A Blog with NoName

S2 Research Team

January 27, 2023

Further Insight into the Hacktivist Operation Targeting NATO and Affiliated Nations

Key Findings

- NoName057(16) is a pro-Russian hacktivist operator / group, which has claimed responsibility for repeated Distributed Denial of Service (DDoS) attacks against entities in perceived anti-Russian countries since March 2022.
- NoName057(16) back-end infrastructure is hosted in Russia and likely operated by individual(s) with experience in systems design / maintenance.
- DDoS attack targeting instructions include timestamps that align with Moscow Standard Time.
- Recent targets have included entities with infrastructure hosted in Czechia, Denmark, Estonia, Germany, Slovakia, and Slovenia.
- The majority of DDoS attack infrastructure used in NoName057(16) campaigns is assigned to two interlinked hosting providers; MIRhosting and Stark Industries.
- A limited number of netblocks are used in the DDoS attacks, providing a potential mitigation / defense opportunity

Introduction

NoName057(16) attacks have targeted government / military departments in Ukraine and NATO countries, as well as organizations from core sectors such as finance, freight, and media.

Recent reporting (Avast, SentinelLabs) has revealed that NoName057(16) relies upon a “volunteer” system (rather than a botnet of infected hosts), in which the “volunteers” are rewarded financially for contributing attack infrastructure. This system is managed via two Telegram channels (@noname05716 and @nn05716chat).

In this blog post we will examine two elements of NoName057(16)’s infrastructure; the management infrastructure sitting behind the known C2 servers, and the attack infrastructure which is purportedly donated by their “volunteers”. In doing so we will seek to understand how the operation functions, and provide information for cyber defenders to protect their interests from future attacks.

Infrastructure

The starting point for this analysis is the current C2 server used to coordinate NoName057(16)'s campaigns; as previously reported by SentinelLabs - **31.13.195.87** (NETERRA, BG). According to our records this server became operational on 19 December 2022.

Two Dynamic DNS (DDNS) domains, registered with No-IP, currently resolve to **31.13.195.87**:

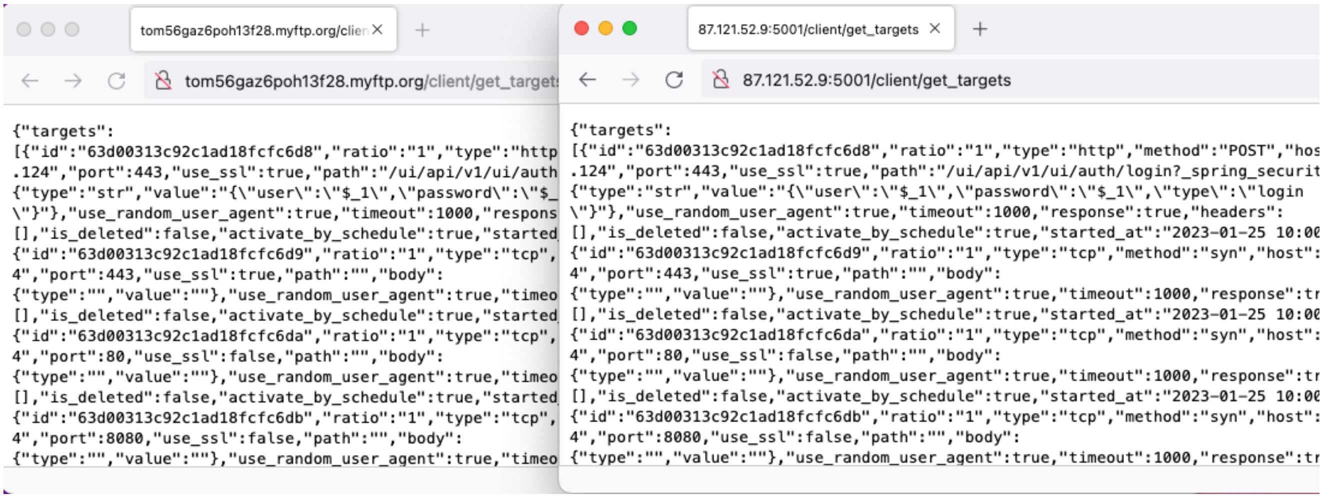
- tom56gaz6poh13f28[.]myftp.org
- zig35m48zur14nel40[.]myftp.org

The DDoS tool (DDOSIA) receives targeting information from the /client/get_targets URL path on either of these domains (over HTTP on TCP/80).

Examining network telemetry for **31.13.195.87**, we observe a high volume of outbound connections to TCP/5001 of **87.121.52.9** (NETERRA, BG).

*The use of TCP/5001 is notable as this port was used for communications with the previous C2 server (**77.91.122.69**), which was active until 16 December 2022.*

When '**87.121.52.9**:5001/client/get_targets' was accessed, we noted that the same targeting information was returned, as observed on the C2 domains. It is therefore plausible that the published C2 servers are mirrors of **87.121.52.9**.



tom56gaz6poh13f28.myftp.org/client/get_targets

```
{"targets":
[{"id":"63d00313c92c1ad18fcfc6d8","ratio":"1","type":"http
.124","port":443,"use_ssl":true,"path":"/ui/api/v1/ui/auth
{"type":"str","value":"{\"user\":\"$_1\",\"password\":\"$_
\"}"},"use_random_user_agent":true,"timeout":1000,"respons
[],"is_deleted":false,"activate_by_schedule":true,"started
{"id":"63d00313c92c1ad18fcfc6d9","ratio":"1","type":"tcp",
4","port":443,"use_ssl":true,"path":"","body":
{"type":"","value":""},"use_random_user_agent":true,"timeo
[],"is_deleted":false,"activate_by_schedule":true,"started
{"id":"63d00313c92c1ad18fcfc6da","ratio":"1","type":"tcp",
4","port":80,"use_ssl":false,"path":"","body":
{"type":"","value":""},"use_random_user_agent":true,"timeo
[],"is_deleted":false,"activate_by_schedule":true,"started
{"id":"63d00313c92c1ad18fcfc6db","ratio":"1","type":"tcp",
4","port":8080,"use_ssl":false,"path":"","body":
{"type":"","value":""},"use_random_user_agent":true,"timeo
```

