

Unmasking the Actors Behind Russian Intelligence-Linked Phishing Operations

Joint investigation with [Aleksandr Litreev](#) – a cybersecurity researcher, founder of intelligence data platform OSEENT.

Executive Summary

We identified the individual behind a phishing campaign that targets Ukraine sympathizers in Russia with high confidence as **Aleksandr Ostaenkov**, a 25-years old from Polevskoy, Sverdlovskaya oblast', Russia.

Aleksandr Ostaenkov **operates several phishing websites** and Telegram channels/bots impersonating Freedom of Russia Legion (Ukrainian Armed Forces unit consisting of Russians) and I Want To Live (a helpline of Ukrainian Military Intelligence for Russians).

Although there is no direct evidence, **we assess that Ostaenkov collaborates with Russian intelligence services** and/or law enforcement forwarding the information obtained via phishing to them.

Background

Malfors has been tracking a large-scale impersonation campaign linked to the Russian intelligence services since August 2024.

The campaign targets Ukraine and the West sympathizers in Russia with a set of phishing websites, Telegram channels, and bots that impersonate Ukrainian Armed Forces units, Ukrainian Intelligence projects, the CIA, and other organizations. The objective of the campaign is to catch and retaliate Russian citizens not loyal to the regime.

A detailed report by SilentPush, in collaboration with Malfors, has been published earlier on this campaign: silentpush.com/blog/russian-intelligence-phishing/.

Earlier, [we have also published 60+ domains](#) we identified that are a part of this campaign. Impersonated organizations include:

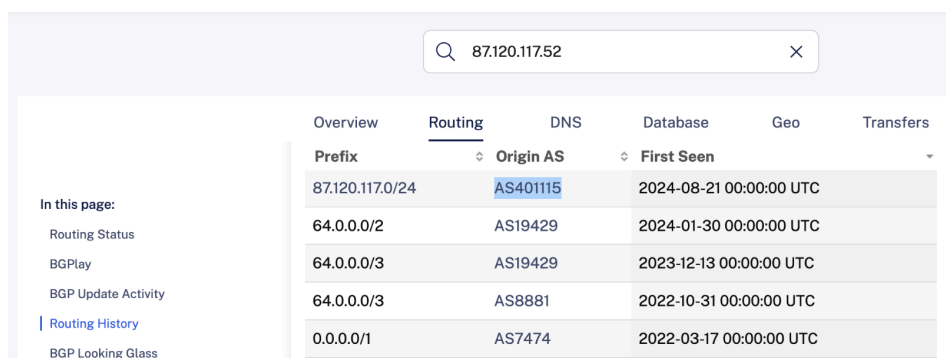
- CIA (Central Intelligence Agency)
- Freedom of Russia Legion (Ukrainian army unit consisting of Russians)
- Russian Volunteer Corps (Ukrainian army unit consisting of Russians)
- I Want To Live (Ukrainian helpline for Russian servicemen attempting to surrender)

The campaign started in 2023 and remains active as of May 2025.

Initial Findings

While conducting a routine check of newly registered domains that might be affiliated with the campaign, we identified a new suspicious domain: **legionliberty[.]space**.

legionliberty[.]space points to **87.120.117[.]52** which belonged to **AS401115 (Ekabi LLC)**:



The screenshot shows the RIPEstat routing table for the IP address 87.120.117.52. The 'Routing' tab is selected, showing a table with columns: Prefix, Origin AS, and First Seen. The first entry is 87.120.117.0/24 originating from AS401115, first seen on 2024-08-21. Other entries include 64.0.0.0/2 from AS19429, 64.0.0.0/3 from AS19429, 64.0.0.0/3 from AS8881, and 0.0.0.0/1 from AS7474.

Prefix	Origin AS	First Seen
87.120.117.0/24	AS401115	2024-08-21 00:00:00 UTC
64.0.0.0/2	AS19429	2024-01-30 00:00:00 UTC
64.0.0.0/3	AS19429	2023-12-13 00:00:00 UTC
64.0.0.0/3	AS8881	2022-10-31 00:00:00 UTC
0.0.0.0/1	AS7474	2022-03-17 00:00:00 UTC


<https://stat.ripe.net/resource/87.120.117.52#tab=routing>

AS401115 (Ekabi LLC) is a well-known bulletproof hosting indicating a malicious intent.

ASN report for AS401115

You are viewing the database entry for AS401115 (EKABI).

Database Entry

AS number:	AS401115
AS name:	EKABI
Country:	 US
Spamhaus ASN-DROP ⓘ:	Blocked ⓘ - This ASN should not be routed or peered with. It is under control of cyber-criminals
Total IPs observed ⓘ:	⌌ Loading
Online malware site ⓘ:	⌌ Loading
Offline malware site ⓘ:	⌌ Loading

<https://urlhaus.abuse.ch/asn/401115>

Ekabi's only upstream, **AS401110 (Sovy Cloud Services LLC)**, [has been disconnected](#) from its upstreams for ignoring abuse reports and hosting malicious activity.

