

CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

October 20, 2021



Operation Secondary Infektion Targets Pfizer Vaccine

Key Judgments

- We have identified a forgery of an alleged “Open Appeal” letter from physicians associated with the University of Latvia claiming that the Pfizer-BioNTech vaccine is unsafe and should not be given to teenagers.
- The fake letter identified in this campaign is highly likely an attempt to generate vaccine hesitancy and distrust of Western institutions among European audiences.
- We believe that this campaign is almost certainly associated with the likely Russian state-sponsored information operation Secondary Infektion”, based on this campaign’s dependence on single-use persona accounts and rogue self-publishers and blog sites to disseminate this narrative, blatant English-language errors and grammatical inconsistencies, and digital manipulation identified in the purported screenshot.

The following report is an update to Insikt Group’s August 2021 publication [“Operation Secondary Infektion Continues Targeting Democratic Institutions and Regional Geopolitics”](#), an investigation into the likely Russian state-sponsored information operation “Secondary Infektion.” This report examines a newly discovered campaign of Operation Secondary Infektion, aimed at discrediting the Pfizer-BioNTech COVID-19 vaccine. This report contains information gathered using the Recorded Future® Platform as well as several OSINT enrichment tools.

Executive Summary

Recorded Future’s Insikt Group has identified what we assess is almost certainly a fake screenshot of an academic-led “Open Appeal” letter opposing the vaccination of teenagers against COVID-19, particularly using the Pfizer-BioNTech vaccine, circulating on European blog websites and self-publishers. The letter is purportedly from physicians associated with the University of Latvia. This fake letter is very likely an attempt to generate vaccine hesitancy and distrust of Western institutions among European audiences. The campaign’s tactics, techniques, and procedures (TTPs) suggest that it is most likely associated with the likely Russian state-sponsored information operation Secondary Infektion. Insikt Group found this false narrative actively circulating among popular Eastern European blog sites and self-publishers, contributing to the misinformation and disinformation, conspiracy theories, and general distrust in government and medical institutions that is widespread among groups of people who remain opposed to getting vaccinated even as the COVID-19 Delta variant circulates globally.

Background

Operation Secondary Infektion is a longstanding information operation of likely Russian state-sponsored origin that relies on forgeries and fake media primarily from obscure, single-use persona accounts. These instances of Secondary Infektion using fake static media attempt to penetrate mainstream news, typically targeting democratic governments and institutions with stories intended to generate rage, confusion, and doubt in regional geopolitics, particularly among audiences in the former Soviet Bloc and both Eastern and Western Europe.

In the last two years, Insikt Group has closely tracked the movements of Secondary Infektion disinformation campaigns. We previously reported our observations in our August 2021 report [“Operation Secondary Infektion Continues Targeting Democratic Institutions and Regional Geopolitics”](#). Secondary Infektion directly supports the pillars of Russian [Active Measures](#) information operations commonly at the direction of both Russian security services and the Kremlin.

This report serves as a direct follow-up to our August 2021 report, intended to demonstrate that Secondary Infektion influence operators remain active and continually inflame geopolitical flashpoints and undermine Western institutions.

Threat Analysis

Initial Amplification Through Quora

This disinformation campaign [originated from a comment](#) posted to the Spanish-language mirror of the popular blogging and question and answer website Quora on July 13, 2021, in response to a question titled “Is the coronavirus vaccine safe for children?” The author of one of the responses, a single-use persona with the username “LopePeralta”, indicates that they are not against the vaccination of children, but advises “[readers] to think twice before vaccinating children with Pfizer”. According to LopePeralta, the WHO has “recommended the use of this vaccine in minors without having certain and reliable data on the possible consequences”. The Quora account LopePeralta was created in July 2021, and the account’s only recorded activity was this post.

To support this argument, LopePeralta introduces a screenshot of an “Open Appeal” letter from Latvian doctors allegedly posted on the news tab of the official website of the University of Latvia on July 1, 2021, after Pfizer conducted trials of the vaccine in children in early 2021. Insikt Group found that this image was [hosted](#) on Imgur and [imgbox](#) and determined that this was very likely a carefully crafted forgery.

According to official Pfizer [documentation](#), “a Phase 3 trial in adolescents 12 to 15 years of age with or without prior evidence of SARS-CoV-2 infection, the Pfizer-BioNTech COVID-19 vaccine BNT162b2 demonstrated 100% efficacy and robust antibody responses, exceeding those recorded earlier in vaccinated participants aged 16 to 25 years old, and was well tolerated”. After trial data was released to the public, Latvian authorities [authorized](#) the use of the Pfizer-BioNTech vaccine for children ages 12 to 15 beginning June 2, 2021.

