



ThreatMon



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

Anonymous Russia



@threatmon



@MonThreat

Summary	3
Cyber Wars in The Ukraine-Russia War	3
Threat Actor Review: Anonymous Russia	4
Who is Anonymous Russia?	4
What are the Activities of Anonymous Russia?	5
Which Side They Supports?	5
What Types of Attacks Does Anonymous Russia Execute?	5
Which Industries Is Anonymous Russia Targeting?	5
Anonymous Russia's Attacks	6
10 July 2022	6
10 July 2022	7
20 July 2022	8
22 July 2022	9
24 July 2022	10
25 July 2022	11
7 August 2022	12
14 August 2022	13
15 August 2022	14
16 September 2022	14
18 November 2022	15
12 February 2023	15
20 February 2023	16
22 March 2023	17
22 March 2023	18
28 March 2023	19
28 March 2023	20
Technical-Tactical-Procedures(TTP)	22
Anonymous Russia's Attack TTPs	23
Anonymous Russia's Attack IOCs	24

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 3rd Report in a series of investigations on threat actors playing an active role in the Ukraine-Russia war, based on the Anonymous Russia 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: Anonymous Russia

Who is Anonymous Russia?

The Russian-based members of the group called Anonymous, which made its name known before the war, started to operate as Anonymous Russia, as if to reveal their identities with this crisis between Russia and Ukraine. The opening of the current Telegram group is based on July 10, 2022. With the appearance of Anonymous on the side of Ukraine during the war, these two became two separate groups carrying out their own activities. However, in line with the evidence obtained, Anonymous Russia reveals that although it continues its activities on the side of and in favor of Russia, it still carries the Anonymous mask that is the basis of some of its posts.

Anonymous Russia is known to collaborate with many pro-Russian threat actor groups such as KillNet, DeaDNET, Legion, XakNet, Beregini, CyberArmy, RaHDit, DPR Joker, NoName057 and Zsecnet.



What are the Activities of Anonymous Russia?

Anonymous Russia is known for keeping close to the Russian state. Almost all of its attacks consist of DDoS attacks. These attacks use a dashboard they call STRESSID.CLUB. Therefore, it stands out that there is a certain strategy that is well-established. Even if the technical details are added and changed depending on the return of the situation, the general approach in the attack continues with the same strategies. In any situation that may conflict with the interests of the Russian state, they take action by damaging the assets of the other side of the war.

Which Side They Supports?

When we look at the posts in the Telegram group of Anonymous Russia, the comments made and most importantly, the target of the aggressive behavior it exhibits, it is clearly seen that it is on the side of the Russian State. Although it has carried out cyber attacks on many places within the borders of Russia, it is seen that they have never left the Russian State alone, which is faced with different parties.

What Types of Attacks Does Anonymous Russia Execute?

Except in cases where they do not attack by joining forces, Anonymous Russia often carries out its activities with a single method. This consists of denial-of-service attacks, that is, DDoS attacks. These aggressive activities are mostly carried out on a platform called "STRESSID.CLUB". Apart from this situation, it also exchanges information and data with other threat actor groups with which it operates.

Which Industries Is Anonymous Russia Targeting?

The sectors that Anonymous Russia targets are shaped by topics such as security, health, transportation and communication, which are of critical importance in case of war.

Anonymous Russia's Attacks

Here are some examples of cyber attacks involving Anonymous Russia directly or indirectly:

10 July 2022

Chocolate brand Roshen became the group's first target soon after Anonymous Russia launched its own Telegram group.

ANONYMOUS | RUSSIA
10,571 subscribers

Pinned message #1
Привет, мир. Мы Анонимус . Мы хакеры, взломщики, агенты, шпион

ANONYMOUS | RUSSIA July 10, 2022

Проверка веб-сайта <https://www.roshen.com/ua/ru/>

Постоянная ссылка на этот отчет | Поделиться отчетом в Твиттере

Местонахождение	Результат	Время	Код	IP адрес
Austria, Salzburg	Connection timed out			185.65.244.138
Czechia, C. Budejovice	Connection timed out			185.65.244.138
Finland, Helsinki	Connection timed out			185.65.244.138
Germany, Frankfurt	Connection timed out			185.65.244.138
Iran, Tehran	Connection reset by peer			185.65.244.138
Italy, Milan	Broken pipe			185.65.244.138
Kazakhstan, Karaganda	Connection reset by peer			185.65.244.138
Lithuania, Vilnius	Connection timed out			185.65.244.138
Moldova, Chisinau	Connection timed out			185.65.244.138
Netherlands, Amsterdam	Broken pipe			185.65.244.138
Poland, Olsztyn	Connection timed out			185.65.244.138
Portugal, Viana	Connection timed out			185.65.244.138
Russia, Moscow	Connection timed out			185.65.244.138
Russia, Moscow	Connection reset by peer			185.65.244.138
Serbia, Belgrade	Connection timed out			185.65.244.138
Switzerland, Zurich	Connection timed out			185.65.244.138
Turkey, Istanbul	Connection reset by peer			185.65.244.138
Ukraine, Khmelnytskyi	Connection timed out			185.65.244.138
Ukraine, Kyiv	Connection timed out			185.65.244.138
USA, Atlanta	Connection timed out			185.65.244.138
USA, Los Angeles	Connection reset by peer			185.65.244.138

