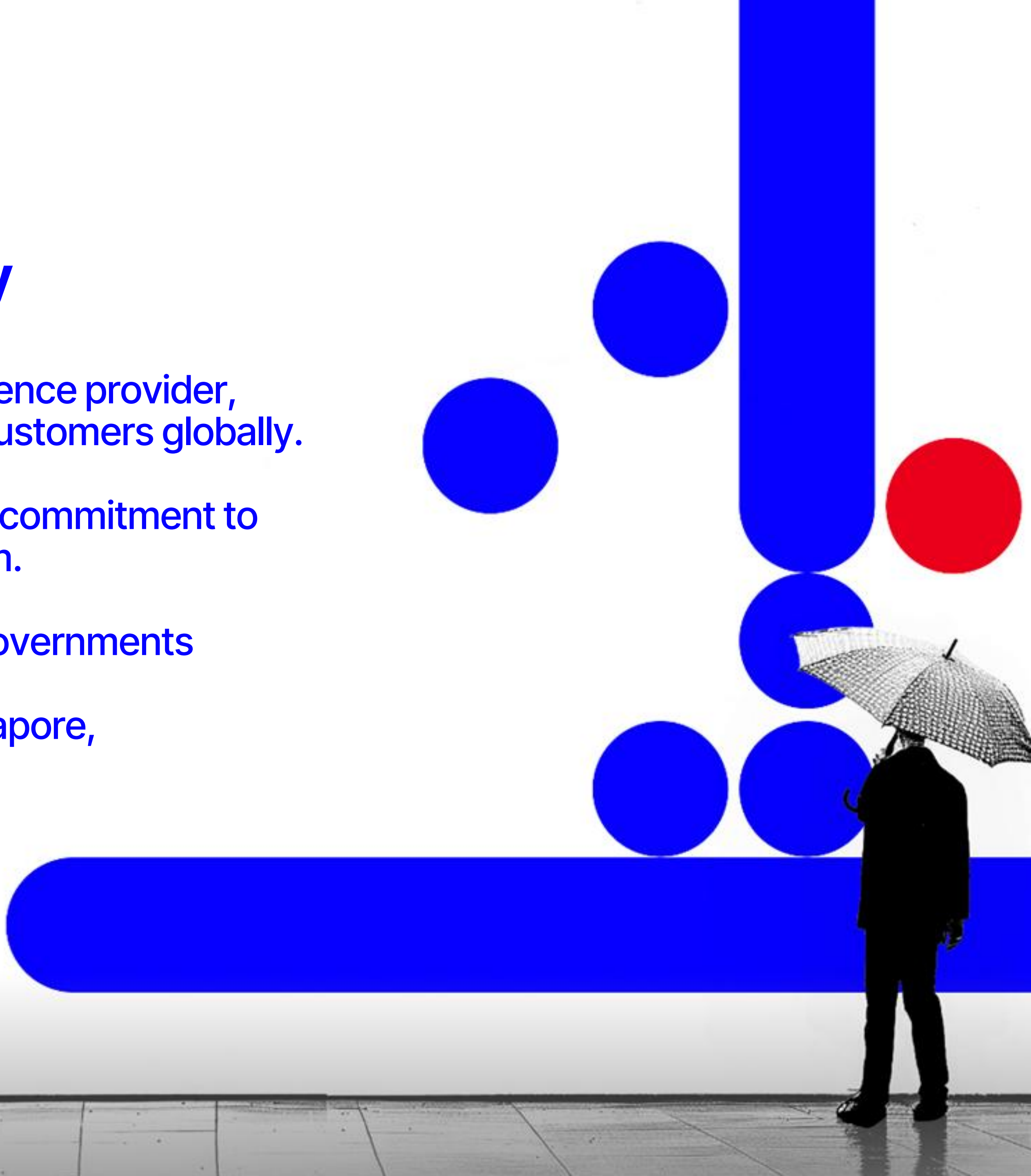
Recorded Future®

RONOG_10 Presentation

Recorded Future®

Quick Facts about our company

- Recorded Future is the world’s largest threat intelligence provider, offering real-time, AI-driven insights to over 1,900 customers globally.
- Acquired by Mastercard in 2024, strengthening our commitment to threat intelligence and safeguarding financial system.
- Customers in 80 countries and over 45 sovereign governments
- We have offices in the United States, Sweden, Singapore, London,Japan, and Dubai



Global Network Intelligence Team

- We support Recorded Future’s network intelligence, which is leveraged by our Insikt Team and clients to mitigate threats and conduct research.

- We partner with and support global network infrastructure operators, by providing proactive analysis to block threats to their business and clients.

- These partnerships also enable threat intelligence sharing, helping the public and private sectors stay ahead of emerging risks.

- We can support your SOC teams and security personnel through network security and threat intelligence training.

How do these cyber criminal groups organize?

- Recrutement from dark web forums and other cyber criminal organizations
- reputation is everything
- Operate on Tor, p2p services like ToX, jabber,and private servers
- DDoS as a service
- leverage a backdoor RAT, then load additional malware
- leveraging other botnets to conduct DDoS attacks
- Will typically clean funds through a criminal money laundering group. Illegal access transfer / wire / crypto

Recorded Future®

Anatomy of DDoSia: A Technical Analysis of the Cybercriminal Group and Defense Strategies for Organizations

NoName057(16): Hacktivists Group

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 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.