87.121.52.9:5001/client/get_targets

```
{"targets":
[{"id":"63d00313c92c1ad18fcfc6d8","ratio":"1","type":"http","method":"POST","hos
.124","port":443,"use_ssl":true,"path":"/ui/api/v1/ui/auth/login?_spring_securit
{"type":"str","value":"{\"user\":\"$_1\",\"password\":\"$_1\",\"type\":\"login
\"}"},"use_random_user_agent":true,"timeout":1000,"response":true,"headers":
[],"is_deleted":false,"activate_by_schedule":true,"started_at":"2023-01-25 10:00
{"id":"63d00313c92c1ad18fcfc6d9","ratio":"1","type":"tcp","method":"syn","host":
4","port":443,"use_ssl":true,"path":"","body":
{"type":"","value":""},"use_random_user_agent":true,"timeout":1000,"response":tr
[],"is_deleted":false,"activate_by_schedule":true,"started_at":"2023-01-25 10:00
{"id":"63d00313c92c1ad18fcfc6da","ratio":"1","type":"tcp","method":"syn","host":
4","port":80,"use_ssl":false,"path":"","body":
{"type":"","value":""},"use_random_user_agent":true,"timeout":1000,"response":tr
[],"is_deleted":false,"activate_by_schedule":true,"started_at":"2023-01-25 10:00
{"id":"63d00313c92c1ad18fcfc6db","ratio":"1","type":"tcp","method":"syn","host":
4","port":8080,"use_ssl":false,"path":"","body":
{"type":"","value":""},"use_random_user_agent":true,"timeout":1000,"response":tr
```

Figure 1: Targeting Information

Pivoting to examine network telemetry for **87.121.52.9**, we observe a number of interesting communications.

Telegram

Regular connections are made to api.telegram[.]org, potentially indicative of Telegram bot interactions. It is possible that these connections relate to updates made to the Telegram channels associated with NoName057(16)'s DDoS campaigns.

CLOUDASSETS, RU

A high volume of traffic is observed to two IP addresses assigned to CLOUDASSETS, RU (AS212441).

109.107.184.11

Connections are made to TCP/27017 of **109.107.184.11**, this port is commonly associated with MongoDB. It is likely that data transferred from the attack infrastructure is stored in a database hosted on this IP address.

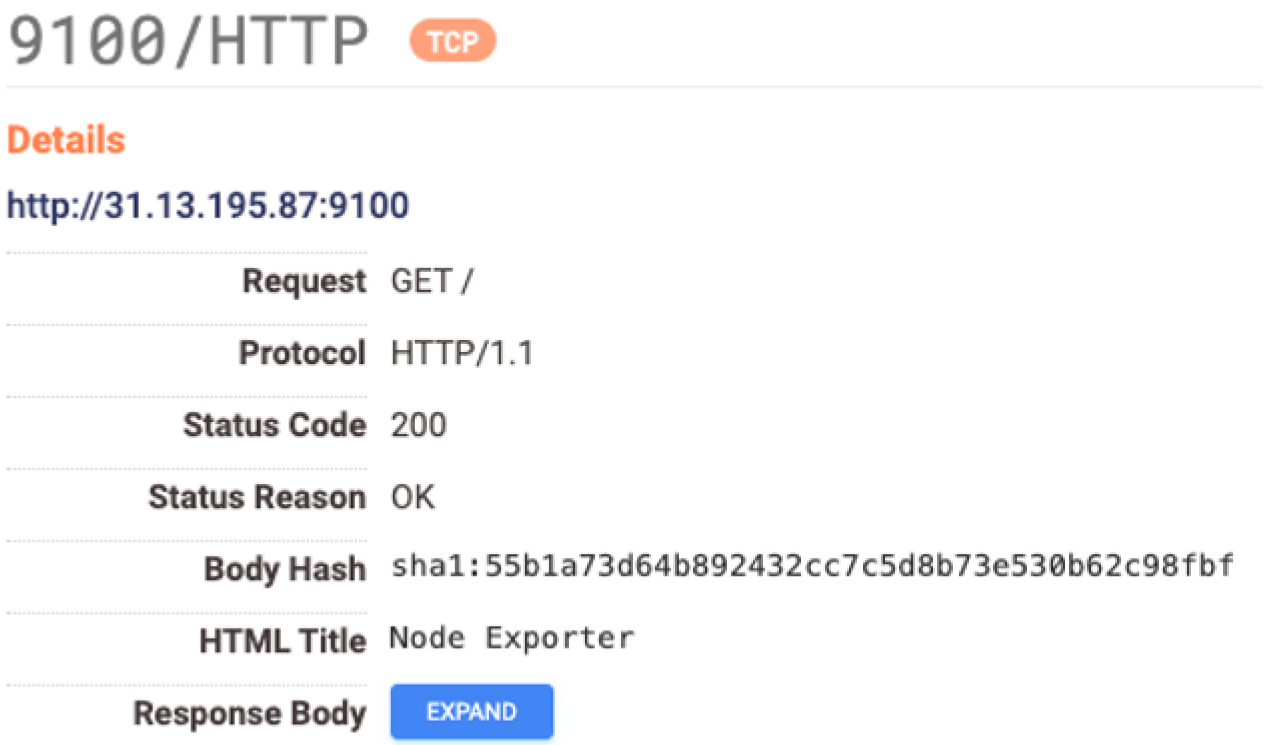
185.173.37.220

Connections are made to TCP/5672 and TCP/6379 of **185.173.37.220**, these ports are commonly associated with RabbitMQ and Redis respectively. This host is therefore likely used to store events / commands from the operator(s) of this infrastructure.

