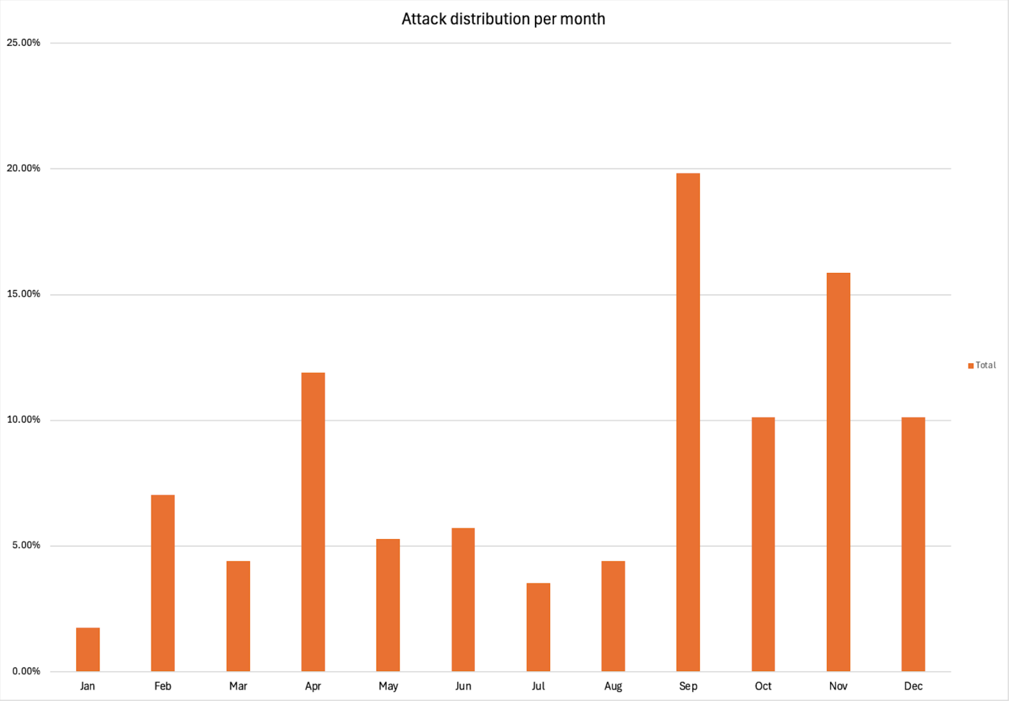


The largest attack during 2024 measured at 500 Gpbs and targeted a customer in the financial sector. The average attack duration for all industry sectors was 15.4 minutes.

Attack frequency per month

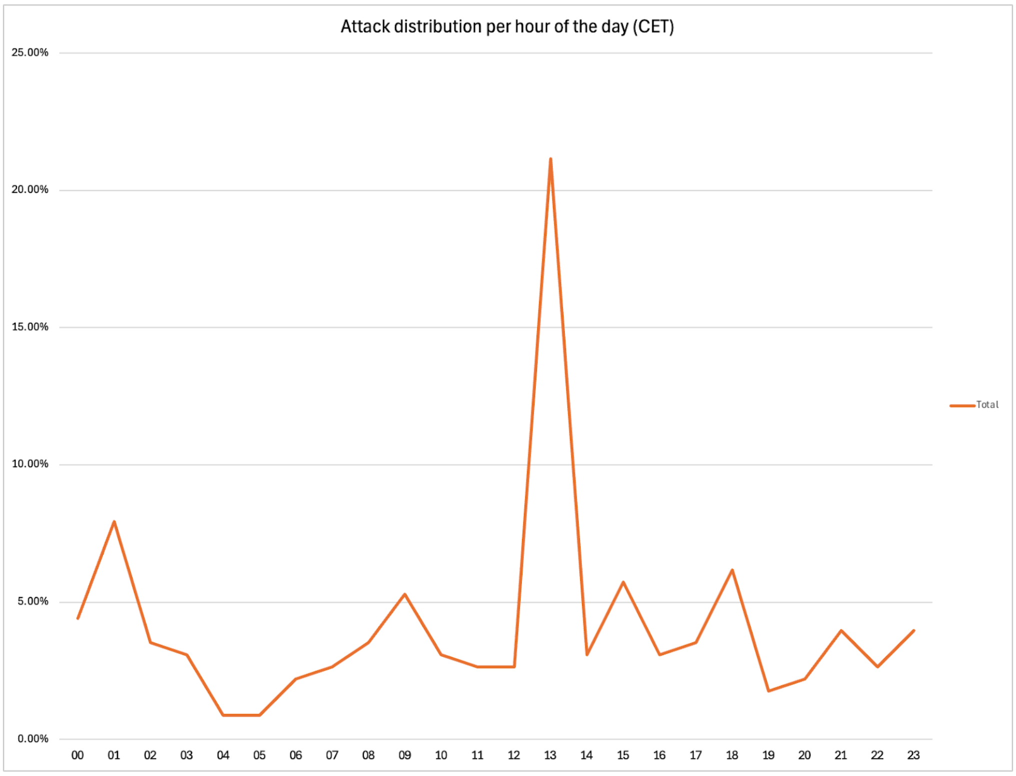
With varying levels of attack intensity throughout 2024, we saw a peak in September where the total volume of malicious traffic accounted for nearly 20% of the annual share. The cause behind the heightened attack volumes remains unknown.