Previously, we observed a different phishing website of this campaign hosted at **AS401120 (cheapy.host LLC)** whose single upstream is also AS401110 (Sovy Cloud Services LLC) – **rusvolcorps[.]net** at **196.251.84[.]42** – **AS401120 (cheapy.host LLC)**.

Though, we weren't able to confirm the relation between legionliberty[.]space and rusvolcorps[.]net, yet.

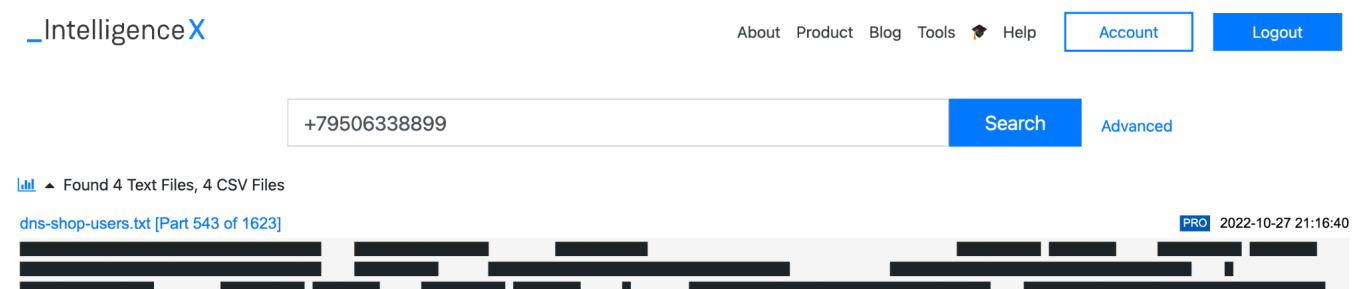
Details Exposure via WHOIS

We check WHOIS data as a standard procedure of handling malicious domains. legionliberty[.]space is registered with Russian registrar REG[.]RU and exposes the following potentially useful data about the domain owner:

Admin Phone	+7.9506338899
Admin Email	illegalmercy92@gmail.com

Registrars, [including REG.RU](#), are obliged to require email confirmation to register domains in gTLD, so Admin Email has to be an existing email.

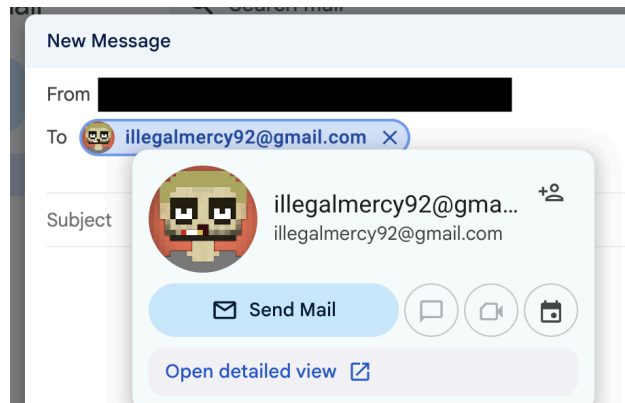
Usually, we see random contact details, emails are usually registered just for the domain registration and never re-used. This time it was different.



The screenshot shows a search interface with the following elements:

- Top left: **_IntelligenceX**
- Top right: Navigation links (About, Product, Blog, Tools, Help) and buttons (Account, Logout).
- Search bar: Contains the phone number **+79506338899** and a **Search** button. A link to **Advanced** search is also present.
- Results: A message states "Found 4 Text Files, 4 CSV Files". Below this, a file named **dns-shop-users.txt [Part 543 of 1623]** is listed. The content of the file is redacted with black bars.
- Bottom right: A status bar showing **PRO** and the timestamp **2022-10-27 21:16:40**.

Phone number from WHOIS [appears in known breaches](#)

