Identifying Yutek-NN Personnel Linked to Past Cyber Campaigns Serving Russian State Interests

Disclaimer

This report describes events that occurred in 2021. It is based on investigations conducted by our team and independent journalists between 2021 and 2024, with additional details incorporated in 2026.

We are publishing this report in 2026 because the **identified individuals were or are employed by Yutek-NN** – a private Russian company that the United States has indicted for conducting cyber espionage on behalf of the Russian government.

The associated threat activity is tracked as **Void Blizzard / Laundry Bear**.

Key Judgements

- We identified **Anton Listarov** as the individual who controlled the accounts and infrastructure used in the 2021 email campaigns targeting Russian opposition activists.
- We independently corroborated Current Time's identification of **Vyacheslav Zubkov** as a participant in related data and operational activity.
- Listarov and Zubkov were **both employed at IAC EMERCOM and later at Yutek-NN**, where they likely **reported directly to Denis Obrezko, a former FSB officer** indicted in the U.S. for cyber espionage.
- We assess with low confidence that Listarov and Zubkov acted at **Mikhail Dudin**'s direction to advance his interests and interests associated with **the FSB and Presidential Administration**.

Background

Alexei Navalny[1] was a Russian opposition leader and anti-corruption activist. In early 2021, his team launched the Free Navalny campaign[2] to mobilize support for his release from prison, allowing supporters to register at free[.]navalny[.]com.

In April 2021, a database containing registrants' email addresses was obtained and leaked. The records were enriched with data from other leaks to identify individuals and published on the XSS[.]is forum.

The data were also used in an email campaign targeting those listed in the database. The messages included recipients' personal information and threats of prosecution.

Ahead of Russia's September 2021 State Duma election, Navalny's team promoted Smart Voting[3] – a tactical initiative supporting candidates considered most likely to defeat the ruling United Russia party's nominees.

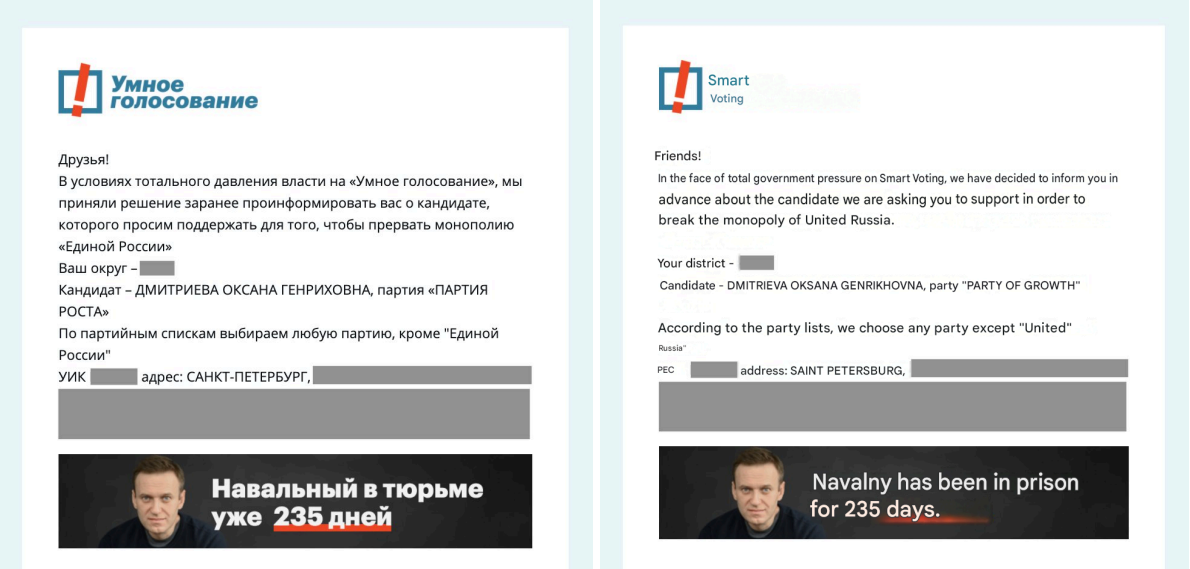
[1] https://en.wikipedia.org/wiki/Alexei_Navalny
[2] https://navalny.com/en/materials/free-navalny-kampaniya-za-osvobozhdenie-alekseya-navalnogo
[3] https://en.wikipedia.org/wiki/Smart_Voting

Shortly before the election, the leaked database was used in a second email campaign to distribute fake Smart Voting recommendations and undermine the initiative.

Fake “Smart Voting” Recommendations

In September 2021, shortly before voting began, a mass email campaign was carried out using the leaked database. We investigated the campaign at the time.

The emails resembled legitimate “Smart Voting” recommendations but promoted different candidates to confuse voters and split the opposition vote.



Fake “Smart Voting” recommendation email.
Left – original, right – Google Translated

Emails were sent from **vote@fbkinfo[.]tech**. The domain resembles fbk[.]info, the legitimate domain of Navalny’s organization, the Anti-Corruption Foundation (FBK)[4].

The WHOIS record for **fbkinfo[.]tech** included the following details:

Registrant Name	**Gennadii Babkov**
Registrant Email	**babkov@protonmail[.]com**

We found no evidence that Gennadii Babkov is a real identity and assess that the registrant information was fabricated. However, a reverse WHOIS search revealed additional infrastructure linked through shared registration details.

