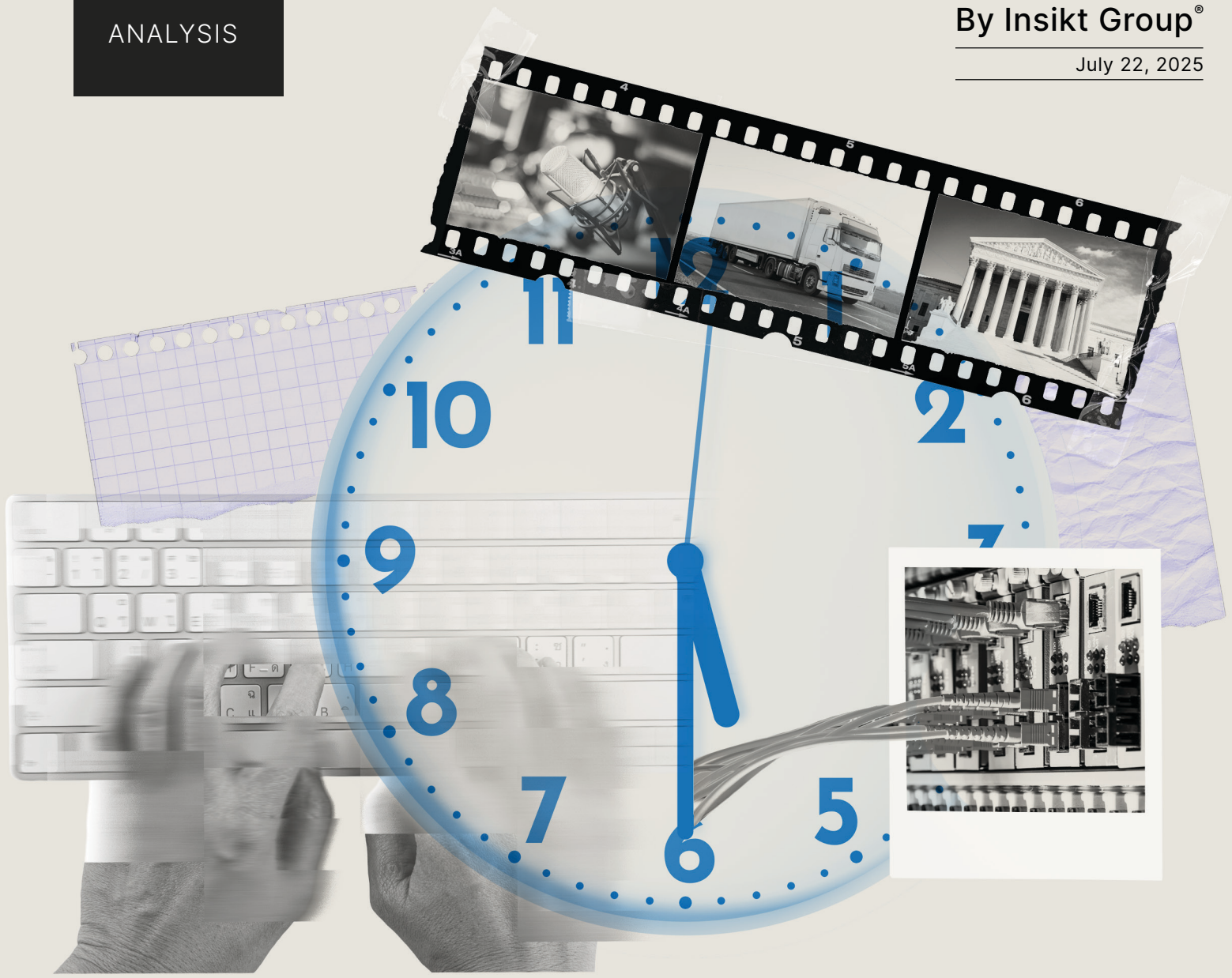
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 22, 2025



Anatomy of DDoSia:
NoName057(16)'s DDoS Infrastructure and Targeting

Pro-Russian hacktivists NoName057(16) targeted over 3,700 unique hosts from July 2024 to July 2025, primarily government and public-sector entities in European nations opposing Russia's invasion of Ukraine.

NoName057(16) uses a resilient, multi-tiered infrastructure featuring rapidly rotated Tier 1 command-and-control (C2) servers and access-controlled Tier 2 servers to enhance operational security.

NoName057(16) maintains a high operational tempo, averaging 50 unique targets daily, with activity patterns strongly indicating operations from within a Russian time zone.

Analysis cut-off date: July 17, 2025

Executive Summary

Insikt Group tracked pro-Russian hacktivists "NoName057(16)" targeting more than 3,700 unique hosts over the last thirteen months (July 1, 2024, to July 14, 2025). Targeted hosts were primarily government and public-sector entities in European nations opposing Russia's invasion of Ukraine. NoName057(16) emerged in March 2022, just days after Russia's full-scale invasion of Ukraine, and has since waged a sustained, large-scale distributed denial-of-service (DDoS) campaign through its volunteer-driven "DDoSia" platform. The threat group maintains a high operational tempo, averaging 50 unique targets daily, with intense bursts of activity correlating to geopolitical and military developments in Ukraine. In addition, leveraging Recorded Future Network Intelligence and additional methodologies, Insikt Group conducted a comprehensive technical analysis that revealed a multi-tiered infrastructure consisting of rapidly rotated Tier 1 command-and-control (C2) servers and Tier 2 servers protected by access control lists (ACLs) to restrict upstream access and maintain reliable C2 functionality. Finally, pattern-of-life analysis strongly indicates that NoName057(16) conducts its operations from within a Russian time zone.

In the short term, defenders should adopt security best practices by deploying layered DDoS protection, leveraging content delivery networks (CDNs), configuring web application firewalls (WAFs), enforcing network controls such as IP blocking and rate limiting, and establishing a tested incident response plan that includes business continuity, communication, and escalation procedures. These defensive strategies should be complemented by investments in situational awareness to anticipate emerging DDoS campaigns, monitor threat actor activity across forums and coordination channels, and track incidents affecting peer organizations and countries, which often serve as early indicators of broader targeting. Additionally, law enforcement is expected to continue playing a role in countering such activities, as demonstrated by Operation Eastwood between July 14 and 17, 2025, though the long-term effectiveness of such efforts remains uncertain.

Hacktivist-driven DDoS attacks, state-sponsored or state-encouraged pseudo-ransomware operations, disinformation campaigns, acts of physical sabotage, and other asymmetric operations have become a persistent feature of geopolitical conflict deliberately calibrated to remain below the threshold of conventional warfare. Organizations operating in these hybrid warzones — in this case, within NATO-aligned European countries — must prepare for this threat to be a long-term reality. Regardless of the specific geopolitical context, it is increasingly clear that states will both conduct such activities directly and co-opt non-state threat actors to advance their strategic agendas. Accordingly, maintaining close visibility into this evolving threat landscape and monitoring geopolitical tensions should be integral to any effective risk management strategy.

Key Findings

- NoName057(16) has implemented a multi-tiered infrastructure in which Tier 1 C2 servers rapidly refresh, with an average lifespan of nine days. These Tier 1 C2 servers are exclusively permitted to establish connections to Tier 2 servers, which are secured via ACLs.
- From June 2024 to July 2025, NoName057(16) sustained a high and steady operational tempo, launching attacks against an average of 50 unique hosts per day, with activity peaking at 91 in a single day. Over the course of the analysis period, a total of 3,776 distinct hosts were targeted.
- The attacks demonstrated clear geographic concentration, with Ukrainian organizations comprising the largest share of targets (29.47%), followed by allied countries including France (6.09%), Italy (5.39%), and Sweden (5.29%). Notably, the US has not been a primary target of DDoSia, despite its support for Ukraine.
- By sector, the government and public sectors were the most heavily targeted, accounting for 41.09% of all observed attacks. This was followed by the transportation and logistics sectors at 12.44% and the technology, media, and communications sectors at 10.19%.
- NoName057(16)'s operators likely adhere to a standard Russian work schedule as new targets are consistently added in two distinct waves daily, peaking between 05:00 and 07:00 UTC and around 11:00 UTC on weekdays.

Background

NoName057(16)

NoName057(16) is a pro-Russian hacktivist group that emerged in March 2022, shortly after Russia's full-scale invasion of Ukraine. The threat group is known for conducting distributed denial-of-service (DDoS) attacks against Ukraine and its allies, particularly NATO members. The threat group's activities are not financially motivated but are driven by a political agenda rooted in Russian nationalism. NoName057(16) operates a volunteer-based model, recruiting participants via its Telegram channels, providing them with the necessary tools and infrastructure, and rewarding contributors with cryptocurrency.

The threat group's alignment with Russia's strategic interests is clear and functions as an unofficial cyber warfare asset for Russia. This connection is consistently reinforced through the threat group's public communications on Telegram, where it frames its attacks as direct retaliation for actions taken by Russia's adversaries. For example, NoName057(16) justified attacks on Lithuanian infrastructure as "revenge for Kaliningrad" after the enforcement of EU sanctions[1], targeted Danish financial institutions for Denmark's support of Ukraine, and attacked Italian websites following "Russophobic" comments by the Italian president. This pattern highlights the threat group's role as digital partisans acting on Russia's geopolitical narrative, aiming to disrupt organizations it deems hostile.

The DDoSia Project

The threat group's primary weapon is a custom DDoS tool named "DDoSia", the successor to an earlier botnet called Bobik. The tool facilitates application-layer DDoS attacks by inundating target websites with a high volume of junk requests. The operational framework surrounding this tool is known as the "DDoSia Project", which encompasses the entire ecosystem of tools, infrastructure, and volunteers. The DDoSia client is a user-friendly, Go-based tool that communicates with a C2 server to obtain a list of targets. Volunteers run the tool on their devices, using a unique "User Hash" as an access key. This key is required to receive targets and contribute to attacks, a method likely intended to hinder analysis by security researchers. The tool is designed to be easy to use, allowing individuals with little to no technical expertise to participate in the threat group's operations.

In this report, "operators" refers to the threat actors responsible for developing the DDoSia Project and creating target lists for NoName057(16), while "volunteers" refer to the individuals who execute attacks using the DDoSia tool.

[1] *hxxps://ria[.]ru/20220627/khakery-1798513241[.]html*

Operation Eastwood

Operation Eastwood, carried out between July 14, 2025, and July 17, 2025, involved international law enforcement actions against the NoName057(16) hacktivist group. These efforts included two arrests (one preliminary arrest in France and one in Spain), seven arrest warrants issued (six by Germany and one by Spain), and 24 house searches across the Czech Republic (Czechia), France, Germany, Italy, Poland, and Spain.

In response to Operation Eastwood, the official Telegram account of NoName057(16) dismissed the law enforcement operation, urging followers not to believe "all this nonsense of foreign special services" and reaffirmed its continued commitment to the information war in support of Russia.

Threat/Technical Analysis

DDoSia Communication

Insikt Group's analysis of the DDoSia client noted a two-step process for obtaining the target list from the C2 server. The process begins with an initial client registration and authentication, after which the client fetches the encrypted target list. The entire DDoSia communication flow is illustrated in **Figure 1**.

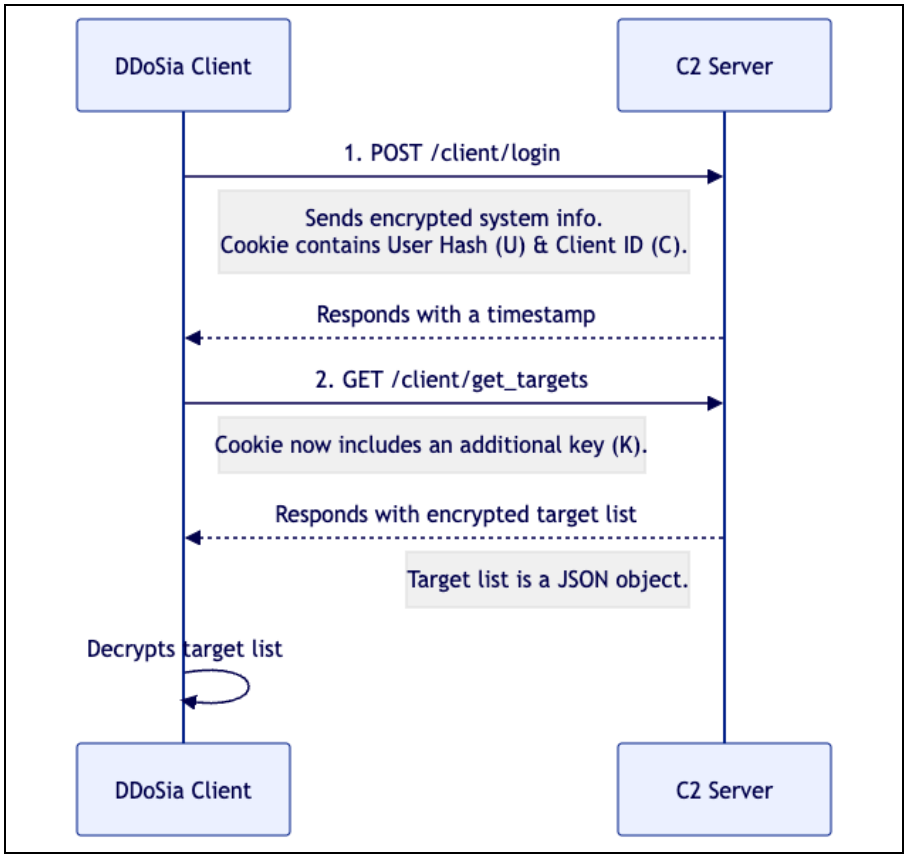


Figure 1: *DDoSia C2 communication flow (Source: Recorded Future)*

Stage 1: Client Login and Registration

The DDoSia client initiates communication by sending an HTTP POST request to the C2 server's `/client/login` endpoint. This request registers the client with the C2 server and validates its authenticity.