It is plausible that further operator hosts sit beyond this IP address, to either update or read messages from the RabbitMQ bus, however due to the geolocation of **185.173.37.220** further upstream insights are not available.

In addition to the outbound connections, inbound traffic to local ports TCP/5051 and TCP/9100 was observed, sourced from **91.142.79.201** (also CLOUDASSETS, RU). Pivoting on **91.142.79.201**, additional traffic was also observed sourced from this IP to TCP/9100 of **31.13.195.87** (the original C2 server).

TCP/9100 is commonly associated with Prometheus Node Exporter, a platform used for collecting metrics / alerts from remote servers. Indeed, open ports information for **31.13.195.87**:9100 shows an instance of Node Exporter running as of the time of writing.



9100/HTTP TCP

Details

http://31.13.195.87:9100

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK
Body Hash	sha1:55b1a73d64b892432cc7c5d8b73e530b62c98fbf
HTML Title	Node Exporter
Response Body	EXPAND

Figure 2: Open Ports Data for 31.13.195.87 - Censys

91.142.79.201 is therefore likely used for monitoring the operator's infrastructure and collecting metrics on usage; possibly providing updates on campaign effectiveness and the number of active 'bots'.

In a few instances, we also observed **91.142.79.201** making connections to TCP/9100 of IP addresses used in the attack infrastructure of NoName057(16)'s operation.

When reviewing the infrastructure in its totality, it is clear that the operator(s) behind NoName057(16) is familiar with systems design / maintenance; potentially pointing towards a threat actor(s) with legitimate work experience in this area.