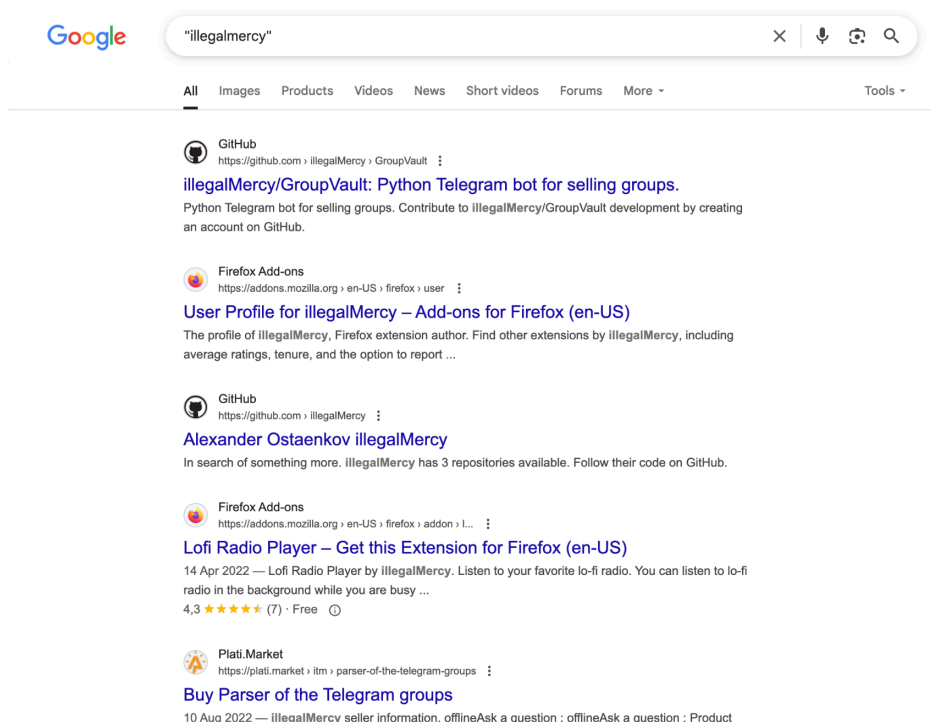


Gmail exposes user avatar of the WHOIS contact email

Identification

Seeing clear indications that details exposed in WHOIS might be used by a real person, we decided to dive deeper in an attempt to identify them.

illegalmercy92@gmail.com is nowhere to be found in open sources; however, we quickly find a person using a very similar username: "illegalmercy":



Google Search results for "illegalmercy"

From Google Search, we found out that "IllegalMercy" published a Firefox extension to listen for Lo-Fi music. The Firefox developer's profile has exactly same picture as we have seen in Gmail earlier:

<https://addons.mozilla.org/en-US/firefox/user/17367180/>

From Firefox developer contact's section we extract another email of the person: **guppson@yandex.ru**.

The Github account with the same username hosts the code of the above mentioned Firefox extension:

Alexander Ostaenkov
illegalMercy

Follow

In search of something more

📍 Russia, Yekaterinburg

✉ al.ostaenkov@gmail.com

<https://t.me/illegalMercy>

Achievements



Block or Report

illegalMercy / README.md

```
illegalMercy@github:~$ Hey, net wanderer!
```

```
illegalmercy@github:~$ hey, net wanderer:
illegalmercy@github:~$ Take a load off and chill for a minute
```

illegalMercy@github

Language: Python

Development: Telegram Bots / GUI Apps

Popular repositories

LoFi-radio-player

Listen to your favorite lo-fi radio

HTML ☆ 3

Public archive

Public

GroupVault

Python Telegram bot for selling groups.

Python ☆ 2

illegalMercy

Public

<https://github.com/illegalMercy>

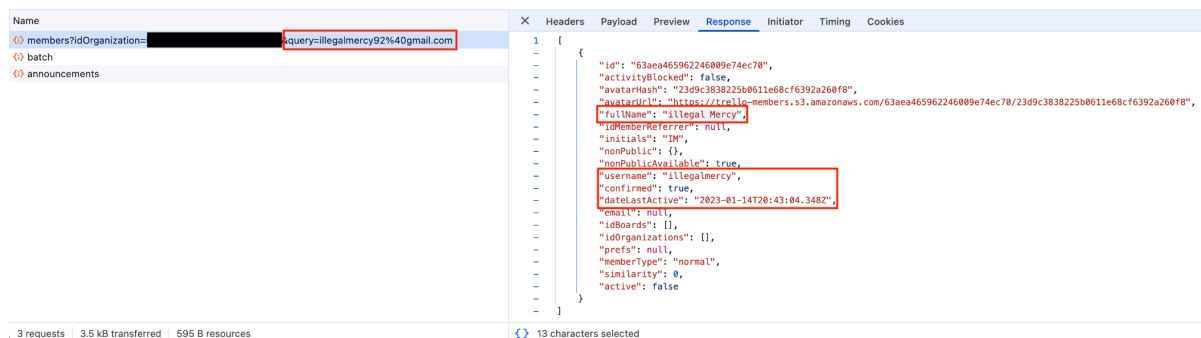
We extract the following information from that Github account:

Full name	Alexander Ostankov
Email	al.ostaenkov@gmail.com
Location	Russia, Yekaterinburg
Telegram	@illegalMercy

Note that the phone number from WHOIS has a region code of Sverdlovsk oblast (the region where Yekaterinburg is located). With this information, we are looking for more evidence that illegalmercy92@gmail.com indeed belongs to Ostankov.

Additional Confirmations

We were able to find a Trello account registered with illegalmercy92@gmail.com. Trello performs a lookup of a Trello user by email when inviting one to a board, exposing profile details:



Trello lookup result by illegalmercy92@gmail.com

Full name of the account is "illegal Mercy" with lowercase "i" and capital "M" – consistent with other accounts that belong to Aleksandr.

Also, the account was last active in January 2023 – almost 2 years before the first phishing website managed by Aleksandr came up.