Based on domain naming, registration links, and observed content, we assess that those domains supported anti-Navalny activity:

rusvote[.]press
navalny[.]host
rusvote[.]uno
navalnylive[.]tech
rusvote[.]pw

[4] https://en.wikipedia.org/wiki/Anti-Corruption_Foundation

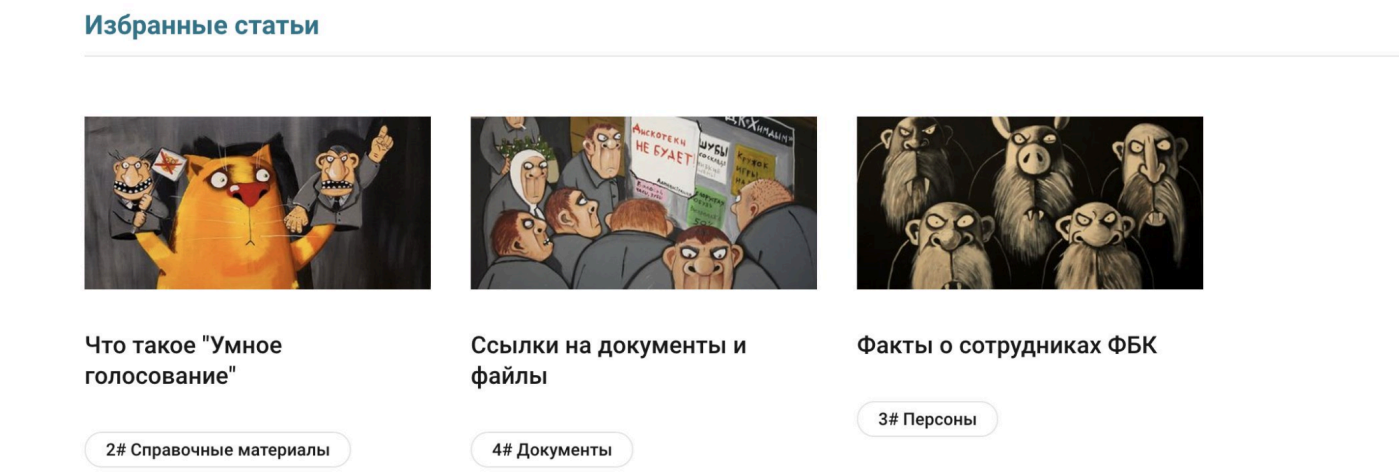
rusvote[.]tech
rusvote[.]space
rus-vote[.]online
navalnydream[.]online
Navalny-team[.]com

The second group of domains likely supported one or more separate phishing campaigns:

eshche[.]pw
eshche[.]tech
eshche[.]space
darkweb[.]pw
gosuslugi[.]uno
kryptonite[.]ru[.]com
rostec[.]online
sulcron[.]com
flyugegekhaymen[.]xyz
kammesant[.]com
reo[.]ru[.]com
veld-21[.]com

We do not know what was hosted on most of those domains at the time or how exactly each of them was used.

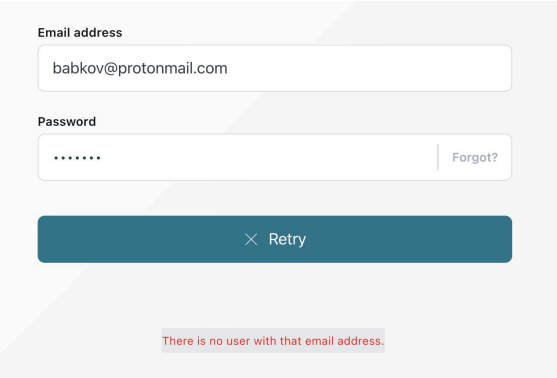
However, **navalny-team[.]com** stood out to us at the time – it hosted a blog containing articles criticizing Navalny and FBK. The blog was powered by the Ghost[5] publishing platform.



Navalny-team[.]com screenshot, three articles about Smart Voting and FBK

We attempted to sign in to the site's admin panel using babkov@protonmail[.]com. The application indicated that no user account was associated with that email address.

[5] https://ghost.org/

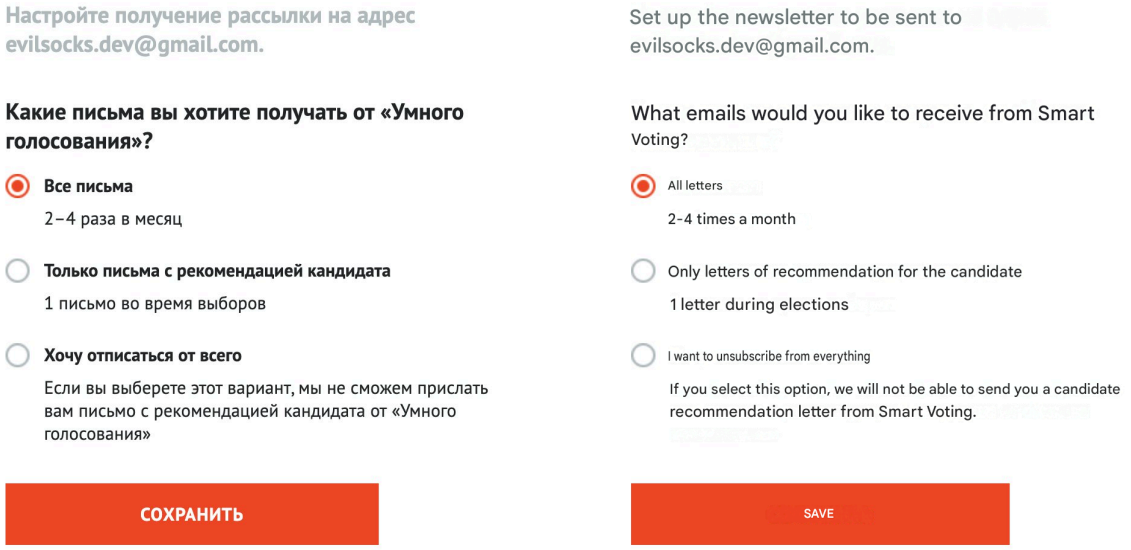


babkov@protonmail[.]com was not an admin user at navalny-team[.]com

Email Exposure

The fake “Smart Voting” email was an exact copy of the legitimate email except for the recommended candidate. We assess that the operator likely received a legitimate recommendation email, copied its layout and styling, and replaced the candidate details before distributing the fraudulent version.

