



ThreatMon



IN-DEPTH ANALYSIS ON THE ROLES OF THREAT ACTORS AND ATTACKS IN THE UKRAINE-RUSSIA WAR

Noname057(16)



@threatmon



@MonThreat

Summary	3
Cyber Wars in The Ukraine-Russia War	3
Threat Actor Review: Noname057(16)	4
Who is Noname057(16)?	4
What are the Activities of Noname057(16)?	5
Which Side They Supports?	6
What Types of Attacks Does Noname057(16) Execute?	6
Which Industries Is Noname057(16) Targeting?	6
Noname057(16)'s Attacks	8
49000.com.ua Attack:	8
Passazieru Villciens Attack:	9
Latvian Seimas Attack:	10
Lithuanian Ministry of Foreign Affairs Attack:,	11
Poland Attack:	12
Europe Attack:	13
Noname057(16)'s Announcement:	14
DDoSia Project:	15
Czech Republic Attack:	16
Noname057(16)'s Country Based Announcements:	17
Germany:	17
Japan:	17
Poland:	18
Denmark:	18
Ukraine:	18
Macedonia:	19
Italy:	19
Poland:	20
Italy:	21
Japan:	21
Noname057(16)'s Attack TTPs	22
Noname057(16)'s Attack IOCs	23

Summary

The beginning of the Russia-Ukraine war dates back to Russia's annexation of Crimea in 2014. The political tension that erupted in 2021-2022 was the last straw and Russian forces took action on Putin's orders. Taking action on February 24, 2022, Russian forces launched a large-scale invasion of Ukraine. Russian President Vladimir Putin claims that this is not an invasion, but that Russia is protecting its geopolitical interests in the region, its citizens and its deployed soldiers.

This report is the 2nd Report in a series of investigations on threat actors playing an active role in the Ukraine-Russia war, based on the KillNet report shared by ThreatMon earlier.

Cyber Wars in The Ukraine-Russia War

In 2014, Russia annexed Crimea, leading to conflict in the Donbass region and the start of a cyber war between Ukraine and Russia. Since then, Ukraine has been a frequent target of Russian cyber attacks, including ransomware, DDoS, and data manipulation. These attacks have targeted critical sectors such as energy, finance, and communication.

One of the most notable cyber attacks on Ukraine occurred in 2015 when parts of the country experienced power cuts. The attack was allegedly carried out by the pro-Russian group Sandworm, which targeted the country's electricity grid. This cyber attack caused a worldwide debate on cybersecurity and served as a wake-up call for Ukraine to take stronger measures on cybersecurity.

Following the attack, Ukraine implemented several measures to enhance its cybersecurity capabilities. The country established a National Coordination Center for Cybersecurity and developed a national cybersecurity strategy. Additionally, the government introduced legislation to strengthen cybersecurity regulations and established partnerships with international organizations to share best practices and expertise.

Despite these efforts, Ukraine remains a target for cyber attacks from Russia. In 2017, the country was hit by another cyber attack, the NotPetya ransomware attack, which caused widespread disruption in Ukraine and other countries. The attack is believed to have been carried out by Russian hackers and caused billions of dollars in damage.

Ukraine's experience highlights the growing threat of cyber attacks and the need for countries to take cybersecurity seriously. As technology continues to advance, the risk of cyber attacks is only going to increase. Therefore, countries must continue to invest in cybersecurity measures to protect themselves from these threats.

Threat Actor Review: Noname057(16)

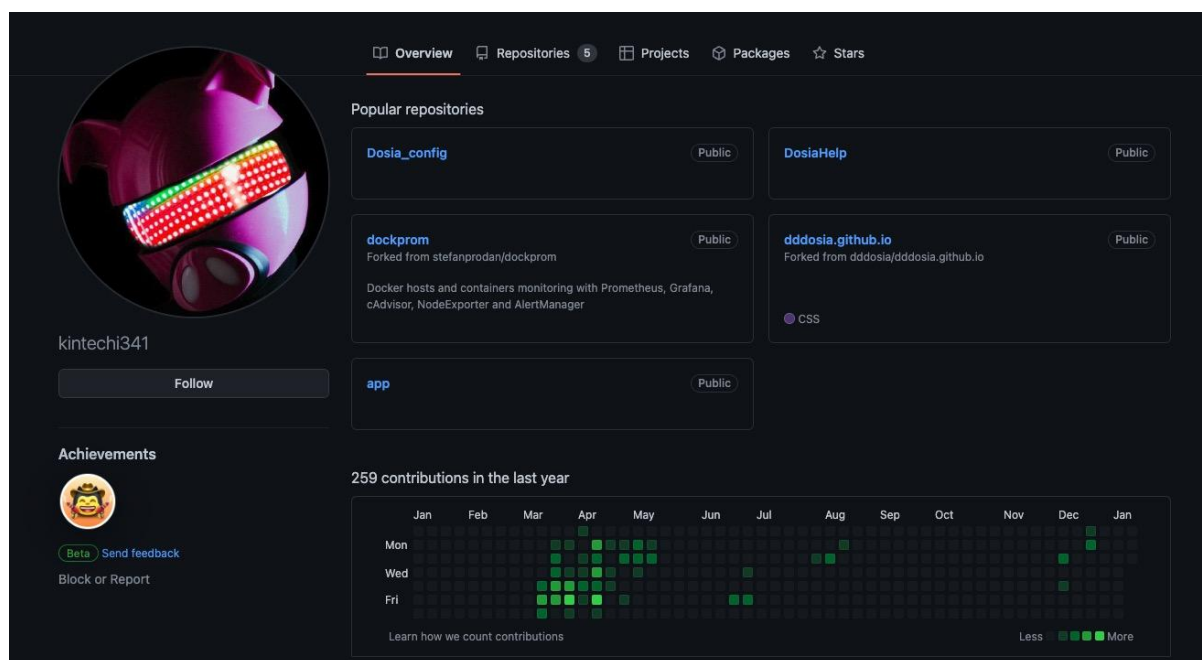
Who is Noname057(16)?

Self-proclaimed in March 2022, hacker group NoName057(16) is a notorious pro-Russian cybercriminal organization that conducts distributed denial-of-service (DDoS) attacks on Ukraine and NATO-affiliated countries. Reacting to the evolving political situation, it targets pro-Ukrainian companies and institutions in Ukraine and neighboring countries such as Estonia, Lithuania, Norway and Poland.

The group, which has more than 32,000 followers on Telegram, first began appearing in the media in early August 2022 after successfully attacking the Finnish and Polish parliaments.

Additionally, the group had a GitHub presence, according to some research firms. NoName057 used the GitHub platform to perform DDoS attacks on targets in various NATO countries and host the code used in their attacks. GitHub then disabled accounts belonging to the group. The two GitHub profiles the group uses are dddosia and kintechi341.

