2024 updates and behavioural shifts

blog.sekoia.io/Noname05716-Ddosia-project-2024-updates-and-behavioural-shifts/

1 March 2024

Sekoia TDR, Amaury G. and Maxime A. March 1 2024

11 minutes reading

Context

Since the onset of the War in Ukraine, various groups identified as “nationalist hacktivists” have emerged, particularly on the Russian side, to contribute to the confrontation between Kyiv and Moscow. Among these entities, the pro-Russian group **NoName057(16) has garnered attention through the initiation of Project DDoSia,** a collective endeavour aimed at conducting large-scale distributed denial-of-service (DDoS) attacks, targeting entities (private corporations, ministries and public institutions) belonging to countries supporting Ukraine, predominantly NATO member states.

As of 2024, Project DDoSia and the group operating it are now familiar names, **Sekoia.io continues to proactively monitor the Command and Control (C2)** infrastructure of the DDoS tool. Specifically, we implemented an automated system for real-time target collection and regular monitoring of communication channels wherein NoName057(16) claims responsibility for its attacks, as mentioned in our blog post from June 2023: Following NoName057(16) DDoSia Project’s Targets. Even more recently in 2024, we discussed the monitoring of this group’s infrastructure in our annual report: Adversary infrastructures tracked in 2023.

This current report will detail **an overview of the changes made**, both from the perspective of the software shared by the group to generate DDoS attacks and the specifics of the evolution of the C2 servers, culminating in the targeting of countries and sectors for 2024.

System-level analysis of newly shared files by the adminstrators of DDoSia project

On 11 November 2023, the administrators of the Telegram channel for Project DDoSia shared a new version. Without any prior announcement, the newly shared version now includes compatibility with more types of processor architectures. The update added compatibility for 32-bit, as well as support for the FreeBSD operating system. Of note, they already supported AMD64, ARM, and ARM64 in previous versions. As of 21 February 2024, the shared ZIP archive contains the following files:

Filename	Filetype
d_freebsd_arm	ELF 32-bit LSB executable, ARM
d_freebsd_x32	ELF 32-bit LSB executable, Intel 80386
d_freebsd_x64	ELF 64-bit LSB executable, x86-64
d_lin_arm	ELF 32-bit LSB executable, ARM
d_lin_x32	ELF 32-bit LSB executable, Intel 80386
d_lin_x64	ELF 64-bit LSB executable, x86-64
d_mac_arm64	Mach-O 64-bit arm64 executable
d_mac_x64	Mach-O 64-bit x86_64 executable
d_win_arm64.exe	PE32+ executable (console) Aarch64
d_win_x32.exe	PE32 executable (console) Intel 80386
d_win_x64.exe	PE32+ executable (console) x86-64

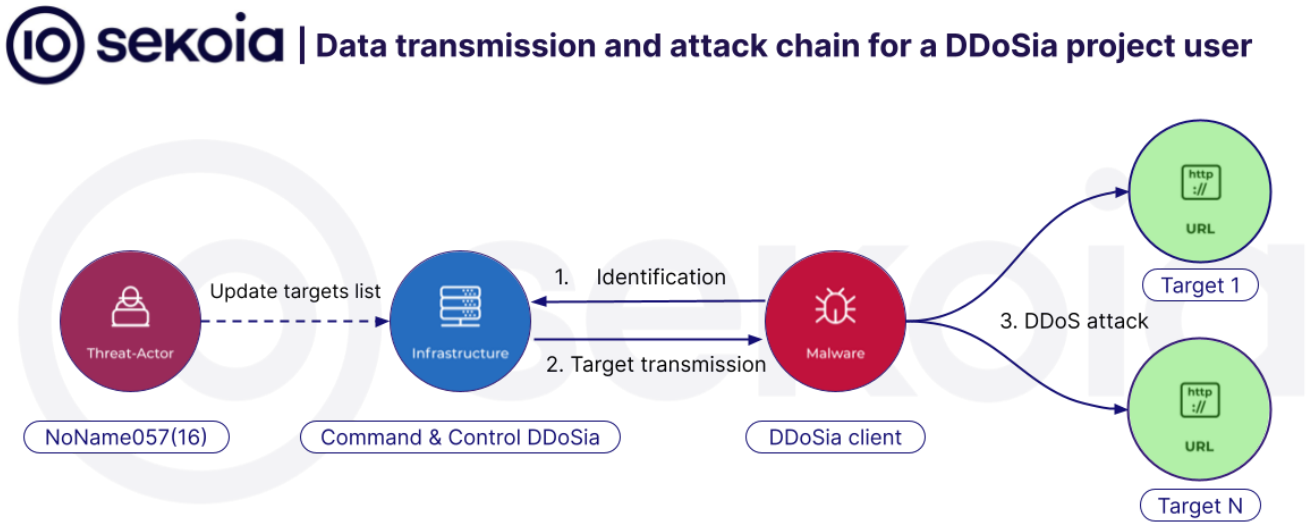
Table 1 – Contents of the ZIP archive shared by DDoSia administrators