▼ **Официальный Рошен**
<https://www.roshen.com/ua/>
<https://check-host.net/check-report/ac1a2cck312>

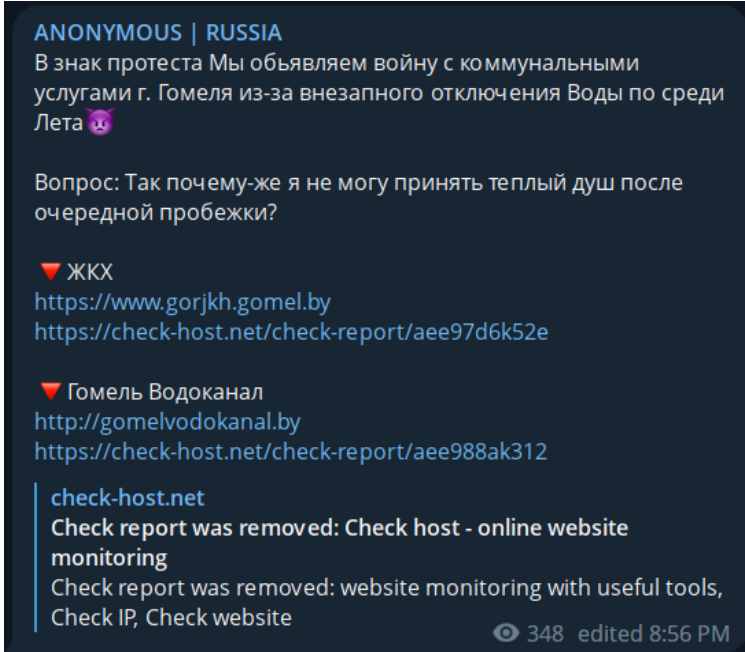
▼ **Официальный Рошен Стор**
<https://roshenstores.com/>
<https://check-host.net/check-report/ac29e08k80b>

367 7:49 PM

10 July 2022

They declared that they were waging a cyber war on the public services of the city of Gomel, citing a water shortage.

“As a sign of protest, we declare war on the public services of the city of Gomel due to the sudden cutoff of water in midsummer.”



ANONYMOUS | RUSSIA
В знак протеста Мы объявляем войну с коммунальными услугами г. Гомеля из-за внезапного отключения Воды по среди Лета 🇷🇺

Вопрос: Так почему-же я не могу принять теплый душ после очередной пробежки?

▼ ЖКХ
<https://www.gorjkh.gomel.by>
<https://check-host.net/check-report/aee97d6k52e>

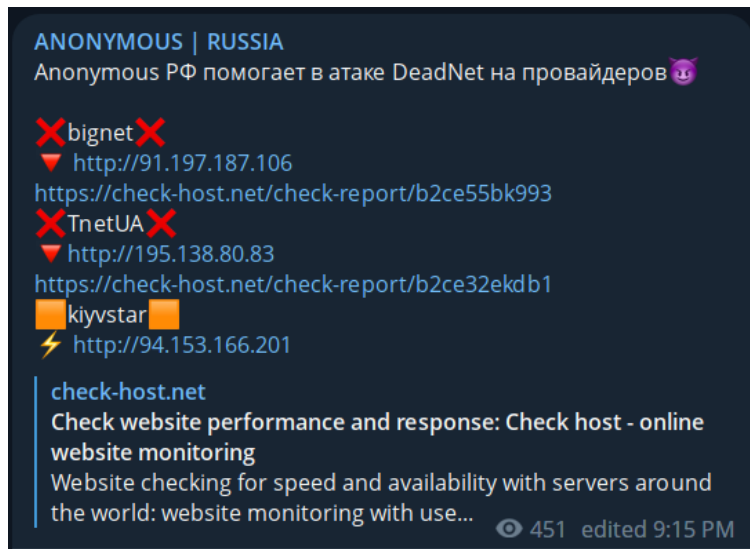
▼ Гомель Водоканал
<http://gomelvodokanal.by>
<https://check-host.net/check-report/aee988ak312>

check-host.net
Check report was removed: Check host - online website monitoring
Check report was removed: website monitoring with useful tools, Check IP, Check website