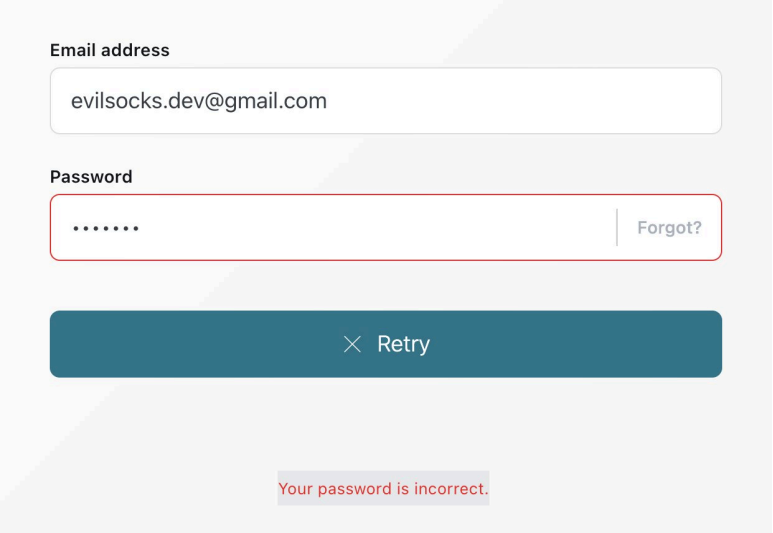
The threat actor also copied the legitimate email’s “Unsubscribe” link, forgetting to change it. It led to a “What emails would you like to receive?” page that exposed the address to which the original email had been sent:



Newsletter settings opened via “Unsubscribe” link in a fake email
Left – original, right – Google Translated

This indicates with high confidence that **evilsocks.dev@gmail[.]com** was the recipient of the original email that was subsequently used as the template for the campaign.

We tested the address in the navalny-team[.]com Ghost admin panel and found that an account associated with it existed. This supports our assessment that evilsocks.dev@gmail[.]com was controlled by the threat actor.

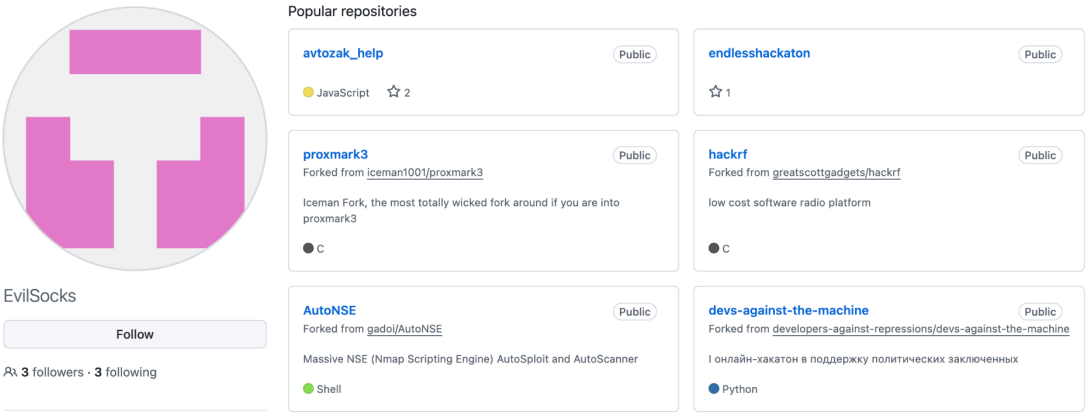


evilsocks.dev@gmail[.]com admin user exists at navalny-team[.]com

Additional Details

To identify the person associated with evilsocks.dev@gmail[.]com, we generated possible usernames based on the email address, including **“evilsocks.dev”** and “**evilsocks**.”

This led us to a GitHub account that we assess is likely operated by the same threat actor:



https://github.com/EvilSocks

The threat actor’s email address, evilsocks.dev@gmail[.]com, was exposed in multiple Git commits associated with the account, for example:

```
From 524993311a904548effe929d457608401bae5277 Mon Sep 17 00:00:00 2001
From: Evil Socks <EvilSocks.Dev@gmail.com>
Date: Sun, 15 Dec 2019 00:25:54 +0300
Subject: [PATCH] 0.0001

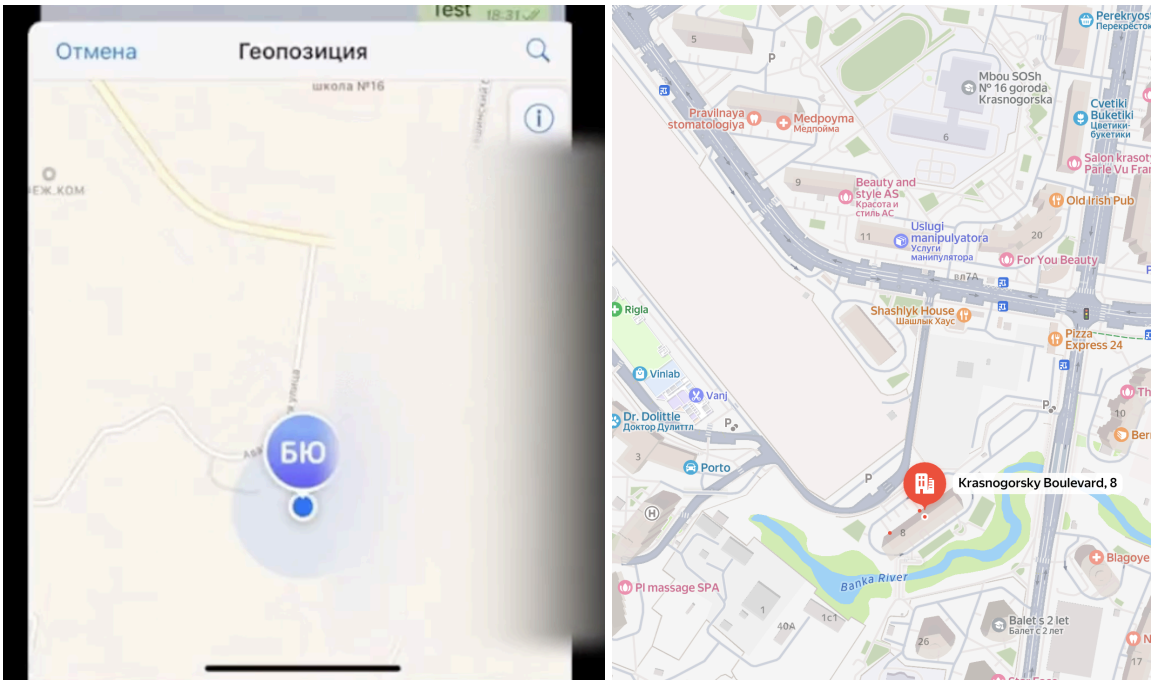
---
 .gitignore                                    |   8 +
 .npmignore                                    |   3 +
 LICENSE                                       |  21 +
 api-scheme/GenerateTGModels.js                |  43 ++
 api-scheme/models/ModelsGenerator.js          | 159 +++++
 api-scheme/models/SchemeClass.js              | 281 ++++++++
 api-scheme/models/SchemeClassField.js         | 130 ++++
 jsdoc.json                                    |  15 +
 lib/BaseTelegramDataSource.js                 |  40 ++
 lib/Telegram.js                               | 365 ++++++++++
```

https://github.com/EvilSocks/avtozak_help/commit/524993311a904548effe929d457608401bae5277.patch

One of his GitHub repositories, *avtozak_help*[6], was created during an online hackathon supporting political prisoners. The project was designed as a Telegram bot that connected unlawfully detained activists with volunteers who could assist them.