The request headers are designed to mimic legitimate browser traffic, using a randomized legitimate User-Agent string. A key component of the request is the Cookie header, which contains two critical values:

- **User Hash (U):** A unique identifier for the volunteer, this hash is provided to the volunteer in a `client_id.txt` file after they register via the DDoSia Project's Telegram Bot (t[.]me/DDosiabot)
- **Client ID (C):** A unique identifier for the specific client instance, generated by the bot as a UUID4 and appended with the process ID of the running executable

The body of the POST request contains a JSON payload with detailed system information of the client machine (see **Figure 2**). This information includes the `SystemUserName`, `OS`, `KernelVersion`, `PlatformFamily`, and `CPUCores`, among other details.

```
POST /client/login HTTP/1.1
Host: 38.180.143[.]83
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_1 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 [LinkedInApp]/9.28.7586
Content-Length: 515
Accept: text/html,application/xhtml+xml,application/xml,
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Cookie: U=<REDACTED>; C=<REDACTED>

{"body":"Eo+B/j5dX0s7QoVL+74DQxkUqE460PLgskFIPfAKzr4DHK6hpoYbe74kkXJLub9OSKfSt
A1mrXv4757OygFXvR89IYbjay9rzxdpNBMWEaQYag7SE6z4Ge3iqnMvN3rGRvrUI50cqcbl0Jzbav7
Kmzvt3k0H+eYgwjOI8OnG3Fuuhp+xOkPjakOmJkLrJJOTompsrIsiK7dbtFG08xp8R04S+YnCqCgRu
fYpHmQLJ0IpNy4+MKyfpzDL0bv46SSqcLZuFZdZHzaUdRjHCAglbdGNYDMeO8FU93xWbh6k/3KPk8u
5pXgSHNvLc11Ly+EddgeWjJr8qZDRr/N/HL3bhLLNqBFKKOj04aWnbg7FdspSbyF7OReIAEr2utUc7
eKAPbc6eXa2g5YcsclgdCJ1ofc0SvNZ7wiXdnkI11XRTAvaX/drsLvjAJmJ58YF2H471mVvaBIjGmV
2N8ig1ErdoHRegy7F0F1x5b6SHbcLQ5KL836olsl/722a"}
```

Figure 2: *Client login POST request (Source: Recorded Future)*

This payload is encrypted using AES-GCM before being sent to the C2 server. The encryption key is dynamically generated using a combination of the User Hash and the Client ID. The decrypted value of the body field in **Figure 2** can be seen in **Figure 3**.

```
{
    "key": "<REDACTED>",
    "user": "<REDACTED>",
    "client": "<REDACTED>",
    "inf": {
        "SystemUserName": "DESKTOP-QOG2741",
        "OS": "windows",
        "KernelVersion": "10.0.19041.2965 Build 19041.2965",
        "KernelArch": "x86_64",
        "PlatformFamily": "Standalone Workstation",
        "CPUCores": 8,
        "RegisterTime": "2025-07-10T14:22:18.134954+01:00",
        "TimeZone": "CEST"
    }
}
```


Figure 3: *Decrypted client login payload (Source: Recorded Future)*

Upon successful validation, the C2 server responds with a 200 OK status and a body containing a UNIX timestamp (As seen in **Figure 4**), which is not required in subsequent requests.


```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 14 Jun 2024 15:18:17 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 19
Connection: keep-alive

1718378297196554765
```


Figure 4: *C2 server response to login request (Source: Recorded Future)*

Stage 2: Fetching Targets

After successfully registering, the client proceeds to the second stage: fetching the list of attack targets. It sends an HTTP GET request to the `/client/get_targets` endpoint.

The headers for this request are similar to the first, but the `Cookie` header is updated to include a third parameter `K`. This `K` value is a randomly generated, Base32-encoded 256-byte sequence.

```
GET /client/get_targets HTTP/1.1
Host: 38[.]180[.]143[.]83
User-Agent: Mozilla/5.0 (X11; U; Linux i586; en-US; rv:1.0.0) Gecko/20020623
Debian/1.0.0-0.woody.1
Accept: text/html,application/xhtml+xml,application/xml,
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Cookie: U=<REDACTED>; C=<REDACTED>; K=NUYZ6Z7M42<REDACTED>DMA6NLJ4YAM======
```

Figure 5: *GET request for attack targets (Source: Recorded Future)*

The C2 server responds with a JSON object containing the attack targets. This data is encrypted using the same AES-GCM algorithm and key from the login stage. The client decrypts this response to retrieve the plaintext JSON configuration, which contains the list of targets to be targeted in the DDoS attack.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 14 Jun 2024 15:18:17 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 549871
Connection: keep-alive

{"data":"aCeegN8A+CvFX11L17b8dZpk67zwVZtTMR8R0ZhDrn3rNpFTq55dyjJ2pw8etiyLlW3SI
r8c3XVcmBpjzNXdHZYyqi8SVByLp4clIi+7gGT84…<REDACTED>.../rblN+dJq8037tw9y7HtnapY
887JRLFP0ao83w1YYed3jvjwFWWCu0vMvTjjKzuxXPDFb8KXWUMJw=="}
```

Figure 6: *Encrypted C2 response with target list (Source: Recorded Future)*

The decrypted plaintext is a JSON object containing two primary keys: `targets` and `randoms`. The `targets` key holds an array of objects, each defining a specific attack destination. Every target object includes details such as a `target_id`, `host`, `port`, and the attack `type` (for example, `http2`). The `randoms` key contains an array of objects that define parameters for generating random data to append to requests. This is likely a technique to add variability to the attack traffic, helping to bypass simple filtering mechanisms and caching. For example, one object specifies generating an 11-digit numerical string, which could be used as a random parameter in a URL (see **Figure 7**).