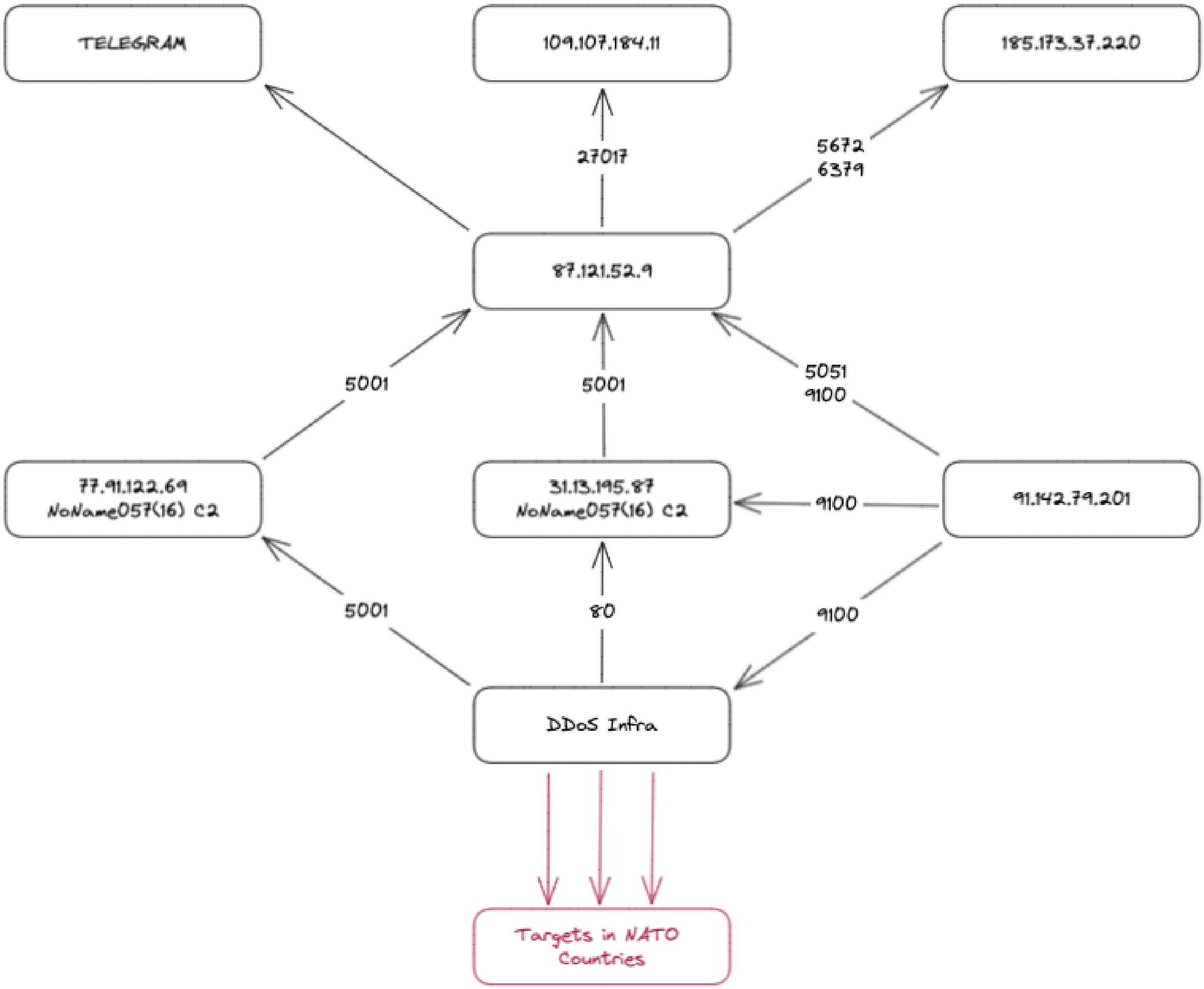
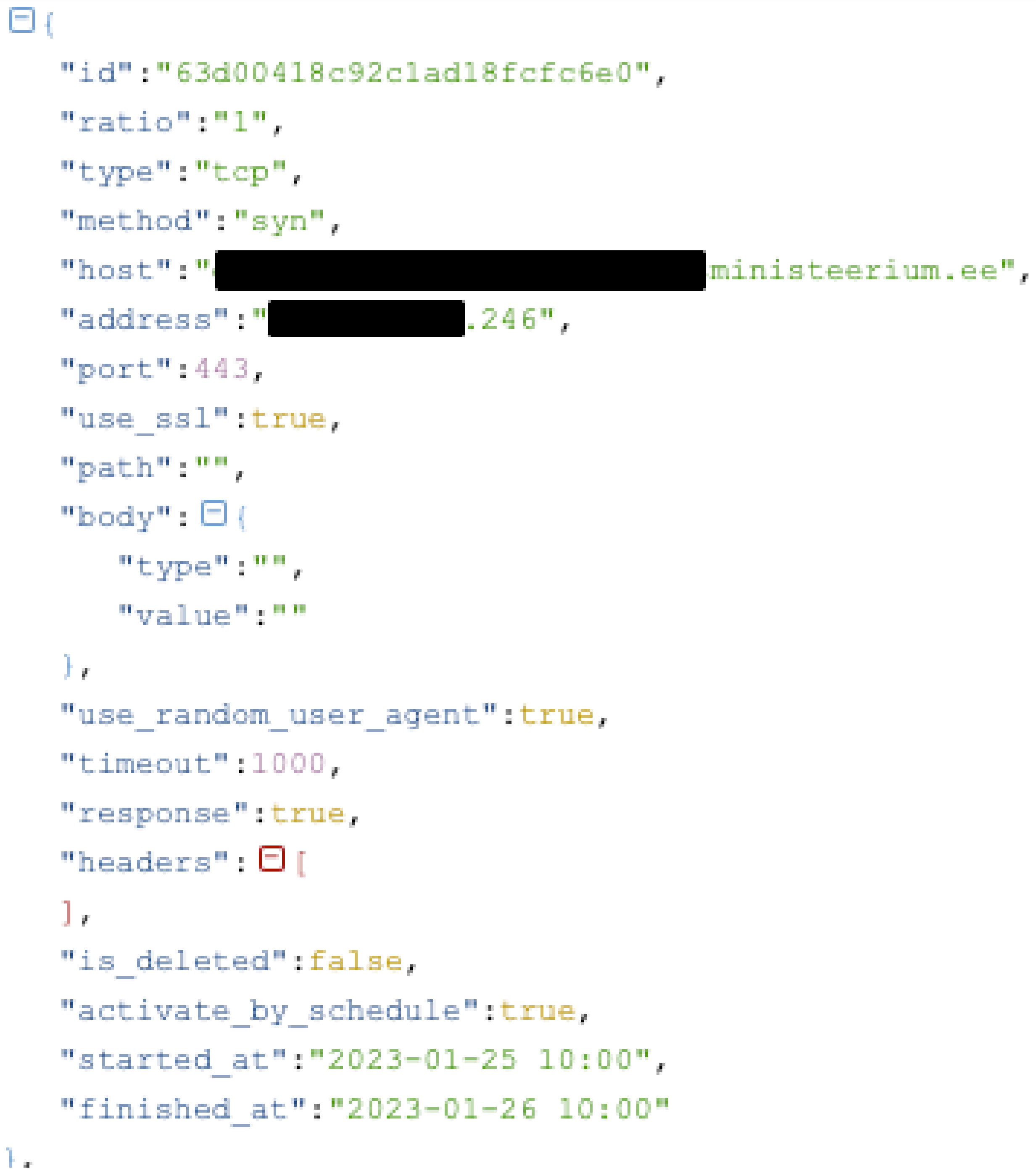


Figure 3: An Overview of NoName057(16) Infrastructure

Targeting

Previous reporting on NoName057(16) has highlighted DDoS attacks against an array of targets across business sectors and nations, including government / military departments.

At the time of writing this report, we took a look at the ‘current’ targets of the operation; one which stood out was the Estonian Ministry of Finance, with a particular subdomain being targeted.



```
{
   "id":"63d00418c92c1ad18fcfc6e0",
   "ratio":"1",
   "type":"tcp",
   "method":"syn",
   "host":"[redacted]ministeerium.ee",
   "address":"[redacted].246",
   "port":443,
   "use_ssl":true,
   "path":"",
   "body":{
      "type":"",
      "value":""
   },
   "use_random_user_agent":true,
   "timeout":1000,
   "response":true,
   "headers":[
   ],
   "is_deleted":false,
   "activate_by_schedule":true,
   "started_at":"2023-01-25 10:00",
   "finished_at":"2023-01-26 10:00"
},
```