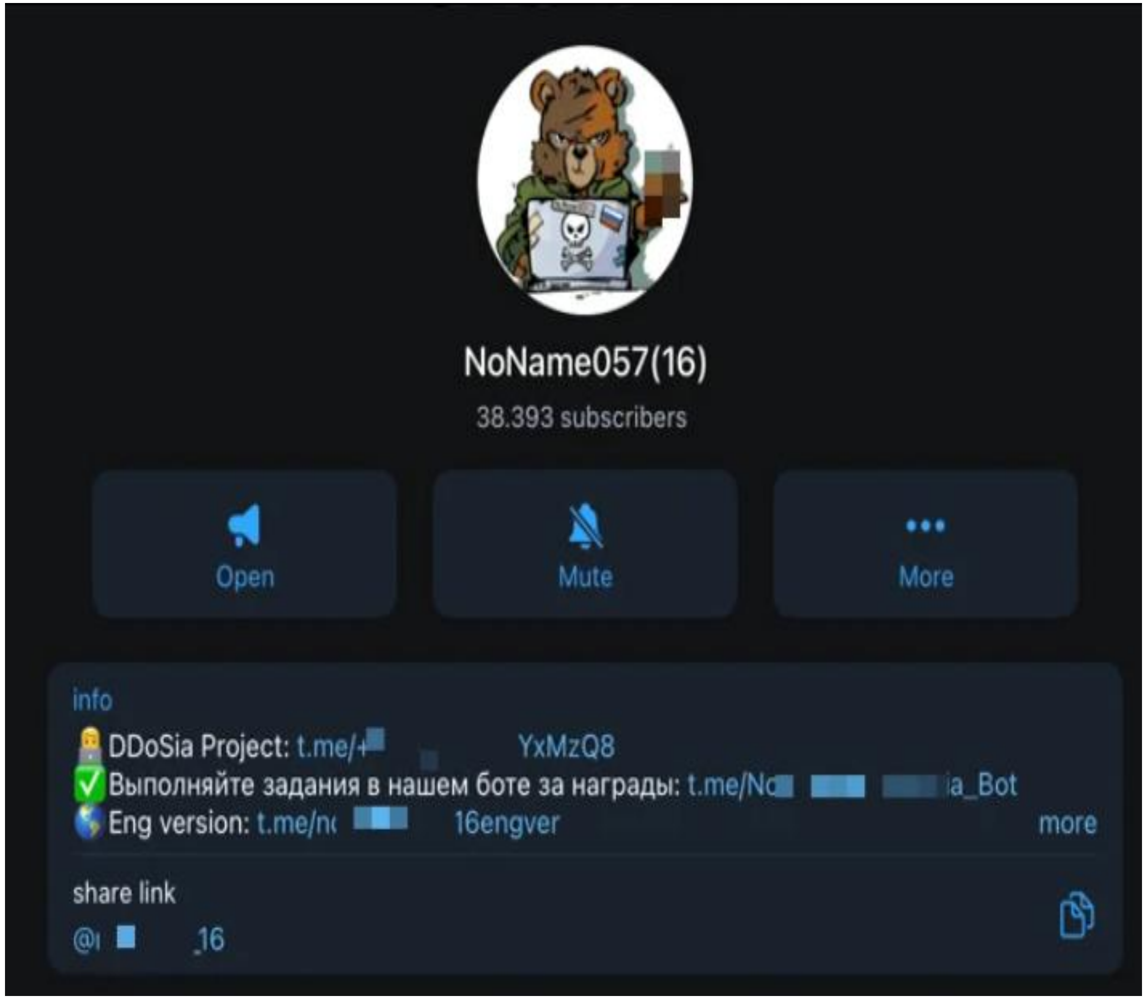
The operational framework surrounding this tool is known as the "DDoSia Project", which encompasses the entire ecosystem of tools, infrastructure, and volunteers.

How the DDoSia malware works

A prospective client registered with the DDoSia bot using their Telegram account.

Clients then download a binary that leverages their botnet, and can execute for multiple operating systems, including Windows, Linux, and macOS.