Via OSEENT platform, we verified that the phone number exposed in WHOIS (+7.9506338899) appears publically available breached data and belongs to Aleksandr:

Summary

Name
Александр Александрович Остаенков

Phone
+79506338899

Email
quppson@yandex.ru

Addresses
[Map showing location in Yekaterinburg]

Documents
No Data

Vehicles
No Data

Identities

ID	First Name	Middle Name	Last Name	Sex	Date of Birth	Source
347e246b1f9d	Александр	Александрович	Остаенков	Male	10.09.1999	Sberbank Russia (RU)

Phone Numbers

ID	Phone Number	Person ID	Source
c8011e0b14d9	+79506338899	347e246b1f9d	Sberbank Russia (RU)

Emails

ID	Email	Person ID	Source
776b6002d57b	quppson@yandex.ru	347e246b1f9d	Sberbank Russia (RU)

Publicly breached data confirms name, phone number, residential location in Yekaterinburg of Aleksandr

Despite all the evidence, we have to note that we were not able to fully rule out a false flag operation. Although highly unlikely, a sophisticated actor is theoretically able to frame Aleksandr and act on his behalf.

More Phishing Infrastructure

Having confirmed the actor, we are looking for more phishing infrastructure that the actor has managed. Starting point is malicious domain legionliberty[.]space and its IP address 87.120.117[.]52.

87.120.117.52 Enrich X

IP Address: 87.120.117.52
Added at: May 3, 2025, 2:40 PM

Details **IPInfo – IP Details** **SecurityTrails – Reverse IP**

Shodan – InternetDB **Urlscan – Search**

Executed at May 6, 2025, 4:44 PM ↻

Domains ...

Domain ⌵

- hochuzhit.tech
- legionliberty.space
- www.hochuzhit.tech
- www.legionliberty.space

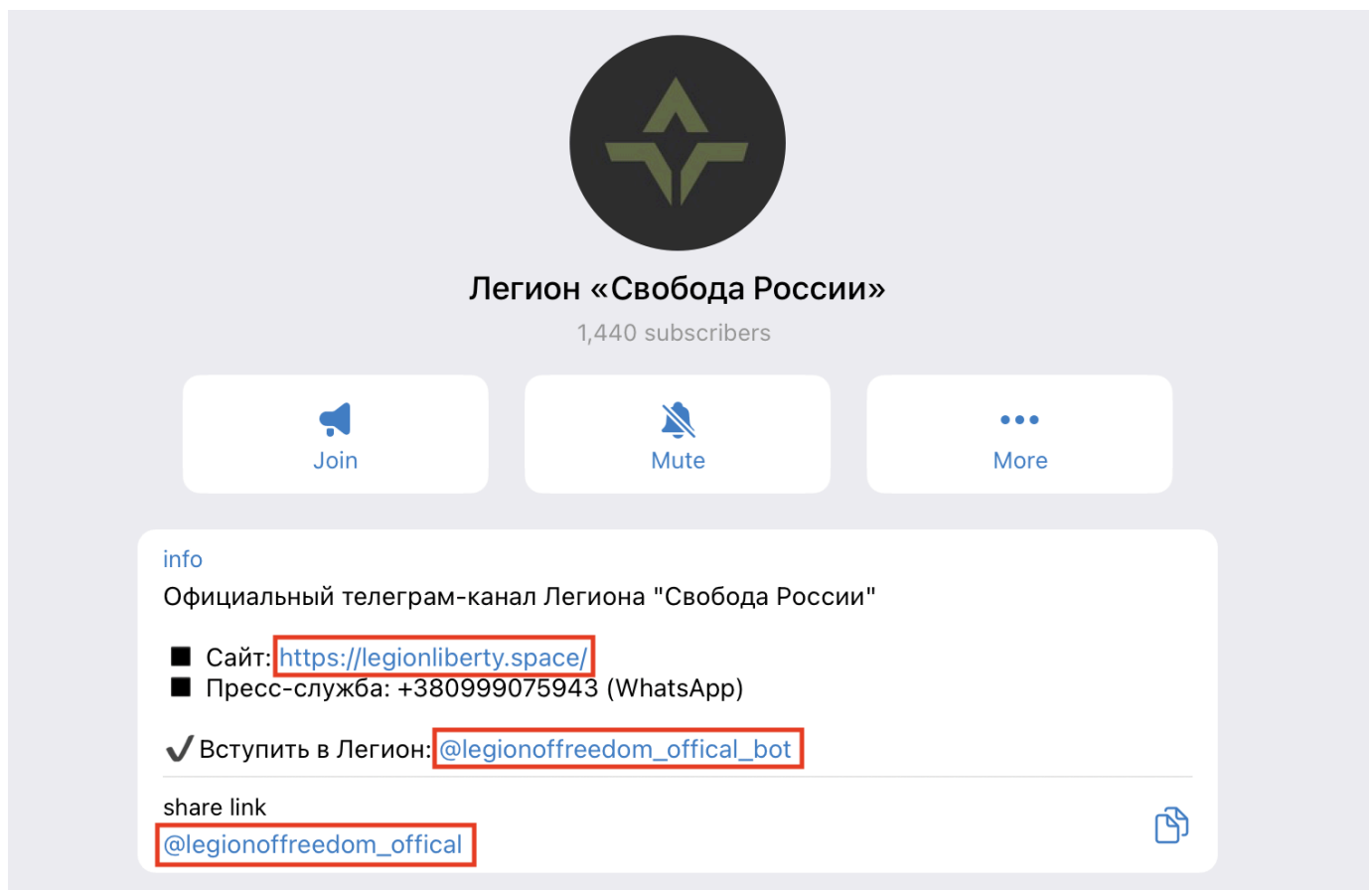
Pivoting on the IP address returns another domain: **hochuzhit[.]tech**