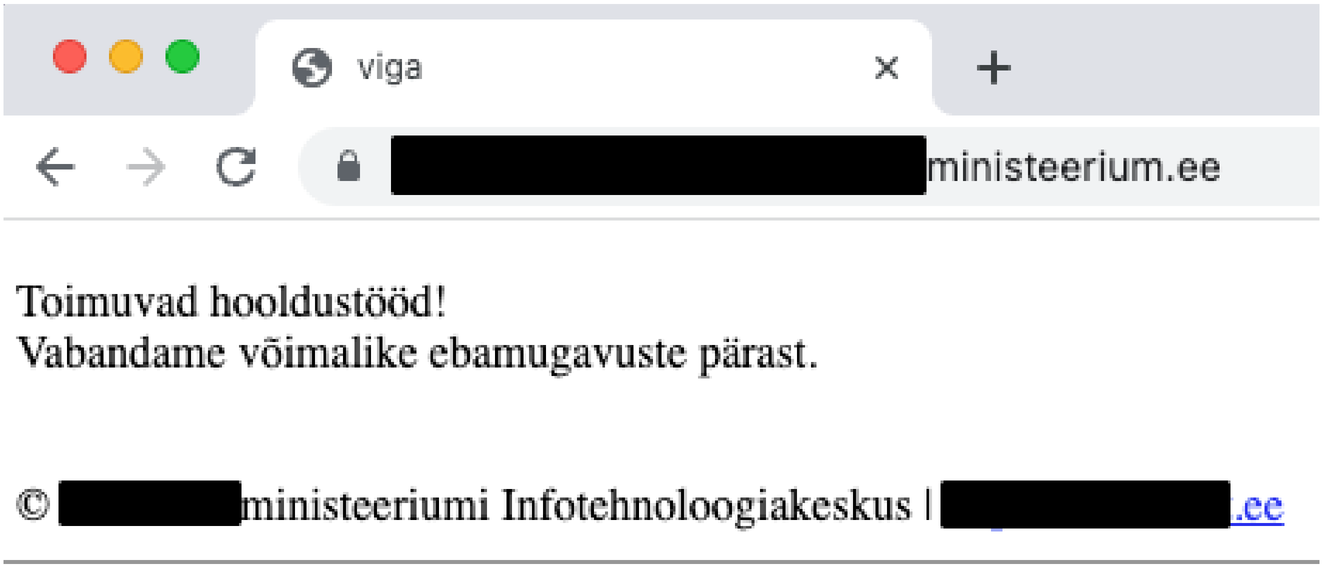
Figure 4: Targeting Details for the Estonian Ministry of Finance

From this entry on the C2 target list, we can see that a domain hosted on **xx.xx.xx.246** is the target of the attack, which was set to commence at 10:00 on 25 January 2023.

We initially assumed this meant 10:00 UTC, however, when looking into our threat telemetry for **xx.xx.xx.246** the attack appears to have commenced at 07:00 UTC; so the start time in the C2 target list in fact refers to UTC+3, which happens to coincide with Moscow Standard

Time.

As of 17:00 UTC on 25 January 2023 the target subdomain was displaying a ‘down for maintenance’ message, likely indicating that the attack had achieved a degree of success.



[redacted]ministeerium.ee

Toimuvad hooldustööd!
Vabandame võimalike ebamugavuste pärast.

© [redacted]ministeeriumi Infotehnoloogiakeskus | [redacted].ee

Figure 5: Maintenance Message

Returning to the aforementioned threat telemetry data for this target, the DDoS attack is evident in the data; which we have mapped below looking at the last seven days of traffic to/from **xx.xx.xx.246** (19 - 25 January 2023).