👁 348 edited 8:56 PM

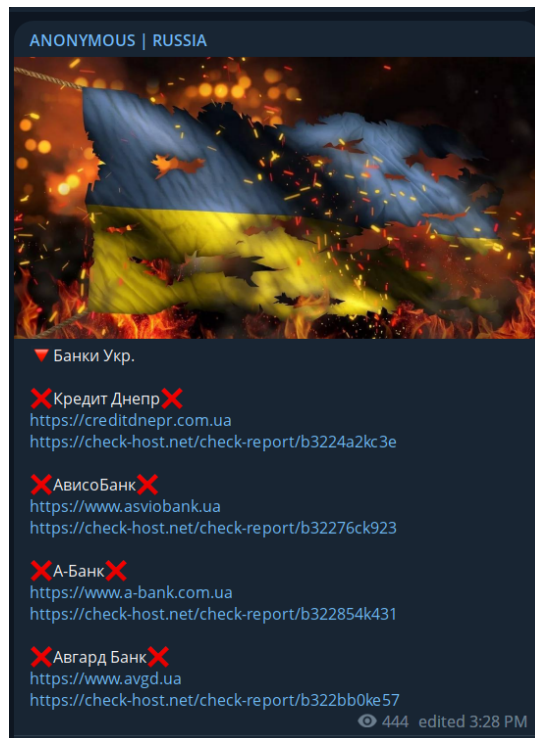
22 July 2022

In his Telegram post, which he interpreted as “Anonymous RF helps ISPs attack DeadNet 🤩”, there are 3 different IP addresses that he attacked.



24 July 2022

Ukrainian banks were attacked by Anonymous Russia. Banks affected by these attacks: Credit Dnipro, AvisoBank, A-Bank, Avgard Bank.



ANONYMOUS | RUSSIA

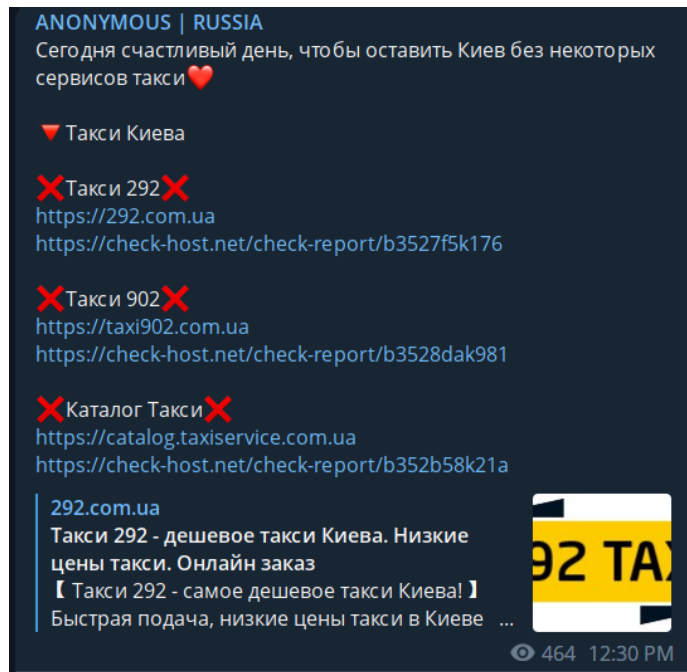
▼ Банки Укр.

- ✘ Кредит Днепр ✘
<https://creditdnpr.com.ua>
<https://check-host.net/check-report/b3224a2kc3e>
- ✘ АвісоБанк ✘
<https://www.asviobank.ua>
<https://check-host.net/check-report/b32276ck923>
- ✘ А-Банк ✘
<https://www.a-bank.com.ua>
<https://check-host.net/check-report/b322854k431>
- ✘ Авігарт Банк ✘
<https://www.avgd.ua>
<https://check-host.net/check-report/b322bb0ke57>

444 edited 3:28 PM

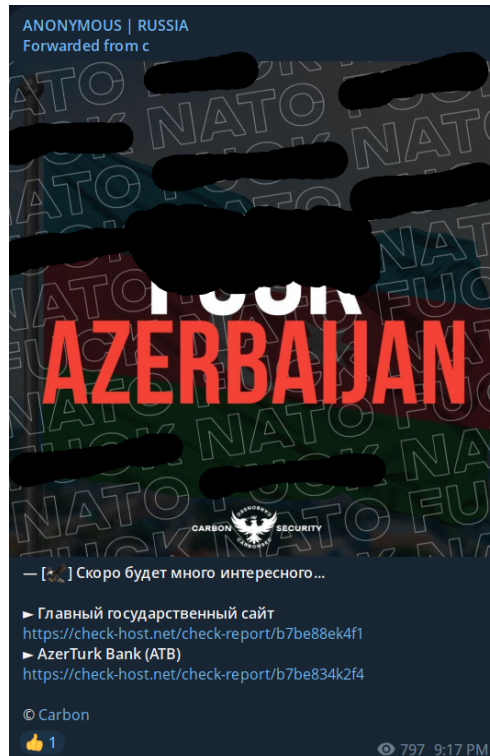
25 July 2022

Anonymous Russia has blocked the services of the online taxi calling service operating in Ukraine.