"Hochu Zhit" is a transliteration of "[Хочу Жить](#)" ([I Want To Live](#)) – a helpline for surrendering Russian servicemen operated by the Ukrainian Military Intelligence.

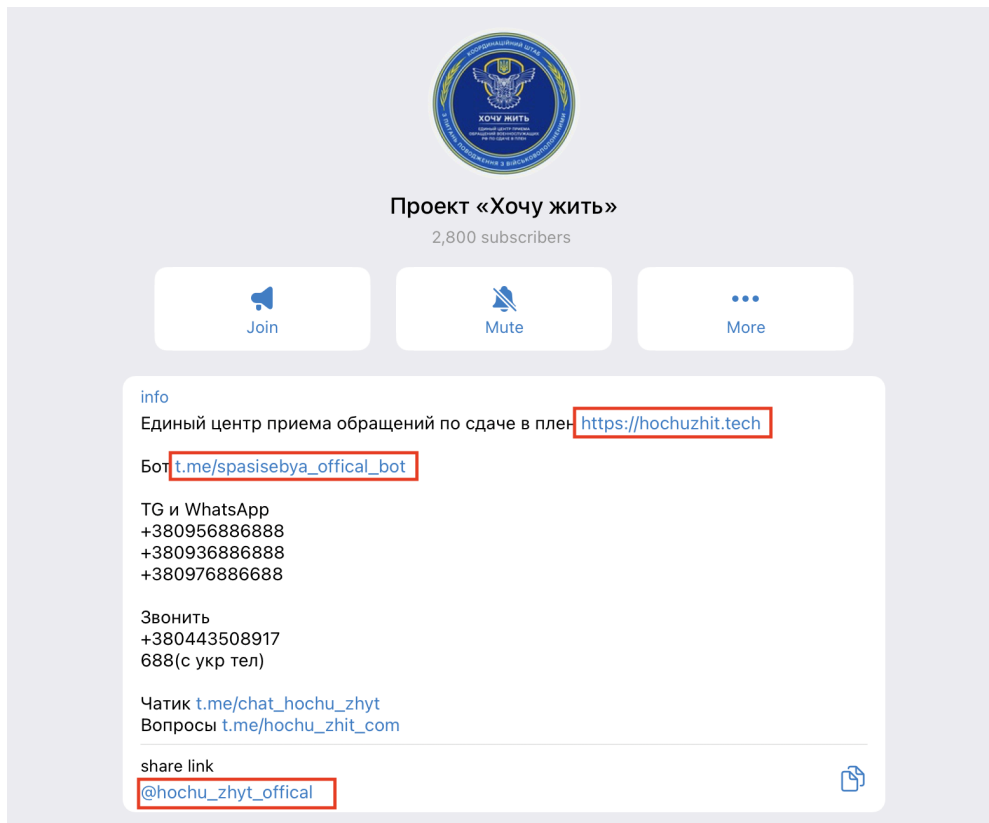
We have already seen several "Hochu Zhit" impersonations within this campaign, this one is a new one. hochuzhit[.]tech's WHOIS returns the same contact details confirming that it is indeed the same actor.

We were not able to confirm that either of two domains ever hosted phishing content. Past scans on Urlscan.io indicate that the domains redirected to legitimate websites of Freedom of Russian Legion and Hochu Zhit.

However, quick Google Search of the domain names reveals fake Telegram channels impersonating legitimate ones.