Furthermore, it is observed that the main ZIP archive contains two folders: one named `d_eu` and the other `d_ru`, which are adapted, according to the administrators, for users wishing to execute the file based on their geographical location. When launching the executable, a warning message is displayed to the user, advising them to use a VPN if they are located in Russia, as shown in the following extract:

```
C:\[…]\d(27)\d_eu>d_win_x64.exe
Go-Stresser версия 2.0 | PID 10912
© NoName057(16)
```

login success…
try get target list…
loaded 285 targets…
–If you work from Russia, then switch the VPN to a foreign one. You will have 1 minutes for this.
–Если вы работаете из России, то переключите vpn на зарубежный. У вас на это будет 1 минуты
Regardless of which folder the executable is launched from, this warning message will appear. The main distinction is that in the "d_ru" folder, all files are appended with the `_ru` suffix. On 4 December 2023, following the rollout of these new files, the administrators also shared a page on `telegra.ph` (`hxxps://telegra[.]ph/Instrukciya-dlya-uchastnikov-proekta-DDoSia-Project-12-04`), providing detailed instructions for users, along with a FAQ section. In item number 2, responding to the query "*Does the provider see my actions or law enforcement agencies see my IP?*", the answer given is as follows:*"If the computer is located on the territory of the Russian Federation, then even without using a VPN,* ***it is extremely unlikely that there will be any problems with the law****, since the software is designed for stress testing. At least that's what we think. If the computer is located outside the Russian Federation, it is strongly recommended to use a VPN to change the IP address. You can check the change in IP address, for example, on myip.com.*
*It is recommended to monitor the VPN in action to avoid being disabled or use a VPN with an Internet killswitch option."*The decision not to mandate VPN usage in Russia, especially given their statement "*it is extremely unlikely that there will be any problems*", suggests a possible collaboration between the NoName057(16) group and the Russian state. This inference is drawn despite the absence of any publicly claimed connection and the lack of official attribution at present.

In terms of development, this latest version introduces a change in the way data transmitted between a user and their C2 server is encrypted. As a reminder, here is the overall operating diagram when a user joins the project and runs the DDoSia program:



Compared with the previous version, additional data is now sent to uniquely identify the user's machine running the program. During the first step of identification, the following data is transmitted via a POST request to the URL: `[ip]:[port]/client/login`, including the following metadata:

POST /client/login HTTP/1.1
Host: [C2 IP]
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.2.1) Gecko/20021208 Debian/1.2.1-2
Content-Length: 527
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=$2a$16$UhwrgtnQQZX7.kfsw5QBh.[…]Qdi; C=2bc08885-84ed-4233-a9d5-XXXXXXXXXXXX-X

A new feature has been added to the latest update, involving the encryption of data within the content of this HTTP POST request, a functionality not present in the previous version. Once decrypted, the content of this request is as follows:

{
"key":"**[…]AVlZLw**",
"user":"**MZDZQwuID[…]nOEHQdi**",
"client":"**2bc08885-84ed-4233-a9d5-XXXXXXXXXXXX-X**",
"inf":{
"SystemUserName":"**User**",
"OS":"**windows**",
"KernelVersion":"**10.0.22621.2428 Build 22621.2428**",
"KernelArch":"**x86_64**",
"PlatformFamily":"**Standalone Workstation**",
"CPUCores":**1**,
"RegisterTime":"**2023-11-XXT22:50:20.1536289Z**",
"TimeZone":"**UTC**"
}
}