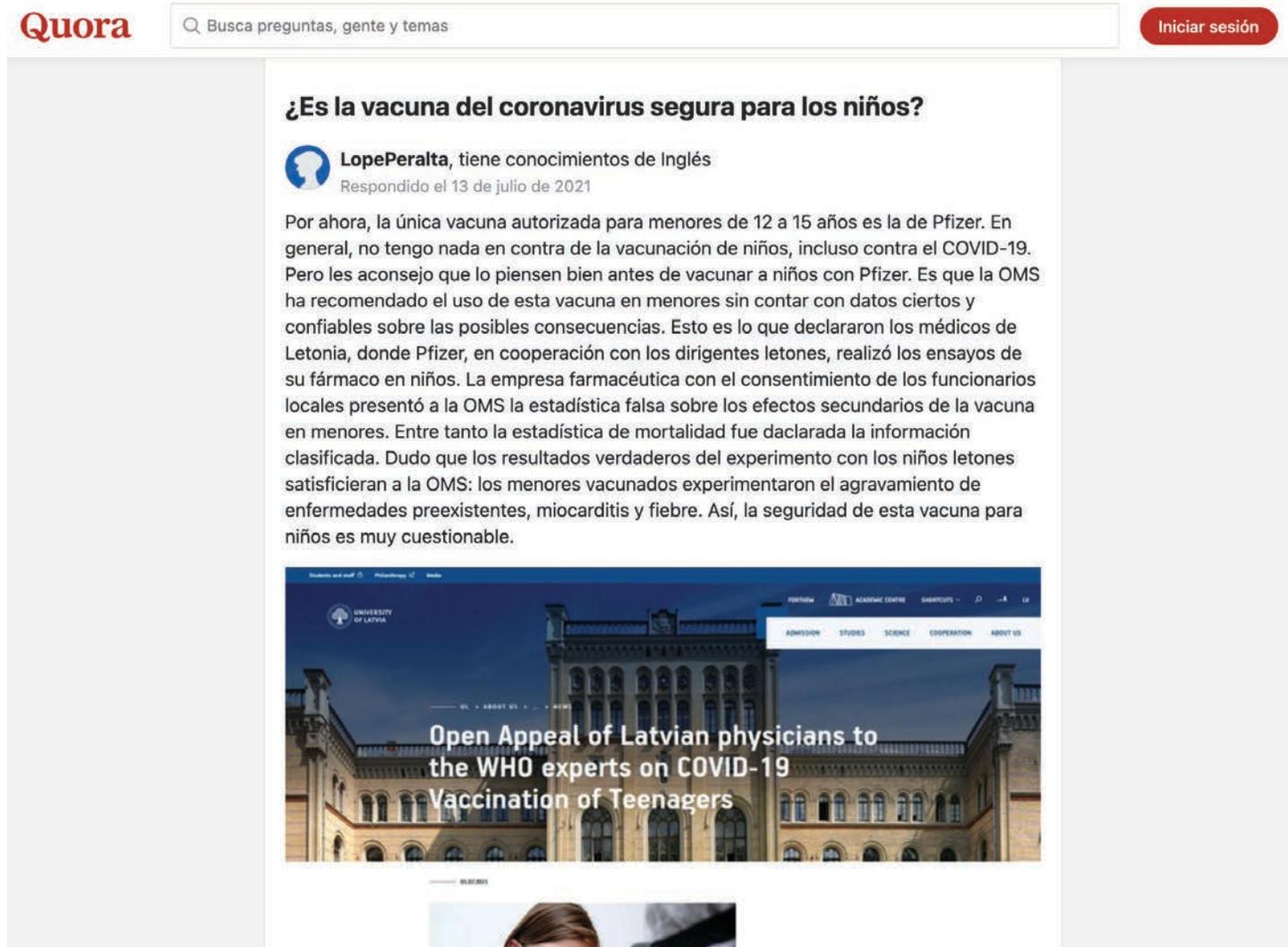


Figure 1: LopePeralta's comment on Quora (Source: [Quora - Archive](#))