The repository contains a link to a demonstration video published on YouTube[7] by a channel[8] called “Evil Socks.”

Although many details in the video are blurred, the redaction is incomplete. In several frames, the location of the person demonstrating the bot is visible:



Left – a frame from the video showing a Telegram user sharing their location with the bot.
Right – the corresponding location identified on Yandex Maps

Based on visible details in the video, we geolocated the recording to Krasnogorskiy Bul'var, 8, Krasnogorsk, Moskovskaya oblast', Russia, 143401[9].

The Telegram user’s initials appear as “БЮ,” with “Б” apparently representing the first letter of the user’s given name. Relatively common Russian male names beginning with “Б” include “Борис” (Boris) and “Богдан” (Bogdan).

We also found “evilsocks.dev” mentioned in a forum thread discussing another mass email campaign from April 2021. In that campaign, the same leaked database was used to send threats. The forum post includes an email header snippet showing “evilsocks.dev” as the recipient name in the “To” header:

[6] https://github.com/EvilSocks/avtozak_help
[7] https://www.youtube.com/watch?v=HTlT4nJhVk4
[8] https://www.youtube.com/@evilsocks1403
[9] https://maps.app.goo.gl/ZZPUfjsJZfrAaNuS8



Аноним 16/04/21 Птн 05:56:20 №244560453 197

>Received: from [FF80:0000:0000:0000:0123:1234:ABCD:EF12] ([46.39.55.180])
by smtp.gmail.com with ESMTPSA id f17sm708530lfl.260.2021.04.15.10.03.15
for <xxxxxxxxxxxxx@gmail.com>
(version=TLS1_2 cipher=ECDHE-RSA-CHACHA20-POLY1305 bits=256/256);
Thu, 15 Apr 2021 10:03:42 -0700 (PDT)
Message-Id: <6BGPDSXB-ED58-4PYK-V0EH-3SDA054NGFL@gmail.com>
Mime-Version: 1.0
Organization: xxxxxxxxxxxxx@gmail.com
From: =?utf-8?Q?=D0=A1=D0=B2=D0=BE=D0=B1=D0=BE=D0=B4=D1=83_=D0=9D=D0=B0=D0=B2=D0=B0=D0=BB=D1=8C=D0=BD=D0=BE=D0=BC=D1=83!?=
<noreply@navalnyfail.online>
To: evilsocks.dev <xxxxxxxxxxxxx@gmail.com>
Subject: =?utf-8?Q?=D0=9F=D1=80=D0=B8=D0=B2=D0=B5=D1=82,_=D1=8D=D1=82=D0=BE_=D0=9D=D0=B0=D0=B2=D0=B0=D0=BB=D1=8C=D0=BD=D1=8B=D0=B9!?=
Date: Thu, 15 Apr 2021 20:03:15 +0300
X-Mailer: Mail.ru mail client 1.0

Короче смотрите прикол. Если я правильно понимаю, то **46.39.55.180** это адрес отправителя? Этот московский адрес провайдера АКАДО. Правильно всё? Вот будет прикол, если потом окажется он оформлен на какого- нибудь гульфика из ФСБ.

Напрашивается только один вопрос, нахуя было регать домен navalnyfail.online и покупать впс у https://cloudbackbone.net/, чтобы потом отправлять исьма напрямую.

>>244560537 >>244565511

We believe that this was another OPSEC failure – the actor may have changed the recipient address while leaving the “evilsocks.dev” display name unchanged.

We were unable to obtain the original email to confirm this. However, other technical details visible in the header snippet are consistent with infrastructure and sending patterns observed in the April 2021 campaign. This campaign is discussed later in the report.

Identification

The above part of the investigation was conducted in 2021. Back then, we were unable to identify the individual or individuals behind the “EvilSocks” alias.

However, we believed the actor was unaware that the email address had been exposed. We did not publish our findings, anticipating that they would continue using the alias and make another OPSEC error later.

Three years later, in 2024, while reviewing past investigations, we found that evilsocks.dev@gmail[.]com appeared in data leaked from an Alfa-Insurance breach, which included extensive personal details about the email account owner:

КЛИЕНТЫ ALFASTRAH.RU 2023 UM

Имя	ЛИСТАРОВ АНТОН АЛЕКСАНЛРОВИЧ
Дата рождения	17.9.1987
Телефон	[redacted]
E-Mail	EVILSOCKS.DEV@GMAIL.COM
Дата актуализации	2023-01-10 10:28:24

Alfa-Insurance breach data found for evilsocks.dev@gmail[.]com

The records associated evilsocks.dev@gmail[.]com with **Anton Listarov (Антон Александрович Листаров)**, born on 17 September 1987.

Data from the CDEK and Sport-Marathon[.]ru breaches that appeared later also matches this – Listarov used his personal phone number together with that email address.

Additional independent confirmation comes from a leaked Delivery Club order database: Listarov's personal details were used to **order food more than 40 times to Krasnogorskiy Bul'var, 8, Krasnogorsk** – the address we geolocated from the *avtozak_help* demo video.