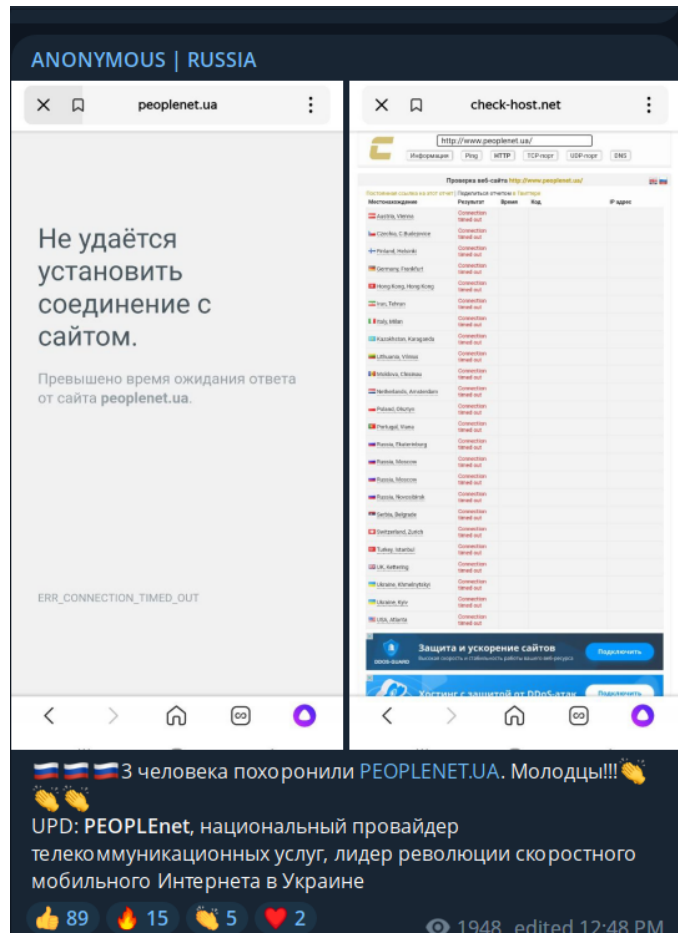
7 August 2022

Anonymous Russia attacked a bank named Azerturk Bank, based in Azerbaijan.



14 August 2022

An internet service provider was attacked in Ukraine.



18 November 2022

The Russian hacktivist group Killnet claimed responsibility for the DDOS attack against satellite service provider Starlink as it supported Ukraine following the Russian invasion. Anonymous Russia is among the collaborating groups mentioned in this attack.

12 February 2023

AnonymousRussia, Killnet, Killmilk and other Russian Hacking and HackTivist Groups have carried out DDOS attacks against NATO's Special Operations Headquarters (NSHQ) website.

ANONYMOUS | RUSSIA

ANONYMOUS | RUSSIA
★ Всеми коллективу KILLNET - объявляю START Атак...

▼ Штаб специальных операций НАТО
<https://www.nshq.nato.int/>
<https://check-host.net/check-report/ea0d98akf51>

▼ Военное командование НАТО
<https://www.act.nato.int/>
<https://check-host.net/check-report/ea0da4ek347>

▼ Объединенный военный центр НАТО
<https://www.jwc.nato.int/>
<https://check-host.net/check-report/ea0de72kcd4>

▼ Ведущий агент НАТО по обобщению извлеченных уроков
<https://www.jallc.nato.int/>
<https://check-host.net/check-report/ea0e011kd89>

www.nshq.nato.int
NATO Special Operations Headquarters (NSHQ) - NSHQ Portal


🔥 62 👍 10 ❤️ 5 🔔 2 🔥 1 👁 30.9K edited 6:49 PM

20 February 2023

Anonymous Russia, targeted Polish airports.

Due to DDOS attacks on many international airports in Poland, flights were canceled for a certain period of time.

ANONYMOUS | RUSSIA



Понедельник Польши начался с нелётной погоды - все рейсы отменены 🐱🔥

- ▼ Международный аэропорт им. Игнация Яна Падеревского Быдгощ-Шведерово
<https://plb.pl/en/>
<https://check-host.net/check-report/eb9c521kb7c>
- ▼ Международный аэропорт Варшава-Модлин
<https://modlinaairport.pl/>
<https://check-host.net/check-report/eb9c586kb71>

Check website <https://plb.pl/en/>

Permanent link to this check report | Share report on Twitter

Checked on **Mon Feb 20 08:35:34 UTC 2023** | Check again

Location	Result	Time	Code	IP address
Austria, Vienna	Server error	0.135 s	503 (Service Unavailable)	193.10.252.101
Brazil, Sao Paulo	Connection timed out			177.71.222.101
Bulgaria, Sofia	Server error	0.347 s	503 (Service Unavailable)	193.10.252.101
Czechia, C. Budejovice	Server error	0.188 s	503 (Service Unavailable)	193.10.252.101
Finland, Helsinki	Server error	0.096 s	503 (Service Unavailable)	193.10.252.101
France, Paris	Server error	0.158 s	503 (Service Unavailable)	193.10.252.101
France, Roubaix	Connection timed out			193.10.252.101
Germany, Frankfurt	Connection timed out			193.10.252.101
Germany, Nuremberg	Server error	0.150 s	503 (Service Unavailable)	193.10.252.101
India, New Delhi	Server error	0.588 s	503 (Service Unavailable)	193.10.252.101

22 March 2023

AnonymousRussia and UserSec supported each other and organized a massive DDoS attack against UK structures.



