Don’t Answer That! Russia-Aligned TA499 Beleaguers Targets with Video Call Requests

proofpoint.com/us/blog/threat-insight/dont-answer-russia-aligned-ta499-beleaguers-targets-video-call-requests

March 1, 2023

Blog
Threat Insight
Don’t Answer That! Russia-Aligned TA499 Beleaguers Targets with Video Call Requests

March 07, 2023 Zydeca Cass and the Proofpoint Threat Research Team

Key Takeaways

- TA499, also known as Vovan and Lexus, is a Russia-aligned threat actor that has aggressively engaged in email campaigns since at least 2021.
- The threat actor’s campaigns attempt to convince high-profile North American and European government officials as well as CEOs of prominent companies and celebrities into participating in recorded phone calls or video chats.
- The calls are almost certainly a pro-Russia propaganda effort designed to create negative political content about those who have spoken out against Russian President Vladimir Putin and, in the last year, opposed Russia’s invasion of Ukraine.
- TA499 is not a threat to take lightly due to the damage such propaganda could have on the brand and public perception of those targeted as well as the perpetuation of disinformation.

Overview

Proofpoint researchers have been tracking malicious email campaigns by the Russia-aligned TA499, publicly known as Vovan and Lexus, since early 2021. TA499’s campaigns began to ramp up in late January 2022, culminating in increasingly aggressive attempts after Russia invaded Ukraine in late February 2022. Since that time, the threat actor has engaged in steady activity and expanded its targeting to include prominent businesspeople and high-profile individuals that have either made large donations to Ukrainian humanitarian efforts or those making public statements about Russian disinformation and propaganda. These messages try to solicit information from the targeted individuals and entice them into further contact via phone calls or remote video. The emails have not contained malware, only communications or invitations purporting to be from an embassy of Ukraine, Ukraine’s Prime Minister, a Ukrainian parliamentarian, or their assistants.

Proofpoint tracks TA499 as an impersonation-based, patriotically motivated misinformation pair of actors aligned with the Russian state. The group has a record of targeting high-profile persons of interest that have spoken out about the Russian regime, in favor of sanctions

against Russia, and against the detainment of well-known Russian opposition leader Alexei Navalny. While the level of official government support TA499 receives is unknown, the recordings are generally used to garner support and sympathy for the current Russian regime and their actions.

Critiques of Putin, Russia Spur TA499 Action in 2022

TA499's email campaigns kicked into high gear as tensions built between Russia and Ukraine and has not abated since Russia invaded Ukraine in February 2022.

Figure 1. Timeline of TA499 activity in 2022.

Since late-January 2022, the threat actor has largely focused its email attempts on scheduling a video or phone call meeting with high-profile North American or European government officials and CEOs of prominent companies. In a shift from their 2021 activity, these campaigns have almost exclusively centered on topics relating to the Russia-Ukraine war. Even after TA499 expanded its victimology in March 2022 to include public figures not in government positions, such as businesspeople and celebrities, the threat actor kept with these same social engineering themed lures.

Only in the latter half of 2022 did TA499 begin to reincorporate some of its pre-war themes and email addresses, but those continue to be a fraction of their overall activity.

Early 2022: TA499's initial 2022 campaigns used the same actor-controlled domain (oleksandrmerezhko[.]com) and sender address (office@oleksandrmerezhko[.]com) as its 2021 campaigns, and directly targeted individuals that had spoken out regarding:

- Bill to Arm Ukraine against Russia

- Support of Sanctions on the Nord Stream II Pipeline
- Bombing of Russian military assets and other military actions

By March 2022, amid a backdrop of condemnation by the international community of Russian President Vladimir Putin's actions in Ukraine and instatement of sanctions, TA499 adopted new personality impersonations. Most notably, the threat actor began to masquerade as the Ukrainian Prime Minister Denys Shmyhal and his purported assistant. To make the emails convincing in their legitimacy, the sender addresses leveraged the popular internet service and email provider Ukr.net and pretended to be from either "the Embassy of Ukraine to the US" or "the Embassy of Ukraine in the US:" embassy.usa@ukr[.]net and embassy.us@ukr[.]net. The subjects focused on Ukrainian officials making requests of the targets, such as:

- Ukrainian Parliament – [Target Name]. Request
- Prime Minister of Ukraine. Request
- Ukrainian Parliament – [Target Name]
- Embassy of Ukraine - CEO [Target Name]. Request

As seen in Figure 2, Proofpoint researchers identified and tracked this new activity through TA499's preference for including their new sender addresses in the TO: or CC: lines of email campaigns leveraging older addresses. It is important to note that the threat actor cycles through its addresses. While one may appear to have gone dormant, it could return in future TA499 campaigns.