Fake Telegram channel of Freedom of Russia Legion



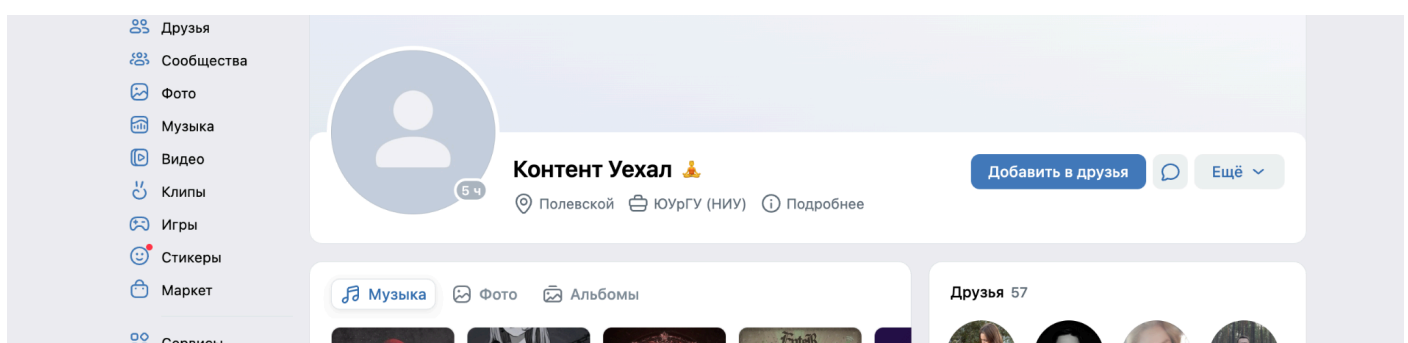
Fake Telegram channel of Hochu Zhit

Those channels are auto-posting content of legitimate channels while replacing legitimate contact details. Bio and posts link to **fake Telegram bots** impersonating legitimate Telegram bots of the respective organizations.

Actor's Profile

Aleksandr Ostaenkov behaves cautiously in the digital space. His online presence is minimal, he uses made up aliases in social media, and never posts photos of himself.

For example, his profile on the social network VK.com changed its name from his real one to “Контент Уехал”, which is translated as “Content has left”.

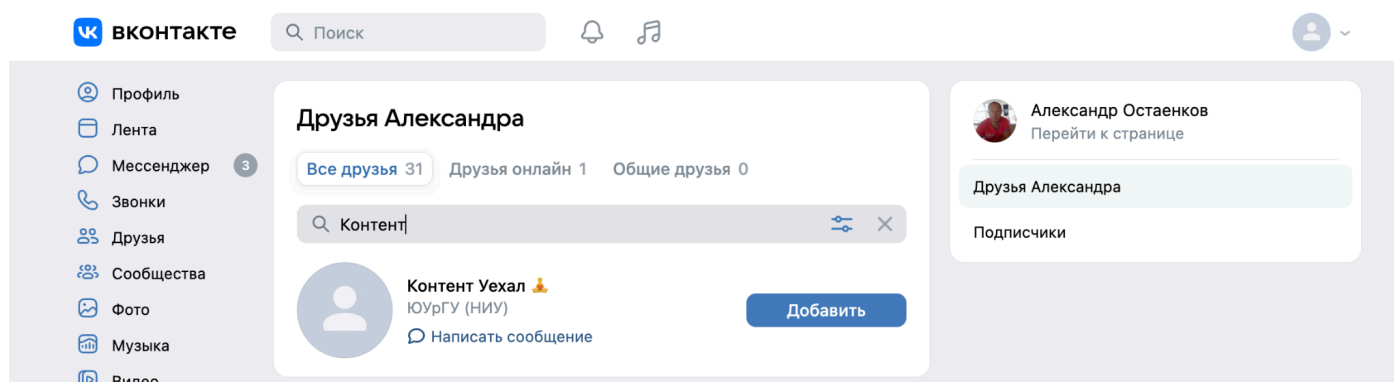


Aleksandr's VK.com profile: <https://vk.com/id220540855>

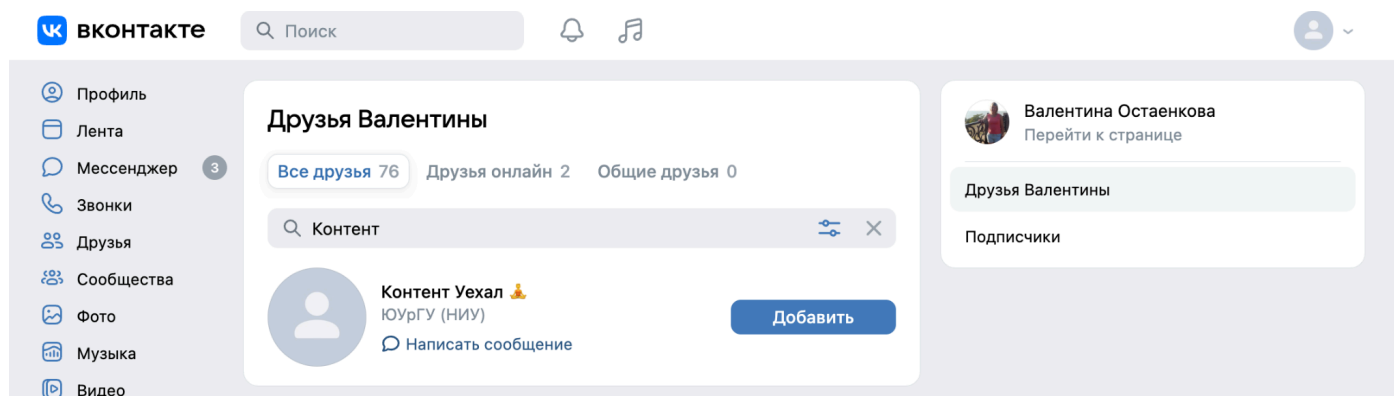
The account uses the familiar username “illegalmercy.”; the date of birth matches Aleksandr's data from publicly available leaks. The profile also states that he lives in the city of Polevskoy and has an interest in Retrowave/Synthwave music.