What are the Activities of Noname057(16)?



NoName057(16) specifically performs DDoS attacks. It uses public Telegram channels, a volunteer-based DDoS payment program, to carry out its attacks.

NoName057(16) uses Telegram to take responsibility for their attacks, make fun of targets, make threats and justify their actions as a group.

The group's targets include government organizations and critical infrastructures, where the hacking group has launched a project called DDOSIA and invited volunteers to participate in activities to launch DDoS attacks on targets they find "anti-Russian".

DDOSIA is a multi-threaded application that performs denial-of-service attacks against target sites by repeatedly issuing network requests. DDOSIA issues requests as instructed by a configuration file that the malware receives from a C2 server when it launches.

The group only reports successful DDoS attacks.

Which Side They Supports?

NoName057 is a Russian-affiliated hacking group that has been observed operating since March 2022.

What Types of Attacks Does Noname057(16) Execute?

Distributed Denial of Service (DDoS) is the group's most commonly used attack method. In September, they launched their DDoS service Project DDoSia, aiming to reach more people with the project and continue their activities.

Which Industries Is Noname057(16) Targeting?

The group targets Ukraine and NATO countries. (Ukraine, Latvia, Poland, Estonia, Finland, Germany, Japan etc.)

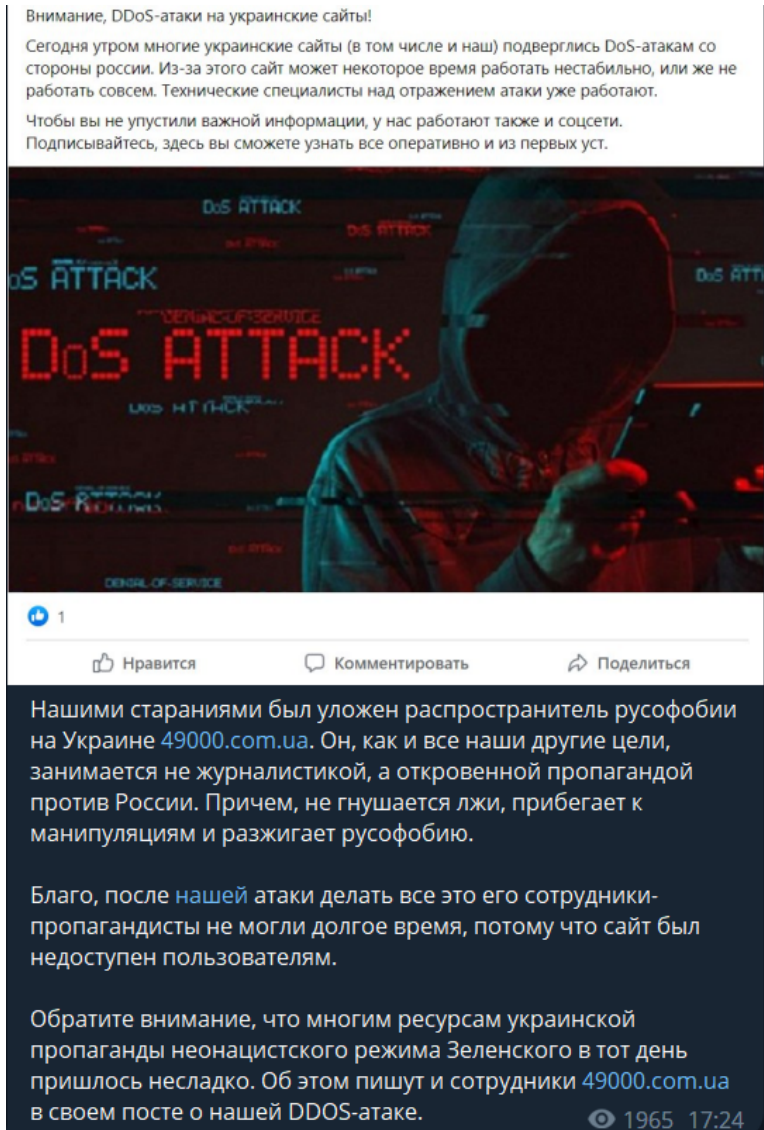
It appears that they have organized attacks on a wide range of sectors.

These sectors are :

- Journalism - News
- Law
- National Security and International Relations
- Telecommunications
- Banking
- Public Administration
- Transportation and Storage
- Finance and insurance
- Delivery Services and more.

Noname057(16)'s Attacks

49000.com.ua Attack:



In March-April 2022, mainly the newspaper and media sector was targeted. DDOS attacks were organized on all newspaper websites that they thought were engaged in propaganda. In mid-April, they stated, "We carry out DDOS attacks not only on Ukrainian media websites, but also on the resources of Russophobic MPs."

Passazieru Villciens Attack:

NoName057(16)



Электричка на станции Дубулты. Иллюстративное фото
ФОТО: Rebeka Žeire/LETA

В среду была нарушена торговля билетами на сайте Pasažieru vilciens, в том числе и в мобильном приложении, сообщает компания в Twitter. Вечером торговля билетами Pasažieru vilciens в интернете была возобновлена, проинформировали на предприятии.

Как сообщалось, в среду после обеда **приложение e-bileti** в торговле онлайн-билетов Pasažieru vilciens на сайте и в приложении.

Сайт Pasažieru vilciens подвергается DDoS атаке - кибератаке, связанной с отказом доступа, объяснила представительница предприятия Сигита Занедра агентству LETA.

Атака началась 1 июня в 11:00 и с того момента число запросов стало увеличиваться волнообразно. **Атака продолжается до сих пор, и мешает на работу сайта компании.**