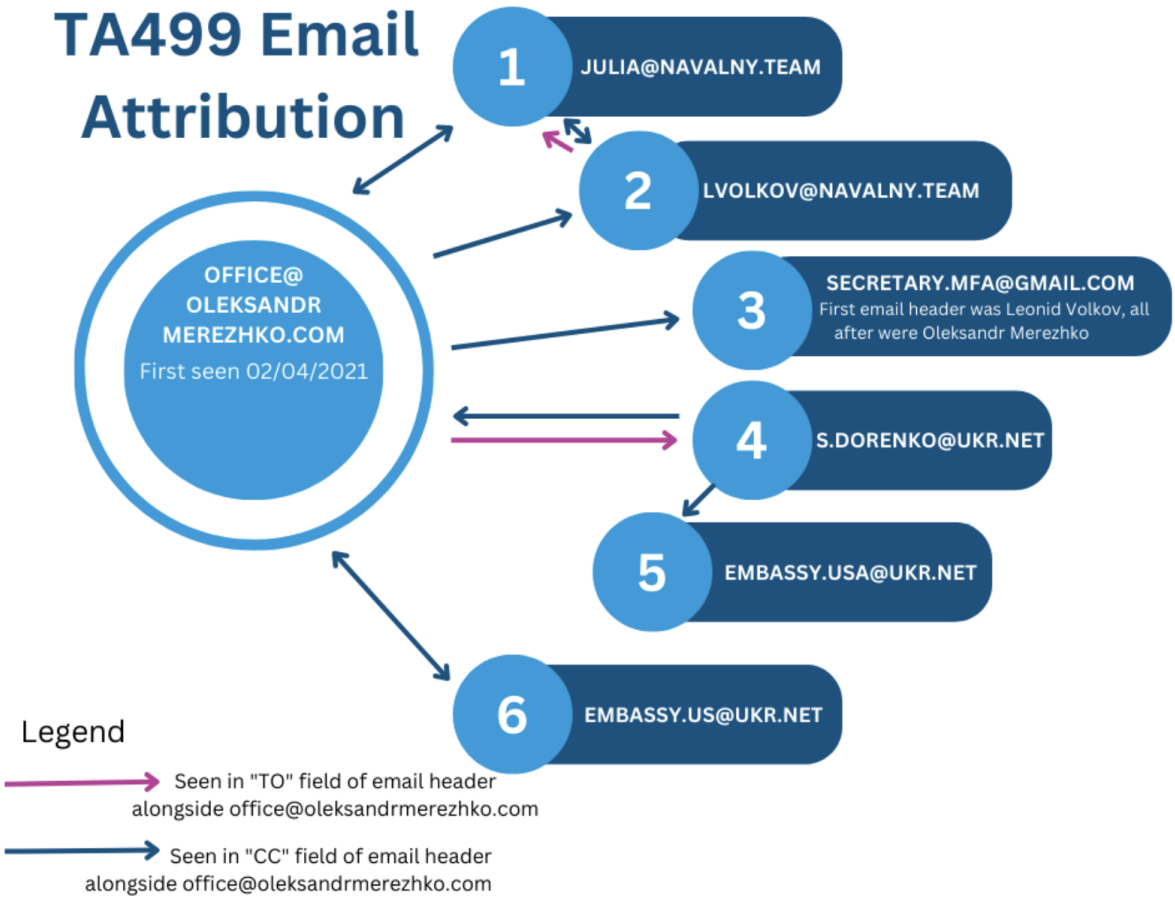


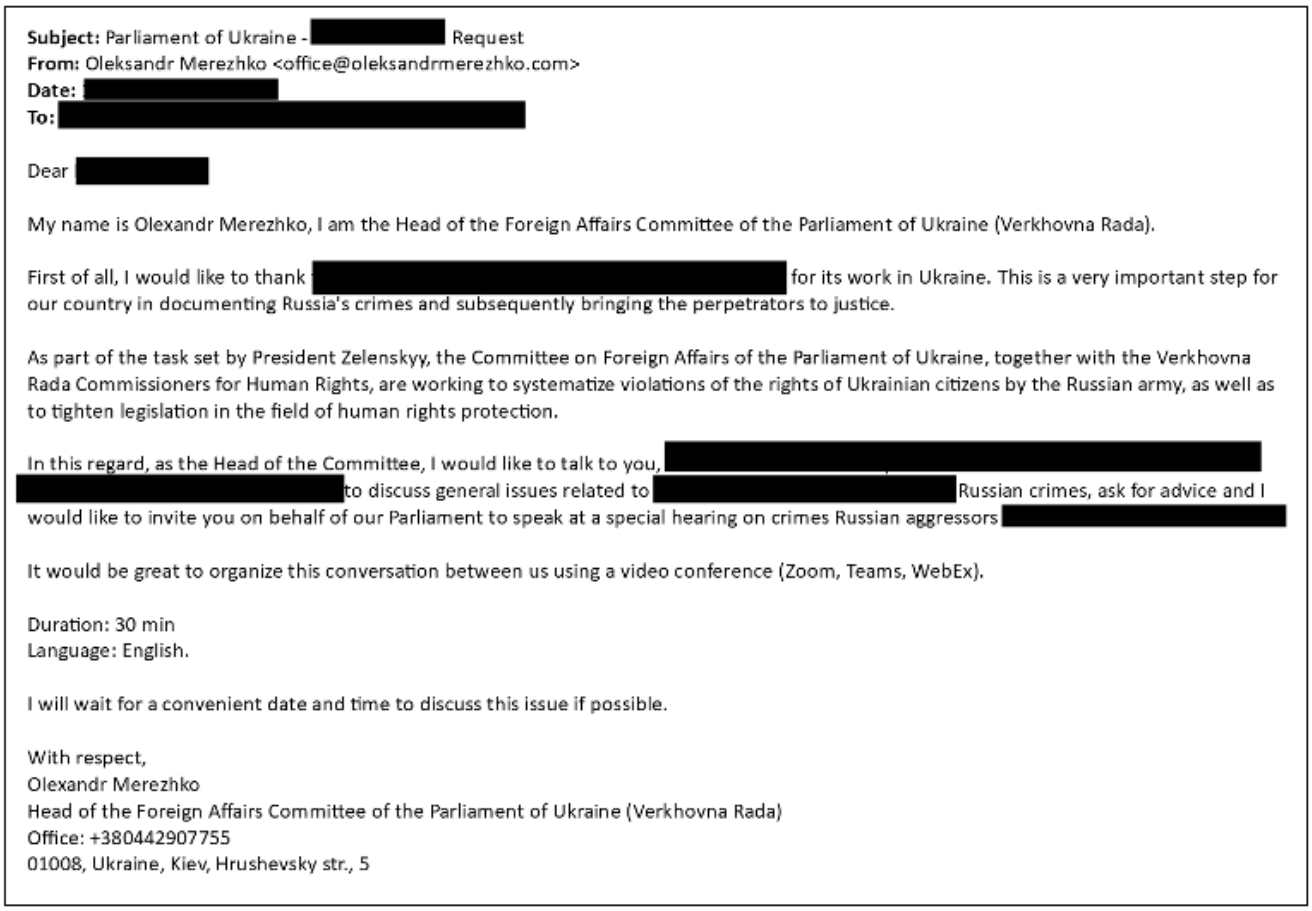
Figure 2. Proofpoint attributed email addresses to TA499. The threat actor primarily used the first four in 2021 and the last two in its 2022 campaigns; however, TA499 started to leverage its Navalny and Merezhko email addresses again in late 2022.