Checked on **Wed Mar 22 06:50:40 UTC 2023** | [Check again](#)

Location ▾	Result	Time	Code	IP address
Austria, Vienna	Server error	12.856 s	503 (Service Unavailable)	193.50.135.135
Brazil, Sao Paulo	Server error	11.121 s	503 (Service Unavailable)	193.50.135.135
Bulgaria, Sofia	Server error	9.259 s	503 (Service Unavailable)	193.50.135.135
Czechia, C.Budejovice	Server error	5.713 s	503 (Service Unavailable)	193.50.135.135
Finland, Helsinki	Server error	18.642 s	503 (Service Unavailable)	193.50.135.135
France, Paris	Server error	5.544 s	503 (Service Unavailable)	193.50.135.135
France, Roubaix	Server error	18.136 s	503 (Service Unavailable)	193.50.135.135
Germany, Frankfurt	Server error	11.599 s	503 (Service Unavailable)	193.50.135.135
Germany, Nuremberg	Server error	11.682 s	503 (Service Unavailable)	193.50.135.135

22 March 2023

After the AnonymousRussia and AnonymousSudan team announced "We will attack in 15 minutes" on 22 March 2023 at 11:46, many airports and hospitals in France were targeted.

ANONYMOUS | RUSSIA
Forwarded from Anonymous Sudan



! Мы все будем атаковать через 15 минут | We'll all attack After
15 Min from now

Airports:

<https://www.parisaeroport.fr/>
<https://www.annecy-airport.com/>
<https://www.parisvatry.com/>
<https://www.euroairport.com/>
<https://www.pau.aeroport.fr/>
<http://www.brest.aeroport.bzh/>

Hospitals:

<https://www.american-hospital.org/>
<https://www.aphp.fr/>
<https://pitiealpetriere.aphp.fr/>
<https://hopital-necker.aphp.fr/>
<https://hopital-georgespompidou.aphp.fr/>
<https://hopital-bichat.aphp.fr/>

28 March 2023

March 28, 2023 The Slovak Republic was targeted by AnonymousRussia for supporting the Banderite government in Ukraine and delivering the MIG-29. It made its servers inaccessible with DDoS attacks.

Victims:

National Bank of Slovakia
People's Parliament
Slovak Ministry of Justice
EximBanka
JtBanka

ANONYMOUS | RUSSIA
За поддержку бандеровской власти на Украине и передачу МИГ - 29 выносим предупреждение Словацкой Республике!

▼ Национальный банк Словакии
<https://nbs.sk/en/>
<https://check-host.net/check-report/f5756e0k224>


▼ Народный Парламент
<https://www.nrsr.sk/web/>
<https://check-host.net/check-report/f5755cak1b3>

▼ Министерство юстиции Словакии
<https://www.justice.gov.sk>
<https://check-host.net/check-report/f575a15k9e0>

▼ EximBanka
Лучший Словацкий Банк
(1-ое Место)
<https://www.eximbanka.sk/>
<https://check-host.net/check-report/f57684dka85>

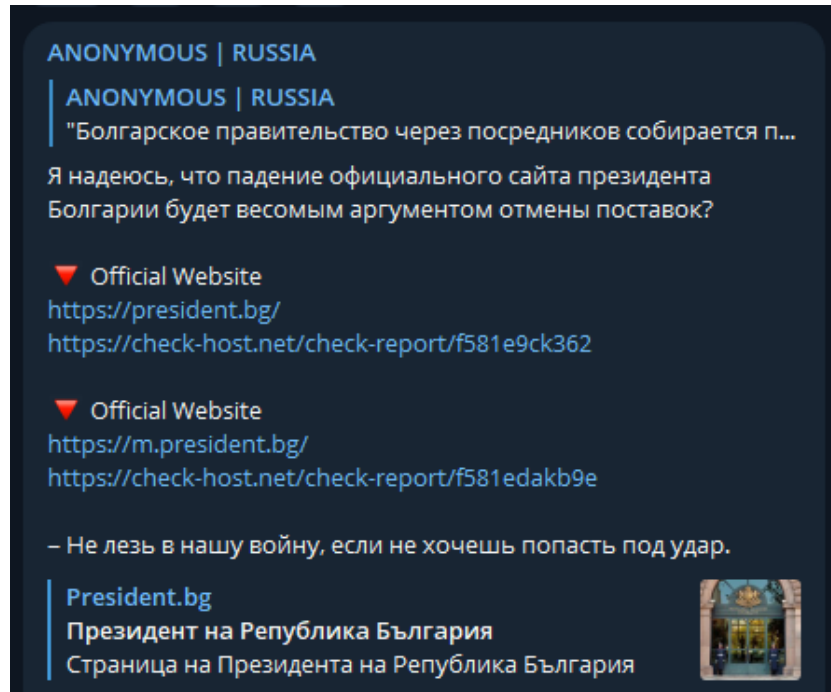
▼ JtBanka
Лучший Словацкий Банк
(2-ое Место)
<https://www.jtbanka.sk/>
<https://check-host.net/check-report/f576908k1a6>

Národná banka Slovenska
Homepage - Národná banka Slovenska
The National Bank of Slovakia (NBS) is the central bank of Slovakia.