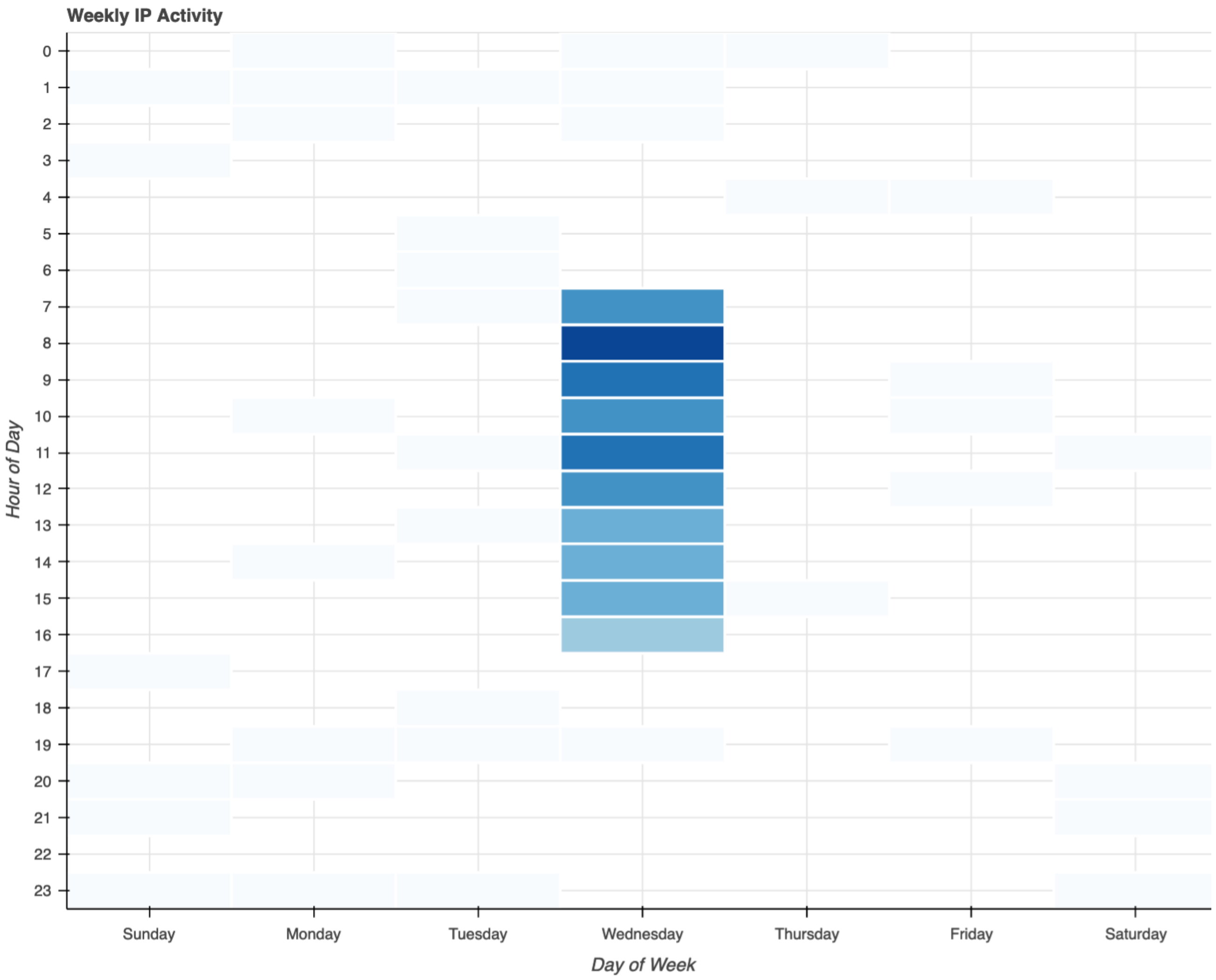


Figure 6: DDoS Attack Data - Target One

As of 17:00 UTC on 25 January, we can see that the attack began at 07:00 UTC (as mentioned previously), with a peak in activity between 08:00 UTC - 09:00 UTC, and a large volume of traffic has been received since that time; significantly outside the usual expected norms for this IP address.

Looking at a previous Estonian target from the same seven-day time period, we see that the attack lasted for 24 hours, commencing and ending at 07:00 UTC. As previously, activity peaked in the first few hours of the attack; this period is likely when the DDoS is most effective, before mitigating actions can be undertaken.

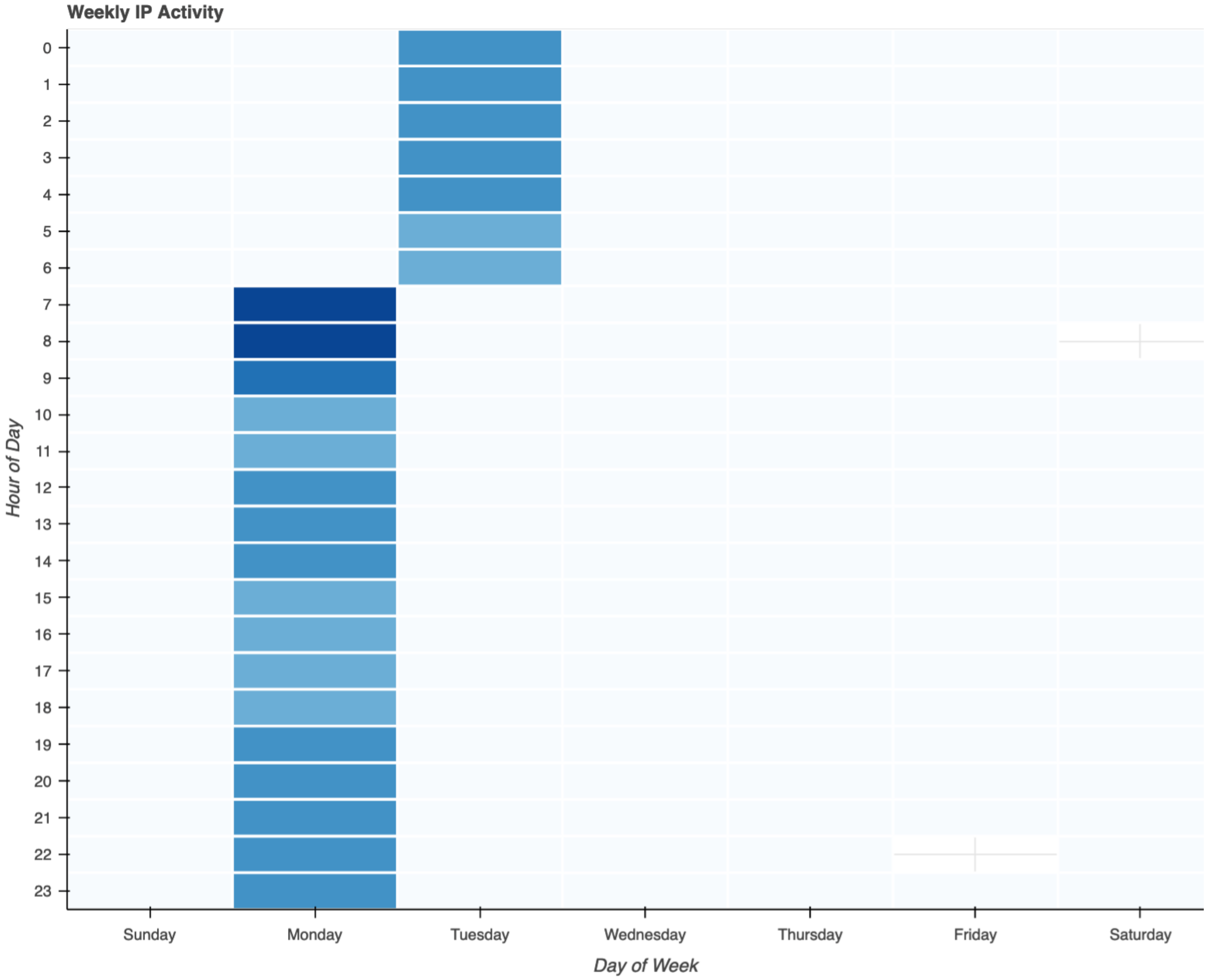


Figure 7: DDoS Attack Data - Target Two

Overall, since the beginning of 2023, we have been able to confirm attacks against entities with infrastructure hosted in Czechia, Denmark, Estonia, Germany, Slovakia, and Slovenia.