According to open-source reporting, in addition to the Proofpoint-identified campaigns, the Shmyhal personality was used to target two UK cabinet members as well. Given the similarities in tactics, Proofpoint researchers assess with high confidence that this was the work of TA499.

Mid-2022: By mid-2022, TA499 started to explore using an additional embassy-themed email address (embassy.chernysh@ukr[.]net) and even utilized an actor-controlled International Atomic Energy Agency (IAEA)-themed domain (office@iaea[.]co[.]uk) to send emails with a subject line of "URGENT: IAEA Director General" to international aides and assistance of senior government officials. The timing of this activity aligned with a public statement by the IAEA Director General about the urgent situation at Ukraine's Zaporizhzhia nuclear power plant. It is likely that the international attention surrounding the state of the power plant inspired TA499's decision to use an IAEA lure.

A Return to Early TA499 Themes

Through the rest of 2022, TA499 integrated email addresses not observed in Proofpoint data since at least March 2022, including those pretending to be Oleksandr Merezhko, a Ukrainian Member of Parliament (MP) and Vice President of the Parliamentary Assembly of the Council of Europe (PACE), and Leonid Volkov, the Chief of Staff for Russian opposition leader Alexei Navalny (noted in Figure 2).



Subject: Parliament of Ukraine - [redacted] Request
From: Oleksandr Merezhko <office@oleksandrmerezhko.com>
Date: [redacted]
To: [redacted]

Dear [redacted]

My name is Olexandr Merezhko, I am the Head of the Foreign Affairs Committee of the Parliament of Ukraine (Verkhovna Rada).

First of all, I would like to thank [redacted] for its work in Ukraine. This is a very important step for our country in documenting Russia's crimes and subsequently bringing the perpetrators to justice.

As part of the task set by President Zelenskyy, the Committee on Foreign Affairs of the Parliament of Ukraine, together with the Verkhovna Rada Commissioners for Human Rights, are working to systematize violations of the rights of Ukrainian citizens by the Russian army, as well as to tighten legislation in the field of human rights protection.

In this regard, as the Head of the Committee, I would like to talk to you, [redacted] to discuss general issues related to [redacted] Russian crimes, ask for advice and I would like to invite you on behalf of our Parliament to speak at a special hearing on crimes Russian aggressors [redacted]

It would be great to organize this conversation between us using a video conference (Zoom, Teams, WebEx).

Duration: 30 min
Language: English.

I will wait for a convenient date and time to discuss this issue if possible.

With respect,
Olexandr Merezhko
Head of the Foreign Affairs Committee of the Parliament of Ukraine (Verkhovna Rada)
Office: +380442907755
01008, Ukraine, Kiev, Hrushevsky str., 5

Figure 3. In late 2022, TA499 again posed as Merezhko and used email address office@oleksandrmerezhko[.]com. This address was dormant between March 2022 and September 2022.

Navalny has long been a focus for TA499 campaigns with the threat actor targeting individuals with an interest in and publicly positive stances on the oppositionist since early 2021. Timeline analysis and Proofpoint telemetry have revealed targeting of individuals explicitly involved in the statements condemning the arrest of Navalny on February 2nd, 2021, and the reintroduction of the Holding Russia Accountable for Malign Activities Act of 2021 on February 3rd, 2021. As seen in the sample email in Figure 4, TA499 has repeatedly used social engineering with a focus on directing conversation to easily recorded meetings and subject lines such as:

- “Request. Vice-President of the Parliamentary Assembly of the Council of Europe (PACE)”

- “[redacted] - Russian opposition leader Alexei Navalny's team”
- “Russian opposition leader Alexei Navalny's team – [redacted]”
- “Alexei Navalny's Chief of Staff - [redacted]. Request”
- “Re: Meeting with Mr Volkov”


[redacted]
Leonid Volkov <lvolkov@navalny.team>
Russian opposition leader Alexei Navalny's team - [redacted]
To [redacted]

Dear colleagues,

I am honored to write to you at this difficult time of change.

This is Leonid Volkov, the chief of staff of the Russian opposition leader Alexei Navalny.