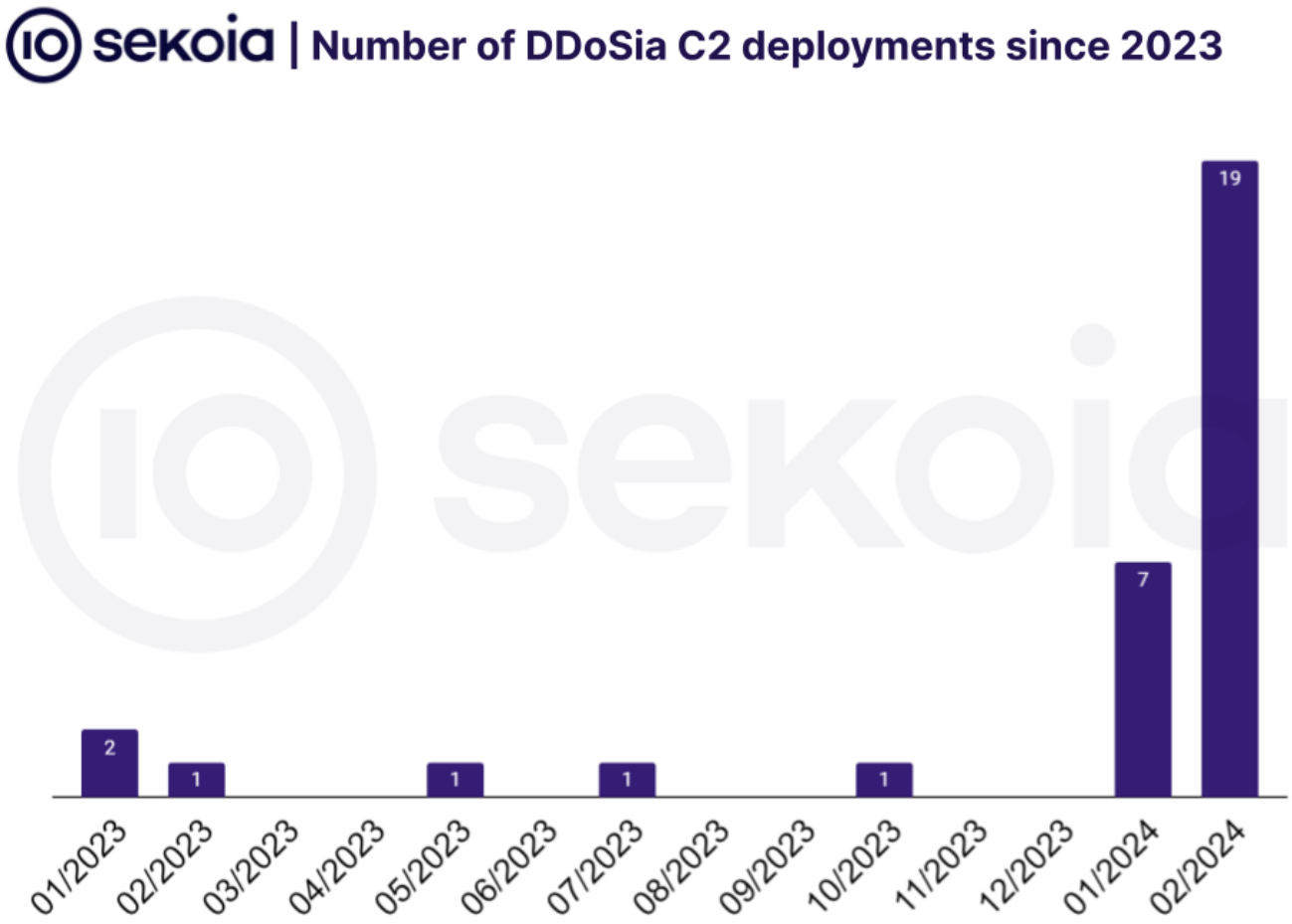
The `C` value, integrated into both the request data (named as `client`) and the request cookie, is a GUID which uniquely identifies the user's machine. On Windows, this value, which is encrypted during transmission, is extracted from the registry key `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid`. The `U` value corresponds to the contents of the `client_id.txt` file, accessible after registration via the DDoSia project's Telegram Bot (`t[.]me/DDosiabot`).