Once executed, the tool connects to a command-and-control (C2) server and retrieves an encrypted configuration file. This file contains a list of active attack targets along with detailed instructions for executing the attacks.



NoName057(16)

38.393 subscribers

info

DDoSia Project: t.me/+[redacted] YxMzQ8

✅Выполняйте задания в нашем боте за награды: t.me/No[redacted] [redacted] [redacted]ia_Bot

Eng version: t.me/n[redacted] 16engver

more

share link

@[redacted] _16

Technical Analysis of DDoSia Communication

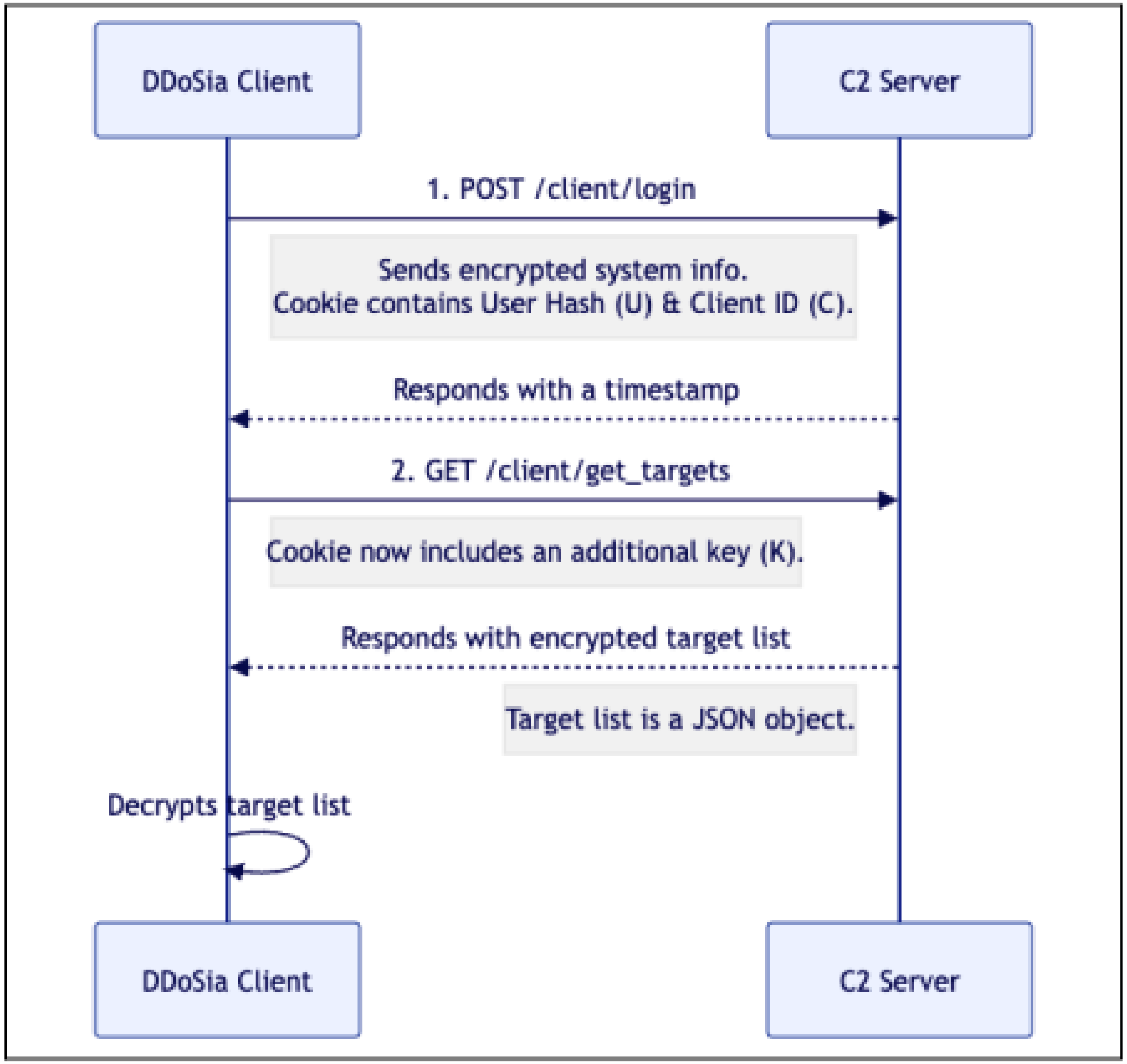
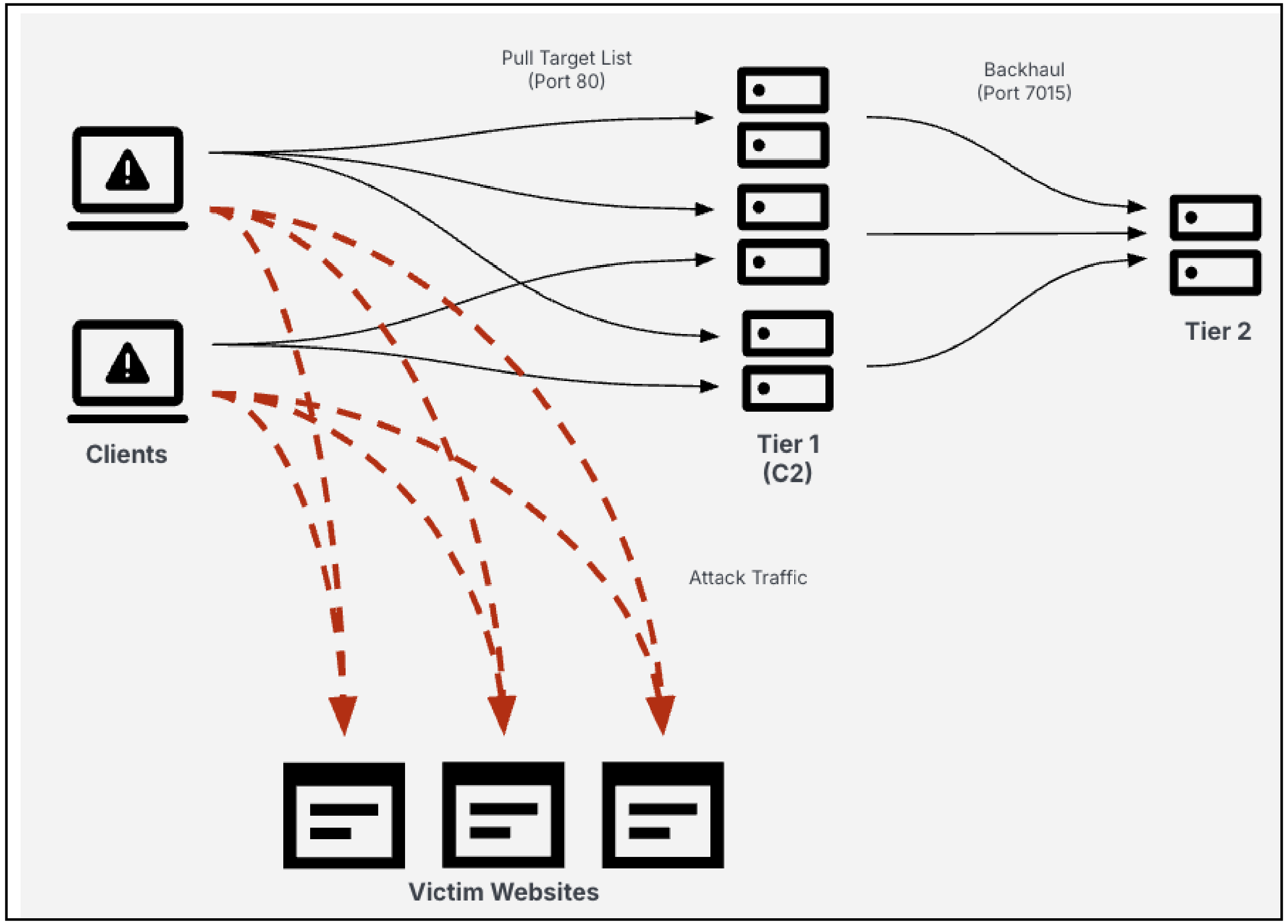