28 March 2023

March 28, 2023 AnonymousRussia crashed the official website of the President of Bulgaria with DDoS attacks. AnonymousRussia stated that the attack was a message to the President of Bulgaria .



Check website <https://m.president.bg/>

Permanent link to this check report | Share report on Twitter

Checked on **Tue Mar 28 13:08:10 UTC 2023** | [Check again](#)

Location ▾	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Roubaix	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			
India, New Delhi	Connection timed out			
Iran, Shiraz	Connection timed out			

Anonymous Russia's Attack TTPs

By observing the attacks and behaviors of Anonymous Russia since its emergence, some inferences can be made about whether they are applied repetitively or in a consistent manner.

It targets websites of governments or public institutions. In this way, it gives a clear message to victims that the victims are on the wrong side.

It prefers DDoS attacks against its targets. Victims can recover their systems from attacks, which usually take 1 to 3 days, with appropriate measures in a matter of hours.

They use DDoS attacks against the OSI model. Layer 4 (SYN flood attacks) and layer 7 (high volume POST/GET requests) cause resource exhaustion and system failure.

They announce their attacks, the groups they work with, and the targeted country, organization, domain information via Telegram channels.

It is also associated with other hacker groups that have common goals with them or act in Russian interests. They collaborate with KillNet, DeaDNET, and Legion.

Although he took a stance of defending Russia, from time to time he also targeted organizations within Russia that had nothing to do with the state. (Shoe stores, video sharing platforms, etc.)

Thinking that it would give an advantage to Russia or by displaying a retaliatory attitude, it chose its targets among NATO-linked countries in the steps they took.

It can also be described as a potential threat to countries whose political interests do not match with Russia's.

Tactics	Technique	Technique ID
Reconnaissance	Active Scanning	T1595
Reconnaissance	Gather Victim Host Information	T1592
Reconnaissance	Gather Victim Identity Information	T1589
Reconnaissance	Gather Victim Network Information	T1590
Reconnaissance	Gather Victim Network Information	T1591
Reconnaissance	Search Open Technical Databases	T1596
Reconnaissance	Search Open Websites/Domains	T1593
Reconnaissance	Search Victim-Owned Websites	T1594
Resource Development	Acquire Infrastructure	T1583
Resource Development	Compromise Infrastructure	T1584
Resource Development	Compromise Accounts	T1586
Credential Access	Brute Force	T1110
Inhibit Response Function	Denial of Service	T0814
Impact	Network Denial of Service	T1498
Impact	Service Stop	T489

Anonymous Russia's Attack IOCs

Communication Channels

Telegram	Status	Category
https://t.me/anon_by	ONLINE	Anonymous Russia channel

Forums

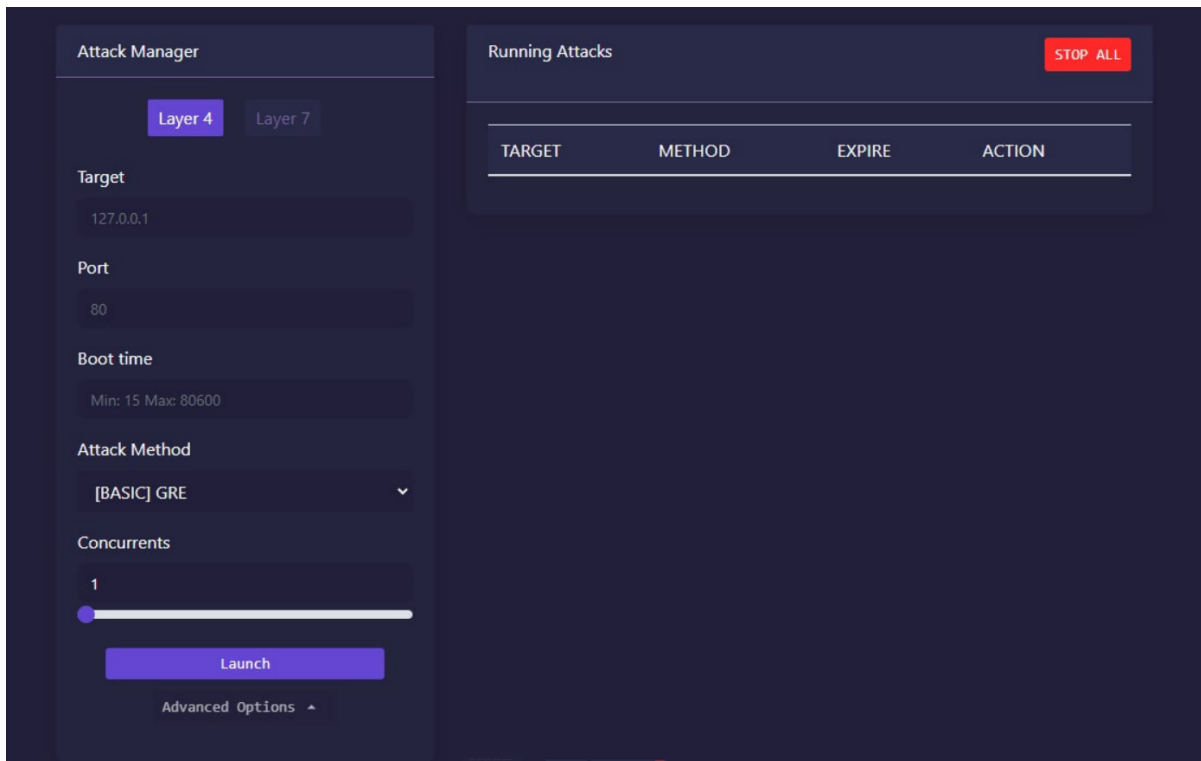
Web Address	Status	Category
https://infinity.ink/	ONLINE	Forum including Anonymous Russia