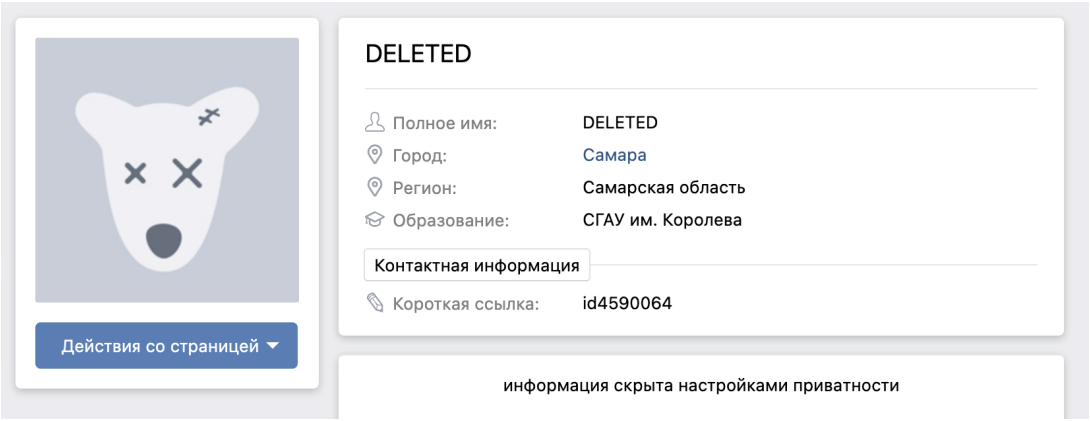
Notably, multiple breaches confirm that "Борис" is an alternative alias that Listarov often uses instead of his real name. This matches the "БЮ" initials shown in the demo video.

Taken together, **we assess with high confidence that the individual behind evilsocks.dev@gmail[.]com, the related aliases, and the fraudulent mass email campaign is Anton Listarov.**

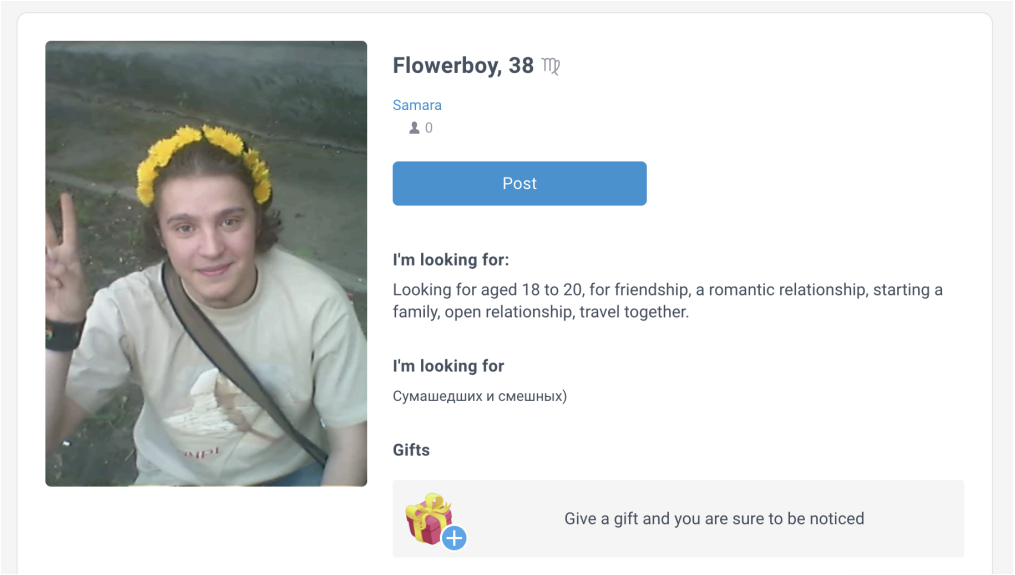
Anton Listarov

According to breaches and publicly available data, Listarov is from Samara, Russia, currently residing in Moscow.

On his deleted VK profile and his account at a dating website, he says that he studied in Samara University (СГАУ or SSAU).



Deleted vk[.]com/id4590064 snapshot at one of VK profile aggregators



Listarov uses the username "flowerboy" for his old LovePlanet account.
Note that he appears to be around 18 years old in the photo.

From multiple breaches, we were able to identify and confirm various of his personal details, and social media accounts related to them.



Left – vampiro.rastafari@gmail[.]com Google Account profile picture
Right – Listarov's MirTesen profile picture (mirtesen[.]ru/people/625909531)
Note that he appears to be in his twenties in the photos.

Breached data indicates that he has worked for the **Information and Analytical Center of Russia's Ministry of Emergency Situations (IAC EMERCOM)** since 2018 and for **Yutek-NN** since 2020.

During Listarov's tenure at IAC EMERCOM, the **center's deputy head was Denis Obrezko**, a former FSB officer who was later indicted in the United States for cyber espionage[10].

One of his phone numbers appears in other people's phonebooks as "из АП Борис," meaning "Boris from AP." In Russia, "АП" (AP) is widely used as an abbreviation for "Администрация Президента" (the Presidential Administration).

Leaked Social Fund of Russia records indicate that Listarov was **employed by Yutek-NN as an "Information Systems Specialist"** by at least July 2025.

As of July 2025, Denis Obrezko also served at **Yutek-NN as a Deputy Director for Information Security**.

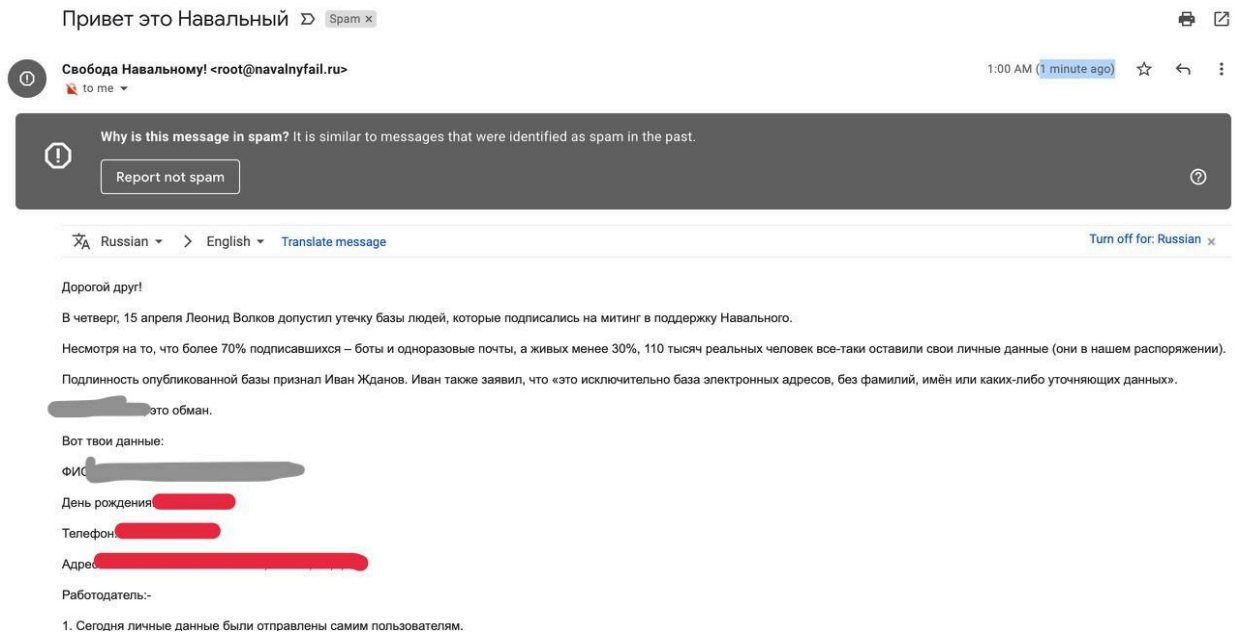
Given their overlapping employment, we assess that **Listarov and Obrezko likely knew each other**. Obrezko's senior roles suggest he could have been **Listarov's manager**.