DDoSia Client
C2 Server
1. POST /client/login
Sends encrypted system info.
Cookie contains User Hash (U) & Client ID (C).
Responds with a timestamp
2. GET /client/get_targets
Cookie now includes an additional key (K).
Responds with encrypted target list
Target list is a JSON object.
Decrypts target list
DDoSia Client
C2 Server

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

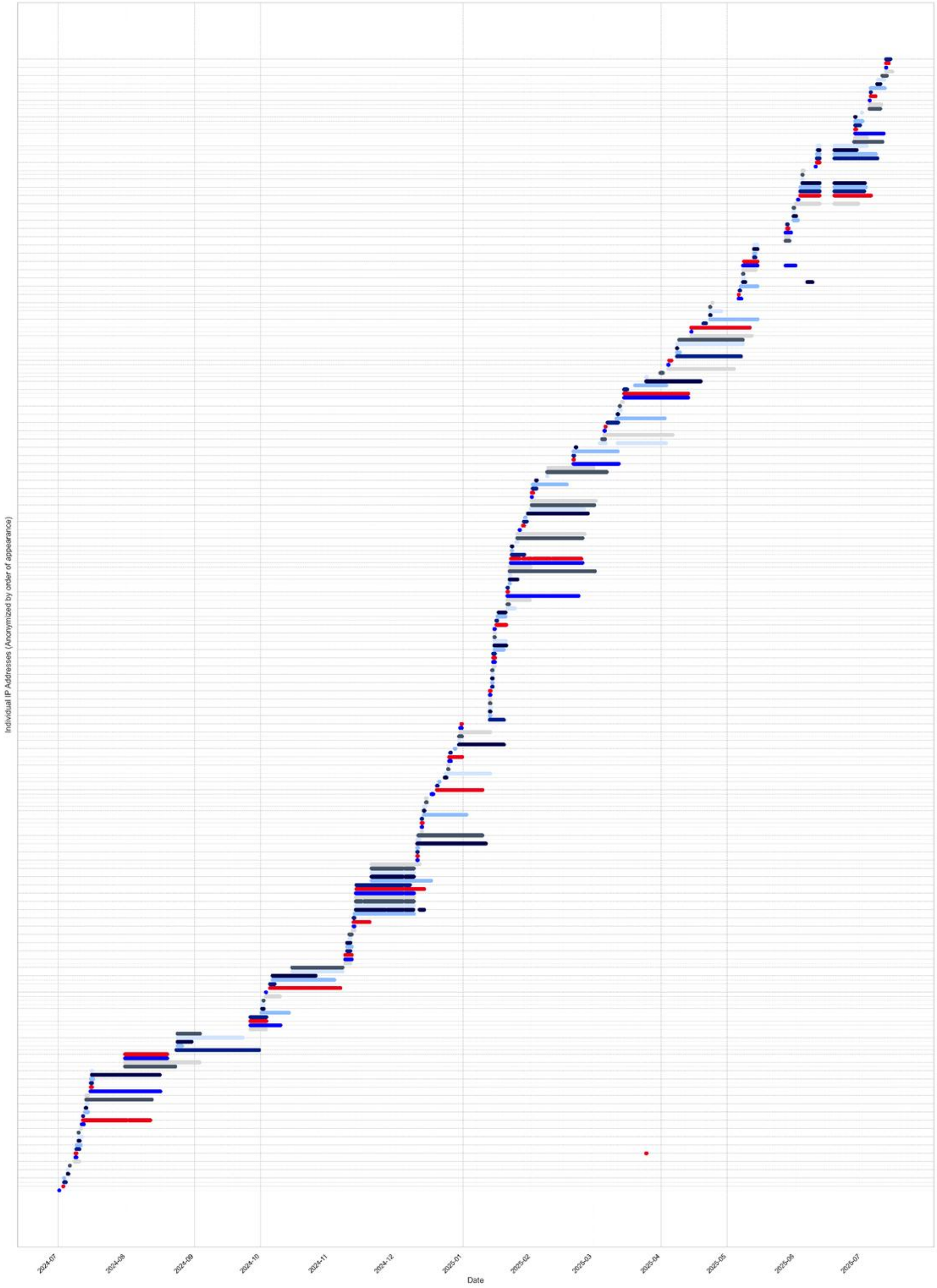
DDoSia: Infrastructure

- **Tier 1 C2 Servers:**
  - Public-facing and numerous.
  - Constantly rotated with a short lifespan (~9 days).
- **Tier 2 Servers:**
  - Fewer in number and more static.
  - Shielded from public view by Access Control Lists (ACLs), whihc defines what traffic/ users are allowed or blocked



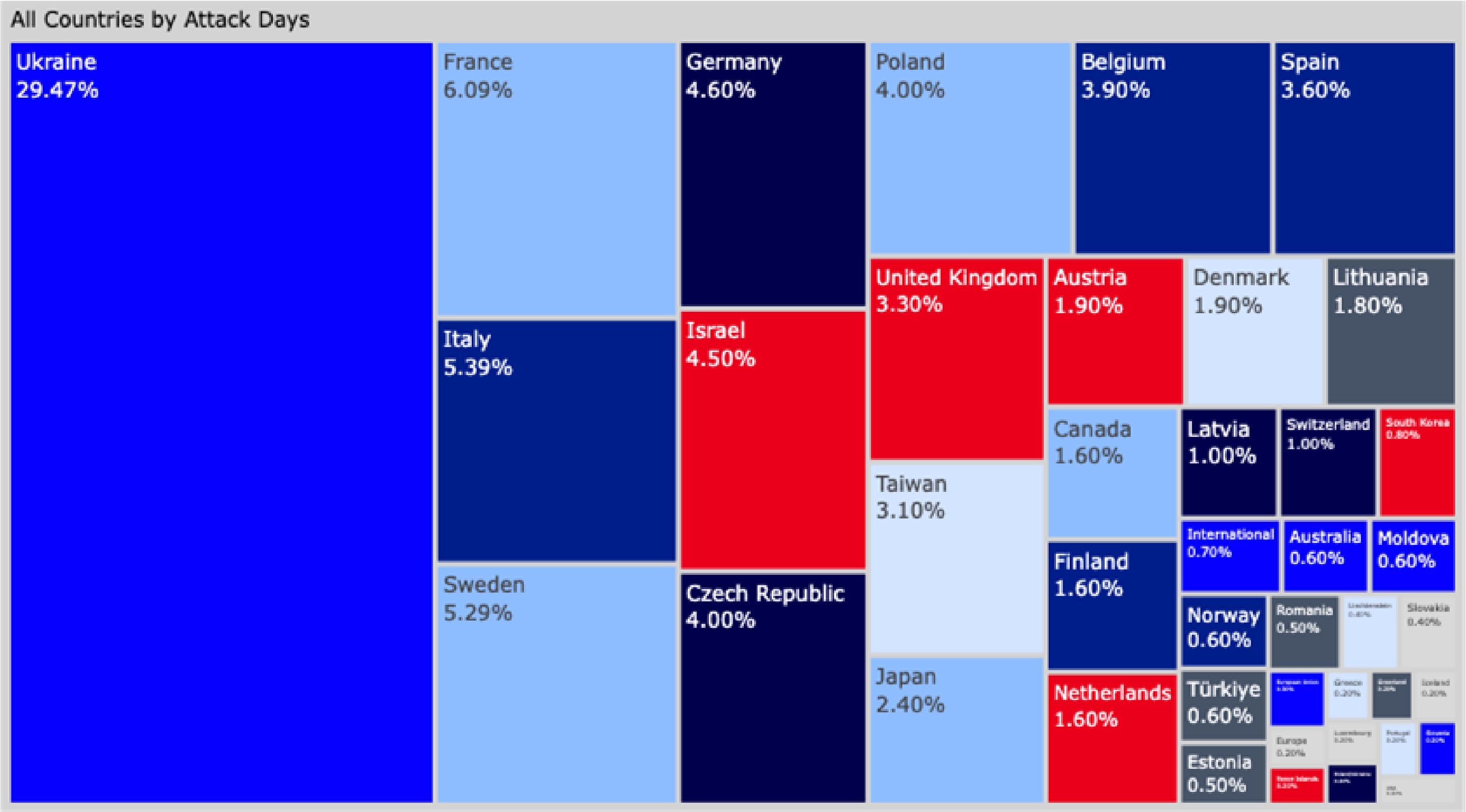
DDoSia: Tier 1 C2 Rotation

- **The pattern of resilience:**
  - A visual representation of their continuous C2 rotation.
- Each line represents a new server brought online and quickly taken offline.
- Its plausible to suspect that abuse reporting for the C2 servers had an impact on my infrastructure rotation as well.