In November, a pro-Russian hacktivist group attacked Swedish targets for multiple days, among them customers of Threat Protection, which is reflected in the second highest peak of the year.



Attack frequency per hour of the day

Most DDoS attacks against Threat Protection’s customers took place between 12-14 PM CET, while the lowest volumes were recorded between 04-05 AM. A likely reason behind these trends is that attackers seek to cause maximal disruption and affect as many customers of web services as possible, which can typically be achieved during daytime.



Top attack vectors for L3/L4 attacks

UDP Flood and UDP Reflection were the most commonly attacked vectors on L3/L4, accounting for nearly 39% and 34% of the total recorded attack volume.

Top 3	Vector	Share of total attack volume
1	UDP Flood	39 %
2	UDP Reflection	34 %
3	SYN Flood	14 %

3. Hacktivism and state-sponsored cyber operations: an alarming fusion

Overview

As mentioned in the previous section, DDoS attacks are generally considered hard to attribute and fingerprint. For the vast majority of attacks, the adversary who launched them remain unknown. However, hacktivism and its publicity-seeking habits offer unique opportunities to trace threat actors and their motives, which in turn yields interesting insights.

As a brief background, the concept of hacktivism saw a resurgence after Russia's invasion of Ukraine in 2022; hacker groups on both sides took on political agendas and launched DDoS campaigns across countries and organizations perceived as hostile to their nation's interests. Hacktivists are on the more volatile spectrum among cyber threat actors and may switch focus overnight based on affiliations, perceptions of world events or simply opportunistic goals as easy targets present themselves. During 2024, the hacktivist ecosystem continued to grow and cause both unsophisticated provocations but also more severe disruptions. This development can partly be attributed to the blurring lines between hacktivists and other types of adversaries; the anonymous yet noisy nature of hacktivists is leveraged by state-actors as a proxy for operational objectives that go beyond political activism. In essence, this marks an evolution where state-aligned information-campaigns become increasingly embedded into hacktivists' agendas.

One notable example is Cyber Army of Russia Reborn (CARR), a Russian state-affiliated hacktivist group with two members sanctioned by the US government[1] due to attacks against critical infrastructure in the energy sector. CARR has formed a myriad of alliances with hacker groups loyal to its anti-Western cause and reportedly share operational ties with the notorious Russian APT-group Sandworm. While the exact nature of the relationship between Russian security services and CARR remains unclear, any

[1] https://home.treasury.gov/news/press-releases/jy2473

association between hacktivist groups and state-sponsored cyber threat actors is a growing concern and warrants dedicated research-efforts from defenders, as they can be expected to amplify each other's capabilities and gain a higher level of persistence.

Another example can be found in the cybercrime ecosystem, where FunkSec, a ransomware group that emerged in 2024, shows overlap to hacktivism through its criminal activity and members. The group has been called out for recycling leaks from previously posted hacktivism campaigns, casting doubts about the accuracy of their claimed victims and level of skill. Potentially, the actors behind FunkSec have been engaged in cyber activism prior to pivoting to ransomware, which could explain their lack of sophistication. Due to the almost inherent social-media presence of hacktivists, it likely that many inexperienced threat actors become introduced to other types of malicious tradecraft and tactics than DDoS attacks.

Actor deep-dive

NoName(057)

NoName is a hacktivist group focused on countries perceived as hostile towards Russia. A distinguishing feature of the group is their reliance on volunteers who actively participate in conducting denial-of-service attacks by installing software on their own devices through the so-called "DDosia-project". The most active volunteers are allegedly rewarded with cryptocurrency. NoName's mission agendas are communicated to the volunteers through target files listing the intended targets with detailed attack calls, offered through a proxy server. This proxy appears to constitute an important choke point in the group's infrastructure, making it an obvious aimpoint for forces looking to counter or track its action. Evidence pointing to this includes frequent updates of proxy IPs and implementation of obfuscation mechanisms, well-documented by Sekoia[1], who have also observed that NoName

[1] https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/

carries out attacks when the first-level proxy server has been unreachable, suggesting the group maintains its own set of attack tools.