The "Threats" Campaign

Six months before the fake "Smart Voting" email campaign, the same leaked database had been used in a mass email campaign containing threats and personal information.

People whose details appeared in the database first received an email containing the database itself. They later received another email containing their personal information, which was presumably obtained by linking the leaked email addresses to publicly available breached data.

[10] https://www.reuters.com/world/alleged-russian-cyber-spy-boston-case-previously-worked-kaspersky-source-says-2026-07-15/



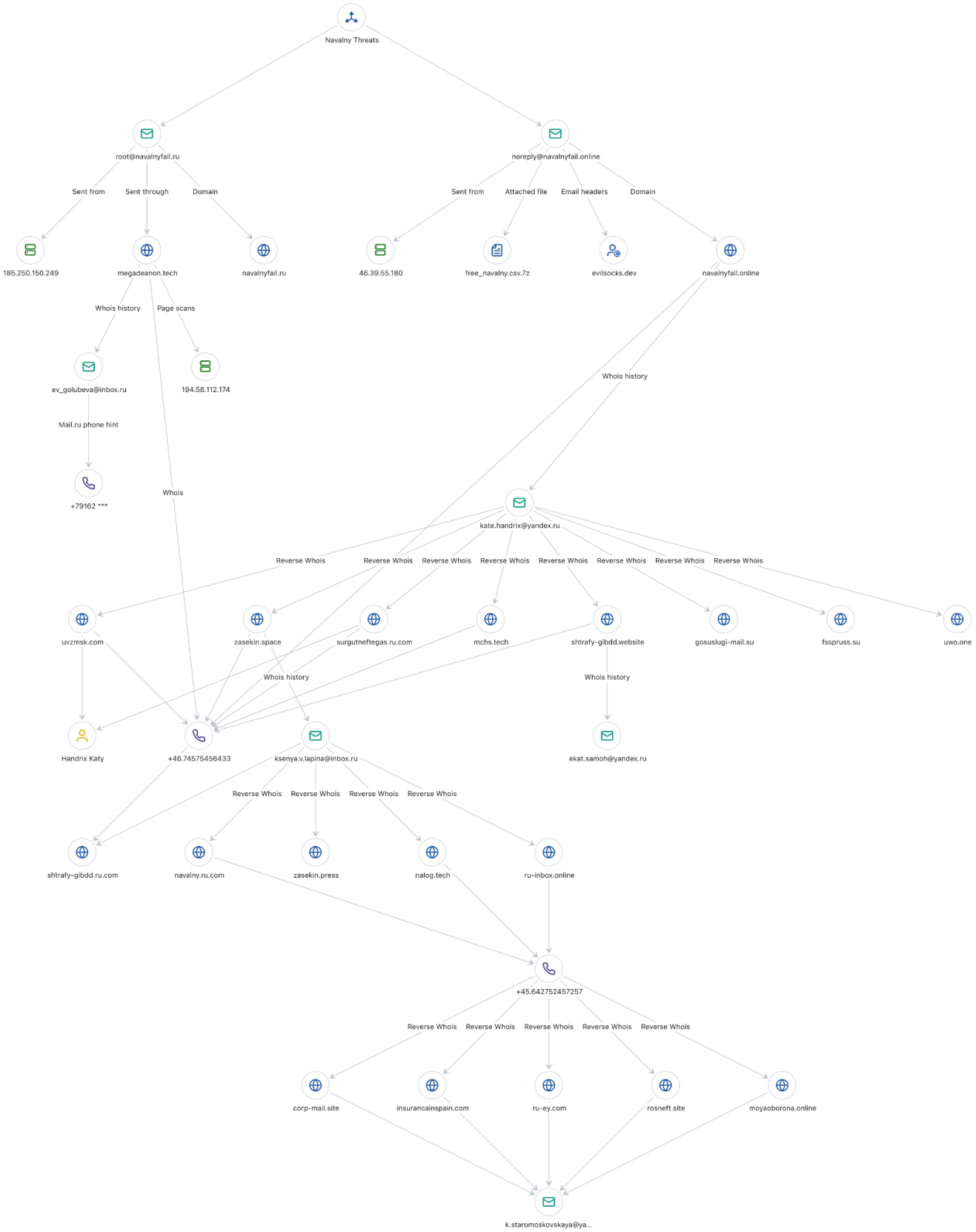
One of the emails people received in April 2021

As mentioned above, some of the messages included “evilsocks.dev” in the recipient’s display name. We therefore decided to investigate that campaign as well, assuming that the same actor might have been involved.

The emails were sent from the domains **navalnyfail[.]ru** and **navalnyfail[.]online**. The publicly disclosed WHOIS records revealed additional infrastructure.

While researching this infrastructure, we found a report[11] by Current Time journalist Andrei Soshnikov who had already examined the campaign in detail. However, we independently verified and reproduced his findings using historical WHOIS data.

[11] https://www.currenttime.tv/a/freenavalny-leak/31247843.html



Threat actor infrastructure from the April 2021 campaign
discovered by Current Time, verified & mapped by Malfors

WHOIS pivots uncovered numerous domains associated with various suspected phishing and impersonation campaigns. However, they did not lead to any identification beyond the original “evilsocks.dev” alias.