The JSON table named `inf` contains seven elements that enable the project's administrators to keep precise track of users. Operating under Windows, the program collects the name of the user of the machine, the kernel version, the architecture, the type of machine, the number of processors available, and the registration date of the user in the DDoSia project.

These elements are probably intended for statistical analysis, as they are intended to structure the mapping of the technical characteristics of the machines running the DDoSia software and uniquely identify the users. Overall, this reflects the increased sophistication of the transmission mechanisms, in line with our medium-term development hypothesis set out in our blog in June 2023.

Service instability: impact of recurring C2 changes

Although the latest version has improved the software's data transmission capabilities, **DDoSia administrators have frequently changed C2 servers in recent weeks**. Below is a graph illustrating the evolution of the number of servers used from 2023 to 23 February 2024.



In 2024, several dozen changes took place in the space of just a few weeks. These changes illustrate the challenges faced by NoName057(16) in maintaining the stability of its C2 servers over an extended period. Every time the configuration of their server changed, the group had to publish an updated version on its Telegram channel. Users then had to download and install the new version to continue participating in the attacks and receive their compensation.

Since 2023, **our research has enabled us to trace C2 servers** distinctively, **even before they are put into operational use** for users. This technique has made it easier to track the progress of deployed C2s, as illustrated in the table below.

IPv4	Date of activation (YYYY/MM/DD)	Host country	Autonomus System (AS)	ASN
38.180.95[.]29	2024-02-23	Hong Kong	M247	AS9009
38.180.101[.]98	2024-02-22	Serbia	M247	AS9009
185.39.204[.]86	2024-02-22	Turkey	GIR-AS	AS207713
195.133.88[.]73	2024-02-21	Germany	GIR-AS	AS207713
185.239.48[.]70	2024-02-21	Israel	IL	AS42474
5.252.23[.]100	2024-02-20	Slovakia	STARK-INDUSTRIES	AS44477
193.17.183[.]18	2024-02-19	Spain	NEARIP	AS49600
193.233.193[.]65	2024-02-12	Hong Kong	ADCDATACOM-AS-AP	AS135330
77.75.230[.]221	2024-02-10	Czech Republic	STARK-INDUSTRIES	AS44477
185.234.66[.]239	2024-02-09	Turkey	STARK-INDUSTRIES	AS44477
83.217.9[.]33	2024-02-08	Turkey	GIR-AS	AS207713
83.217.9[.]48	2024-02-08	Turkey	GIR-AS	AS207713
193.187.175[.]252	2024-02-08	France	CLOUDBACKBONE	AS56971
45.84.0[.]235	2024-02-08	Moldova	STARK-INDUSTRIES	AS44477
45.136.199[.]235	2024-02-07	Romania	M247	AS9009
185.234.66[.]126	2024-02-06	Turkey	STARK-INDUSTRIES	AS44477
193.233.193[.]90	2024-02-04	Hong Kong	ADCDATACOM-AS-AP	AS135330
45.89.55[.]4	2024-02-02	Serbia	STARK-INDUSTRIES	AS44477
188.116.20[.]254	2024-02-01	Kazakhstan	ASNLS	AS200590
77.83.246[.]159	2024-01-31	Poland	GIR-AS	AS207713
185.255.123[.]84	2024-01-29	Nigeria	BrainStorm Network	AS136258

195.35.19[.]138	2024-01-26	Brazil	AS-HOSTINGER	AS47583
89.105.201[.]91	2024-01-23	Netherlands	NOVOSERVE-AS	AS24875
5.44.42[.]29	2024-01-23	United Arab Emirates	GIR-AS	AS207713
193.233.193[.]240	2024-01-22	Hong Kong	ADCDATACOM-AS-AP	AS135330
94.131.97[.]202	2024-01-20	Czech Republic	STARK-INDUSTRIES	AS44477
94.140.115[.]89	2023-10-26	Latvia	NANO-AS	AS43513
94.140.115[.]92	2023-07-05	Latvia	NANO-AS	AS43513
77.75.230[.]221	2023-05-15	Czech Republic	STARK-INDUSTRIES	AS44477
161.35.199[.]2	2023-02-10	Germany	DIGITALOCEAN-ASN	AS14061
212.73.134[.]208	2023-01-27	Bulgaria	NETERRA-AS	AS34224
94.140.114[.]239	2023-01-10	Latvia	NANO-AS	AS43513