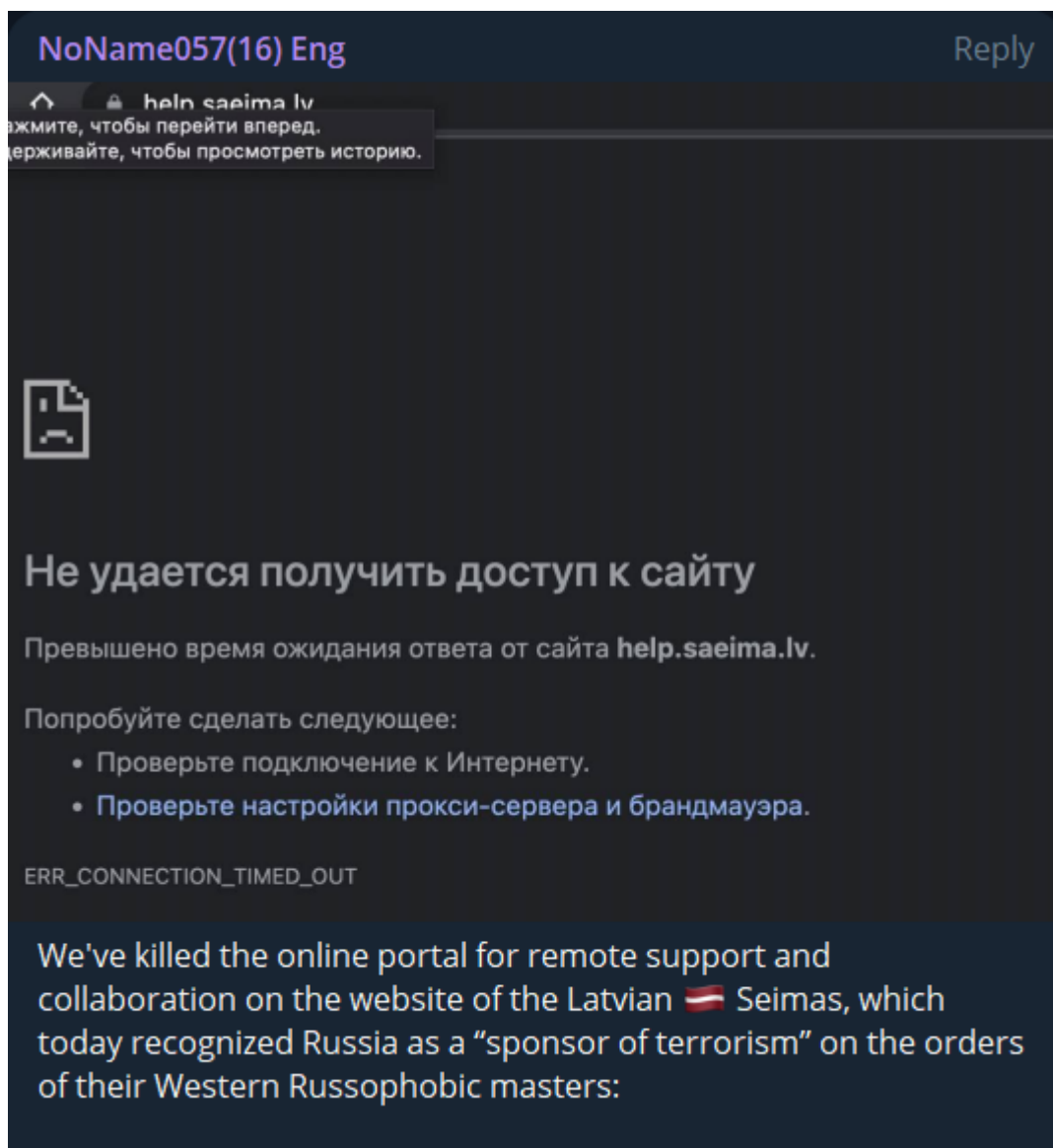


«Ой, а кто это сделал?» 😊

Вчера мы вывели из строя латвийский сайт Pasažieru vilciens («Пассажирский поезд»). Это единственная пассажирская железнодорожная компания в Латвии.

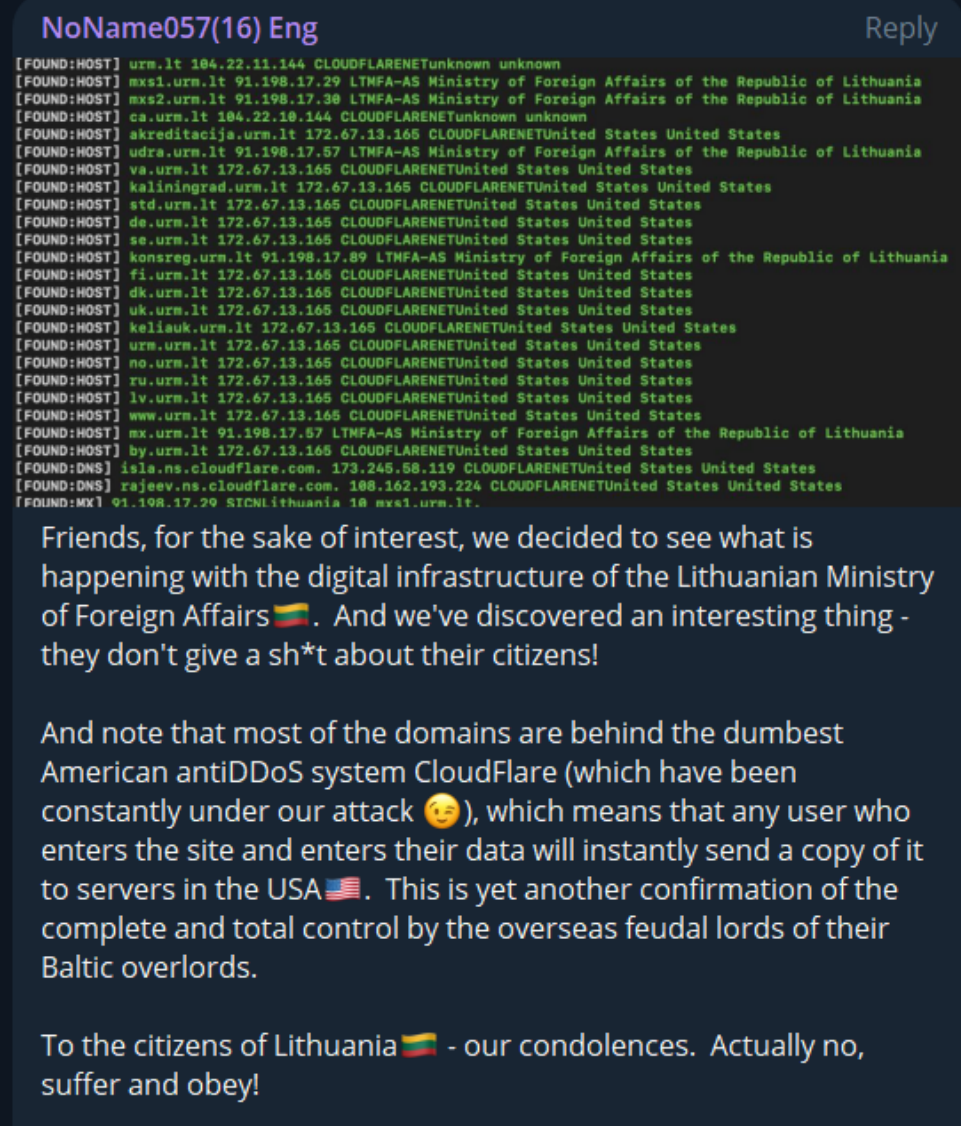
On June 2, 2022, the Latvian website Passazieru villciens (passenger train) was taken down. Due to a DDoS attack by the NoName057(16) team, online ticket sales were not possible for a long time.

Latvian Seimas Attack:



"We killed the online portal for remote support and cooperation on the website of the Latvian 🇱🇻 Seimas, which recognizes Russia as a "sponsor of terrorism", " they explained their actions in a statement. They carried out successive attacks on the same day.