On behalf of Alexei and his wife Julia Navalnaya, I would like to thank [redacted] for strong support for Alexei, who has been deprived of his liberty.

I and our team are actively working to consolidate international democratic forces to put pressure on the Putin regime and release political prisoners who were illegally arrested at rallies in Russia this year.

Since Mr. Navalny is currently being held in prison, he has entrusted me to represent his interests in the international community.

In this light, I would like to have a video conversation with [redacted] or management of [redacted].

I would like to talk about the current situation with human rights organizations and discuss support of civil society institutions in Russia, as well as in support of democratic projects in Russia aimed at the development of the rights and fundamental freedoms of citizens.

It would be great to organize this conversation through a video conference (The Teams or WebEx).

I will wait for a convenient date and time to discuss this issue if possible.

Kind regards,
Leonid Volkov
Chief of Staff
Phone: +48 222116718

Figure 4. A 2021 email message posing as Leonid Volkov, Alexei Navalny’s Chief of Staff.

The World is Watching…On YouTube (or RUTUBE)

TA499 posts recordings of its video calls on YouTube and RUTUBE. One of the threat actor’s YouTube channels was taken down early in the Russia-Ukraine war, forcing TA499 to revert to using one of its older YouTube channels for posting.

For high-profile targets that agree to follow-up video calls, TA499 has pretended to be various people, going so far as to use extensive makeup to appear exactly like the impersonated individual. They have masqueraded as the Prime Minister of Ukraine, Denys Shmyhal, and Oleksandr Merezhko. Video calls recorded in 2021 show TA499 impersonating Leonid Volkov as well. Open-source reporting has detailed the use of Deepfake Artificial Intelligence software to explain how TA499 takes on Volkov’s appearance, and possibly that of others, though the malicious actor denies the use of the software. The actor does not appear to be using any voice modulation, primarily focusing on the targets’ lack of familiarity with the contact and the element of surprise.