To begin with, there has been **a shift in the geolocation of hosting servers**. Whereas in 2023 they were mainly located in Europe, in 2024 there is a diversification on a global scale, encompassing Asia, Africa and South America. This can be explained by the urgency of restoring the service quickly for their users. Furthermore, regarding the IPv4 addresses deployed, the group is reusing some previous addresses, such as `77.75.230[.]221`, used in both 2023 and 2024.

The fact that servers are sometimes disconnected on a daily basis in 2024 suggests that organisations are heavily involved in countering this threat. Of note is the fact that some servers have undergone several changes in a single day, as on 8 February 2024, when four different versions have been deployed. This trend of frequent changes continues, suggesting that infrastructure changes are very likely in the short term. Given the frequency with which C2 IPv4 addresses are changed, it is surprising that the DDoSia client does not yet incorporate automated mechanisms for remotely changing IP addresses.

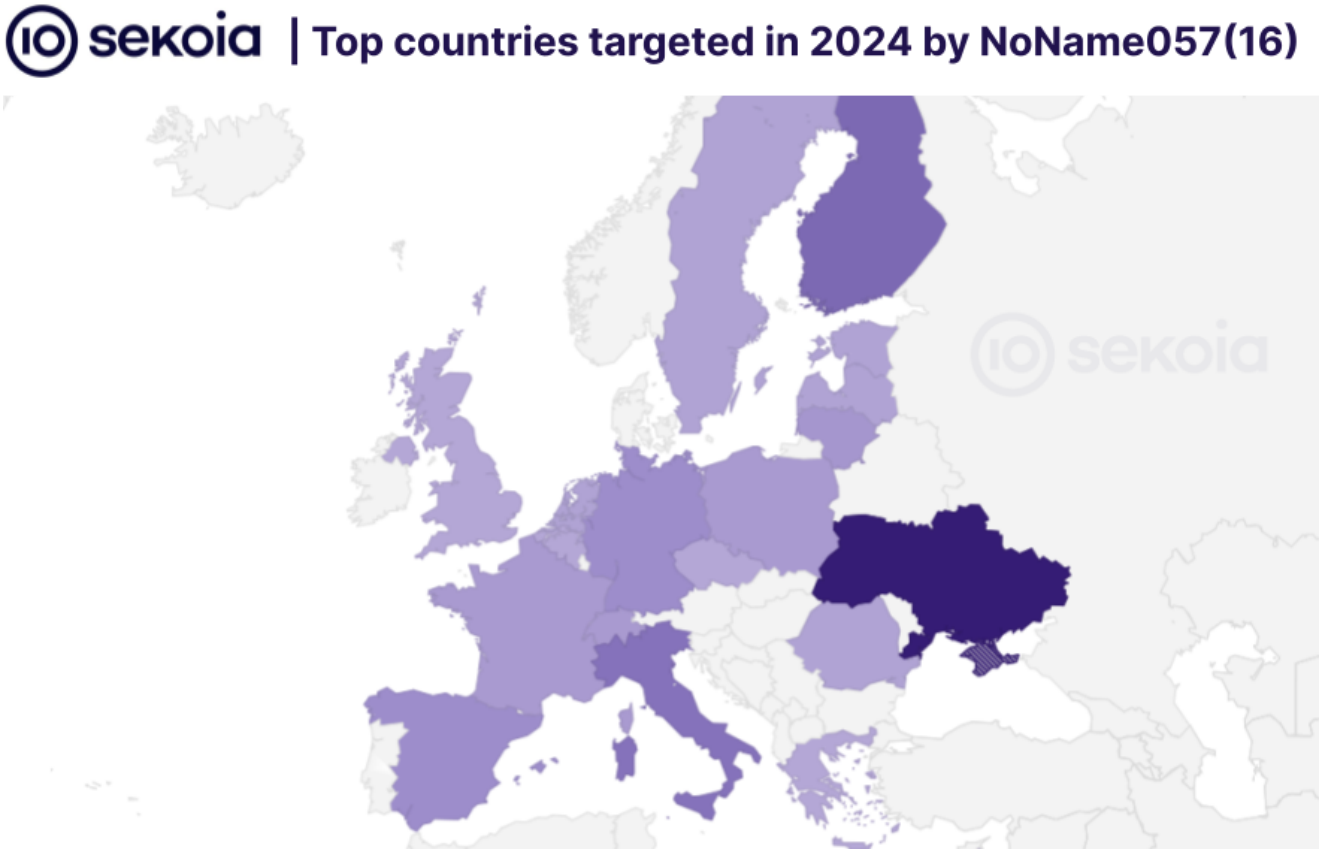
Although the DDoS infrastructure was sometimes temporarily unavailable for several hours, these interruptions did not prevent the NoName057(16) group from asserting its involvement in daily attacks with international repercussions. **This observation reinforces the idea that in addition to the project's users, DDoSia also has its own servers, which participate in the attacks as active users.**