Lithuanian Ministry of Foreign Affairs Attack;



NoName057(16) Eng Reply

```
[FOUND:HOST] urm.lt 104.22.11.144 CLOUDFLARENETunknown unknown
[FOUND:HOST] mxs1.urm.lt 91.198.17.29 LTMFA-AS Ministry of Foreign Affairs of the Republic of Lithuania
[FOUND:HOST] mxs2.urm.lt 91.198.17.30 LTMFA-AS Ministry of Foreign Affairs of the Republic of Lithuania
[FOUND:HOST] ca.urm.lt 104.22.10.144 CLOUDFLARENETunknown unknown
[FOUND:HOST] akreditacija.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] udra.urm.lt 91.198.17.57 LTMFA-AS Ministry of Foreign Affairs of the Republic of Lithuania
[FOUND:HOST] va.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] kaliningrad.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] std.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] de.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] se.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] konsreg.urm.lt 91.198.17.89 LTMFA-AS Ministry of Foreign Affairs of the Republic of Lithuania
[FOUND:HOST] fi.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] dk.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] uk.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] keli auk.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] urm.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] no.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] ru.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] lv.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] www.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:HOST] mx.urm.lt 91.198.17.57 LTMFA-AS Ministry of Foreign Affairs of the Republic of Lithuania
[FOUND:HOST] by.urm.lt 172.67.13.165 CLOUDFLARENETUnited States United States
[FOUND:DNS] isla.ns.cloudflare.com. 173.245.58.119 CLOUDFLARENETUnited States United States
[FOUND:DNS] rajsev.ns.cloudflare.com. 108.162.193.224 CLOUDFLARENETUnited States United States
[FOUND:MX] 91.198.17.29 STONLithuania 10 mxs1.urm.lt.
```

Friends, for the sake of interest, we decided to see what is happening with the digital infrastructure of the Lithuanian Ministry of Foreign Affairs 🇱🇹. And we've discovered an interesting thing - they don't give a sh*t about their citizens!

And note that most of the domains are behind the dumbest American antiDDoS system CloudFlare (which have been constantly under our attack 😏), which means that any user who enters the site and enters their data will instantly send a copy of it to servers in the USA 🇺🇸. This is yet another confirmation of the complete and total control by the overseas feudal lords of their Baltic overlords.

To the citizens of Lithuania 🇱🇹 - our condolences. Actually no, suffer and obey!

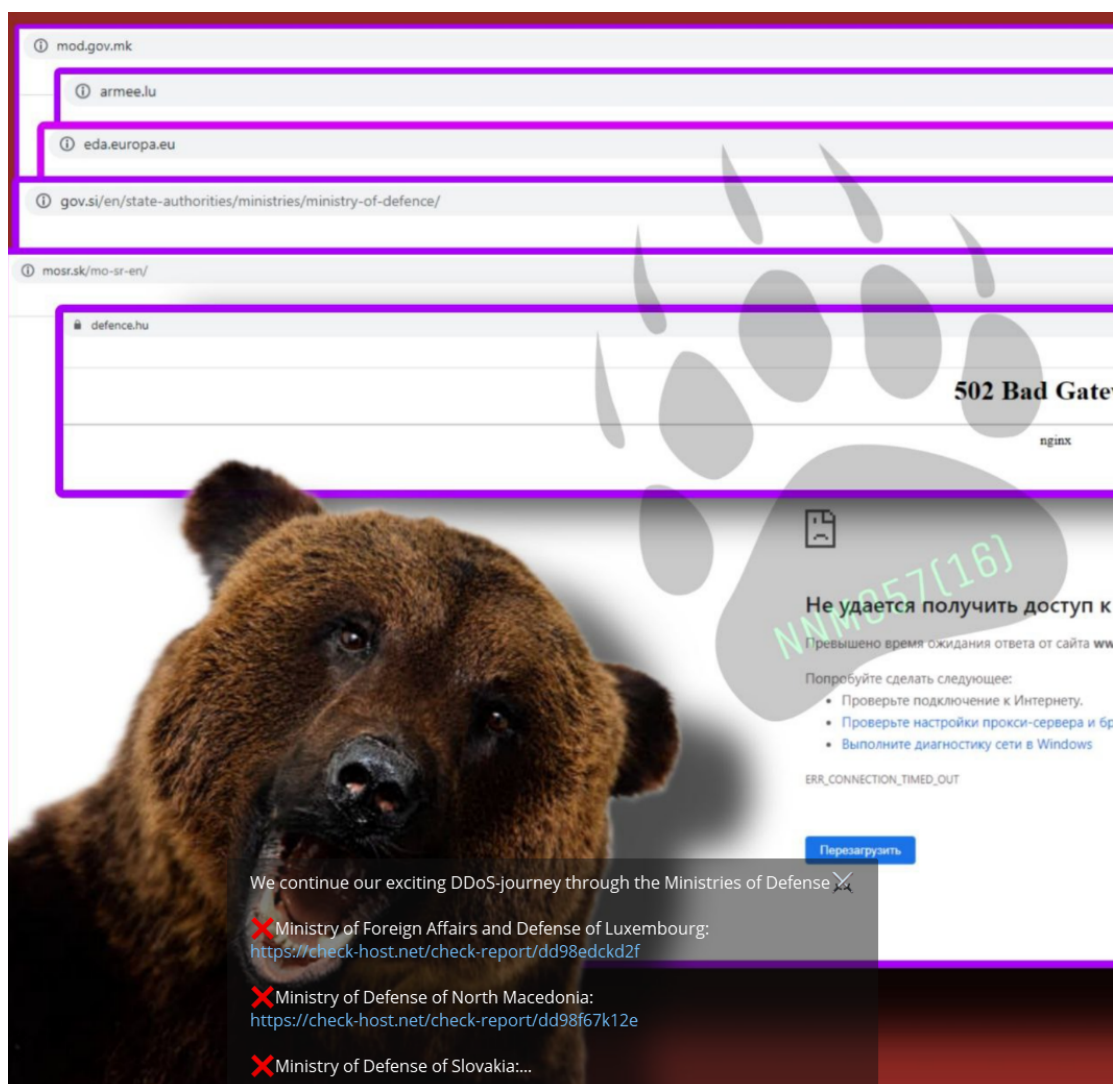
To attract attention, they attacked the digital infrastructure of the Lithuanian Ministry of Foreign Affairs, mocking their systems after the attack.