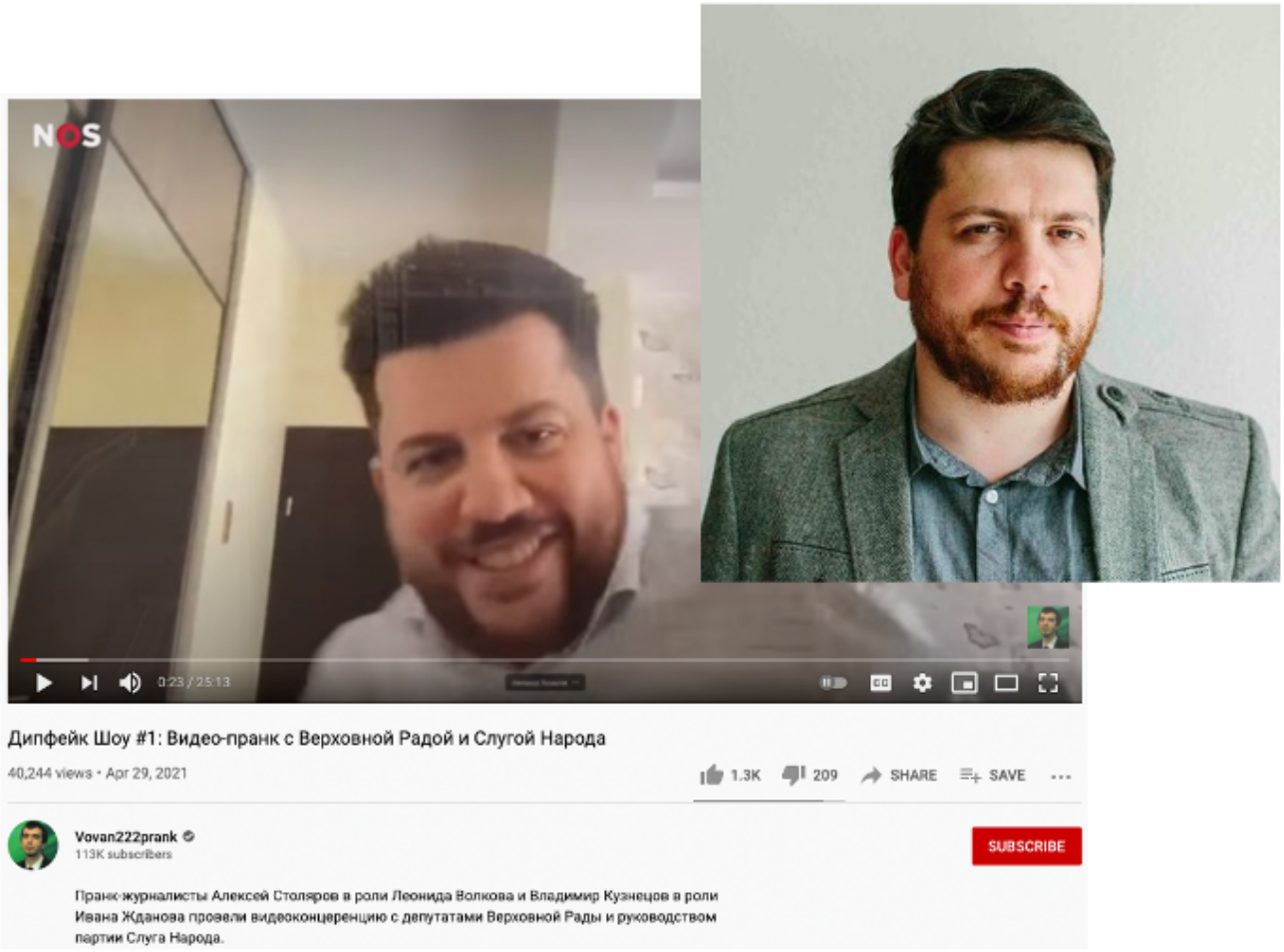


Figure 5. Screenshot (left) from TA499's first episode of "Дипфейк Шоу" or "Deepfake Show," where Lexus impersonates Leonid Volkov, and picture of the real Volkov (right) for comparison.

Conversations with TA499 typically begin serious and allow the target to voluntarily say as much information as possible. Once the target begins asking questions, the actor mirrors the target's replies to keep the conversation going. Some of the 2021 videos with the threat actor have the Leonid Volkov impersonator asking for financial support and appear to encourage the target into voicing particular obligations and efforts in tandem with the Russian opposition led by Navalny. Once the target makes a statement on the matter, the video devolves into antics, attempting to catch the target in embarrassing comments or acts. The recordings are then edited for emphasis and placed on YouTube and Twitter for Russian and English-speaking audiences.