Attack Infrastructure

When examining the data for the DDoS attacks against the two Estonian targets, we found that 99.8% of the traffic inbound to the second (earlier) target was sourced from IP addresses which had later been used in the attack on the first target.

Whilst IPs assigned to 21 distinct ASNs were observed in this ‘common’ dataset, 98.6% of the traffic originated from IPs assigned to STARK-INDUSTRIES, GB. Looking further into the data, IPs residing in two /24 netblocks were responsible for over 65% of this traffic:

- 5.182.39.0/24 (38 IPs)
- 94.131.106.0/24 (21 IPs)

STARK-INDUSTRIES, GB relates to a hosting company ‘Stark Industries Solutions Ltd’ which was incorporated in the United Kingdom through Companies House on 10 February 2022, by Moldovan national Ivan **NECULITI**. **NECULITI** is further associated with several other hosting companies; including MIRhosting and Perfect Quality (PQ) Hosting, which are purported to operate from the Netherlands and Moldova respectively.

We frequently observe all three hosting companies being used to host malicious content, or as in this case, used directly for attack infrastructure. The website hucksters[.]net, which amongst other things seeks to expose individuals involved in fraud and spam, has previously profiled **NECULITI**.

Note, we have seen no evidence which associates NECULITI directly with these malicious activities; nor do we intend to insinuate that he is connected in any way with nefarious pursuits in general. This data point is mentioned as it exists on the public record and is the common tie between the hosting companies highlighted.

Pivoting back to the C2 server (**31.13.195.87**), by examining all inbound connections to TCP/80 since 19 December 2022, when it became operational, we are able to extract a more complete picture of the attack infrastructure.

*This process is caveated by the fact that other ‘non attack infrastructure’ connections are likely to have been made to **31.13.195.87**:80, particularly since the publication of this IP as a C2 server for NoName057(16) activities. However, the idea here is to identify likely attack infrastructure based on the regularity and volume of traffic, and any emerging patterns, for example sequential IPs within the same netblock as seen in the two attacks above.*

In total we observed IPs assigned to 83 distinct ASNs communicating with **31.13.195.87**:80. However, once again infrastructure associated with the previously referenced hosting provider(s) dominated, with 84% of all communications originating from IPs assigned to either MIRhosting or Stark Industries.

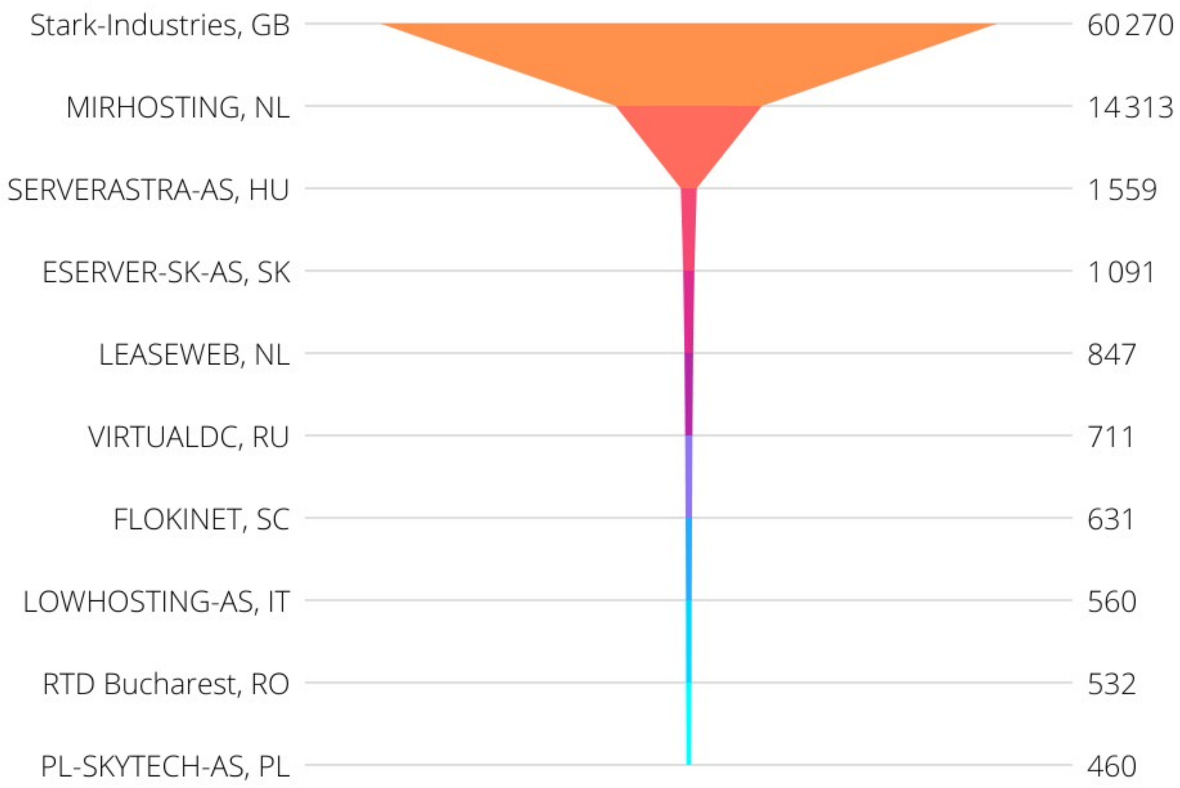


Figure 8: Top-10 Observed ASNs

Looking a little further into this data, IPs residing in a limited number of netbooks generated the majority of the traffic; the top 10 netblocks accounting for 68% of the total.