Aleksandr’s profile also states that he graduated from South Ural State University with a degree in “Fundamental Informatics and Information Technologies,” studying at the Faculty of the Higher School of Electronics and Computer Science.

We have also identified Aleksandr’s parents – Valentina Ostaenkova and Aleksandr Ostaenkov (Sr.).



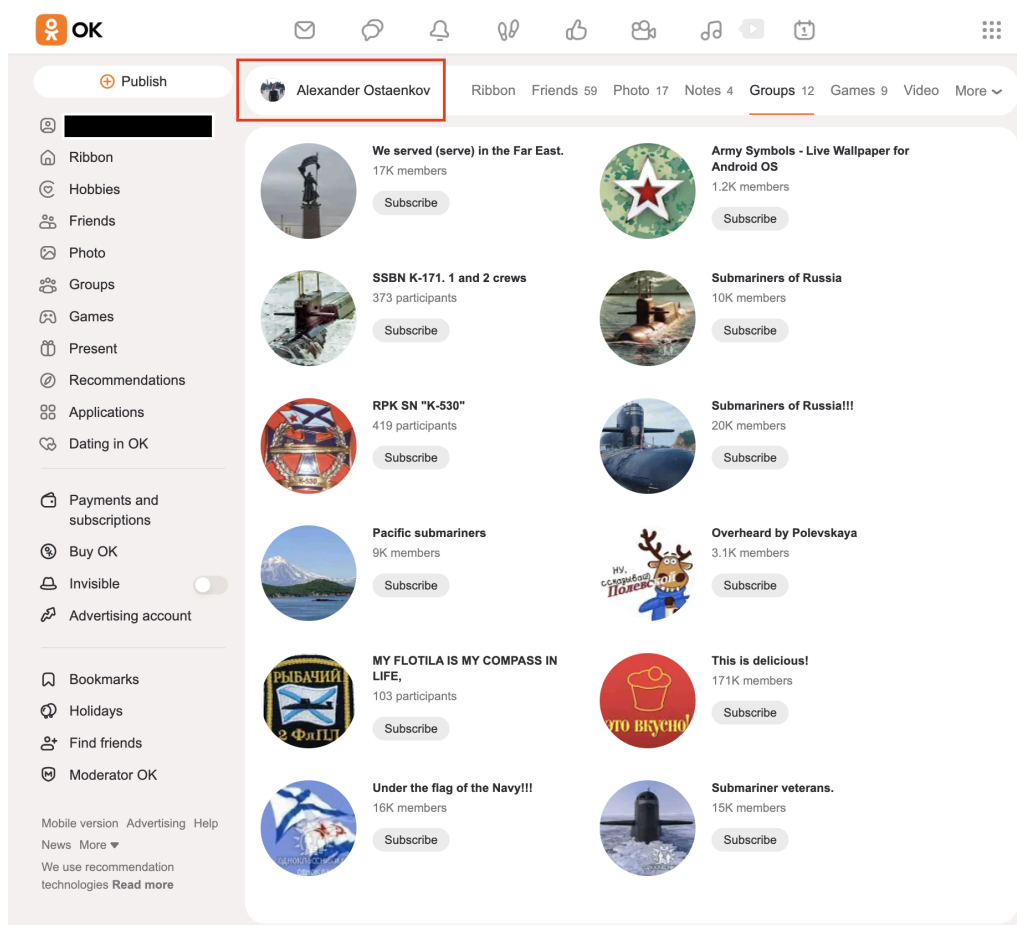
Father’s VK.com list of friends: <https://vk.com/friends?id=349490538§ion=all>



Mother’s VK.com list of friends: <https://vk.com/friends?id=340006292§ion=all>

We confirmed the relationship by numerous photos together that the family members posted publicly. We are not including those photos in the report to respect privacy of uninvolved relatives and Ostaenkov being a minor on them.

We also found Aleksandr's father's profile on another popular Russian social network, Odnoklassniki. There, he is a member of groups related to the Russian military.



Aleksandr Ostienkov (Sr.) Odnoklassniki profile: <https://ok.ru/profile/452371886441>

Some groups are very specific, for example, he is a member of groups for former crew members of specific ballistic missile submarines (SSBN), which are a part of the Russian nuclear triad. Ostienkov (Sr.) also has several friends who identify themselves as former or active duty officers of Russian Army and Law Enforcement.