```
{
    "targets": [
        {
            "target_id": "64865791f747b0b90020d960",
            "request_id": "64865791f747b0b90020d961",
            "host": "<REDACTED>",
            "ip": "<REDACTED>",
            "type": "http2",
            "method": "GET",
            "port": 443,
            "use_ssl": true,
            "path": "",
            "body": {
                "type": "str",
                "value": ""
            },
            "headers": null
        },
        ...
    ],
    "randoms": [
        {
            "name": "\u0422\u0435\u043b\u0435\u0444\u043e\u043d",
            "id": "62d8286fddcbb37b0c77c87f",
            "digit": true,
            "upper": false,
            "lower": false,
            "min": 11,
            "max": 11
        },
        ...
    ]
}
```


Figure 7: *Decrypted JSON object containing attack targets (Source: Recorded Future)*

Targeting Insights

Between July 1, 2024, and July 14, 2025, Insikt Group observed DDoSia activity targeting 3,776 unique hosts to 3,812 distinct IP addresses. This consistent activity primarily focused on European nations and key industries critical to government and economic stability. Overall, the daily number of unique targets attacked ranged from a minimum of 14 to a maximum of 91, with a median of 50 targets per day (see **Figure 8**).

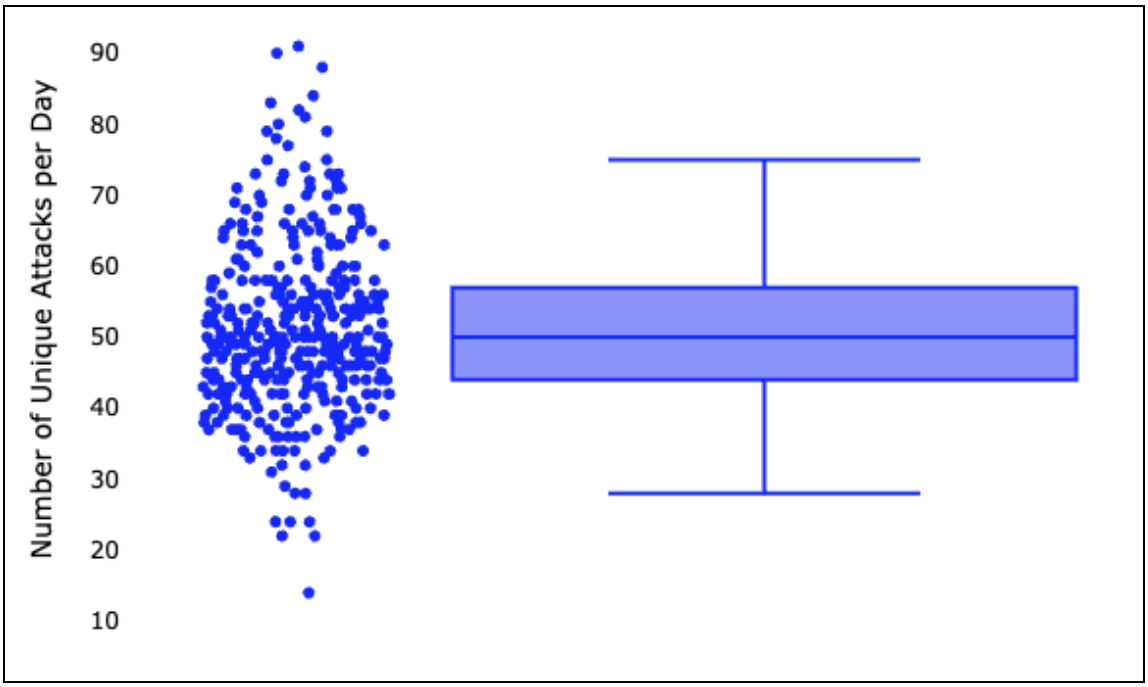


Figure 8: *Distribution of unique attacks per day (Source: Recorded Future)*

The number of unique targets remained relatively stable monthly, averaging 576 (excluding July 2025, as this is only a partial month) and reaching a peak of 669 in January 2025 (**Figure 9**).

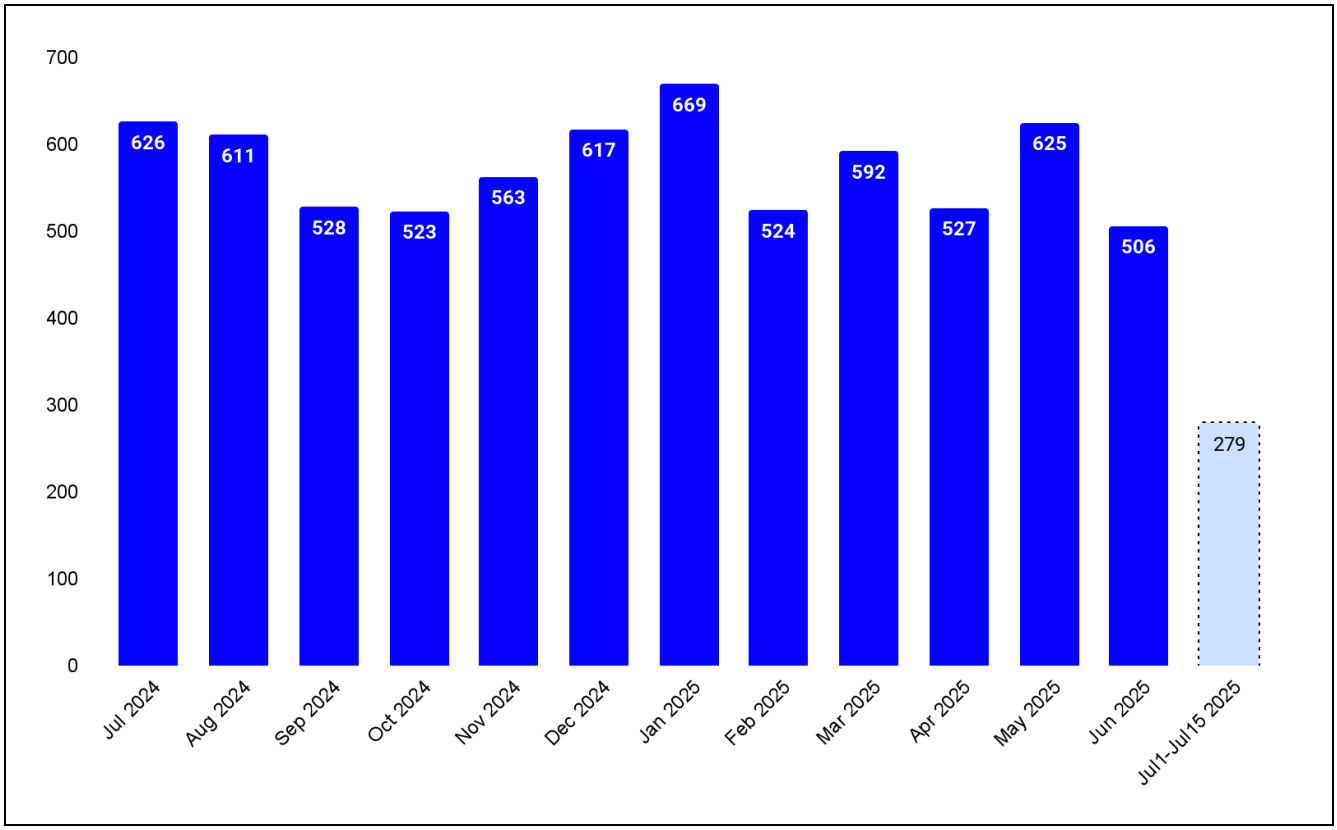


Figure 9: *Total unique targets per month (Source: Recorded Future)*

However, this high-level view obscures the significant day-to-day volatility of the threat group's operations. A more granular view of the daily unique targets reveals a consistently high and reactive operational tempo, punctuated by intense, coordinated attack waves that directly correlate with major geopolitical events (see **Figure 10**).

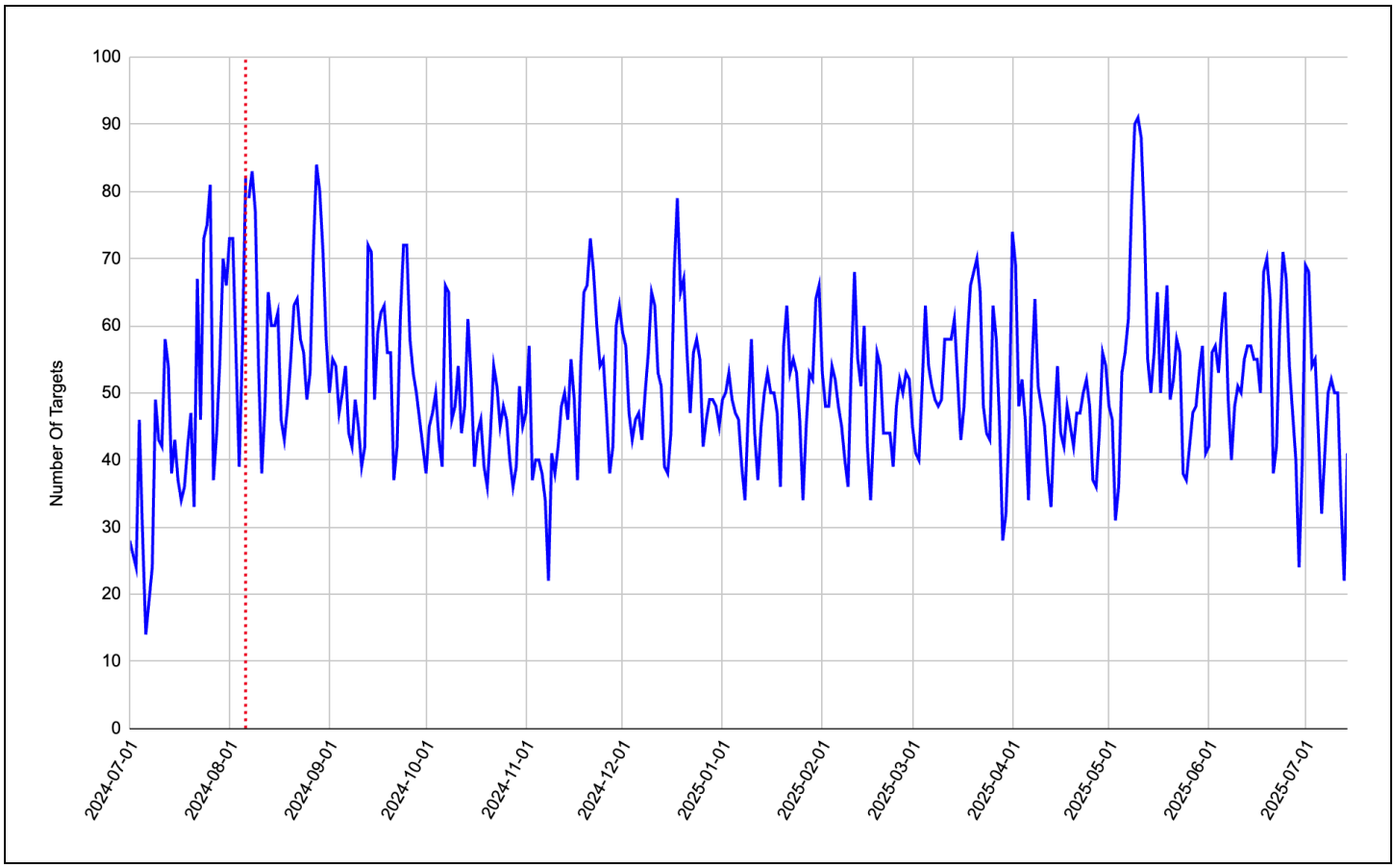


Figure 10: *Daily unique targets (the red line on August 6, 2024, marks Ukraine's ground offensive into Russia's Kursk Oblast) (Source: Recorded Future)*

The month of August 2024 provides a compelling case study of NoName057(16)'s retaliatory model in action. The threat group's attack volume surged in direct response to one of the most significant military escalations of the year: Ukraine's ground offensive into Russia's Kursk Oblast, which began on August 6, 2024.

On the day of the incursion, NoName057(16) launched a sustained, multi-day wave of retaliatory DDoS attacks, with the number of unique daily targets surging to 82 on August 6 from only 57 the day before and peaking at 83 on August 8. The campaign primarily targeted NATO member states that had condemned Russia's actions and supported Ukraine, with a disproportionate focus on entities in Poland, Italy, and Spain, particularly across government, financial, and critical infrastructure sectors. This immediate alignment between kinetic military activity and coordinated cyber operations highlights NoName057(16)'s function as a digital proxy advancing Russian state interests.

Geographic and Sectoral Focus

NoName057(16)'s targeting strategy demonstrates a clear and sustained focus on Ukraine and its European allies, alongside a strategic selection of key industries intended to maximize disruption. Analysis of the threat group's attack data highlights a dual focus on both geopolitical retaliation and the destabilization of critical economic and governmental functions.

Notably, NoName057(16) has not exhibited the same frequency of targeting entities in the US as it has with Ukraine's European allies, likely due to internal strategic choices that, for reasons unknown, appear to deliberately exclude the US.

An analysis of the total number of days each country was targeted reveals the threat group's strategic priorities and the persistent nature of its campaigns (see **Figure 11**). Ukraine was the top target, accounting for nearly 30% of attack days, highlighting the threat group's core alignment with Russia's war effort and its aim to consistently disrupt Ukrainian digital infrastructure.

Beyond Ukraine, a distinct second tier of consistently targeted countries emerges, primarily EU and NATO members, with France (6.09%), Italy (5.39%), and Sweden (5.29%) facing the most sustained campaigns, followed by Germany, (4.60), Israel (4.50%), the Czech Republic (Czechia) (4.00%), and Poland (4.00%). This pattern reflects a strategic effort to disrupt organizations linked to countries supporting Ukraine.

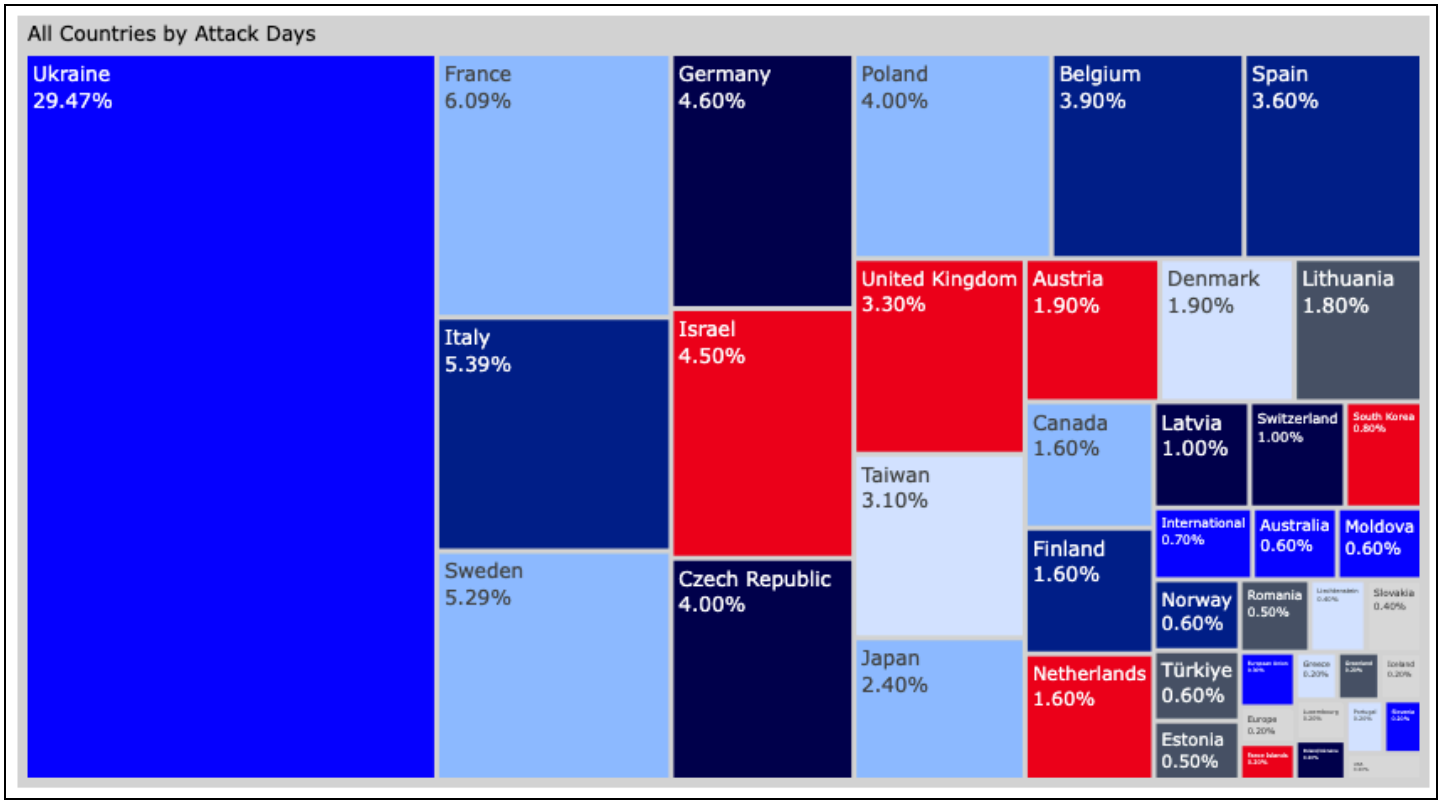


Figure 11: *Countries by total days attacked (Source: Recorded Future)*

From a sectoral standpoint, NoName057(16) concentrates its efforts on disrupting public services and critical economic functions, with the government and public sectors comprising 41.09% of all attacks (see **Figure 12**). This targeting reflects a strategic intent to erode civic trust, disrupt governance, and foster instability in affected nations.

Beyond the government and public sectors, NoName057(16) extends its focus to critical components of national infrastructure and the economy. Transportation and logistics (12.44%) and technology, media, and telecommunications (10.19%) were nearly equally targeted, reflecting an intent to disrupt supply chains and communication networks. The finance and insurance sectors (8.88%) also faced significant targeting, underscoring the threat group's aim to cause economic disruption and undermine confidence in financial systems.

Figure 12: *Target distribution by industry (Source: Recorded Future)*

Targeting Timeline Analysis

The timeline of attacks, as shown in **Figure 13**, illustrates the persistent and widespread nature of the DDoSia campaigns. While some countries experienced brief, sporadic attacks, others endured sustained and repeated targeting over several months. Attacks ranged in duration from single-day events to continuous operations lasting several weeks. Ukraine was the most persistently targeted

country, with near-continuous attack activity across the entire observation period. The longest single campaign observed targeted Ukraine for 44 consecutive days between August and September 2024. During the 13-month analysis period, Ukraine was attacked on around 80% of the days. Across all targeted countries, the average attack campaign lasted approximately four days.

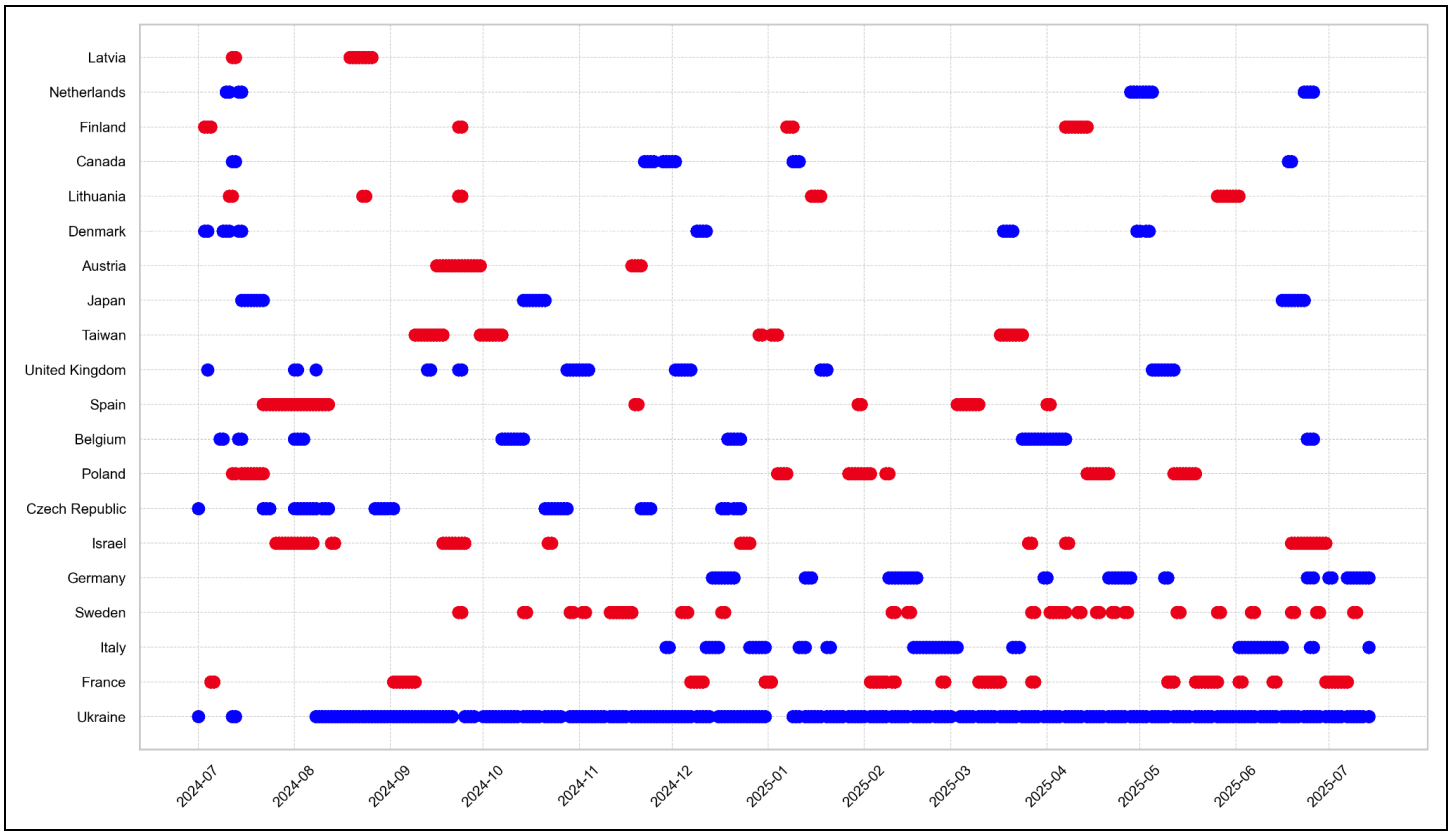


Figure 13: *Top twenty countries' attack timeline (Source: Recorded Future)*

The timeline also reveals that NoName057(16)'s targeting decisions are often highly reactive, with attack waves coinciding with specific geopolitical events and statements from Western leaders. A clear example is the brief but intense targeting of France in March 2025, when NoName057(16) launched a major wave of DDoS attacks on March 10 against multiple French government entities, including local authorities in Loire-Atlantique and Bouches-du-Rhône (1, 2). The threat group explicitly framed the attacks as retaliation for President Emmanuel Macron's statements supporting the creation of a European armed force and pledging unwavering support for Ukraine, demonstrating both the threat group's political motivation and its close monitoring of geopolitical discourse, along with its readiness to respond swiftly to positions countering Russian interests.

Italy offers another clear example, having been one of NoName057(16)'s most consistently targeted countries, with attacks frequently aligned to its political, financial, and military support for Ukraine. A notable instance occurred between February 14 and 15, 2025, when the threat group launched DDoS attacks against Italian ministries and infrastructure, explicitly linking the operation to pro-Ukraine statements made by Italian officials.

A further example is the sustained targeting of Austria in the lead-up to its September 2024 election, during which the far-right, pro-Russia Freedom Party of Austria emerged as the leading vote-getter. This activity abruptly halted following the election and only resumed in mid-November, once it became clear that the Freedom Party would be excluded from the governing coalition.

Lastly, the targeting throughout 2024 of the Czech Republic (Czechia), a major supplier of arms to Ukraine, notably ended in January 2025 after public reporting indicated that the ruling government was expected to lose the October 2025 election to the ANO party. Leaders of the ANO party, which opposes supplying artillery ammunition to Ukraine, openly stated their intention in January 2025 to halt those transfers if elected.

Attack Patterns and Techniques

NoName057(16) uses a mixture of network and application-layer DDoS attacks, selecting methods designed to overwhelm server resources and disrupt availability. The threat group's attack methodology is straightforward yet effective, prioritizing high-volume floods and resource exhaustion techniques. **Figure 14** shows the mappings of the attack methods to attack types.

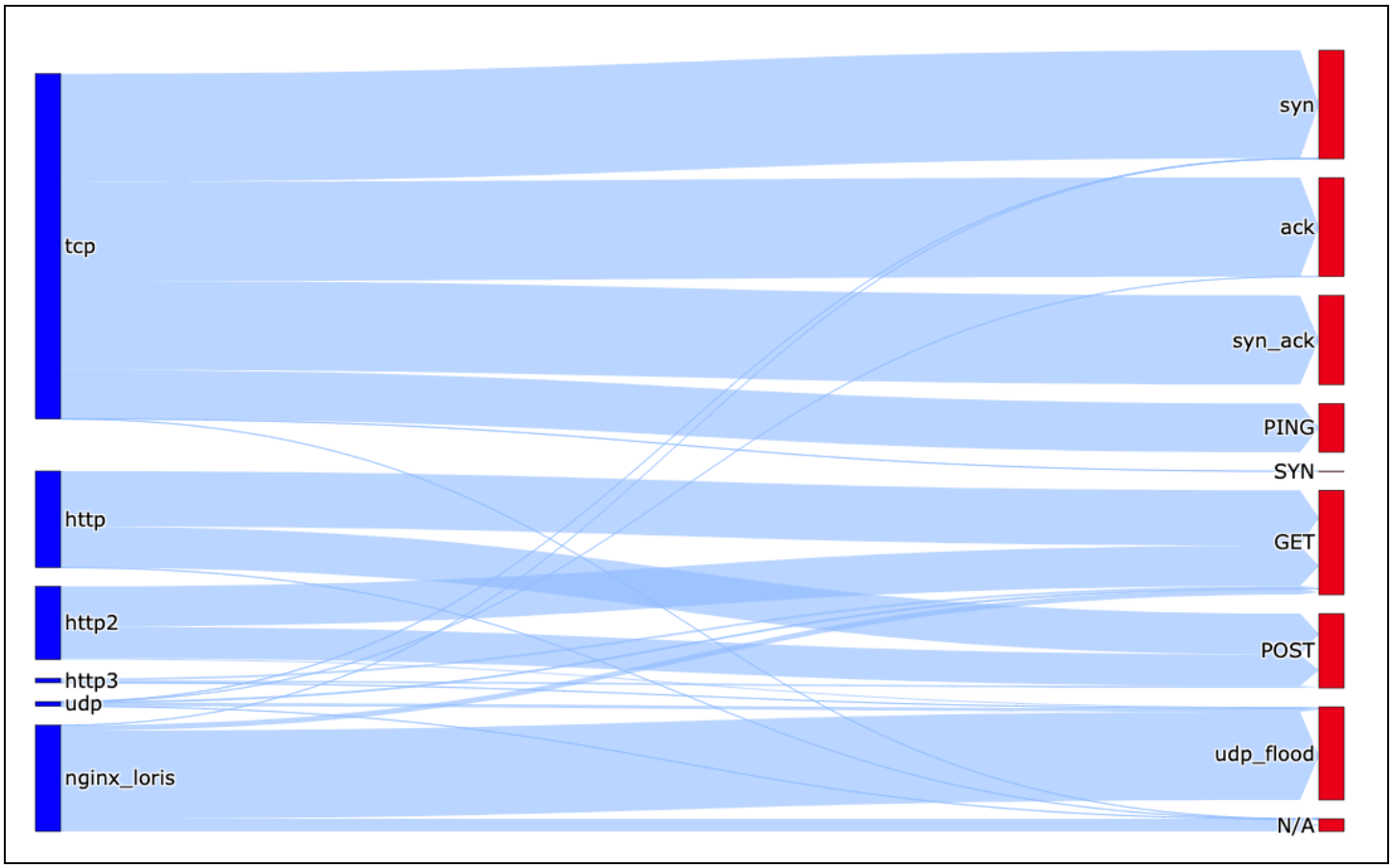


Figure 14: *Mapping of attack methods to attack types (Source: Recorded Future)*

Analysis of the threat group's most common attack methods shows a strong preference for TCP-based floods. SYN floods were the most prevalent technique, accounting for 17.6% of observed methods, followed closely by ACK floods (16.1%) and HTTP GET floods (15.4%). This selection of methods directly informs the broader categories of attacks deployed by the group.

When viewed by overall attack type, the data shows that general TCP attacks (32.7%) and "nginx_loris" attacks (31.5%) are the two most frequently observed categories. The "nginx_loris" type refers to a variant of a slow-loris attack, a low-and-slow technique designed to exhaust a web server's available connections. Unlike volumetric floods, a slow-loris attack sends partial HTTP requests at a very slow rate, keeping connections open for as long as possible. This gradually consumes all available connection slots, preventing legitimate users from accessing the service. The prevalence of both high-volume TCP floods and slow-loris variants indicates a versatile approach, allowing the group to adapt its techniques based on the target's defenses.

Analysis of targeted network ports shows that Port 443 (HTTPS) and Port 80 (HTTP) together accounted for 66% of observed attack traffic (see **Figure 15**), reflecting the threat group's consistent focus on web-facing services and its strategic objective of disrupting and disabling websites and public-facing web applications.

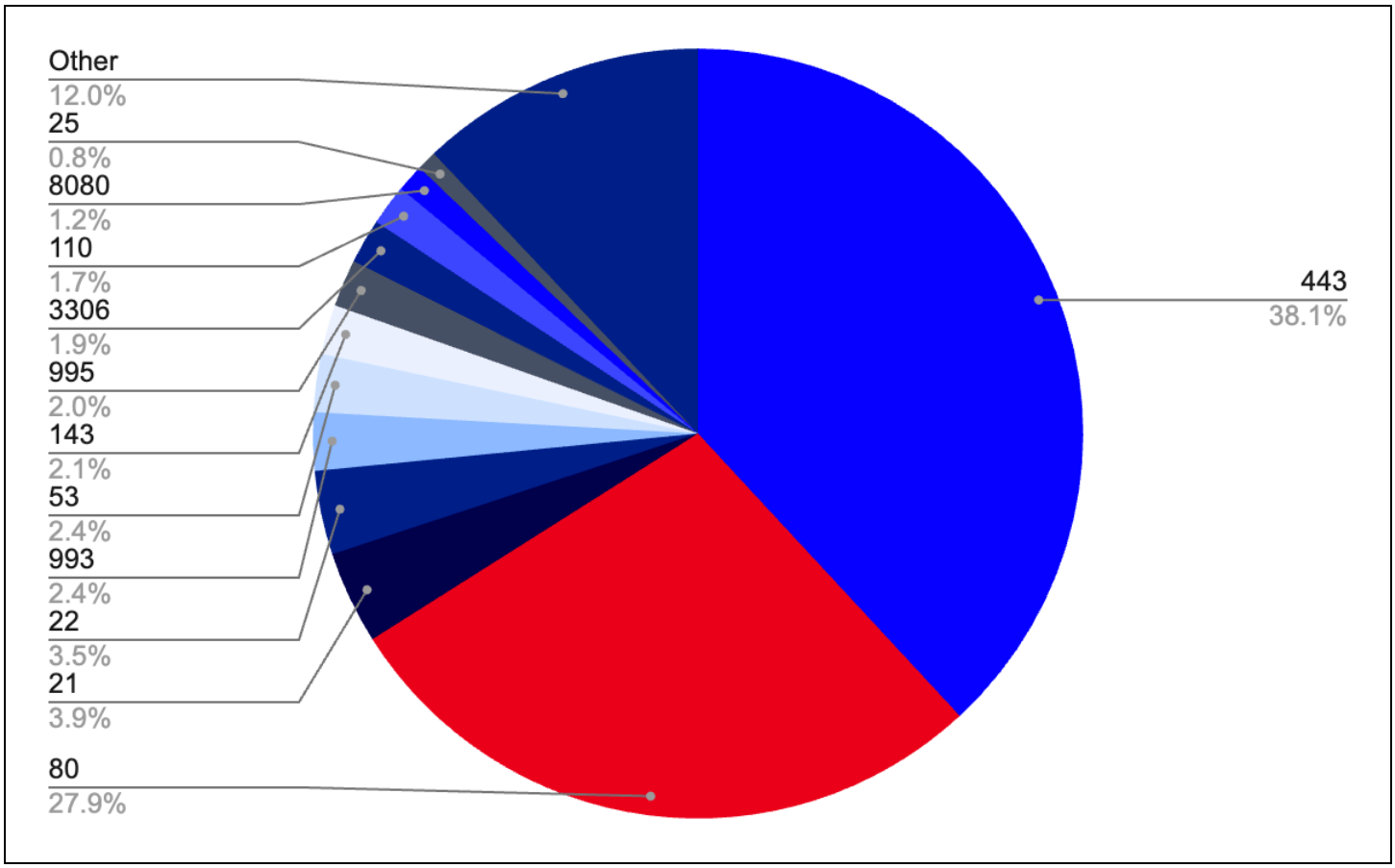


Figure 15: *Port targeting distribution (Source: Recorded Future)*

Temporal Attack Analysis

An analysis of NoName057(16)'s operational tempo reveals distinct patterns that align with a standard work week, suggesting a degree of coordination and operator discipline. Attack operations were persistent throughout the week, with the volume of targets remaining high during the standard Monday-to-Friday work week before decreasing over the weekend (see **Figure 16**). This reduction in targeting over the weekend indicates that the threat group's core operators likely adhere to a conventional work schedule, scaling back their targeting efforts on Saturdays and Sundays.

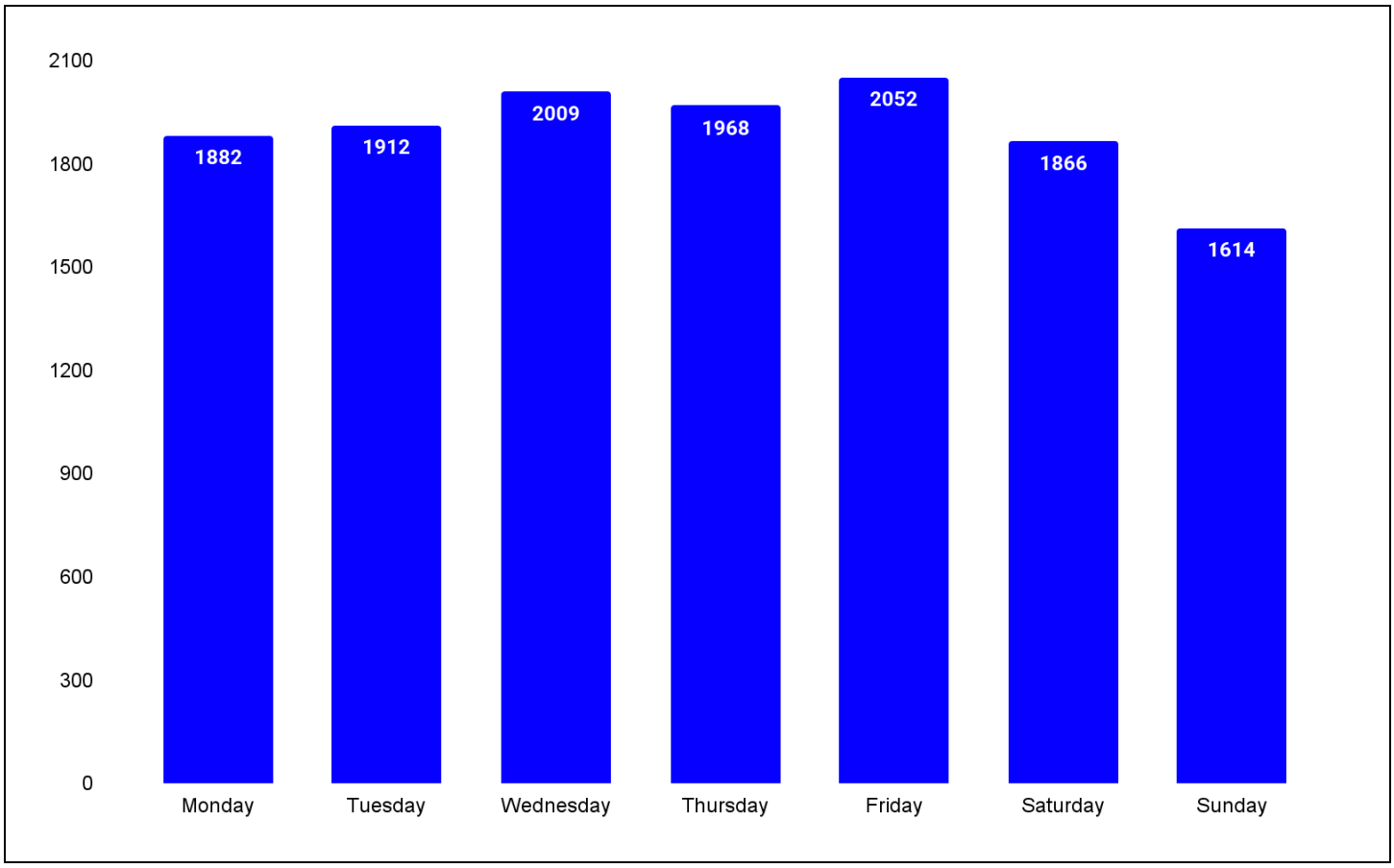


Figure 16: *Total unique targets per day of the week (Source: Recorded Future)*

A more granular "pattern of life" analysis of what hour of the day the new targets were added reveals two distinct daily peaks in activity (see **Figure 17**). A significant surge in new targets occurs between 05:00 and 07:00 UTC, with a secondary wave around 11:00 UTC. These times correspond to the beginning of the workday (08:00 to 10:00) and the early afternoon (14:00) in Moscow (UTC+3), strongly suggesting that the operators align their activities with a standard Russian work schedule.

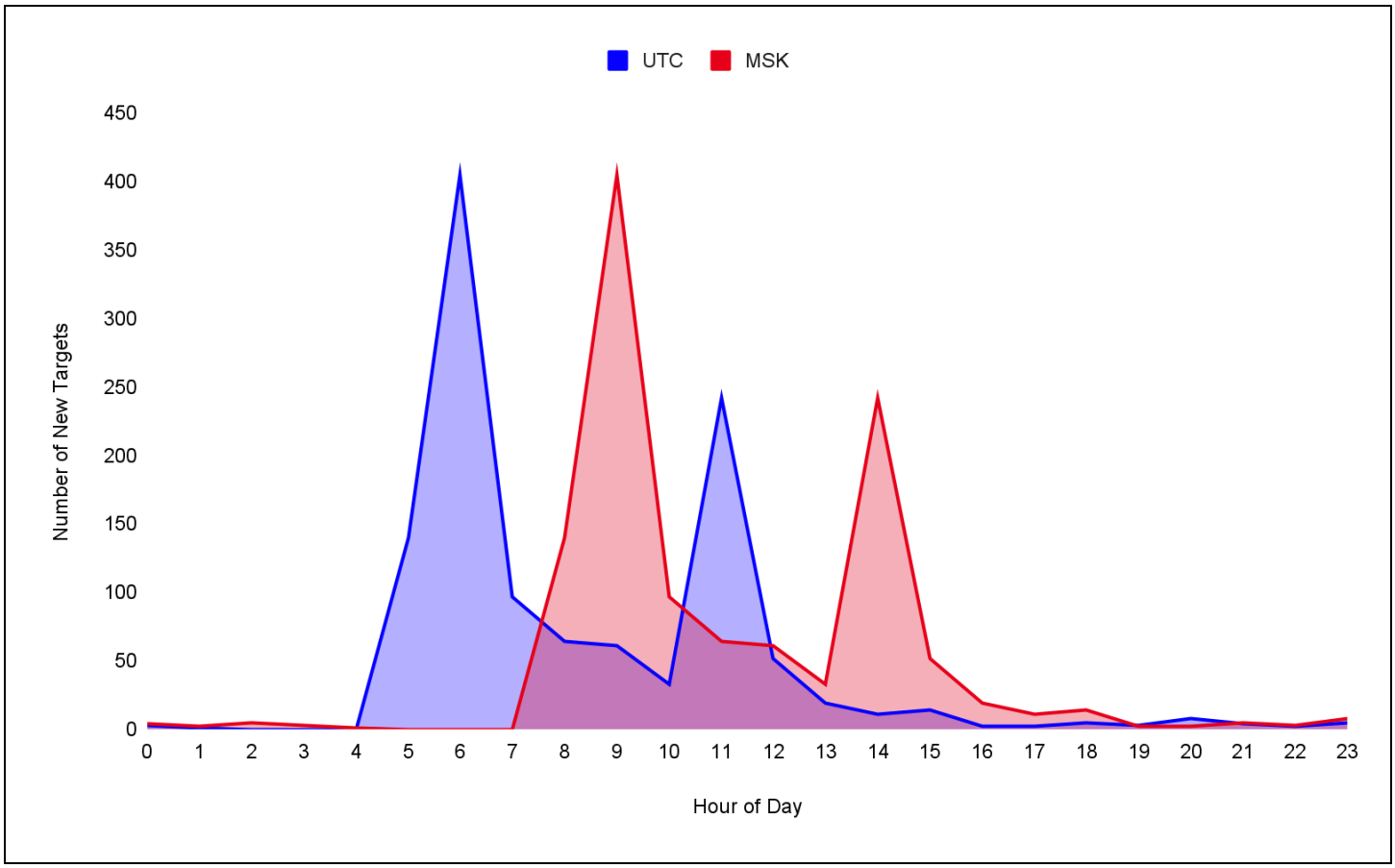


Figure 17: *Number of new targets by hour of the day (Source: Recorded Future)*