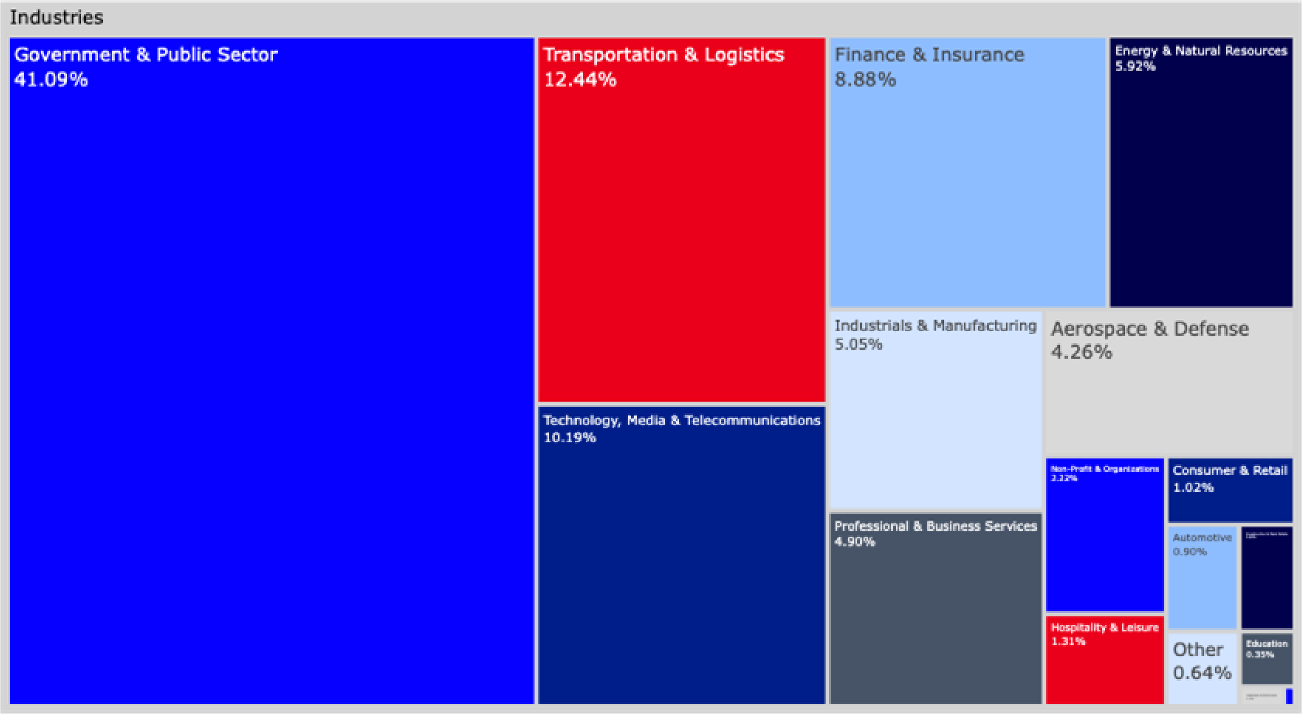
The Targets: A Geopolitical Focus

- **Primary Target:** Ukraine (~30% of attack days).
- **Strategic Targeting:** European nations supporting Ukraine (France, Italy, Sweden, etc.).
- **A telling exclusion:** The U.S. is not a primary target, despite its support.



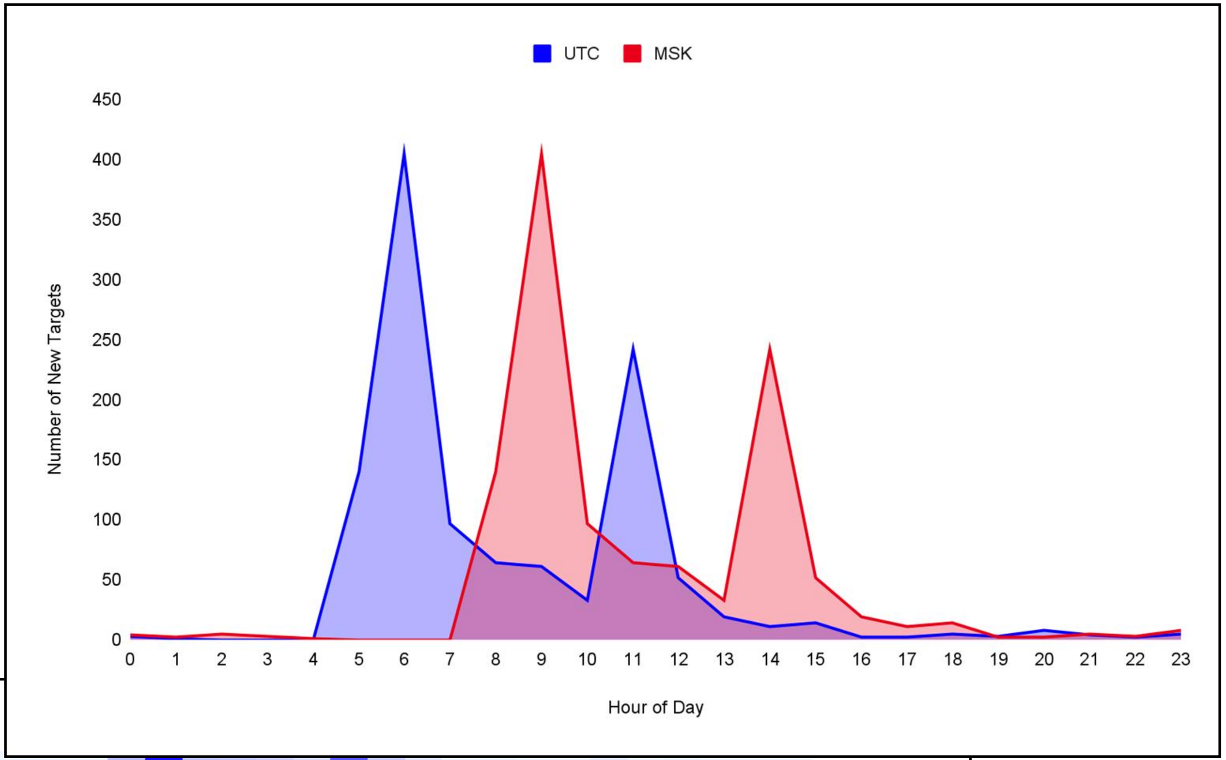
Sectoral Targeting

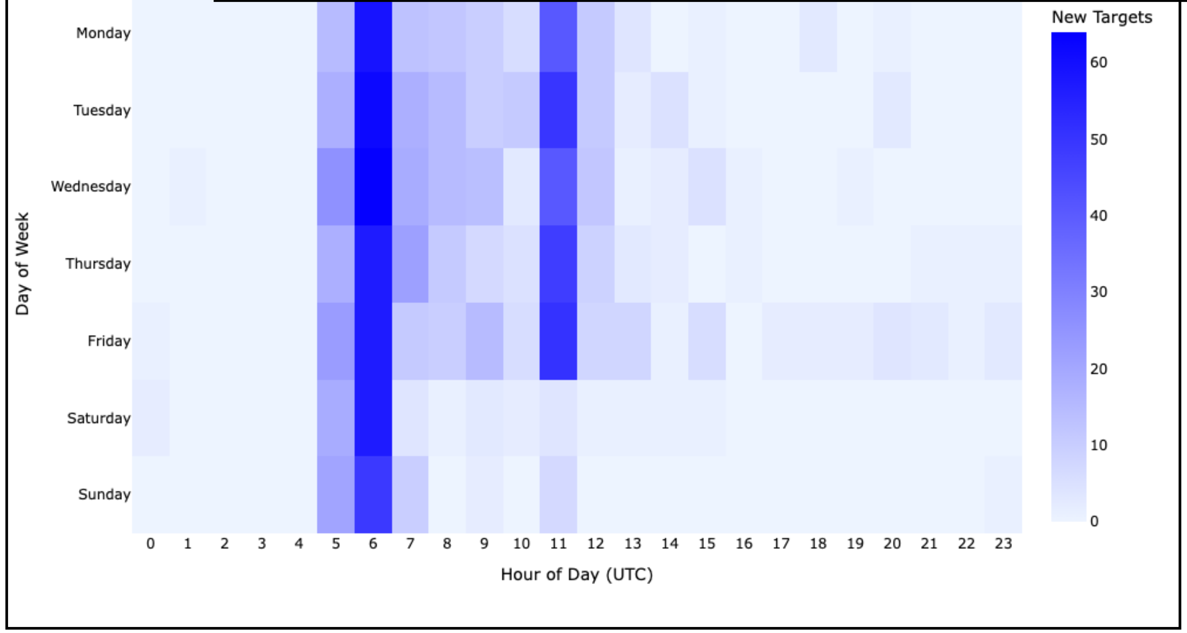
- **Government & Public Sector:**
  - Top target at 41.09%.
- **Critical Infrastructure:**
  - Focus on Transportation & Logistics (12.44%) and Tech/Media/Telecommunications (10.19%).
- **Economic Disruption:**
  - Finance & Insurance sectors targeted at 8.88%.