Victimology analysis: most impacted countries and sectors in early 2024 by NoName057(16)

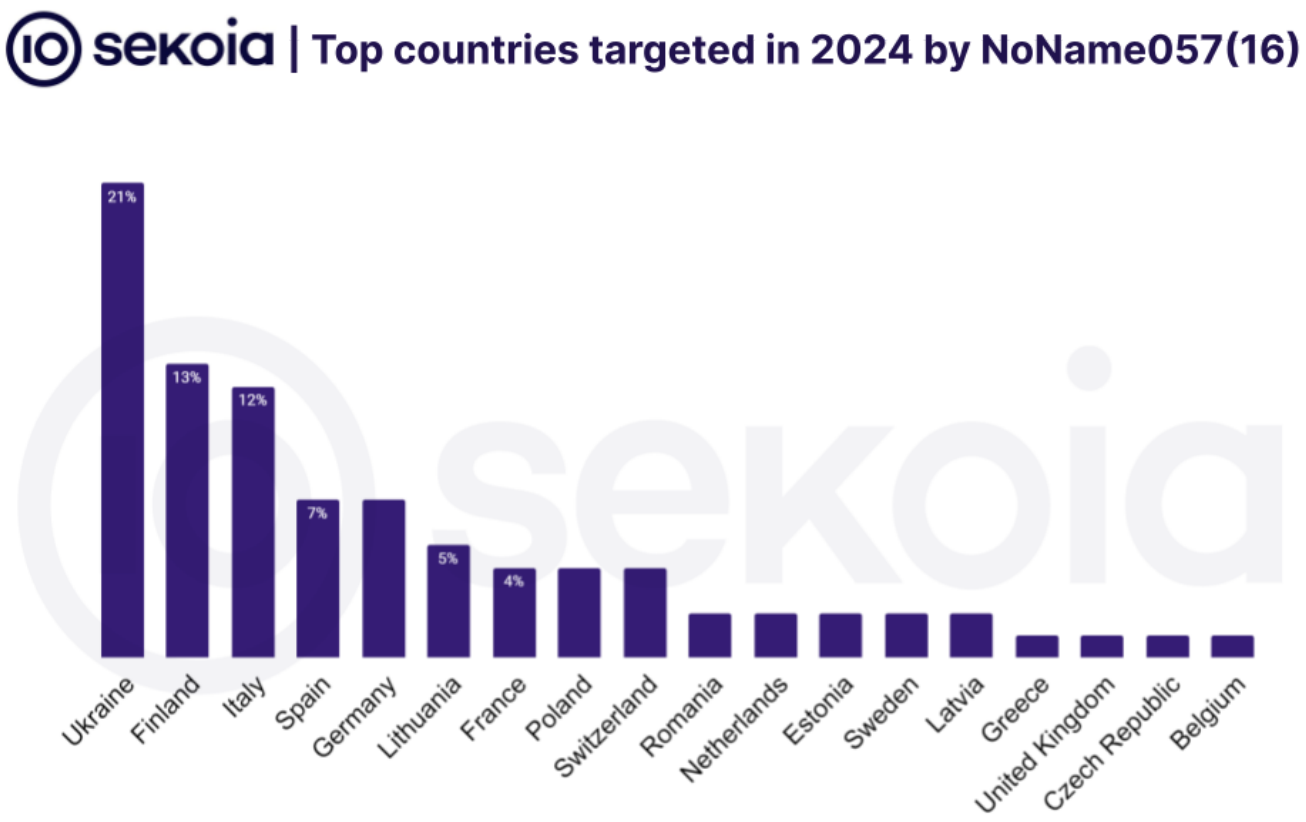
Based on Sekoia.io DDoSia software decryption tool, TDR analysts continue to monitor and analyse targeted domains, to establish a victimology analysis, as already exposed in our previous blogpost.