This hypothesis is further supported by **Figure 18**, a heat map showing which hour of the day the new targets were added. It shows that while the morning surge persists through the weekend, the secondary 11:00 UTC update is absent mainly on Saturdays and Sundays. The persistence of the morning attack wave on weekends could be attributed to automated processes continuing to target existing lists. However, the absence of the second wave suggests that the selection and addition of new targets possibly requires a manual process that scales down significantly over the weekend.

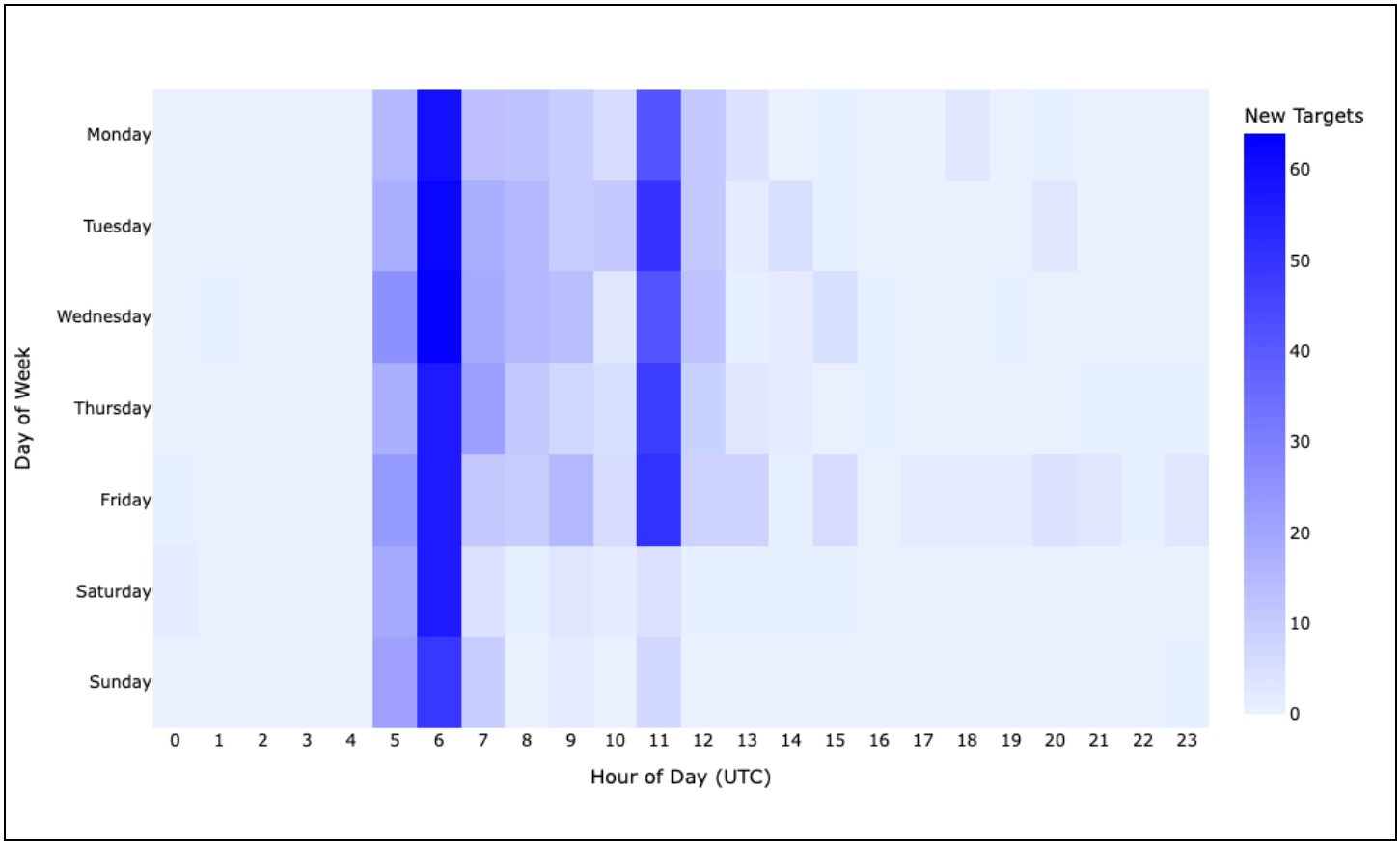


Figure 18: *Total unique targets added per month (Source: Recorded Future)*

Infrastructure

NoName057(16) operates its DDoSia Project using a resilient, multi-tiered infrastructure designed to enhance operational security (OPSEC) and evade takedown efforts (see **Figure 19**). In this model, public-facing Tier 1 C2 servers communicate with DDoSia clients and serve as ephemeral intermediary layers, pulling target lists from a smaller, more static set of backend Tier 2 servers that are shielded from direct public access.

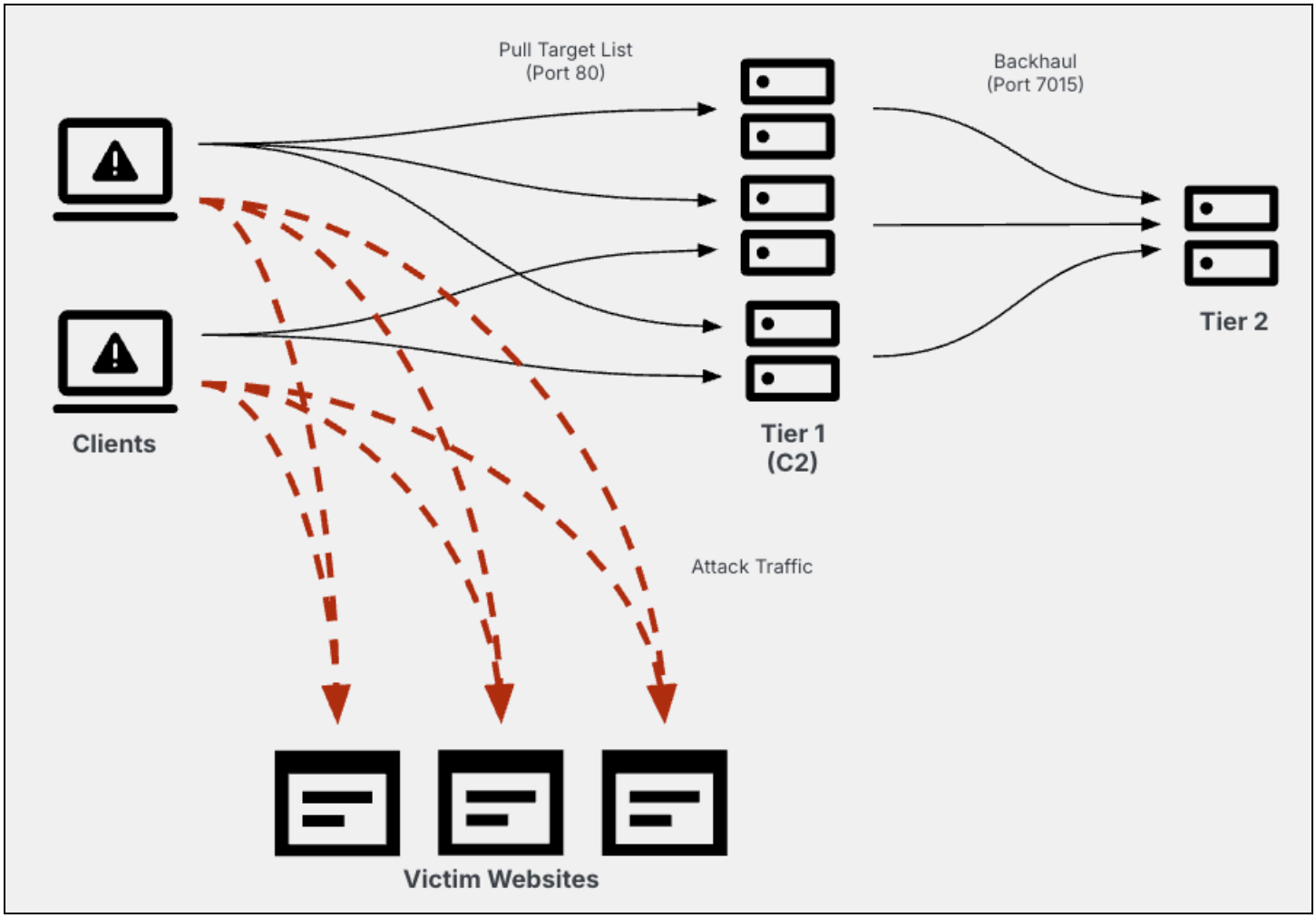


Figure 19: *DDoSia multi-tiered and client overview (Source: Recorded Future)*

A key feature of this architecture is the use of ACLs on the Tier 2 servers. An ACL is a set of rules that dictate which IP addresses are permitted to connect to a server. In this case, the Tier 2 servers are configured only to accept incoming connections from the known IP addresses of the threat group's own Tier 1 C2 infrastructure. ACLs serve as a highly effective security measure, preventing the discovery of core Tier 2 servers via internet-wide scanning and significantly complicating efforts to attribute or disrupt this critical infrastructure. Despite ACL-based protections, Insikt Group, using Recorded Future Network Intelligence, successfully identified the Tier 2 servers, which remained relatively static over time, usually with only one active at any given moment, which is in sharp contrast to the highly volatile and frequently rotated Tier 1 C2 infrastructure.

Insikt Group observed a total of 275 unique Tier 1 C2 IP addresses between July 1, 2024, and July 15, 2025. The average operational lifespan of these servers is 9.33 days, with a median duration of roughly two days. 105 (38.18%) of the IP addresses were only live for a single day. This rapid turnover and continuous rotation of Tier 1 C2 infrastructure significantly complicates tracking and mitigation efforts. While the precise cause of this volatility remains unclear, it likely reflects the threat group's deliberate

rotation of infrastructure to evade detection, as well as potential takedown actions by hosting providers or law enforcement.

ASN Breakdown

57 unique autonomous system numbers (ASNs) were used to announce the 275 Tier 1 C2 IP addresses Insikt Group identified between July 1, 2024, and July 14, 2025. The most prominent ASes included AS399629 (BL Networks), belonging to BitLaunch[.]io, a popular internet service provider (ISP) among threat actors due to the ability to pay with various cryptocurrencies. This was followed closely by AS210644 (AEZA-AS) operated by sanctioned Russian "bulletproof hosting service" Aeza International Ltd, and AS215540 (GCS-AS), operated by Global Connectivity Solutions, the UK front for Russian hoster 4vps (see **Table 1**). Insikt Group has published several reports on these networks to Recorded Future customers, detailing their role in enabling global cyber operations, including DDoSia.

ASN	Name	Percentage
AS399629	BL Networks	8%
AS210644	Aeza International Ltd	7.5%
AS215540	Global Connectivity Solutions	6%
AS56971	CGI Global Limited	5%
AS400992	ZhouyiSat Comms	5%
AS199058	Serva One LTD	4%
AS39798	MivoCloud SRL	4%
AS42624	Global-Data System IT Corporation	4%
AS215311	Regxa Company for Information Technology Ltd	3%
AS62005	Blue VPS OU	3%
AS9009	M247 Europe SRL	3%
AS50053	Individual Entrepreneur Anton Levin	2.5%
AS51395	Datasource AG	2.5%
AS198983	Joseph Hofmann trading as 'Tornado Datacenter GmbH & Co. KG'	2%
AS199785	Cloud Hosting Solutions	2%

***Table 1**: Top fifteen ASes observed announcing DDoSia Tier 1 C2 IP address space (Source: Recorded Future)*

Insikt Group notes that the majority of IP addresses announced via AS9009 (M247) belonged to Russian language ISP Inferno Solutions, via its affiliated companies 3NT Solutions and IROKO Networks Corporation.

Furthermore, approximately 13.5% of DDoSia Tier 1 C2 IP addresses were announced either directly by German ISP Aurologic GmbH or by ASNs receiving upstream transit from it. AS30823 (AUROLOGIC) provided upstream transit for Tier 1 C2 IP addresses announced by:

- AS210644 - Aeza International Ltd
- AS42624 - Global-Data System IT Corporation

Insikt Group notes that Aurologic remains a major upstream provider for Aeza International Ltd, despite the latter's recent designation by the US Department of the Treasury.

Additional C2 IP addresses were originated by:

- AS30823 - AUROLOGIC
- AS198983 - Joseph Hofmann trading as 'Tornado Datacenter GmbH & Co. KG'

Both ASes are operated under the Aurologic banner. In both cases, the IP address space was registered to and operated by ISP RouterHosting LLC, indicating that RouterHosting leverages transit services from Aurologic infrastructure alongside its own ASN (AS14956). AS198983 (TornadoDatacenter) refers to Tornado Datacenter GmbH, a datacenter facility also under the direct control of Aurologic managing director Joseph Hofman, operating in parallel with Aurologic as part of a shared infrastructure network.

Mitigations

- **Use Recorded Future Threat Intelligence:** Recorded Future customers can proactively mitigate this threat by operationalizing Recorded Future Intelligence Cloud data, specifically by leveraging continuously updated Risk Lists and by blocklisting IP addresses linked to DDoSia C2 servers to block internal communication with malicious infrastructure.
- **Use Recorded Future Network Intelligence:** Leverage Recorded Future's DDoS Traffic Analysis events to proactively identify servers involved in DDoS activity, along with targeted infrastructure and attack techniques, powered by Network Intelligence and other proprietary methodologies.
- **Use Recorded Future Threat Monitoring:** Configure alerts in the Recorded Future Intelligence Cloud to track activity across Telegram channels, forums, and other platforms for continuous situational awareness.
- **Geopolitical Awareness**: Continuously monitoring geopolitical developments, especially related to Russian-Ukrainian tensions, enables proactive anticipation of NoName057(16)'s targeting patterns. Early identification of political triggers or diplomatic escalations allows organizations to implement timely DDoS mitigation measures, significantly reducing potential disruptions. Use the Recorded Future Geopolitical Intelligence Module to monitor for geopolitical developments.
- **Deploy DDoS Protection Services:** Organizations should implement a multi-layered DDoS mitigation strategy. This includes using cloud-based services to filter malicious traffic before it reaches the network, leveraging CDNs to absorb and distribute high-volume traffic, and configuring WAFs to protect against application-layer attacks like HTTP floods and SlowLoris variants.
- **Implement Robust Network Security Controls:** Configure perimeter security appliances and network devices to drop traffic from known malicious IP ranges and to enforce rate limiting on incoming connections. This can help mitigate the impact of volumetric TCP-based attacks such as SYN and ACK floods.
- **Develop and Test an Incident Response Plan:** Establish a clear incident response plan specifically for DDoS events. This plan should define roles, outline procedures for activating mitigation services, and establish communication protocols to ensure a swift and coordinated response, minimizing service disruption.

Outlook

NoName057(16) has proven to be a persistent and resilient threat actor in the cyber domain, sustaining a high-tempo DDoS campaign for over three years. Driven by a clear geopolitical agenda aligned with Russian interests, the threat group continues to demonstrate operational longevity through a combination of multi-tiered infrastructure and a motivated volunteer base. These factors suggest that NoName057(16)'s activity is not episodic, but rather a sustained feature of the broader cyber conflict tied to the ongoing war in Ukraine, one likely to persist regardless of defensive countermeasures or future law enforcement interventions, including operations such as Operation Eastwood.

Insikt Group assesses with high confidence that NoName057(16) will maintain its activity for the duration of the conflict. The threat group's targeting strategy is expected to remain closely aligned with Russia's geopolitical objectives, focusing on countries and industries perceived as adversarial to the Kremlin. While the individual attacks lack technical sophistication, the threat group's ability to coordinate large volumes of low-complexity attacks across a wide range of targets makes it a persistent and disruptive force.

Looking forward, organizations operating in countries supporting Ukraine or critical sectors should prepare for continued targeting by NoName057(16). Although the threat group may incrementally refine its tools, such as enhancing the DDoSia client or integrating stronger encryption to evade detection, its core mission of disruption is unlikely to change. This enduring threat must be understood within the broader context of hybrid warfare, where cyber operations, such as hacktivist-led DDoS attacks, pseudo-ransomware, disinformation, and sabotage, are used as tools of state-aligned influence, deliberately kept below the threshold of conventional conflict. These hybrid warfare tactics become especially significant for Russia during periods of perceived vulnerability, such as battlefield setbacks or expressions of support for Ukraine. To respond effectively, organizations must adopt long-term defensive strategies, emphasizing scalable resilience and sustained visibility into threat actors and geopolitical developments.

Appendix A — Indicators of Compromise (IoCs)

IP Addresses C2s:

102[.]129[.]165[.]164	(2025-06-03 to 2025-07-03)
103[.]136[.]69[.]227	(2025-07-01 to 2025-07-01)
103[.]231[.]74[.]10	(2024-12-13 to 2024-12-13)
103[.]249[.]133[.]214	(2025-05-13 to 2025-05-13)
103[.]80[.]86[.]26	(2024-11-12 to 2024-11-19)
103[.]80[.]86[.]98	(2025-05-08 to 2025-06-08)
104[.]194[.]143[.]96	(2024-11-13 to 2024-12-14)
104[.]194[.]144[.]108	(2024-11-20 to 2024-12-17)
104[.]194[.]145[.]88	(2024-12-20 to 2025-01-09)
104[.]194[.]149[.]73	(2024-10-06 to 2024-11-03)
104[.]194[.]149[.]9	(2025-01-21 to 2025-01-24)
104[.]194[.]150[.]61	(2024-10-01 to 2024-10-13)
104[.]249[.]40[.]115	(2024-10-03 to 2024-10-03)
107[.]158[.]128[.]97	(2025-06-01 to 2025-06-29)
107[.]189[.]18[.]52	(2025-06-28 to 2025-07-03)
107[.]189[.]25[.]138	(2025-01-14 to 2025-01-15)
116[.]202[.]251[.]2	(2024-12-14 to 2025-01-02)
116[.]202[.]251[.]23	(2025-01-13 to 2025-01-19)
116[.]202[.]251[.]25	(2025-01-15 to 2025-01-19)
116[.]202[.]251[.]4	(2024-12-30 to 2025-01-19)
138[.]124[.]53[.]59	(2025-02-08 to 2025-02-08)
141[.]11[.]164[.]85	(2025-04-23 to 2025-05-14)
141[.]98[.]233[.]13	(2025-04-20 to 2025-04-21)
145[.]223[.]68[.]151	(2025-05-28 to 2025-05-28)
145[.]223[.]68[.]34	(2025-04-08 to 2025-05-07)
146[.]103[.]41[.]10	(2025-01-25 to 2025-02-24)
146[.]103[.]41[.]3	(2025-07-05 to 2025-07-07)
146[.]19[.]80[.]221	(2024-12-30 to 2025-01-13)
147[.]45[.]114[.]205	(2024-07-13 to 2024-07-14)
147[.]45[.]124[.]28	(2024-07-31 to 2024-08-23)
147[.]45[.]125[.]58	(2024-07-16 to 2024-08-16)
147[.]45[.]179[.]194	(2025-02-01 to 2025-02-03)
147[.]45[.]51[.]140	(2024-12-25 to 2024-12-26)
147[.]45[.]60[.]149	(2024-11-12 to 2024-12-09)
148[.]135[.]195[.]131	(2025-06-28 to 2025-07-11)
150[.]241[.]93[.]244	(2024-11-09 to 2024-11-10)
150[.]241[.]93[.]245	(2024-11-10 to 2024-11-10)
151[.]236[.]12[.]172	(2025-01-14 to 2025-01-14)
151[.]236[.]18[.]220	(2024-12-30 to 2024-12-31)
151[.]236[.]27[.]187	(2024-09-26 to 2024-10-09)
154[.]18[.]239[.]180	(2025-07-04 to 2025-07-09)
154[.]58[.]204[.]118	(2025-04-04 to 2025-05-04)
159[.]100[.]6[.]144	(2025-04-08 to 2025-05-08)
162[.]33[.]178[.]31	(2025-04-04 to 2025-04-04)
168[.]100[.]11[.]21	(2025-07-12 to 2025-07-14)
168[.]100[.]11[.]8	(2025-01-29 to 2025-01-29)
171[.]22[.]16[.]154	(2025-06-02 to 2025-06-02)
172[.]86[.]66[.]222	(2025-02-20 to 2025-03-12)