Pattern of Life

- **A regular schedule:**
  - Two distinct daily peaks in activity.
  - 05:00-07:00 and ~11:00 UTC
- **Moscow time:**
  - Peaks align with a standard Russian work schedule (08:00-10:00 and ~14:00).
- **The weekend signal:**
  - A drop-off in the second peak on weekends suggests manual, human-driven target selection.

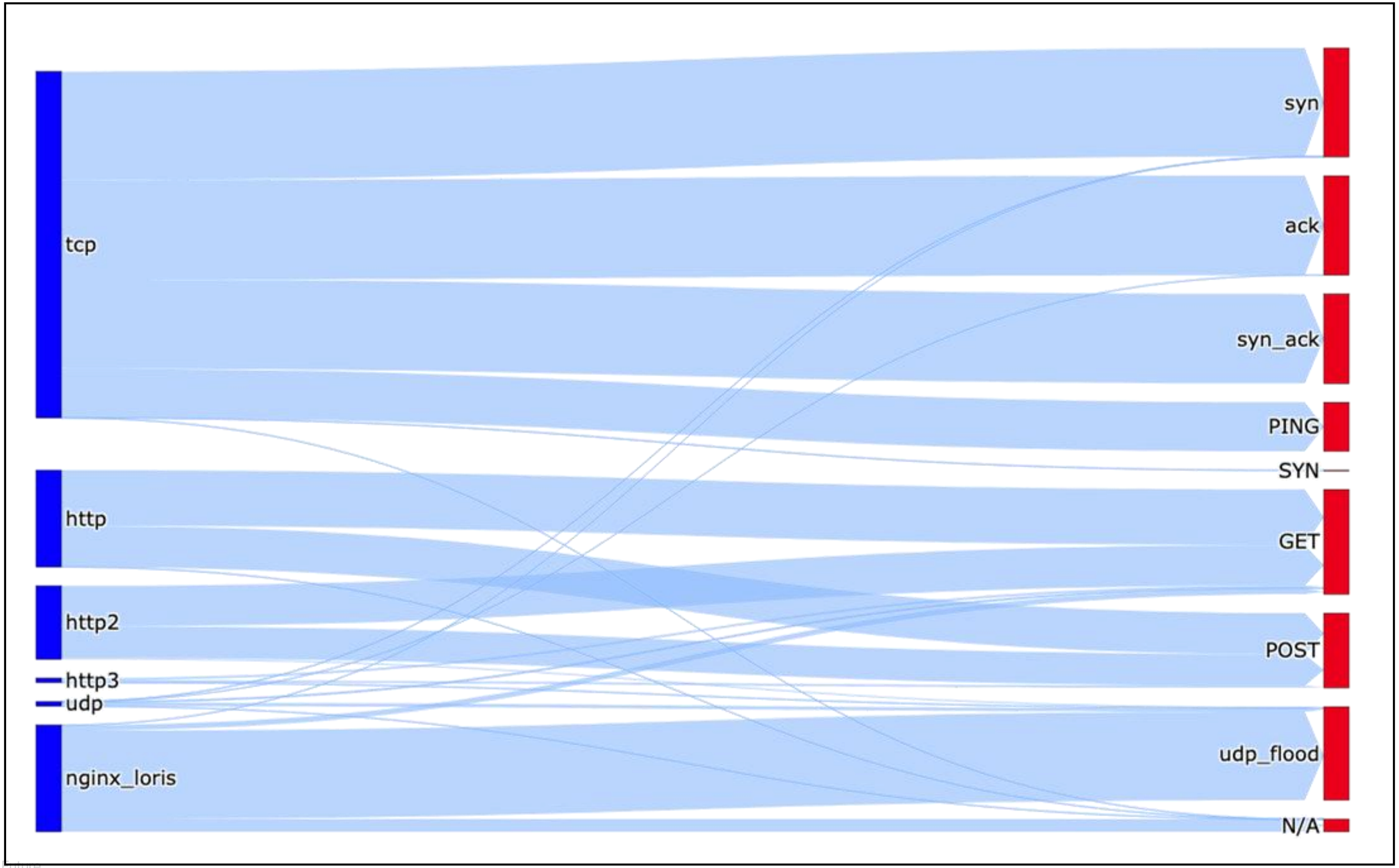




DDoSia Attack Methods

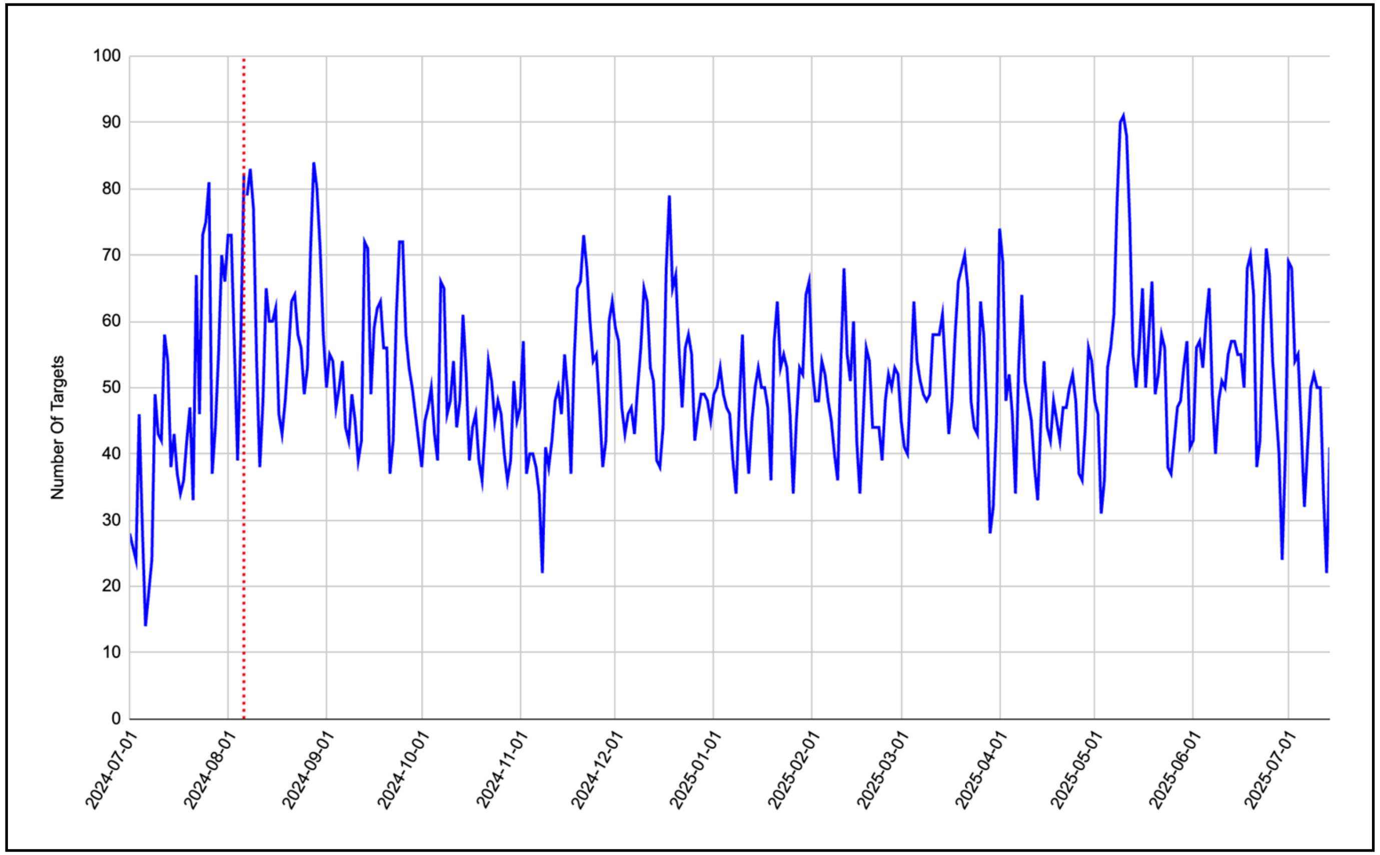
- **Versatile toolkit:**
  - Uses both network-layer and application-layer attacks.(add more)
- **Common methods**
  - SYN attack - A SYN attack floods a server with fake connection requests, leaving connections half-open and consuming resources. This overload prevents legitimate users from connecting, causing a denial of service.