Mirrors

<https://creep.im/tor> - by Soviet Anonymous (Russia)

DDoS Control Panels

IoC	IoC Type
http://stressid.club/	Domain



Indicator	Description
https://40.68.220.40:9443/authenticationendpoint/balگو.jsp	IP
https://182.73.18.131:443/authenticationendpoint/balگو.jsp	IP
https://63.33.121.175:443/authenticationendpoint/balگو.jsp	IP
https://54.228.15.59:443/authenticationendpoint/balgo.jsp	IP
https://18.169.37.128:443/authenticationendpoint/balگو.jsp	IP
https://sklepyabc.pl	Domain
https://marketdino.pl	Domain
https://www.eurosklep.eu	Domain
https://sklepygama.pl	Domain
https://www.groszek.com.pl	Domain
https://lewiatan.pl	Domain
https://www.piotripawel.pl	Domain
https://www.polomarket.pl	Domain
https://wss.spolem.org.pl	Domain
https://www.topmarkety.pl	Domain
https://topaz24.pl	Domain
https://www.paih.gov.pl/en	Domain
https://pan.pl/	Domain
https://www.pot.gov.pl/pl	Domain
https://www.pism.pl/	Domain
https://www.pkn.pl/	Domain
https://www.pcbc.gov.pl/	Domain
https://rf.gov.pl/	Domain
http://www.brpd.gov.pl/	Domain

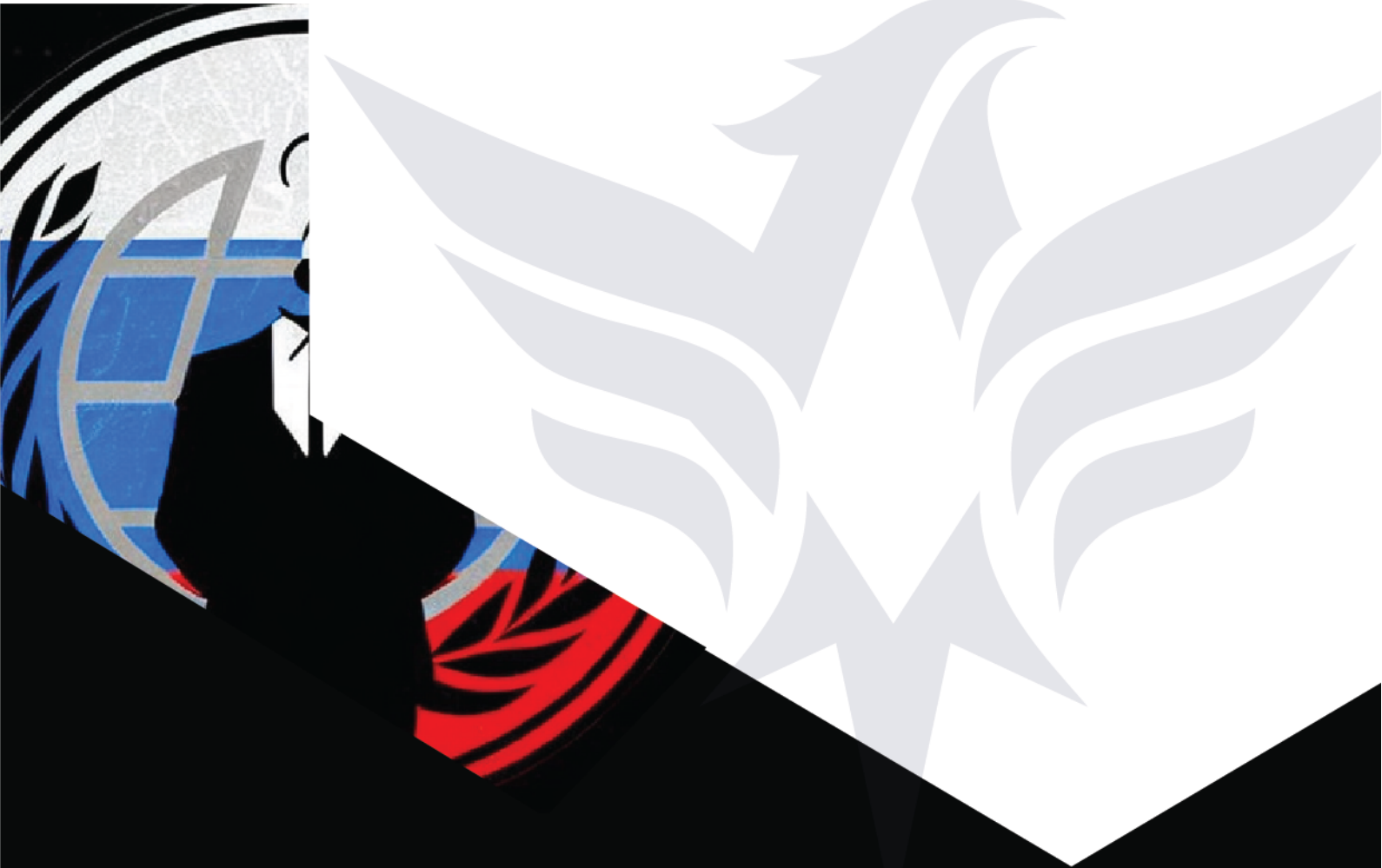
http://www.sop.gov.pl/	Domain
https://www.kombatanci.gov.pl/pl/	Domain
https://www.udt.gov.pl/	Domain
https://www.uodo.gov.pl/	Domain
https://www.uprp.pl/	Domain
https://www.policja.pl/	Domain
http://www.gios.gov.pl/	Domain
https://www.lasy.gov.pl/	Domain
https://www.archiwa.gov.pl/	Domain
https://www.bbn.gov.pl/	Domain
https://www.cba.gov.pl/	Domain
https://www.wetgiw.gov.pl/	Domain
http://www.gum.gov.pl/	Domain
http://www.ncbj.gov.pl/	Domain
https://www.kowr.gov.pl/	Domain
https://www.nfz.gov.pl/	Domain
https://www.pip.gov.pl/	Domain
https://www.polska.pl/	Domain
https://www.msz.gov.pl/	Domain
https://www.mg.gov.pl/	Domain
https://www.granica.gov.pl/	Domain
https://www.sejm.gov.pl/	Domain
https://www.senat.gov.pl/	Domain
https://amw.com.pl/pl/	Domain
https://altbank.ua/	Domain
https://plb.pl/en/	Domain
https://modlinairport.pl/	Domain
https://www.airport.gdansk.pl/	Domain
https://www.rzeszowairport.pl/en/	Domain