```
172[.]86[.]69[.]43       (2024-12-25 to 2024-12-25)
172[.]86[.]75[.]51       (2025-03-05 to 2025-03-06)
172[.]86[.]93[.]59       (2024-12-11 to 2025-01-09)
172[.]86[.]94[.]110      (2025-02-01 to 2025-03-01)
172[.]86[.]95[.]15       (2025-01-30 to 2025-02-26)
176[.]10[.]111[.]111     (2025-06-10 to 2025-06-10)
176[.]10[.]111[.]228     (2025-07-05 to 2025-07-05)
176[.]10[.]119[.]132     (2025-06-04 to 2025-07-02)
176[.]10[.]119[.]245     (2025-03-11 to 2025-04-02)
176[.]10[.]125[.]102     (2024-08-23 to 2024-09-30)
176[.]10[.]125[.]69      (2025-05-07 to 2025-05-14)
176[.]98[.]40[.]6        (2025-05-31 to 2025-06-02)
178[.]22[.]31[.]6        (2024-08-24 to 2024-08-26)
178[.]248[.]75[.]62      (2025-07-04 to 2025-07-09)
181[.]214[.]58[.]100     (2024-12-13 to 2024-12-13)
181[.]214[.]58[.]247     (2025-01-14 to 2025-01-14)
181[.]214[.]58[.]3       (2025-01-13 to 2025-01-13)
181[.]214[.]58[.]35      (2024-12-28 to 2024-12-28)
181[.]214[.]58[.]65      (2025-03-25 to 2025-04-18)
181[.]214[.]58[.]92      (2025-03-15 to 2025-04-13)
184[.]174[.]96[.]147     (2025-02-01 to 2025-03-02)
184[.]174[.]97[.]110     (2025-02-08 to 2025-03-07)
185[.]121[.]15[.]235     (2025-05-31 to 2025-06-01)
185[.]121[.]15[.]251     (2024-11-13 to 2024-12-14)
185[.]121[.]15[.]70      (2025-04-23 to 2025-04-23)
185[.]121[.]15[.]91      (2024-11-08 to 2024-11-10)
185[.]158[.]251[.]46     (2024-09-26 to 2024-10-03)
185[.]167[.]234[.]109    (2025-06-10 to 2025-07-08)
185[.]167[.]234[.]4      (2025-05-08 to 2025-05-14)
185[.]178[.]231[.]30     (2025-06-27 to 2025-07-10)
185[.]189[.]149[.]225    (2025-07-12 to 2025-07-12)
185[.]196[.]10[.]13      (2025-03-12 to 2025-03-13)
185[.]196[.]10[.]251     (2025-01-16 to 2025-01-20)
185[.]196[.]11[.]147     (2025-01-15 to 2025-01-20)
185[.]196[.]11[.]16      (2025-01-15 to 2025-01-20)
185[.]196[.]11[.]216     (2025-01-23 to 2025-01-28)
185[.]196[.]8[.]140      (2025-04-08 to 2025-04-09)
185[.]196[.]9[.]151      (2024-07-15 to 2024-08-16)
185[.]208[.]158[.]23     (2024-12-17 to 2024-12-18)
185[.]208[.]158[.]30     (2024-07-31 to 2024-09-03)
185[.]212[.]47[.]40      (2024-10-15 to 2024-11-07)
185[.]232[.]205[.]16     (2025-06-03 to 2025-07-05)
185[.]232[.]205[.]198    (2025-07-05 to 2025-07-11)
185[.]232[.]205[.]52     (2025-03-20 to 2025-04-03)
185[.]250[.]180[.]171    (2025-07-10 to 2025-07-12)
185[.]92[.]183[.]66      (2025-06-04 to 2025-06-04)
188[.]130[.]207[.]23     (2025-01-14 to 2025-01-14)
188[.]132[.]183[.]175    (2025-03-06 to 2025-04-06)
188[.]214[.]157[.]45     (2025-01-26 to 2025-01-26)
192[.]142[.]10[.]76      (2025-04-09 to 2025-05-08)
192[.]142[.]18[.]133     (2025-01-22 to 2025-02-24)
192[.]142[.]18[.]24      (2025-04-14 to 2025-05-12)
192[.]71[.]211[.]138     (2024-12-14 to 2024-12-14)
```