Poland Attack:



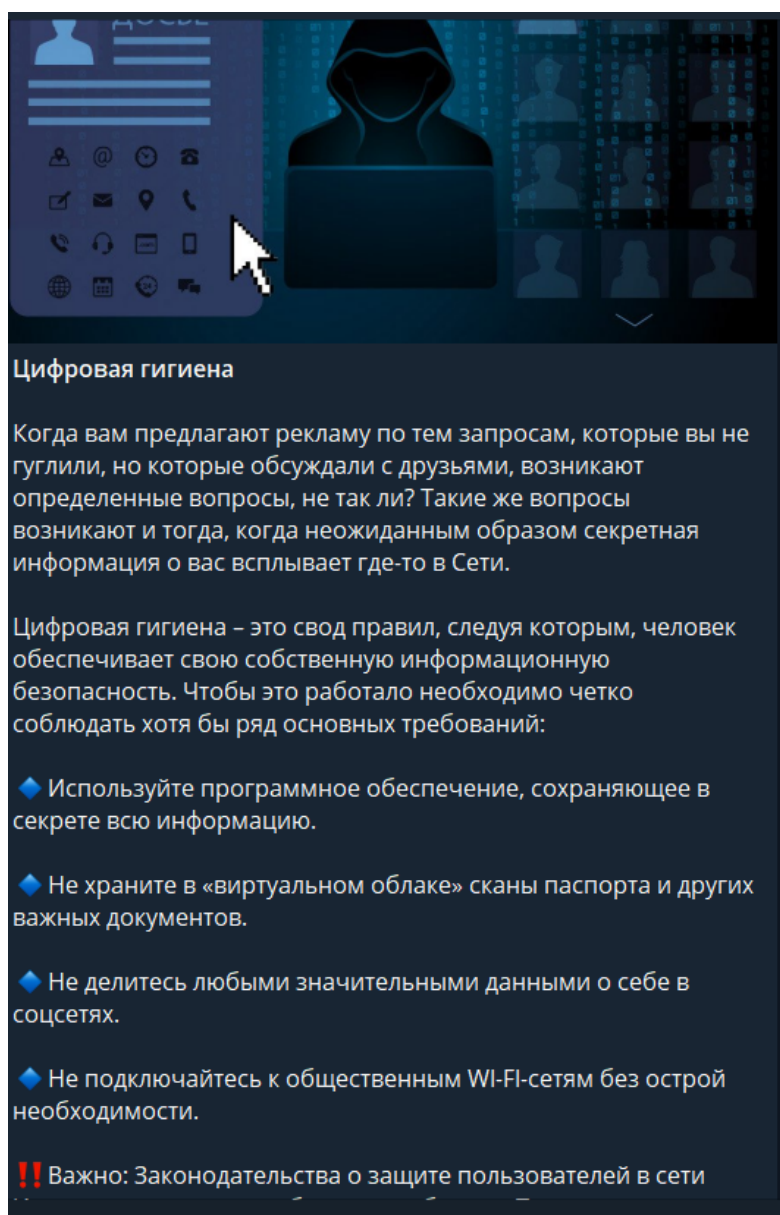
Another sector they target is law. In places where they claim there is no law, they have found the solution in DDOS attacks on websites. They reported that Poland's main courts will attack 16 websites.

Europe Attack:



They excitedly continued their DDoS attacks. They targeted Ministry websites. The attacked websites included Luxembourg, North Macedonia, Slovakia, Slovenia, Hungary and Europe.

Noname057(16)'s Announcement:



They also provide the people who follow them with information on how to ensure digital security. They also announce important developments related to Russia and new services in IT systems.

DDoSia Project:

NoName057(16)



1 000 000 ₺
для активных
участников проекта
DDOSIA PROJECT

Друзья, 9 лет назад – 18 марта 2014 года, Крым вернулся в родную гавань 🇷🇺

Для нас это великий день ❤️ Поэтому, мы решили увеличить фонд вознаграждений для участников нашего проекта DDoSia Project до 1 миллиона рублей! 🙌

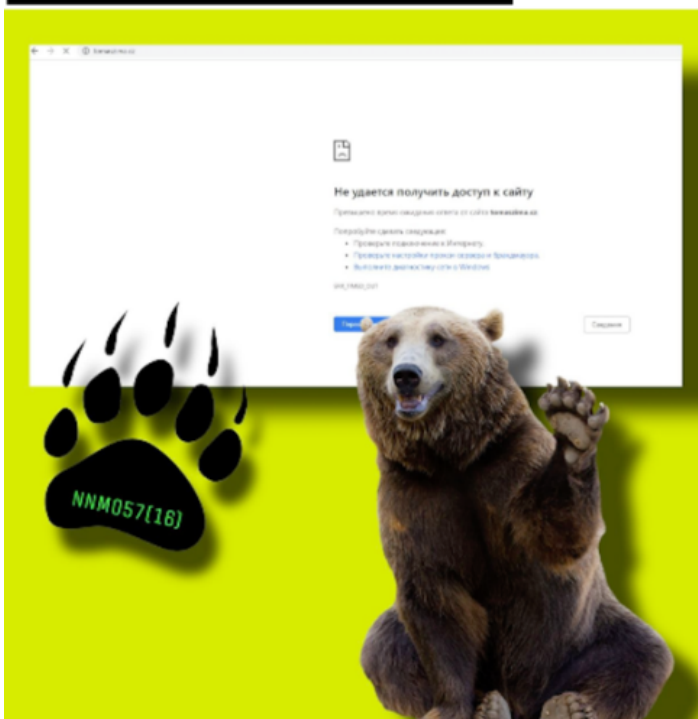
Напомним, что с переходом на новую финансовую модель, все наши активные кибербойцы теперь получают ежедневные вознаграждения.

Вступайте в наш проект по ссылке:
<https://t.me/+fiTz615tQ6BhZWFi>

Да прибудет с нами сила! 🙌 Слава России! 🇷🇺

They announced that they have increased the reward fund for participants in the DDoSia Project to 1 million rubles. They say that they are offering daily rewards to all active cyber warriors, in line with their goal to increase the number of volunteers.

Czech Republic Attack:



We just found out that 4,000 Ukrainian soldiers will soon be trained at the Libava military training ground in the Czech Republic. At the same time, at the end of 2022, the first group of ukrowarriors has already completed this process. It is clear that the Russian authorities strongly condemn such practices on the territory of the European Union. In addition, presidential elections will soon be held in the Czech Republic and we decided to "participate" in them 😏

🔥 Today we crashed the website of one of the candidates - Tomas Zima:

✖ [Redacted]

👉 Subscribe to [Redacted]

🐻 Join our [Redacted]