  - ACK - An ACK attack floods a target with a large number of TCP acknowledgment (ACK) packets, which are used to confirm receipt of data in communications. This overwhelms the target's resources or bypasses security filters, causing network disruption and potential downtime.
  - Slow Loris - A Slowloris attack keeps many connections open by sending partial requests slowly, exhausting server resources. Mitigate with timeouts, connection limits, and reverse proxies like Cloudflare or security tools like fail2ban.
- **Web-focused:**
  - 66% of attacks target ports 443 (HTTPS) and 80 (HTTP).

DDoSia's Attack Statistics



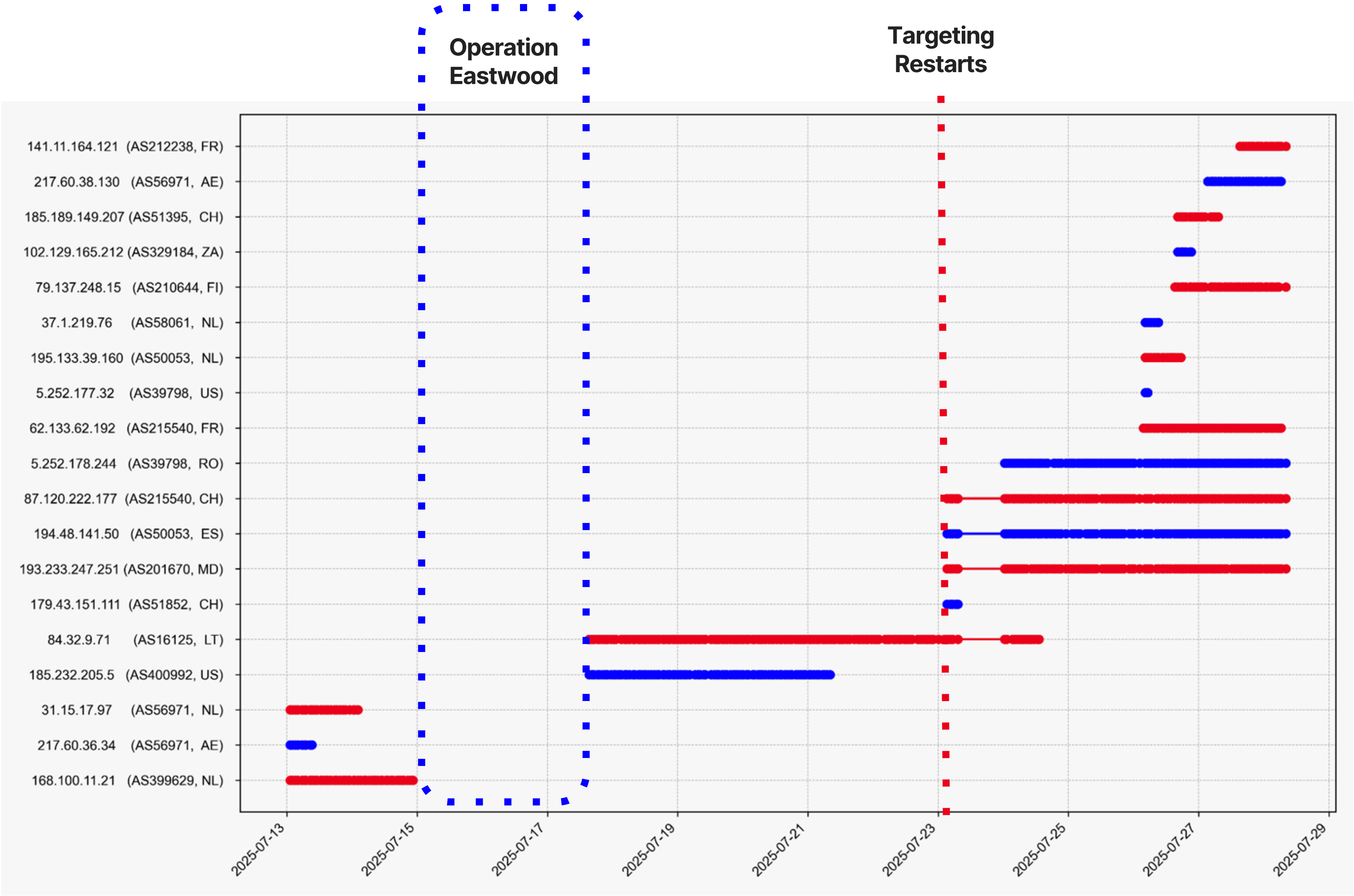
A Closer Look at Attack Volume

- Sustained tempo:
  - Median of 50 unique targets per day.
- Reactive operations:
  - Intense bursts of activity correlate with geopolitical events.
- Case study:
  - A spike to 82 daily targets on August 6, 2024, in response to a Ukrainian ground offensive into Russia's Kursk Oblast.