Impacted countries by DDoSia project

Despite a **noticeable instability of the C2 servers**, the DDoSia project persisted in carrying out and claiming responsibility for its attacks via its Telegram channels. From 1 January 2024 to 18 February 2024 (cut-off date), NoName057(16) pursued its **focus on European targets**, especially countries most involved in Ukraine war support



Like in 2023, **Ukraine remains the primary target**, with intensive targeting justified by the continuing Russia-Ukraine conflict, accounting for **almost a quarter of DDoSia attacks**.



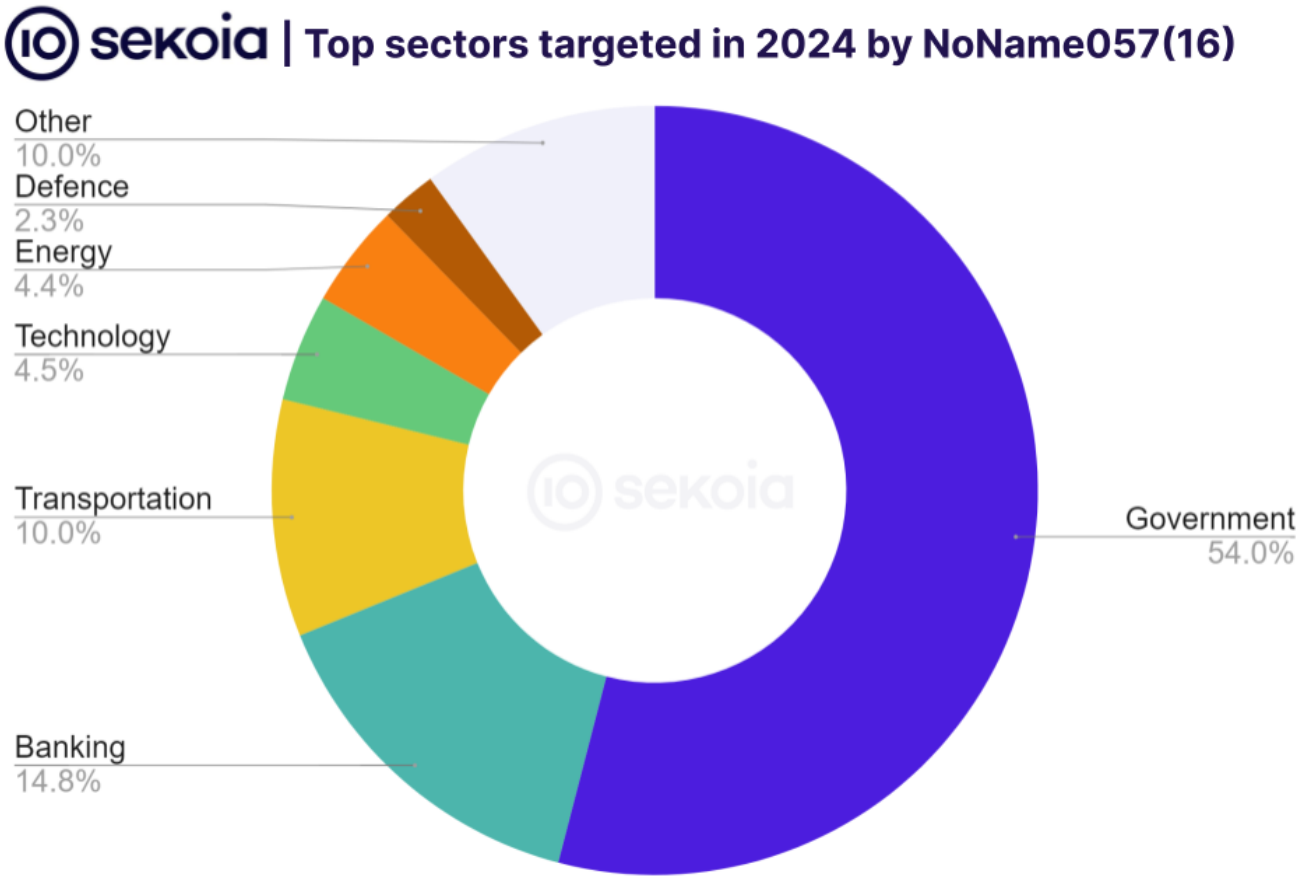
In January and February 2024, **Finland** and **Italy** were especially impacted by NoName057(16), highly likely for their NATO policies. Finland was campaigning for the 11 February presidential election during which the Russian aggression of Ukraine was a central topic. As a reminder, since 24 February 2022, Finland has cut all political and diplomatic relations with its neighbour and decided to join NATO. As for the Italian focus, it may be linked to the perceived efforts of the Italian prime minister Meloni, who helped persuade the Hungarian president, Viktor Orban, to go along with a landmark fund for Ukraine.