```
193[.]109[.]120[.]177    (2025-05-06 to 2025-05-06)
193[.]124[.]44[.]66      (2024-10-05 to 2024-11-06)
193[.]124[.]45[.]158     (2024-07-08 to 2024-07-10)
193[.]124[.]45[.]162     (2024-07-09 to 2024-07-10)
193[.]124[.]45[.]197     (2024-07-16 to 2024-07-16)
193[.]149[.]189[.]208    (2024-11-12 to 2024-11-12)
193[.]149[.]190[.]214    (2025-01-14 to 2025-01-15)
193[.]17[.]183[.]73      (2024-07-11 to 2024-07-12)
193[.]228[.]128[.]107    (2025-01-15 to 2025-01-15)
193[.]228[.]128[.]47     (2024-12-30 to 2024-12-30)
193[.]233[.]127[.]54     (2025-05-08 to 2025-05-08)
193[.]233[.]232[.]162    (2025-03-13 to 2025-03-13)
193[.]235[.]207[.]31     (2024-09-26 to 2024-10-03)
193[.]242[.]145[.]250    (2024-11-08 to 2024-11-11)
193[.]32[.]176[.]11      (2025-04-24 to 2025-04-24)
193[.]37[.]68[.]223      (2024-07-13 to 2024-07-14)
193[.]56[.]135[.]141     (2025-06-28 to 2025-06-28)
193[.]56[.]135[.]169     (2025-04-04 to 2025-04-05)
193[.]56[.]135[.]222     (2025-05-06 to 2025-05-07)
193[.]56[.]135[.]252     (2025-06-03 to 2025-07-02)
194[.]113[.]245[.]201    (2025-01-22 to 2025-02-23)
194[.]113[.]37[.]171     (2025-01-15 to 2025-01-15)
194[.]28[.]224[.]181     (2024-07-13 to 2024-07-13)
194[.]59[.]40[.]153      (2024-07-05 to 2024-07-05)
194[.]61[.]120[.]192     (2025-03-06 to 2025-03-06)
194[.]87[.]186[.]215     (2024-07-31 to 2024-08-19)
194[.]87[.]199[.]69      (2024-08-24 to 2024-09-22)
194[.]87[.]79[.]223      (2024-10-05 to 2024-10-07)
194[.]87[.]97[.]75       (2024-07-13 to 2024-08-12)
195[.]123[.]225[.]222    (2025-01-28 to 2025-01-29)
195[.]133[.]17[.]14      (2025-02-20 to 2025-02-20)
195[.]20[.]19[.]34       (2025-01-21 to 2025-01-21)
195[.]20[.]19[.]76       (2025-03-15 to 2025-04-13)
195[.]85[.]115[.]19      (2025-02-08 to 2025-03-01)
2[.]57[.]122[.]187       (2024-07-10 to 2024-07-10)
2[.]57[.]122[.]213       (2024-07-09 to 2024-07-11)
206[.]166[.]251[.]8      (2024-12-25 to 2024-12-25)
206[.]188[.]196[.]63     (2025-03-06 to 2025-03-06)
212[.]192[.]31[.]34      (2024-10-06 to 2024-10-26)
212[.]73[.]134[.]230     (2025-01-28 to 2025-01-28)
212[.]73[.]134[.]250     (2025-03-25 to 2025-03-25)
212[.]87[.]222[.]25      (2025-04-08 to 2025-04-08)
213[.]109[.]192[.]120    (2025-01-17 to 2025-01-20)
213[.]218[.]212[.]59     (2025-05-13 to 2025-05-14)
213[.]5[.]128[.]212      (2024-12-11 to 2024-12-11)
216[.]185[.]57[.]42      (2025-03-04 to 2025-04-03)
216[.]245[.]184[.]4      (2024-07-08 to 2024-07-09)
217[.]60[.]36[.]34       (2025-07-12 to 2025-07-13)
23[.]177[.]184[.]108     (2024-10-03 to 2024-10-09)
31[.]15[.]17[.]29        (2025-03-14 to 2025-03-14)
31[.]15[.]17[.]97        (2025-07-12 to 2025-07-14)
31[.]214[.]157[.]223     (2025-01-21 to 2025-01-31)
31[.]59[.]114[.]177      (2024-12-21 to 2024-12-21)
```

37[.]10[.]71[.]26	(2024-12-15 to 2024-12-15)
37[.]46[.]19[.]124	(2025-01-31 to 2025-02-24)
38[.]180[.]110[.]212	(2024-07-13 to 2024-07-14)
38[.]180[.]153[.]248	(2024-07-15 to 2024-07-16)
38[.]180[.]236[.]57	(2024-11-10 to 2024-11-11)
38[.]180[.]35[.]217	(2024-07-05 to 2024-07-05)
38[.]180[.]35[.]89	(2024-12-25 to 2024-12-31)
45[.]11[.]181[.]69	(2025-05-08 to 2025-05-08)
45[.]11[.]183[.]187	(2025-04-23 to 2025-04-28)
45[.]128[.]232[.]253	(2024-08-24 to 2024-09-03)
45[.]129[.]199[.]150	(2025-05-27 to 2025-05-29)
45[.]129[.]242[.]163	(2024-12-23 to 2024-12-24)
45[.]129[.]242[.]212	(2024-11-13 to 2024-12-09)
45[.]136[.]196[.]13	(2024-07-12 to 2024-07-12)
45[.]137[.]222[.]24	(2025-01-13 to 2025-01-13)
45[.]137[.]222[.]29	(2024-12-13 to 2024-12-13)
45[.]137[.]222[.]31	(2024-12-26 to 2024-12-26)
45[.]141[.]234[.]33	(2025-06-28 to 2025-06-30)
45[.]143[.]167[.]246	(2025-01-16 to 2025-01-20)
45[.]143[.]200[.]29	(2024-10-01 to 2024-10-02)
45[.]145[.]6[.]134	(2025-01-13 to 2025-01-13)
45[.]150[.]109[.]230	(2025-06-11 to 2025-06-28)
45[.]152[.]115[.]205	(2024-11-09 to 2024-11-11)
45[.]152[.]115[.]216	(2025-04-23 to 2025-04-23)
45[.]156[.]27[.]38	(2025-02-01 to 2025-02-01)
45[.]159[.]209[.]142	(2025-01-14 to 2025-01-15)
45[.]59[.]118[.]247	(2024-08-24 to 2024-08-30)
45[.]61[.]133[.]99	(2025-01-13 to 2025-01-13)
45[.]61[.]139[.]200	(2024-12-11 to 2024-12-11)
45[.]83[.]20[.]176	(2024-12-13 to 2024-12-13)
45[.]85[.]93[.]177	(2025-06-28 to 2025-07-01)
45[.]85[.]93[.]246	(2025-05-27 to 2025-05-28)
45[.]85[.]93[.]34	(2025-02-20 to 2025-02-20)
45[.]85[.]93[.]94	(2025-05-06 to 2025-05-06)
45[.]86[.]231[.]130	(2024-12-11 to 2024-12-11)
45[.]89[.]244[.]159	(2024-11-08 to 2024-11-11)
45[.]91[.]193[.]102	(2024-12-11 to 2024-12-11)
46[.]29[.]238[.]2	(2024-10-02 to 2024-10-02)
5[.]161[.]152[.]94	(2025-01-23 to 2025-01-23)
5[.]180[.]45[.]156	(2024-07-03 to 2024-07-04)
5[.]181[.]156[.]124	(2024-12-24 to 2025-01-13)
5[.]181[.]156[.]65	(2024-11-13 to 2024-12-09)
5[.]181[.]156[.]91	(2024-12-11 to 2025-01-11)
5[.]181[.]159[.]84	(2025-03-12 to 2025-03-12)
5[.]181[.]159[.]9	(2025-02-01 to 2025-02-17)
5[.]181[.]21[.]251	(2025-01-16 to 2025-01-16)
5[.]182[.]37[.]232	(2025-01-23 to 2025-01-23)
5[.]199[.]173[.]17	(2025-01-13 to 2025-01-13)
5[.]252[.]178[.]167	(2025-07-08 to 2025-07-09)
5[.]252[.]178[.]238	(2025-01-13 to 2025-01-13)
5[.]42[.]102[.]70	(2024-07-03 to 2024-07-03)
5[.]42[.]105[.]203	(2024-07-03 to 2024-07-03)
54[.]39[.]83[.]176	(2024-12-20 to 2024-12-20)