Post Eastwood: C2s

- **Rapid recovery:**
  - New C2 servers appeared online the very day the operation ended.
- **Full resurgence:**
  - By July 23, 2025, infrastructure was fully re-established and attacks resumed.
- **A lesson in resilience:**
  - Demonstrates the group's ability to quickly adapt and rebuild, despite law enforcement efforts.



Outlook

- NoName057(16) will remain an active and persistent threat.
- Their actions are a sustained feature of the cyber conflict tied to the war in Ukraine.
- The group's primary goal is a psychological one, aimed at eroding public trust rather than technical disruption.
- The technical effects from Law Enforcement may be temporary, but strategic value lies in stripping away the group's anonymity. Shifting the narrative from a faceless threat to one of individual accountability.

Recorded Future®

Mitigation Strategies for DDoSia

Technical Strategies for your Organization

Deploy DDoS Protection Services:

Organizations should implement a multi-layered DDoS mitigation strategy.

- This includes using cloud-based services like CDNs(content delivery Network),which helps distribute large volume f traffic, reducing exposure to your main server(s).

Configuring WAFs to protect against application-layer attacks like HTTP floods and SlowLoris variants.

- For example, leverage multiple factor captcha configurations and limit size rate requests, to limit massive requests. You can

Technical Strategies for your Organization

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.

Point of Compromise analysis:

If your team can conduct a post infection analysis on bots used for DDoS attacks, look for artifacts that may be in the following areas(leave on if possible).

- NetStat connections / disruption in sys logs recording / unusual file locations / Active Directory changes /

If found, completely wipe the machine, as simply relying on AV, will not be 100% sure.

Intelligence Strategies for your Organization

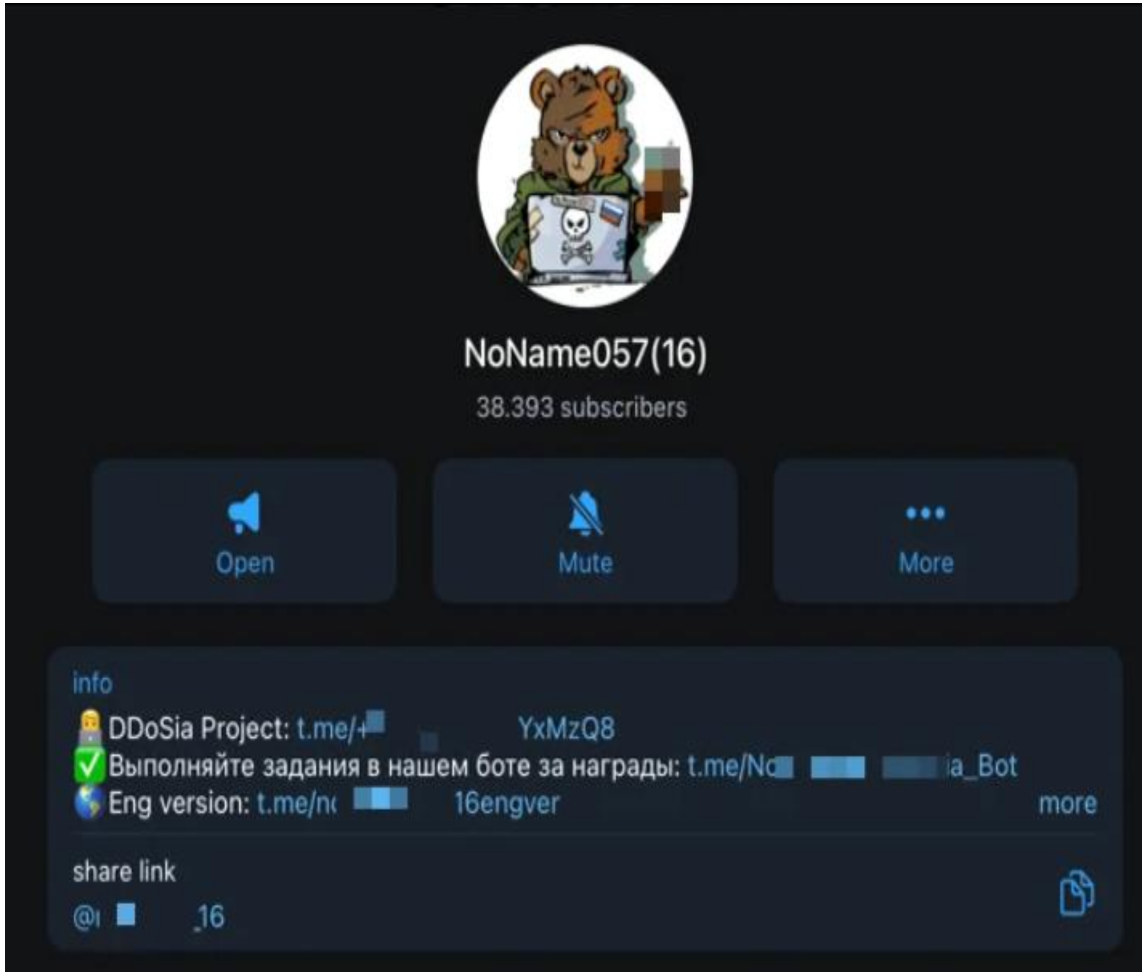
The NoName057(16) group has an active Telegram channel. Historically, they have posted who've they targeted, through their check-host[.]net domain.

Intel teams could track their activity and current geopolitical trends through their other social media channels.

If you have federal/ government clients, provide awareness of the group through the proper SOC channels. Continuously monitoring geopolitical developments, especially related to Russian-Ukrainian tensions, enables proactive anticipation of NoName057(16)'s targeting patterns.

Leverage Insikt group monthly analysis reports on prominent, and up to date criminal activity

https://www.recordedfuture.com/research



NoName057(16)

38.393 subscribers

info

🔒 DDoSia Project: t.me/+[redacted] YxMzQ8

✅ Выполняйте задания в нашем боте за награды: t.me/No[redacted] [redacted]ia_Bot

🌎 Eng version: t.me/n[redacted] 16engver more

share link

@[redacted] 16

We Can Help!

(support network security and vulnerability analysis)

Contact Info:

chase.clowser@recordedfuture.com
jon.morgan@recordedfuture.com