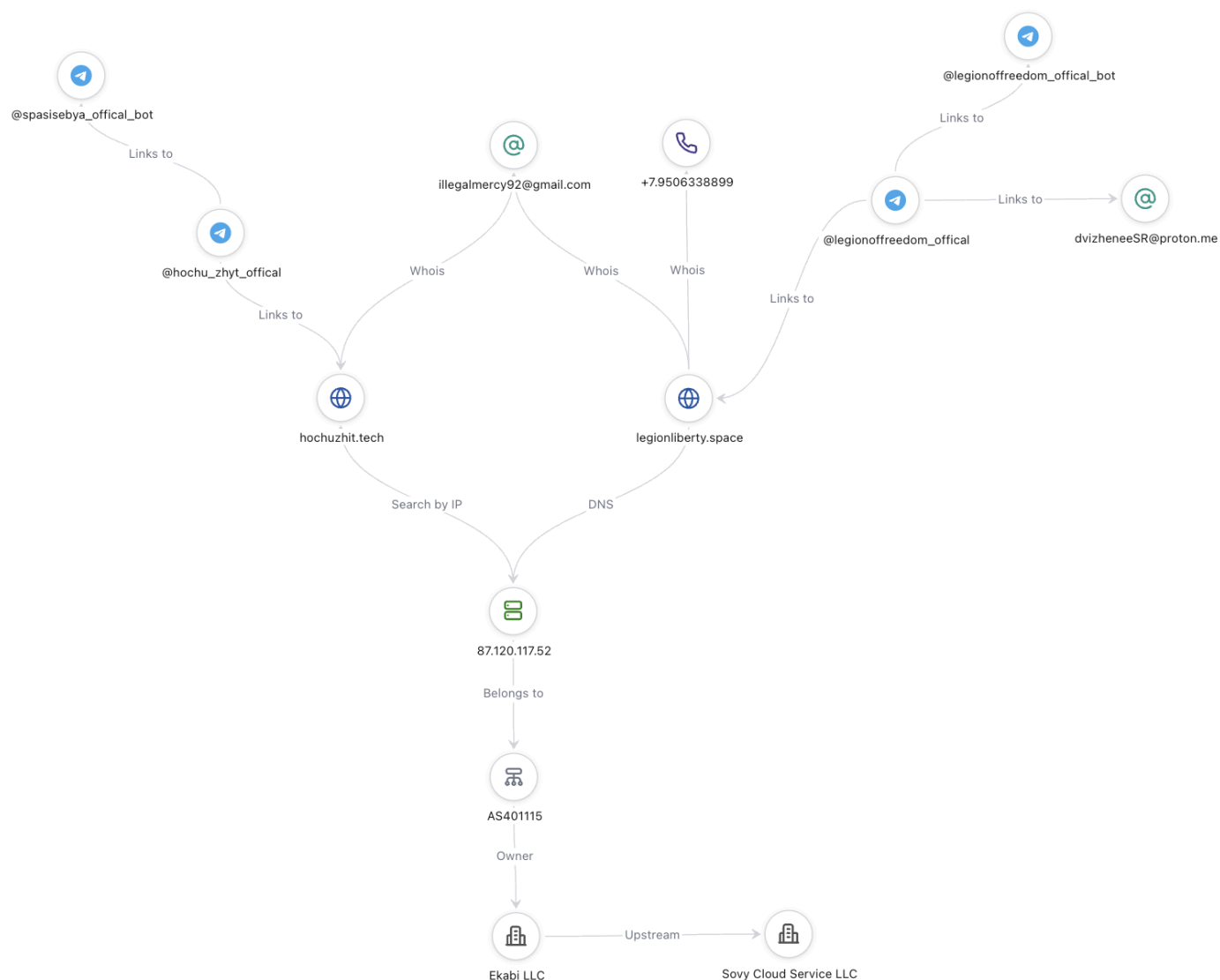
This indicates a pro-regime stance of the Ostienkov family and confirms close connections with Russian military and law enforcement.

Summary

We identified two Telegram channels (~4,000 subscribers combined), two Telegram bots, and two websites that make up the phishing campaign impersonating Hochu Zhit and Freedom of Russia Legion.

We were able to identify and are highly confident about the person behind it – Aleksandr Ostienkov, a 25-years old from Russia.

No connections between Ostaenkov and the rest of the campaign were found yet.



Aleksandr's campaign visualized

Indicators

hochuzhit[.]tech	Phishing website impersonating Hochu Zhit
legionliberty[.]space	Phishing website impersonating Freedom of Russia Legion
87.120.117[.]52	IP of phishing websites
t.me/hochu_zhyt_offical	Fake Hochu Zhit Telegram channel

t.me/legionoffreedom_offical	Fake Freedom of Russia Legion Telegram bot
t.me/spasisebya_offical_bot	Fake Hochu Zhit Telegram bot
t.me/legionoffreedom_offical_bot	Fake Freedom of Russia Legion Telegram bot
dvizhenesSR@proton.me	Fake Freedom of Russia Legion email address