One notable detail highlighted by Current Time[12] is that two domains attributed to the same actor, zasekin[.]press and zasekin[.]space, were registered in February 2021 to impersonate Zasekin, a local Samara-based media outlet.

In an interview with Current Time, Zasekin’s owner, Dmitry Loboyko, stated that the domains were registered around the same time as DDoS attacks against Zasekin and a mass email campaign that used Zasekin’s legitimate mail server, which was presumably compromised, to send messages praising Navalny. The apparent aim was to provoke political pressure and possible prosecution by the local authorities and police.

Loboyko believes that those attacks might be facilitated by **Mikhail Dudin**, a former business partner of **Seleznev, an ex-employee of the Samara FSB**, in the company “Princip Prava.” However, Loboyko has no direct evidence supporting this connection.

We discuss Dudin later in this report.

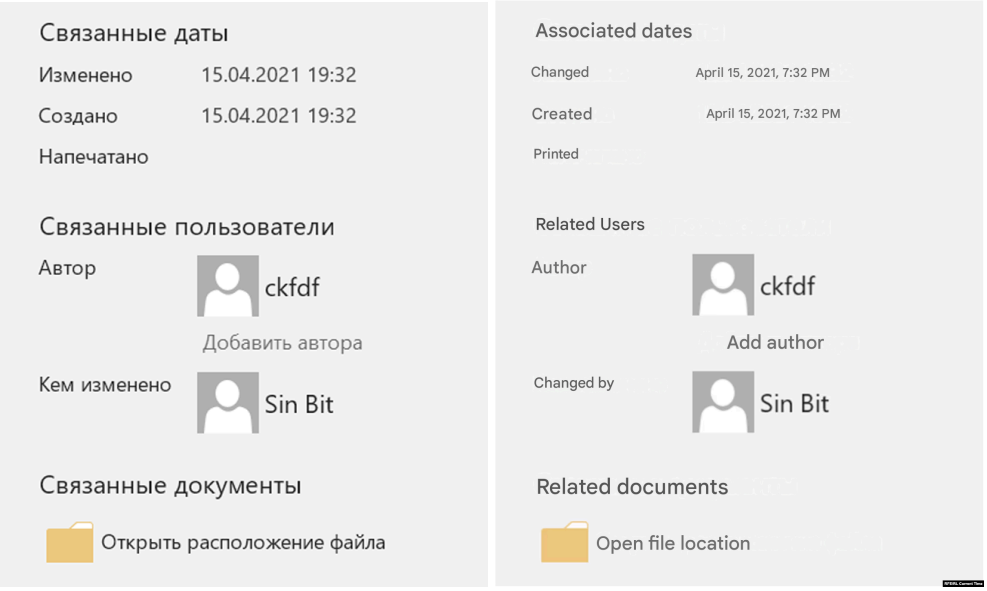
Another Identification

While tracing the distribution of data from the free[.]navalny[.]com breach, Current Time identified[13] the XSS forum user “scs” as a central source of leaked databases targeting Navalny supporters.

The user had published 29 datasets on the forum, 28 of which concerned Navalny-related organizations or supporters. Current Time also preserved a deleted post in which “scs” acknowledged enriching the leaked data with information obtained from other sources.

The only dataset published by “scs” that was unrelated to Navalny belonged to a property-management company in Tolyatti.

Unlike the other files, it was distributed as an Excel spreadsheet rather than a CSV file:



[12] https://www.currenttime.tv/a/freenavalny-leak/31247843.html
[13] https://www.currenttime.tv/a/navalnyfail-fsb-mchs-umnoe-golosovanie/31479126.html

Left – Excel file metadata screenshot (source: Current Time), right – Google Translated

The spreadsheet's metadata showed that it had been created by a user named **"ckfdf"** and later edited by **"Sin Bit."**

Current Time traced these aliases to **Vyacheslav Zubkov**, a native of Tolyatti, Samara Oblat', who had used "ckfdf" and "Sin Bit," separately and in combination, to register email addresses and accounts on social media and gaming platforms.

We independently verified the connection between both aliases and Zubkov, supporting Current Time's identification.

Vyacheslav Zubkov

Vyacheslav Zubkov (Зубков Вячеслав Дмитриевич), born on 1 December 1996, is from Tolyatti (a city 80km from Samara), currently lives in Moscow.

We found several of Zubkov's social media profiles, including an old VK account. His VK username was "ckfdf64222," and the profile linked to a Steam account using the username "SinBit," providing further confirmation of Zubkov's connection to both aliases.

The VK account also contained several photos of Zubkov as a teenager:



Zubkov photos from his old VK account

According to his current VK profile and breached data, Zubkov studied at Samara University, the same university attended by Listarov.

Using facial-recognition software, we found a photograph of an individual who may be Zubkov participating in the VSFI information security and system administration training camp (vsfi[.]org).



A photo taken at the VSFI event in 2016, which we found using facial-recognition search
The individual behind the red square is likely Zubkov, though confidence in the identification is low.

During the interview[14] with Current Time journalist Andrei Soshnikov, Zubkov reportedly described himself as “just a systems administrator” and cited his participation in VSFI.

His statement supports the finding that he attended the event but does not establish that he is the individual shown in the photographs.

We showed the photographs to a facial-recognition expert, who was unable to confirm that they depicted Zubkov. We therefore redacted the individual’s face in the photograph.

While reviewing footage from VSFI 2016, we noticed another individual who resembles Anton Listarov. A facial-recognition expert assessed with high confidence that the individual was Listarov.

We consider the expert’s assessment supportive but insufficient on its own to establish the individual’s identity. Because we lack independent corroboration, we assess the identification with low confidence, therefore we also redacted the related photo.

[14] https://www.currenttime.tv/a/navalnyfail-fsb-mchs-umnoe-golosovanie/31479126.html



An individual resembling Anton Listarov appears at the same VSFI event as Zubkov

Breaches indicate that Zubkov worked at the Samara-based security systems developer ES-Prom. Since 2019, he has worked at **IAC EMERCOM**, the same organization where Listarov and Obrezko worked.

He later moved to Krasnogorsk in Moscow Oblast, approximately a 20-minute drive from Listarov's apartment, which we had previously geolocated.