```
62[.]106[.]66[.]153      (2025-01-21 to 2025-02-22)
62[.]133[.]62[.]190      (2025-01-14 to 2025-01-14)
62[.]133[.]62[.]239      (2024-11-20 to 2024-12-09)
62[.]192[.]174[.]85      (2025-06-04 to 2025-06-04)
62[.]60[.]148[.]63       (2025-02-01 to 2025-02-01)
62[.]60[.]157[.]244      (2025-05-31 to 2025-05-31)
62[.]60[.]234[.]87       (2024-11-11 to 2024-11-12)
62[.]60[.]237[.]103      (2024-11-09 to 2024-11-10)
62[.]60[.]239[.]225      (2024-11-20 to 2024-12-09)
62[.]60[.]245[.]125      (2025-05-08 to 2025-05-13)
63[.]141[.]227[.]132     (2025-01-22 to 2025-01-22)
64[.]190[.]113[.]214     (2025-07-04 to 2025-07-04)
64[.]190[.]113[.]62      (2025-05-08 to 2025-05-31)
64[.]31[.]63[.]21        (2024-12-14 to 2024-12-14)
64[.]52[.]80[.]170       (2024-07-06 to 2024-07-06)
64[.]7[.]199[.]136       (2025-01-21 to 2025-01-21)
64[.]95[.]10[.]185       (2024-07-15 to 2024-07-16)
65[.]38[.]120[.]189      (2024-07-08 to 2024-07-09)
65[.]38[.]120[.]189      (2025-03-25 to 2025-03-25)
65[.]38[.]120[.]73       (2024-12-30 to 2024-12-31)
65[.]38[.]121[.]22       (2024-11-13 to 2024-12-07)
72[.]5[.]42[.]130        (2024-11-20 to 2024-12-09)
77[.]221[.]156[.]12      (2024-07-11 to 2024-07-11)
77[.]238[.]225[.]249     (2024-07-10 to 2024-07-11)
77[.]239[.]101[.]153     (2025-06-11 to 2025-07-03)
78[.]135[.]93[.]117      (2025-05-27 to 2025-05-29)
78[.]153[.]136[.]5       (2024-09-26 to 2024-10-03)
79[.]137[.]184[.]255     (2024-11-13 to 2024-12-09)
79[.]137[.]196[.]166     (2025-05-13 to 2025-05-13)
80[.]77[.]25[.]194       (2024-10-15 to 2024-11-07)
81[.]19[.]141[.]191      (2024-10-01 to 2024-10-02)
83[.]147[.]18[.]227      (2025-02-20 to 2025-03-12)
83[.]147[.]192[.]25      (2025-06-04 to 2025-06-04)
84[.]200[.]154[.]245     (2025-01-25 to 2025-02-25)
84[.]32[.]188[.]17       (2025-01-14 to 2025-01-14)
85[.]158[.]57[.]64       (2025-05-13 to 2025-05-14)
85[.]192[.]27[.]147      (2025-05-28 to 2025-05-28)
85[.]192[.]42[.]32       (2024-11-13 to 2024-12-09)
85[.]239[.]61[.]165      (2025-02-03 to 2025-02-03)
85[.]239[.]62[.]79       (2024-12-31 to 2024-12-31)
86[.]106[.]119[.]170     (2024-12-15 to 2024-12-15)
86[.]54[.]42[.]84        (2025-06-10 to 2025-07-07)
87[.]120[.]37[.]9        (2025-03-31 to 2025-04-01)
87[.]120[.]8[.]110       (2025-03-15 to 2025-03-16)
87[.]121[.]52[.]187      (2025-04-14 to 2025-04-14)
87[.]251[.]79[.]157      (2024-12-11 to 2024-12-12)
87[.]251[.]79[.]210      (2024-11-20 to 2024-12-12)
87[.]251[.]88[.]165      (2024-07-15 to 2024-07-17)
88[.]218[.]248[.]182     (2024-07-31 to 2024-08-19)
89[.]107[.]10[.]231      (2024-07-12 to 2024-08-11)
89[.]208[.]113[.]125     (2025-01-22 to 2025-01-25)
89[.]208[.]113[.]95      (2025-01-21 to 2025-01-21)
89[.]251[.]22[.]154      (2025-01-22 to 2025-01-22)
```