NoName's routine of providing detailed target lists for each attack-wave allows for the material to be researched and documented. However, a mention in a target file does not mean that an attack has been successfully carried out, only attempted. Throughout the year, we have seen several examples of purposely unresponsive nodes among the actor's targets, celebrated as successful disruptions, when in fact no downtime was actually achieved. Despite this, with insufficient protection, the attacks from this threat actor can cause disturbances for any online business, and successful attacks almost always generate future attention. This habit is emblematic of the hacktivist community in general and NoName is no exception.

NoName's routine of providing detailed target lists for each attack wave allows for the material to be researched and documented.

NoName is a good example of how the lines have blurred between cyber criminals, hacktivists and state-sponsored actors. The group combines a clear objective to punish those "unfriendly" to Russia with the ability to offer financial rewards together with persistent attack activity, which requires time and money. Moreover, findings from an Ukrainian research agency have exposed organizational overlaps between NoName and the above mentioned CARR[1]. It is fair to say that the hacktivist denomination simply no longer captures the full picture among groups like NoName.

The below numbers are based on NoName's target files where each row is considered an attempted DDoS attack. Evidently, the groups' attack volumes measured in total attempts towards

[1] https://molfar.com/en/blog/russian-cyber-army

European and non-European targets all increased in the second half of 2024, compared to the same time period in 2023.

Attack attempts	**H2, 2023**	**H2, 2024**
European country domains	87 706	118 555
Non-Europe country domains	4713	26 874
Non-country specific domains	16 900	27 549
Total	*109 319*	*172 978*

Top 3 European countries attacked in 2024.

Country	**Number of attack attempts**
Ukraine	58 176
Spain	21 560
Moldova	19 370

Top 3 Non-European countries attacked in 2024.

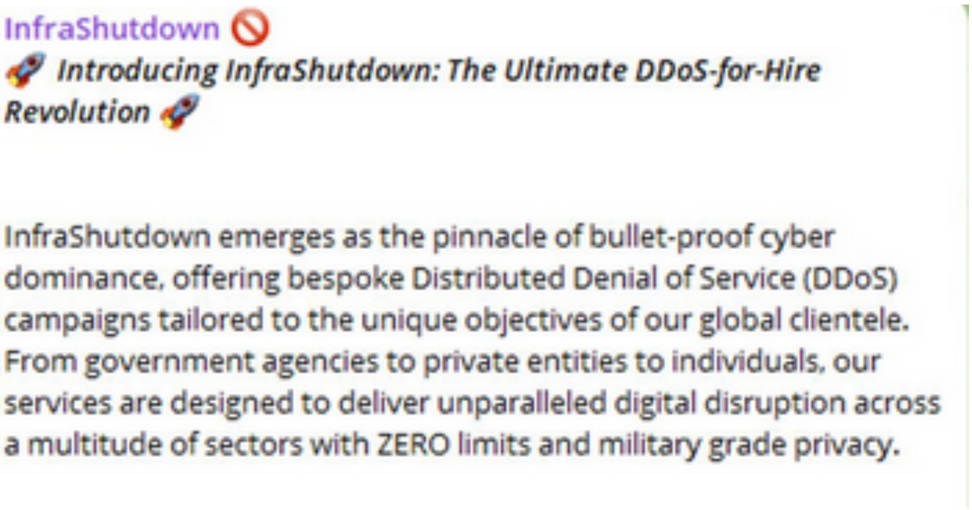
Country	**Number of attack attempts**
Taiwan	7 005
Israel	5 731
Japan	5 709

A vast majority of NoName's attacks during 2024 were geared towards port 443 that serves the HTTPS protocol.

Port number	Protocol	Share of total attack traffic
443	HTTPS	77 %
80	HTTP	18 %
22	SSH	1 %

Anonymous Sudan

In the beginning of 2023, hacktivist group Anonymous Sudan emerged on Telegram and soon became notorious for its powerful and persistent attacks that caused many painful online outages worldwide. Initially, the group communicated in Russian and English on its Telegram channel and clearly aligned itself with pro-Russian hacktivists, but later introduced Arabic as well. The group offered its own DDoS-for-hire-tool under the name Skynet, Godzilla Botnet or InfraShutdown through Telegram. Upon examination of Anonymous Sudan's attacks, it was discovered by Baffin Bay Networks[1] that they did not use a regular botnet, but instead relied on a VPS server structure that relayed attacks through vulnerable proxies. In a disruptive effort, Baffin Bay Networks knocked over 60 of the group's VPS's offline[2], putting a halt to ongoing attacks. Eventually, the group recovered and resumed their operations.