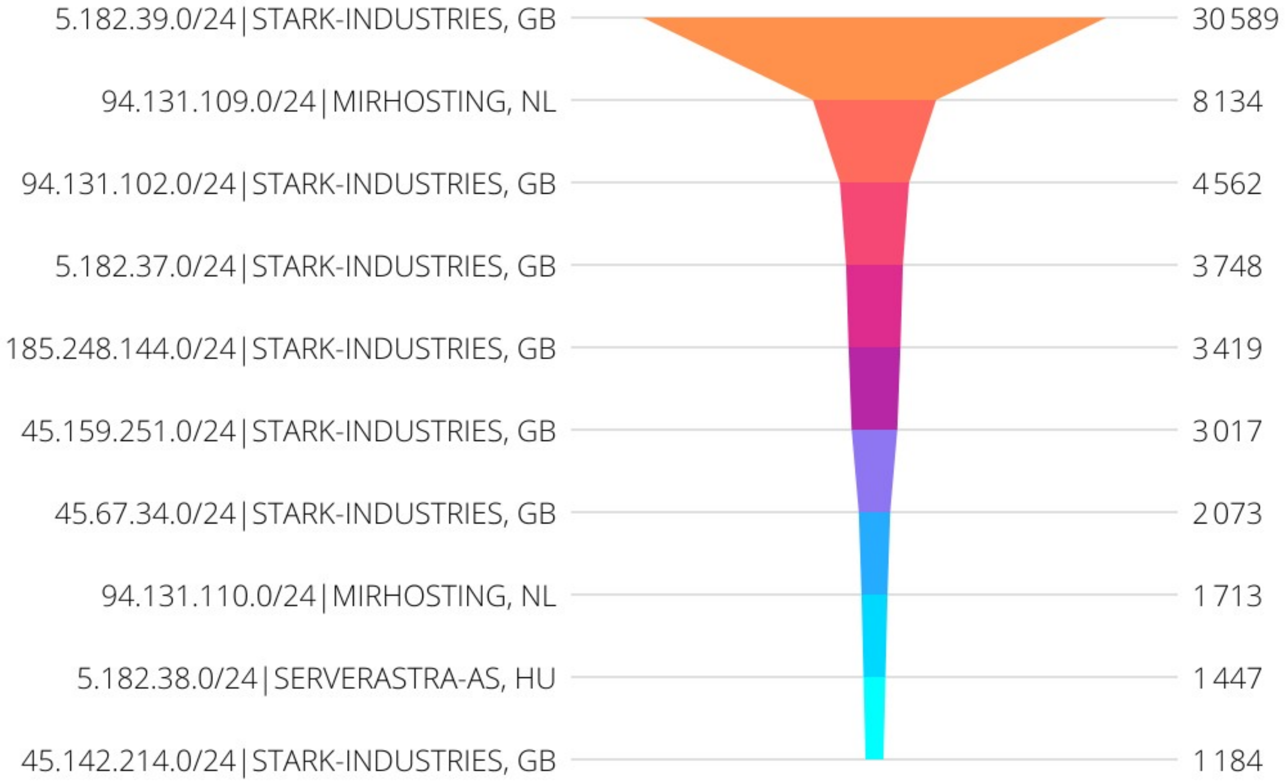


Figure 9: Top-10 Observed Netblocks

5.182.39.0/24, as observed in the data for the Estonian attacks, is the clear number one, the other netblock from that data (94.131.106.0/24) was just outside the top-ten at number thirteen.

What was notable was the fact that many of the IPs had been in communication with **31.13.195.87** since 19 December 2022, continuing up to the time of writing; indicating a broadly static attack infrastructure.

Conclusion

In this post we have examined the infrastructure used to manage the DDoS attacks attributed to NoName057(16); demonstrating a well-thought out structure which includes capacity for monitoring, tasking, and remote storage of data.

As a pro-Russian hacktivist operation, it is no surprise that there are several pointers to a Russian nexus; the use of Russian hosting providers for the management infrastructure, and the use of Moscow Standard Time for targeting instructions.

From our observations, whilst heavily focused on a small number of specific targets, NoName057(16) has had some successes in temporarily disrupting web services, with evidence of their targets being offline or ‘under maintenance’. The broader impacts of these attacks will likely remain limited providing there is no major escalation of activities / or growth in available attack infrastructure.

That brings us to the most significant finding in this blog; the static and limited nature of the attack infrastructure which has been utilized by NoName057(16) to date. For an operation which is labeled as “volunteer” driven; the fact that so much of the infrastructure is sourced from one provider raises questions.

- Is a sizeable chunk donated by one generous “volunteer”?
- How many “volunteers” actively contribute to the operation?
- Are NoName057(16) propping up their operation with infrastructure they have procured themselves?

We have observed a diverse range of IPs being utilized in attacks, but the volume of traffic related to the majority of these IPs is minimal; if you were to deduct the traffic sourced from IPs assigned to Stark Industries there is a question as to what impact the attacks would have.

With all this being said, we will continue to monitor NoName057(16)’s activities, providing updates via our Twitter and Mastodon pages.

Recommendations

- Although not always the best advice with DDoS attacks; we would recommend that inbound connections from the below netblocks are blocked.
- For users of Pure Signal Recon, you can follow this activity by querying for the IPs detailed in Figure 3;
- **31.13.195.87**
- **87.121.52.9**
- **109.107.184.11**
- **185.173.37.220**
- **91.142.79.201**
- If you are an ISP or Network Operator with DDoS challenges, sign up for our no-cost DDoS mitigation service UTRS

IOCs

Key Attack Infrastructure (as of 26 January 2023)

5.182.39.0/24

94.131.109.0/24

94.131.102.0/24

5.182.37.0/24

185.248.144.0/24

45.159.251.0/24

45.67.34.0/24

94.131.110.0/24

5.182.38.0/24

45.142.214.0/24

94.131.99.0/24

5.182.36.0/24

94.131.106.0/24

80.92.204.0/24

45.8.147.0/24