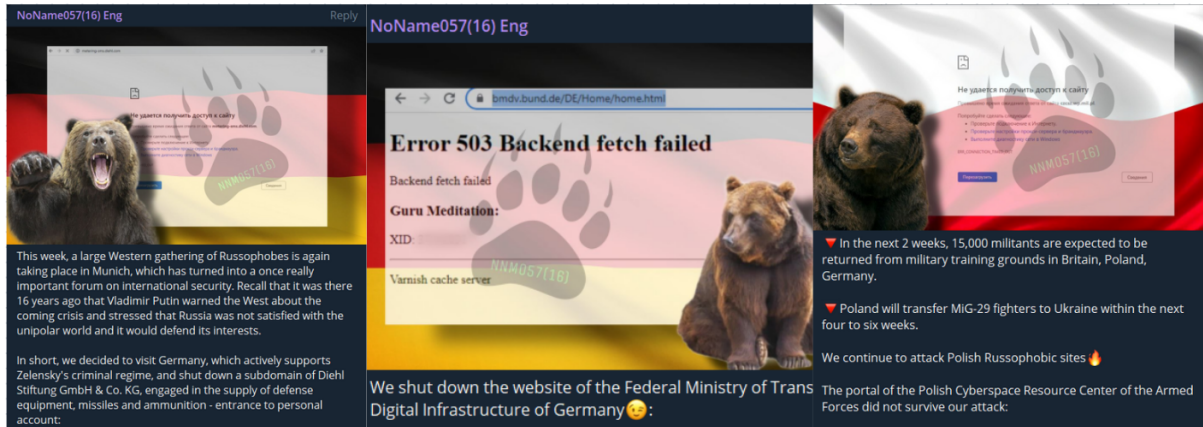
⚠ Subscribe to [Redacted]

🇷🇺 Victory will be ours!

The group targeted the presidential election of the Czech republic held in January 2023. They attacked the websites of presidential candidates. They carried out these attacks using Telegram channels, a distributed denial-of-service (DDoS) payment program managed by volunteers, a multi-OS-supported toolkit, and GitHub.

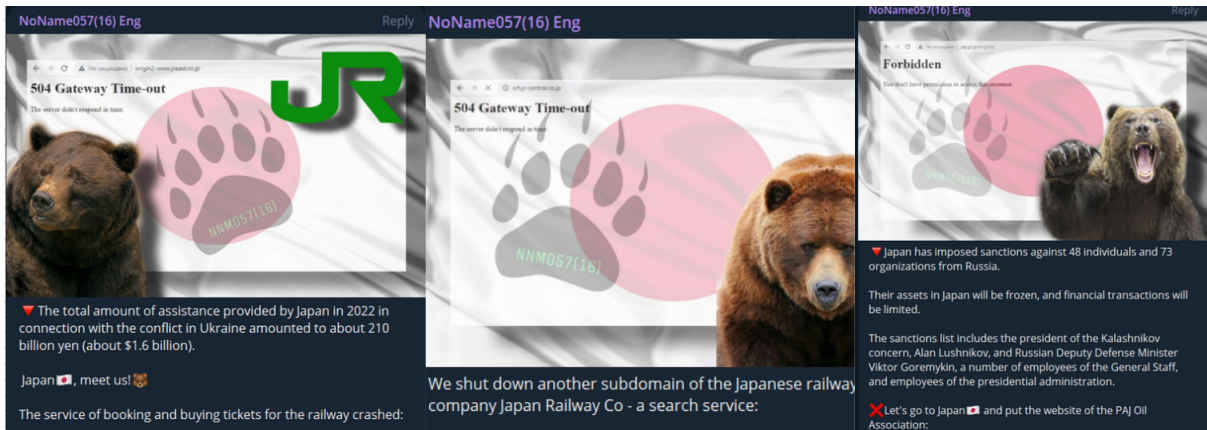
Noname057(16)'s Country Based Announcements:

Germany:



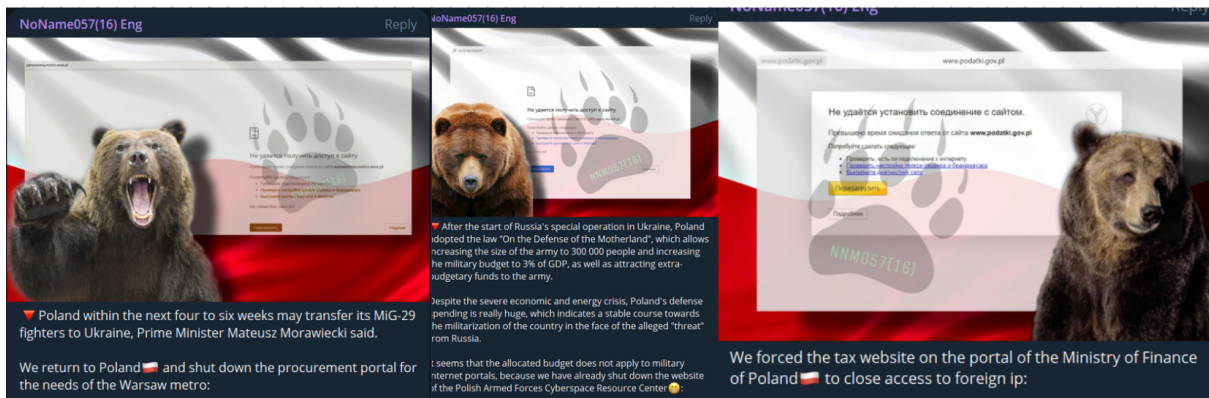
The group's recent announcements about Germany.

Japan:



The group's recent announcements about Japan.

Poland:



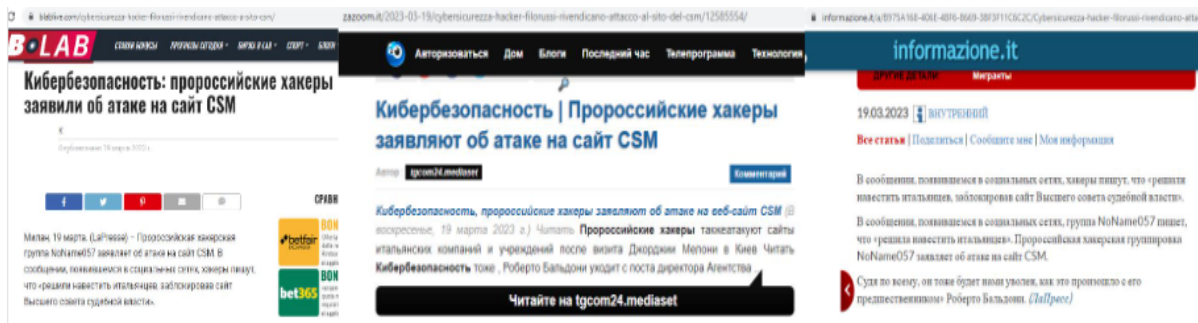
The group also carried out DDOS attacks against Poland's internet infrastructure at different times. They targeted the Polish government after the Sejm of the Republic of Poland officially recognized Russia as a terror sponsor state in mid-December 2022.

Denmark:

The group targeted Danish financial institutions in January 2023 because of Denmark's support for Ukraine. Ministry of Finance, Danske Bank, Danmarks Nationalbank.