```
89[.]251[.]22[.]18       (2025-02-21 to 2025-02-21)
91[.]239[.]148[.]151     (2025-04-14 to 2025-05-11)
91[.]92[.]43[.]61        (2025-01-25 to 2025-01-25)
92[.]243[.]64[.]68       (2025-01-13 to 2025-01-13)
93[.]185[.]165[.]235     (2025-07-08 to 2025-07-11)
93[.]185[.]165[.]246     (2025-06-28 to 2025-06-28)
93[.]185[.]165[.]91      (2025-06-10 to 2025-06-11)
94[.]156[.]250[.]50      (2025-01-22 to 2025-03-01)
94[.]158[.]244[.]113     (2025-01-22 to 2025-01-31)
94[.]158[.]244[.]56      (2025-01-15 to 2025-01-15)
94[.]158[.]244[.]72      (2025-01-14 to 2025-01-15)
94[.]158[.]245[.]50      (2025-03-07 to 2025-03-12)
94[.]228[.]169[.]62      (2024-07-10 to 2024-07-10)
95[.]163[.]152[.]28      (2024-11-12 to 2024-11-12)
95[.]179[.]253[.]195     (2024-07-01 to 2024-07-01)
96[.]9[.]125[.]231       (2025-05-31 to 2025-05-31)
```

Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Discovery: System Information Discovery	T1082
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Ingress Tool Transfer	T1105
Impact: Network Denial of Service	T1498
Impact: Endpoint Denial of Service	T1499
Impact: Endpoint Denial of Service: OS Exhaustion Flood	T1499.001
Impact: Endpoint Denial of Service: Service Exhaustion Flood	T1499.002

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com