Notably, on 19 and 21 February 2024, we observed NoName057(16) leveraged DDoSia to impact multiple Japan-related entities. We assess with high confidence that the focus is a retaliation to the Japan Ukrainian conference for post-war reconstruction, where a 15.8 billion yen (€98 million) aid package was announced.

Thus we assess with high confidence, NoName057(16) group **continues to follow geopolitical developments to determine targeted countries** very closely, almost daily.

Impacted economic verticals

We analysed 700+ URLs and domains impacted by DDoS attacks by NoNames057(16). It shows **more than half of the targets impact government-related entities**, such as public administrations, public services, ministries or official websites. Such focus goes along our hypothesis where NoNames057(16) aims to impact governments for their policies supporting Ukraine.



It is interesting to observe that around 25% of DDoS impacted entities are related to either the **transportation sector** (we also noticed in 2023 days of DDoSia focus on ferry services or train-related entities) or the **banking vertical** (mostly private European and Ukrainian banks).

Conclusion

The **number of users** within the DDoSia project in Telegram is currently approaching **20,000 members**. In contrast, the number of **total users** following the NoName057(16) channels has passed **60,000**, almost **doubling since the beginning of 2023**. This continued growth reflects the sustained expansion of a community engaged for political or economic reasons.

Since December 2023, NoName057(16) has **established collaboration** agreements with **other hacktivist collectives**, focusing their efforts on targeted objectives. In February, the group announced an “alliance” with the groups SoubearArmy, 22C, CyberDragon, Horus Team, UserSec and PHOENIX, notably against Italian infrastructures. This emerging form of cooperation possibly shows a desire to strengthen its presence and influence in the public arena.

Although DDoSia’s infrastructure undergoes **frequent changes** and new software is regularly shared, these factors do not hinder the group’s ability to perpetuate and claim attacks on a daily basis. In the short term, it is highly likely that the group will **continue to**

share new software versions daily, including the C2 server change, and in the medium term, an updated version, including an evolution of the encryption mechanism, will be introduced in 2024.

DDoSia's IoCs

You can find the IoCs as a CSV file on our Community Github here.

Feel free to read other Sekoia TDR (Threat Detection & Research) analysis here :

What's next

The Architects of Evasion: a Crypters Threat Landscape

In this report, we introduce key concepts and analyse the different crypter-related activities and the lucrative ecosystem of threat...

Sekoia TDR and Livia Tibirna

Guidelines for selecting and disseminating Sekoia.io IOCs from CTI sources

In the ever-evolving landscape of cybersecurity, the battle against threats demands a multi-faceted approach. Organizations, now more than ever,...

Julien De Pins

Enhancing security with IOC detection

Indicators of Compromise (IOCs) serve as signals, hinting at potential security breaches or ongoing cyberattacks. These indicators consolidated in...

Mykhailo Shveika and SEKOIA.IO

Comments are closed.