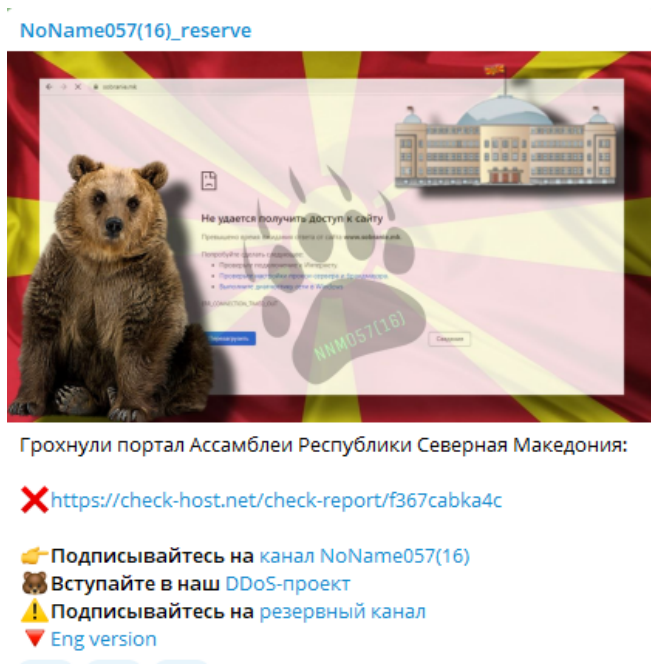
Ukraine:

The group, which learned that the Ukrainian army was training at a base near Rome, specialized in SAMP-T anti-aircraft missile systems, which France supplied to Kiev, carried out numerous cyber attacks on Italy on March 20, 2023.



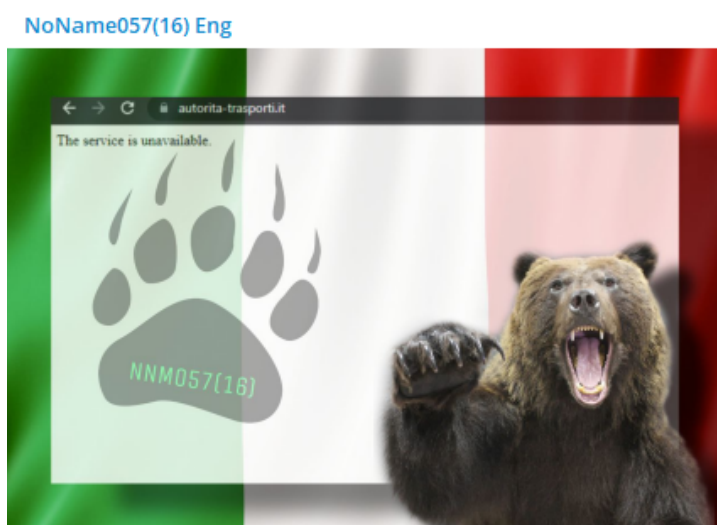
Macedonia:

It was closed due to the DDOS attack on the Parliament of the Republic of North Macedonia at 12:51:50 on March 21, 2023.



Italy:

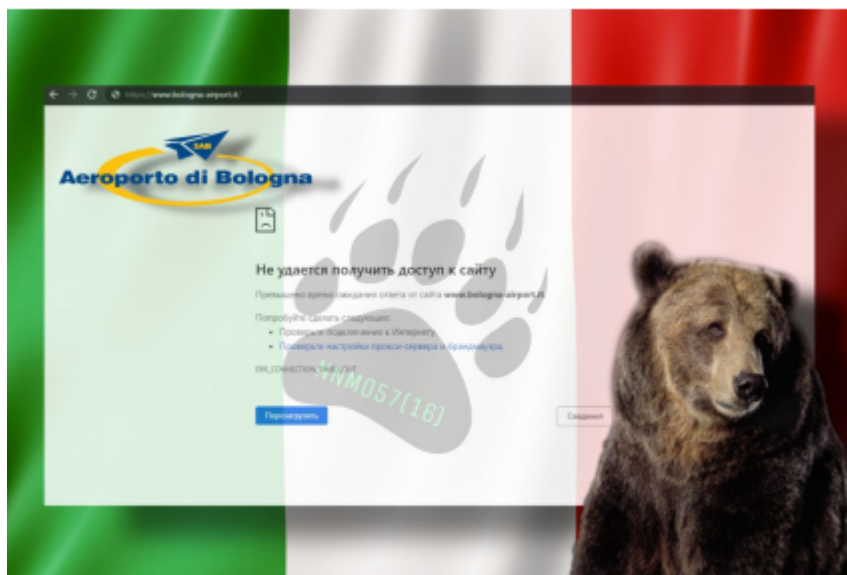
NoName057, on March 22, 2023 It was rendered inaccessible as a result of a DDOS attack on the Italian Transport Regulatory Authority.



In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

22 March 2023 Bologna airport was rendered unusable for a certain period of time as a result of DDoS attacks.

NoName057(16) Eng



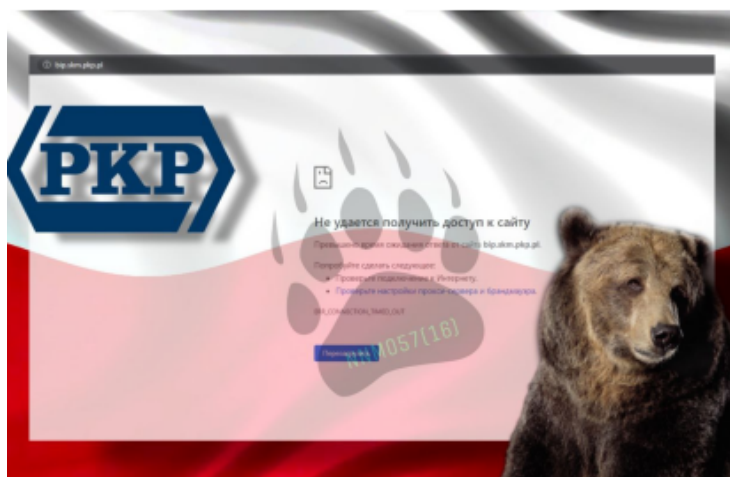
Non-flying weather today for the Bologna airport website:

✗ <https://check-host.net/check-report/f3a3493kc54>

Poland:

On March 23, 2023, the websites of the Polish High-Speed Railways became unavailable due to DDoS attacks.

NoName057(16)_reserve



Отправили DDoS-ракеты на информационный портал сайта городской скоростной железной дороги Польши, теперь ресурс доступен только по польским ир:

✗ <https://check-host.net/check-report/f3fb4d2kc4f>

Italy:

NoNameRus057(16) aimed to cause serious damage by attacking Italy's internet infrastructure because of its support for Ukrainian neo-Nazis.