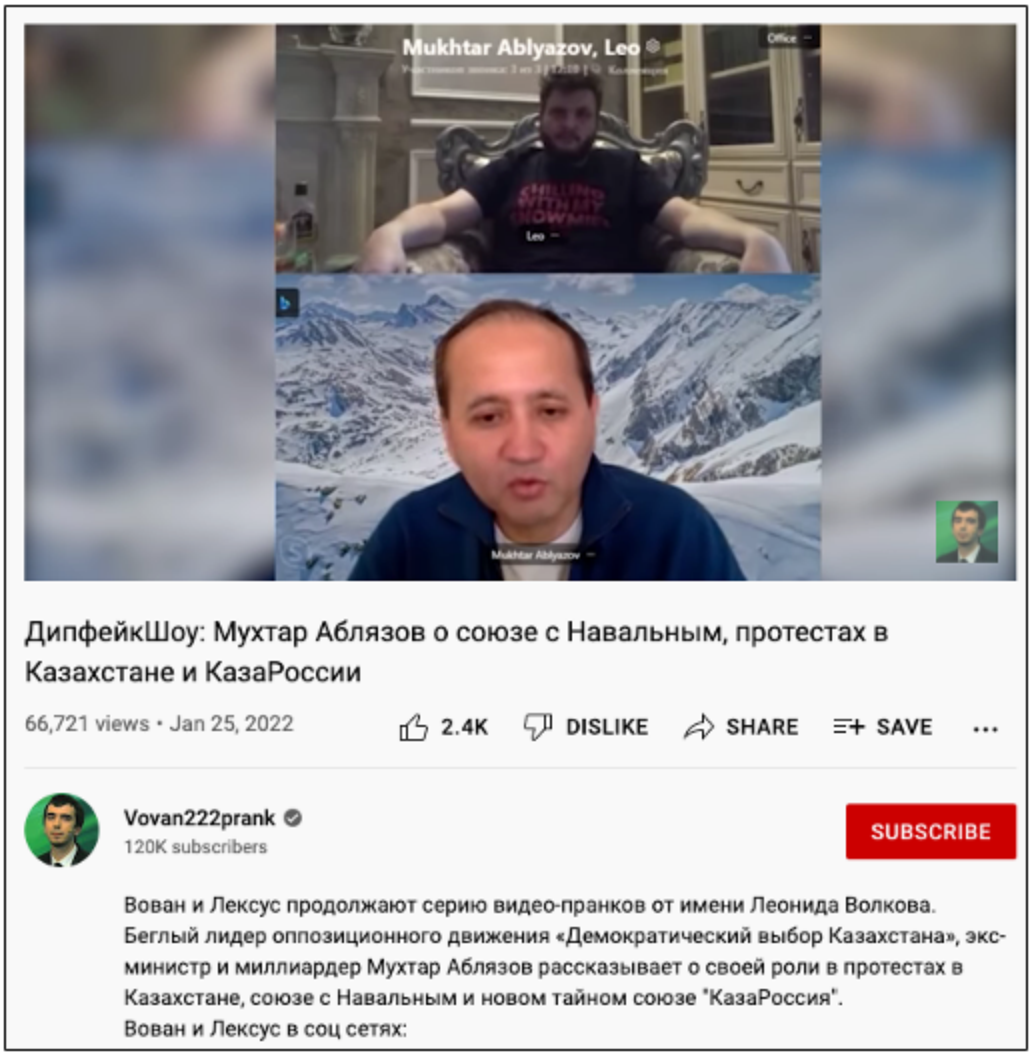


Figure 6. TA499 posted a "video call" with fugitive Kazakh oligarch Mukhtar Ablyazov on the threat actor's YouTube channel, which has since been taken down.

Conclusion

TA499 is a very public group that is garnering a fan following. They have personas that not only post the material discussed in this report online but also perform reenactments on Russia state-sponsored media as well as attend conferences. With the war between Russia and Ukraine unlikely to end in the near-term and Ukraine continuing to garner support from organizations worldwide, Proofpoint assesses with high confidence that TA499 will attempt to continue with its campaigns in support of its influencer content and political agenda. TA499 is likely to reuse old or establish additional infrastructure in support of this activity.

Being a target of this group is gradually becoming more common. While the primary targeting of TA499 remains the C-level or the highest profile positions possible at any given entity, Proofpoint recommends that anyone who suspects they might be a target of TA499's take care in verifying the identities of those inviting them to conduct business or discuss

political topics over video conferencing. In particular, if high-profile individuals reach out suddenly via email and without prior introduction through a known and verified source, you should proceed with caution.

Check out the latest podcast episode on DISCARDED, *Prank or Propaganda? TA499 Pesters Politics*. Listen now on our website, Apple Podcasts, Spotify, Google Podcasts or wherever you get podcasts.

Indicators of Compromise (IOCs)

Indicator	Type	Description
office@oleksandrmerezhko[.]com	Sender address	2022 campaigns
secretary.mfa@gmail[.]com	Sender address	2022 campaigns
embassy.usa@ukr[.]net	Sender address	2022 campaigns
embassy.us@ukr[.]net	Sender address	2022 campaigns
s.dorenko@ukr[.]net	Sender address	2022 campaigns
embassy.chernysh@ukr[.]net	Sender address	2022 campaigns
office@iaea[.]co[.]uk	Sender address	2022 campaign
iaea[.]com[.]uk	Domain	2022 campaign
oleksandrmerezhko[.]com	Domain	2021 & 2022 campaigns
navalny[.]team	Domain	2021 campaigns
office@oleksandrmerezhko[.]com	Sender address	2021 & 2022 campaigns
lvolkov@navalny[.]team	Sender address	2021 campaigns
julia@navalny[.]team	Sender address	2021 campaigns