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.

In 2024, Anonymous Sudan began to attack significant targets in the United States including hospitals, big tech, finance and government, and eventually gained the attention of the FBI. In October last year it was announced[1] that two Sudanese nationals had been indicted by US authorities for their involvement in Anonymous Sudan and their associated DDoS-for-hire services. By examining the group's attack infrastructure, the FBI discovered the same as Baffin Bay Networks had, namely that VPS servers relayed attack traffic through vulnerable proxy servers, creating unusually intense attacks. The FBI-initiated action took Anonymous Sudan and their offered tools completely offline. No further details on the status of the case have been released. In the meantime, the Anonymous Sudan-group as we know it has been silenced, despite the reemergence of a new, unverified iteration on Telegram.

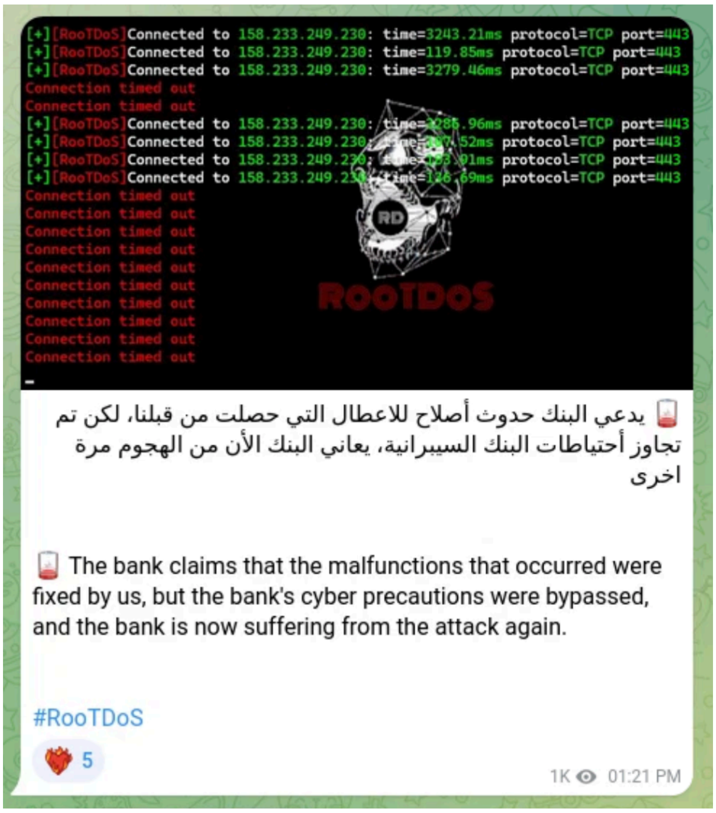
The operations of Anonymous Sudan capture the growing complexities and fusions of interests in today's threat landscape – under a Middle-Eastern hacktivist pretence, the group formed alliances with a wider community of Russian hacker groups while offering DDoS-for-hire tools for monetary gain.

RooTDos

RootDos is a newly formed threat group under a hacktivist umbrella, who claimed responsibility for a month-long, impactful attack on one of the largest banks in Northern Europe during the fall of 2024. This event captured how DDoS attacks can rise beyond background noise to cause serious reputational- and financial harm for large organizations, even when protective measures are in place. Unlike many hacktivists, RootDos has not issued an explicit manifest but expresses pro-Islamic and pro-Palestinian motives for their attacks, with the caveat of a recent anti-Iranian publication. RooTDos also deviates from the typical hacktivists denomination by maintaining an infrequently updated Telegram channel with very few followers, despite taking credit for large successful attacks. The group neither forms nor boasts