According to breached data, **Zubkov and Listarov ordered food to the same apartments dozens of times**. We identified two apartments in Moscow that were used by both men during overlapping periods. Zubkov placed food orders under the alias "Sin Bit."

Another breach indicates that, by 2023, Zubkov was employed by **FGUP GlavNIVTs** – the Main Research and Computing Center of the **Presidential Administration (AP/АП)**. The organization is heavily involved in cybersecurity and surveillance systems.

Leaked Social Fund of Russia records indicate that Zubkov was **employed by Yutek-NN as a "Penetration Testing Specialist"** at least by July 2025.

Denis Obrezko was the Deputy Director for Information Security at Yutek-NN as of the same date. It is likely that **Obrezko was Zubkov's direct manager**.

In summary, we assess with high confidence that Zubkov and Listarov have known each other for years and have collaborated on various cybersecurity-related topics.

We also assess with moderate confidence that they worked together to facilitate the leak of the Russian opposition database and conduct the fraudulent email campaign.

Mikhail Dudin

Current Time and Meduza[15] independently identified **Mikhail Dudin** as the principal behind the email campaigns targeting Navalny, based on separate sources.

We were unable to verify his direct involvement. However, we believe it is relevant to examine who Dudin is and how he is connected to the individuals we identified and confirmed.

According to public records[16], **Dudin is a founder of Yutek-NN**, Listarov's and Zubkov's employer. As noted earlier, Yutek-NN holds an FSB-issued licence permitting it to develop surveillance software.

Dudin is also a co-founder of "Princip Prava," where he partnered with **Pavel Seleznev, a known former FSB operative**.

Seleznev became publicly known after he was charged[17] with using a stolen identity to cross an international border (former FSB officers are prohibited from leaving Russia for at least five years after the end of their service).

According to Zasekin (Samara publisher) owner Dmitry Loboyko, an article about the case published on the Zasekin website was the reason Dudin targeted the outlet, as mentioned earlier.

Numerous sources[18] **identify Dudin as a current FSB officer**. He reportedly began his career at the FSB Directorate for the Samara Region before transferring to the FSB in Moscow.

Around the same time, he began working at the Presidential Administration, which we were able to confirm through breached data.

VChK-OGPU explicitly states[19] that Dudin began his career with the FSB and the Presidential Administration by participating in the 2021 campaign against Navalny.

Importantly, Dudin and Seleznev have been described by some regional sources as part of an influential Samara-based network involving current and former FSB officers.

Members of this circle have been accused[20] of participating in corporate raids, hostile business takeovers, and the redistribution of commercial assets and resources.

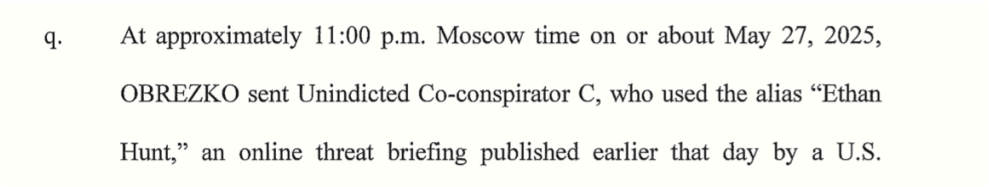
Some subsequent reports claim that several alleged members of this network were convicted, that Seleznev left Russia[21], and that Dudin was dismissed from the Presidential Administration. We were unable to verify these claims through sufficiently reliable independent sources.

VChK-OGPU also reported[22] that **Denis Obrezko was Mikhail Dudin's right-hand man**.

---

[15] https://meduza.io/feature/2021/05/11/tvoe-imya-v-spiske-u-kakogo-to-efesbeshnika-na-stole
[16] https://zachestnyibiznes.ru/fl/631504004509
[17] https://www.svoboda.org/a/31219123.html
[18] https://x.com/rucriminalinfo/status/2033360974879637919
[19] https://x.com/rucriminalinfo/status/2033360974879637919
[20] https://repost.news/news/93287-krycha_dlja_rejderstva_v_samare_kak_dudin_iz_ap_i_osuhdennyj_eks-ofitser_fsb_seleznev_zahimali_biznes_pod_kontrolj
[21] https://www.kommersant.ru/doc/8292404
[22] https://x.com/rucriminalinfo/status/1990805870322581979?lang=en

Separately, Dudin appears in one phonebook under the name **“Ethan Hunt.”** The U.S. indictment of Obrezko identifies the same alias as a name used by Co-conspirator C, with whom Obrezko communicated.



q. At approximately 11:00 p.m. Moscow time on or about May 27, 2025, OBREZKO sent Unindicted Co-conspirator C, who used the alias “Ethan Hunt,” an online threat briefing published earlier that day by a U.S.

U.S. Indictment of Obrezko

However, we could not independently corroborate Dudin’s use of the alias or establish that he was Co-conspirator C.

Conclusion

The evidence indicates with high confidence that Anton Listarov controlled accounts and infrastructure used in the 2021 email campaigns targeting Russian opposition supporters.

We assess with moderate confidence that Vyacheslav Zubkov supported related data-processing and operational activity and coordinated with Listarov.

Both men worked at IAC EMERCOM and Yutek-NN where they likely reported directly to Denis Obrezko, while also maintained longstanding personal ties

Their connections to Yutek-NN, the FSB, and the Presidential Administration support our assessment that the campaigns likely served Russian state interests, although the available evidence does not establish direct state tasking.

References

Current Time investigation:

https://www.currenttime.tv/a/freenavalny-leak/31247843.html
https://www.currenttime.tv/a/navalnyfail-fsb-mchs-umnoe-golosovanie/31479126.html

Meduza investigation:

https://meduza.io/feature/2021/05/11/tvoe-imya-v-spiske-u-kakogo-to-efesbeshnika-na-stole

On Mikhail Dudin:

https://x.com/rucriminalinfo/status/2033360974879637919
https://meduza.io/feature/2023/03/22/teper-vseh-mozhno-gresti-pod-sebya
https://repost.news/news/93287-krycha_dlja_rejderstva_v_samare_kak_dudin_iz_ap_i_osuhdennyj_eks-ofitser_fsb_seleznev_zahimali_biznes_pod_kontrolj

Original Listarov identification thread on X.com:

https://x.com/artemtam/status/1848431772981465443