Name057 снова наносит удар: ерская атака на сайт институционного суда

Что произошло, в частности, с железнодорожной инфраструктурой и аэропортом Болоньи

Кибератака на Конституционный суд. NoName057: «Давайте продолжим наше итальянское путешествие»

The **second day** we are destroying the Internet infrastructure of Italy 🇮🇹 for the fact that its Russophobic authorities **support** Ukrainian neo-Nazis 🇺🇦

Media and social media **users** write about our cyber attacks. Only the prosecutor of Rome, who is supposed to conduct an **investigation** against us, is silent, the director of the Italian National Cybersecurity Agency **Frattasi**, for whose activities are allocated **huge money**. The Italian authorities are also silent.

Japan:

March 23, 2023 Japan became the new target of NoName057(16) after the Japanese Prime Minister visited Kiev. An attack on the reservation and ticket purchasing service for the railway company East Japan Railway Co. crashes the system.

NoName057(16) Reply

▼ **Власти Японии** приняли решение выделить Украине \$470 млн в формате безвозмездной помощи на энергетику и другие нужды, еще \$30 млн — на нелетальное снаряжение, - сообщил премьер-министр Японии Фумио Кисида по итогам визита в Киев.

Отправляемся в трип по Японии 🇯🇵

Грохнули сервис бронирования и покупки билетов на железную дорогу компании East Japan Railway Co:

✖ <https://check-host.net/check-report/f3fe29c811>

Noname057(16)'s Attack TTPs

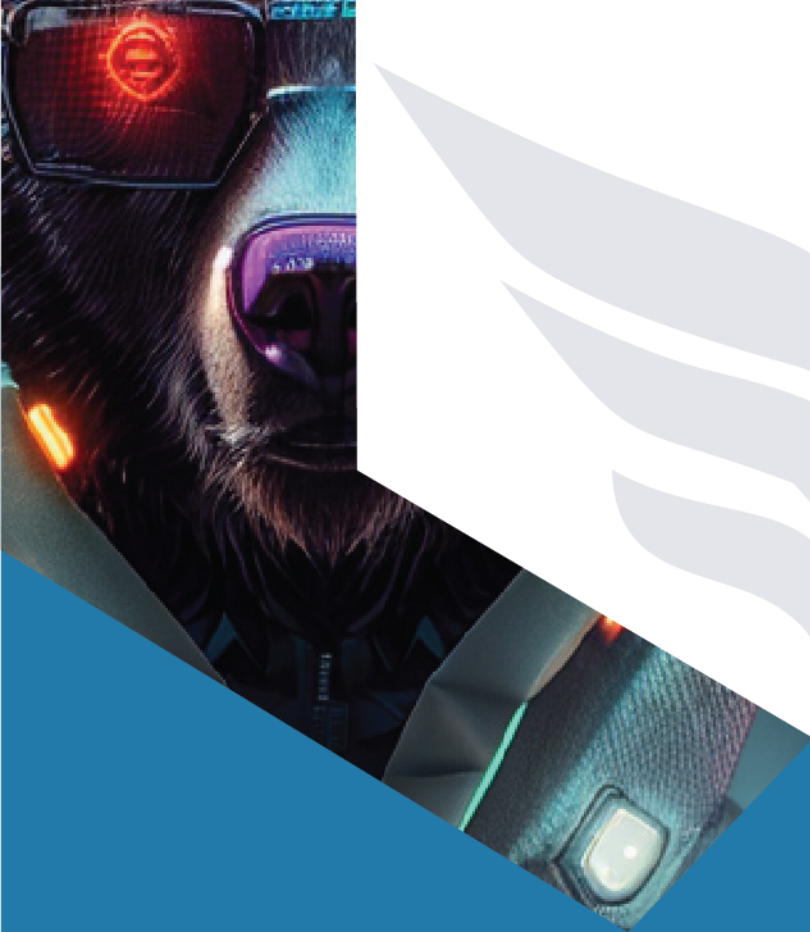
Tactics	Technique	Technique ID
Discovery	System Network Connections Discovery	T1049
Command and Control	Application Layer Protocol	T1071
Impact	Network Denial of Service	T1498
Impact	Endpoint Denial of Service	T1499
Persistence	Boot or Logon Autostart Execution	T1547
Discovery	System Network Connections Discovery	T1049
Command and Control	Application Layer Protocol	T1071

Noname057(16)'s Attack IOCs

Indicator	Description
94d7653ff2f4348ff38ff80098682242ece6c407	DDosia.py encoded installer
e786c3a60e591dec8f4c15571dbb536a44f861c5	DDosia.py encoded installer
c86ae9efcd838d7e0e6d5845908f7d09aa2c09f5	December 2022 DDosia PyInstaller
e78ac830ddc7105290af4c1610482a41771d753f	December 2022 DDosia PyInstaller
09a3b689a5077bd89331acd157ebe621c8714a89	July 2022 DDosia PyInstaller
8f0b4a8c8829a9a944b8417e1609812b2a0ebbbd	dosia_v2_macOSx64 – May 2022
717a034becc125e88dbc85de13e8d650bee907ea	dosia_v2_macOSarm64 – May 2022
ef7b0c626f55e0b13fb1dcf8f6601068b75dc205	dosia_v2_linux_x64 – May 2022
b63ce73842e7662f3d48c5b6f60a47e7e2437a11	dosia_v2.0.1.exe – May 2022
5880d25a8fbe14fe7e20d2751c2b963c85c7d8aa	dosia_v2.0.1 – May 2022
78248539792bfad732c57c4eec814531642e72a0	dosia_v2.exe – May 2022
1dfc6f6c35e76239a35bfaf0b5a9ec65f8f50522	dosia_win_x64.exe – January 2023
2[.]57[.]122[.]82	C2 Server – Overlaps with Avasts Bobik findings
2[.]57[.]122[.]243	C2 Server – Overlaps with Avasts Bobik findings
109[.]107[.]181[.]130	C2 Server – October 2022 and earlier. Overlaps with Avasts Bobik findings
77[.]91[.]122[.]69	C2 Server – December 2022
31[.]13[.]195[.]87	C2 Server – Mid December to Present Day
tom56gaz6poh13f28[.]myftp.org	C2 Domain
zig35m48zur14nel40[.]myftp.org	C2 Domain
05716nnm@proton[.]me	NoName057(16) Email Address

In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

hxxps://t[.]me/noname05716	NoName057(16) Primary Telegram Channel (open group)
hxxps://t[.]me/nn05716chat	NoName057(16) Secondary Telegram Channel (closed group)
hxxps://github[.]com/dddosia	Account hosting DDOSIA downloading GitHub Pages site.
dddosia[.]github.io	Official DDOSIA download site linked to on actors telegram page.
hxxps://github[.]com/kintechi341	Contributor to the DDOSIA toolkit



ThreatMon



45305 Catalina cs St 150, Sterling VA 20166