https://airport.lubuskie.pl/	Domain
https://www.airport.lublin.pl/ru	Domain
https://www.krakowairport.pl/en	Domain
https://www.bundeswehr.de/de/	Domain
https://www.bnd.bund.de/	Domain
https://www.flughafen-erfurt-weimar.de/	Domain
https://www.hannover-airport.de/	Domain
https://www.dortmund-airport.de/	Domain
https://www.airport-nuernberg.de/	Domain
https://www.baden-airpark.de/en/	Domain
https://www.dus.com/	Domain
https://ac.nato.int/	Domain
https://www.gu.se/	Domain
https://www.kth.se/	Domain
https://www.chalmers.se/	Domain
https://www.su.se/	Domain
https://www.lunduniversity.lu.se/	Domain
https://www.uu.se/	Domain
https://login.nspa.nato.int/my.policy	Domain
https://www.nato-pa.int/	Domain
https://nspa.nato.int/	Domain
https://jwc.nato.int/	Domain
https://media.act.nato.int/site/login/	Domain
https://arcc.nato.int/	Domain
https://apx.ndc.nato.int/	Domain
https://www.act.nato.int/	Domain
https://www.jwc.nato.int/	Domain
https://www.jallc.nato.int/	Domain
https://www.abgsc.com/	Domain

https://www.avanza.se/	Domain
https://www.carnegie.se/	Domain
https://www.swedbank.com/	Domain
https://www.jak.se/	Domain
https://onboarding.abgsc.no/Login	Domain
https://pb.carnegie.se/login	Domain
https://www.banknorwegian.se/	Domain
https://www.icabanken.se/	Domain
https://seb.se/	Domain
https://www.handelsbanken.com/en	Domain
https://www.alandsbanken.ax/	Domain
https://app.bankid.com/sv/	Domain
https://identity.banknorwegian.no/MyPage/Login	Domain
https://online.swedbank.se/app/ib/logga-in	Domain
https://edge.carnegie.se	Domain
https://www.nusjukvarden.se/	Domain
https://www.sahlgrenska.se/	Domain
https://www.sodersjukhuset.se/	Domain
https://sjukhus.sophiahemmet.se/	Domain
https://www.akademiska.se/	Domain
https://www.vgregion.se/	Domain
https://www.erstadiakoni.se/	Domain
https://regionkalmar.se/	Domain
https://www.1177.se/	Domain
https://www.lio.se/	Domain
https://regionsormland.se/	Domain
https://www.skane.se/	Domain
https://cancercentrum.se/	Domain
https://www.regionvasterbotten.se/	Domain



https://capiostgoran.se/	Domain
https://www.karolinska.se/	Domain
https://www.regionorebrolan.se/	Domain
https://www.ds.se/	Domain
https://www.radware.com/	Domain



ThreatMon



45305 Catalina cs St 150, Sterling VA 20166