[1] https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals

about alliances with other hacktivists, or displays typical characteristics of profit-driven cyber criminals who often market a criminal service. Long and intense DDoS attacks are costly to execute, which raises further questions about RooTDos's funding and potential allegiances.



```
[+][RooTDoS]Connected to 158.233.249.230: time=3243.21ms protocol=TCP port=443
[+][RooTDoS]Connected to 158.233.249.230: time=119.85ms protocol=TCP port=443
[+][RooTDoS]Connected to 158.233.249.230: time=3279.46ms protocol=TCP port=443
Connection timed out
Connection timed out
[+][RooTDoS]Connected to 158.233.249.230: time=3286.96ms protocol=TCP port=443
[+][RooTDoS]Connected to 158.233.249.230: time=307.52ms protocol=TCP port=443
[+][RooTDoS]Connected to 158.233.249.230: time=123.91ms protocol=TCP port=443
[+][RooTDoS]Connected to 158.233.249.230: time=126.69ms protocol=TCP port=443
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
Connection timed out
_
```

🪫 يدعي البنك حدوث أصلاح للاعطال التي حصلت من قبلنا، لكن تم تجاوز أحتياطات البنك السيبرانية، يعاني البنك الأن من الهجوم مرة اخرى

🪫 The bank claims that the malfunctions that occurred were fixed by us, but the bank's cyber precautions were bypassed, and the bank is now suffering from the attack again.

#RooTDoS

Despite the problematic characterization of RootDos, the above-mentioned Nordic bank suffered from a debilitating DDoS-campaign that affected its website and online banking applications. The bank claims to have mitigated 90% of the attacks but the remaining 10% percent that got through was enough to cause serious issues. The exact cost of RootDos's attacks has not been disclosed, although it was mentioned by bank representatives that they were in the tens of millions of Euros. In addition, the target bank was called into a hearing at the Finnish parliament to discuss service outages among banking- and payment services. This shows how severe the disruptions truly were, given that they attracted interest in the highest political instances. Another lesson learned is that even a small percentage of the total attack traffic can have detrimental consequences if it gets through an organization's defensive layers.

4. Concluding remarks - what can we expect in 2025?

To wrap up, with a new year ahead of us, what can we expect from the community of bad actors deploying DDoS- and web application attacks? Here are five key forecasts:

The growing appetite for residential proxies is a headache that network defenders must prepare to deal with.

First, it is likely that the silent-stream of attacks will continue to dominate the malicious traffic against our customers. This ambiguous yet ubiquitous category of DDoS attacks has prevailed for years and there are no indications that its persistent traffic volumes will decrease in the near future. While attribution remains challenging, these streams allow us to derive both commonalities and deviations, which can in turn be leveraged to improve the defensive capabilities of Threat Protection.

Second, the growing appetite for residential proxies is a headache that network defenders must prepare to deal with. These services equip threat actors with a desirable combination of anonymity and evasion through providing a relay in home routers, devices that often do not ring alarm bells due to their wide adoption among "regular" customers. Moreover, the traffic from these devices can strategically be designed to originate from the same country as the target of the attack, further complicating mitigation efforts such as geofencing. Residential proxies have been in favour among experienced attackers such as state-sponsored groups and cyber criminals, but are now on the rise in the DDoS community. Threat Intelligence becomes a vital tool in identifying residential proxy-providers and tracking their infrastructure.

Third, what about the potential effects of artificial intelligence (AI)? The use of automation and large language models (LLM's) is trending in underground forums where threat actors are looking to find creative ways of improving the capabilities of their DDoS-for-hire-tools and web application attack-kits. This process has been ongoing throughout 2024 and will certainly continue to grow and evolve in 2025, although it is unlikely that the effects will be detrimental. The growth of automation and LLM-adoption in the wider context of cyber security threats has so far been incremental, but it is wise to exercise caution as it is happening alongside the expansion of available Crime-as-a-Service toolkits. For example, automating certain features in the pre-attack reconnaissance process prior to web application attacks could give an edge to criminal products that offer such capabilities. It is therefore critical for defenders to ensure that their protective layers can detect and deter all types of attacks, whether they are manually deployed or launched through automated means.

Fourth, we ought to witness more hybrid warfare operations where both hacktivist groups and hacker collectives are used as tools to achieve goals beyond cyber activism; this includes deceptive operations such as disinformation campaigns and attacks on critical infrastructure, done on behalf of state interests. How pronounced this development will be in 2025 is yet to be seen, but hybrid warfare-events taking place in cyberspace are likely to proliferate. Particularly since geopolitical tensions continue to run high in many regions around the world.

Finally, threat actors and the tradecrafts they employ are dynamic and constantly evolving. Denial-of-service and web application attacks will remain a considerable threat to any organization with online resources, as they represent easy yet impactful attack vectors with a growing offering of tools and services available to facilitate intrusion attempts.

Cyber Threat Intelligence Team

cti@baffinbaynetworks.com

baffin bay

by