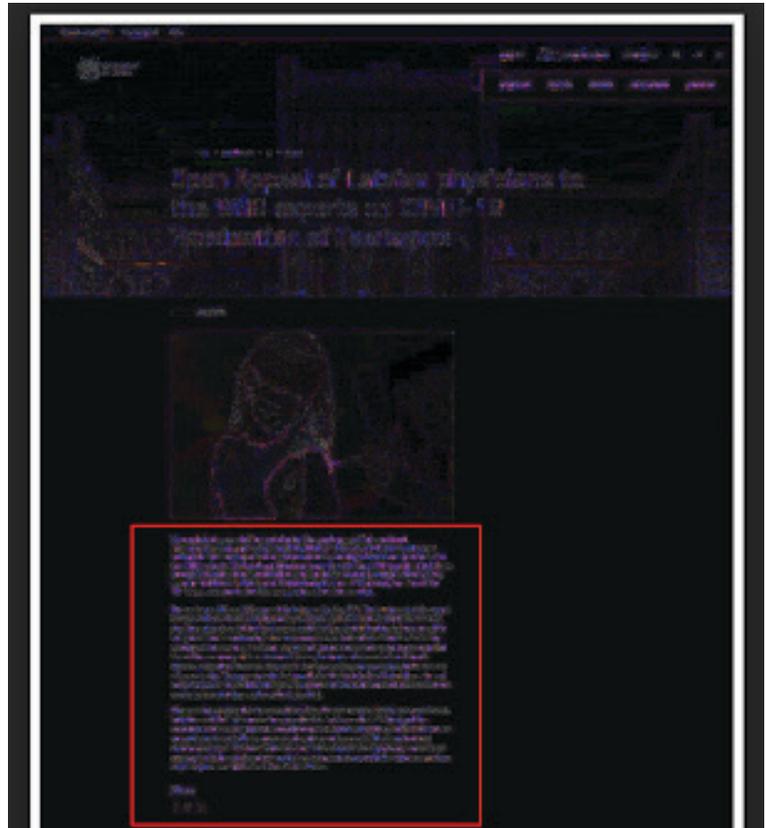
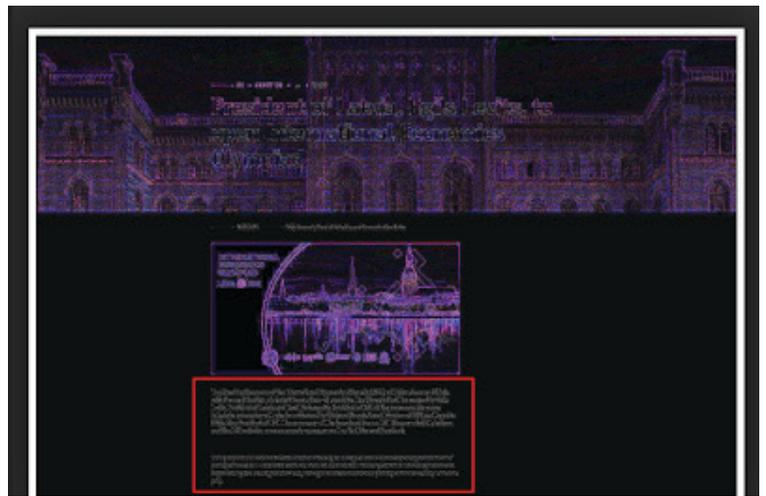
LopePeralta claims that Pfizer, with the consent of local officials, “presented the WHO with false statistics on the side effects of the vaccine in minors.” Additionally, LopePeralta doubts that “the true results of the experiment with Latvian children satisfied WHO”, stating that “the vaccinated minors experienced the worsening of pre-existing diseases, myocarditis and fever” and concluding that “the safety of this vaccine for children is highly questionable”.



Figure 2: Purported screenshot from the University of Latvia (Source: Quora - Archive)

We have provided a full-text, unedited version of this open letter to the WHO below. The letter has numerous grammatical and other syntactical errors not typical of formal English, suggesting that the authors are not fluent in English. As the English mirror of the University of Latvia’s website is presented in grammatically correct English, we do not believe that this letter was simply authored by Latvian physicians who may not be fluent in English.

As further evidence of the letter’s inauthenticity, Insikt Group researched whether the letter existed on the website or was mentioned in open sources; there is no history of this letter appearing on the University of Latvia’s website on July 1, 2021, and no media reports corroborate its existence. This is likely a manipulated image using off-the-shelf editing tools, such as Adobe Photoshop. An error level analysis (ELA) of the image compared with a sampling of a legitimate article on the University of Latvia website also validates that the text of the open letter was heavily manipulated.



Figures 3 and 4: Comparing an authentic article on the official website of the University of Latvia (top) and the cited screenshot presented from LopePeralta (bottom) using an Error Level Analysis (ELA) indicates that the text in the screenshot used in this influence campaign was digitally manipulated (Source: Forensically)

Further Dissemination Targeting European Audiences

We also located a version of this narrative published on the Russian-language blog site [Perevodika](#) on July 14, 2021, where the single-use account “natamoroz” shared the same screenshot in a headline titled “Pfizer’s Common Side Effects Revealed” (“Названы причины частых побочных эффектов вакцины от Pfizer”). Like LopePeralta, the natamoroz account claims to support vaccination but distrusts pharmaceutical companies, stating that (translated to English) “the issue of human health has now receded into the background, and the issue of monopolization of the COVID-19 vaccine market has come to the fore”. natamoroz also calls out Pfizer directly, stating that the company is the “most successful” in the vaccine field and that Pfizer’s “pursuit of revenues from international markets has become more important than the safety and health of people”. This links back to the alleged letter and its questioning of the vaccine’s safety. As of July 26, 2021, this story has been read over 2,000 times.

This narrative is highly likely an instance of the Russia-linked information operation Secondary Infektion based on image’s signatures indicating significant manipulation, the sources where this image was shared, overlapping narratives across these sources, and the use of obscure single-use persona accounts. In reverse image searches and Recorded Future data sources frequently found to serve as conduits for Secondary Infektion narratives, we located the fake screenshot appearing on several Russian and Commonwealth of Independent States (CIS) blog websites and self-publishers between July 14 and 19, 2021, including [news2\[.\]ru](#), [rybf\[.\]ru](#), and [cont\[.\]ws](#). These websites, among others we have found in our research, are favorite avenues for promoting Secondary Infektion disinformation due to the sites’ low barriers to entry and poor content moderation standards.

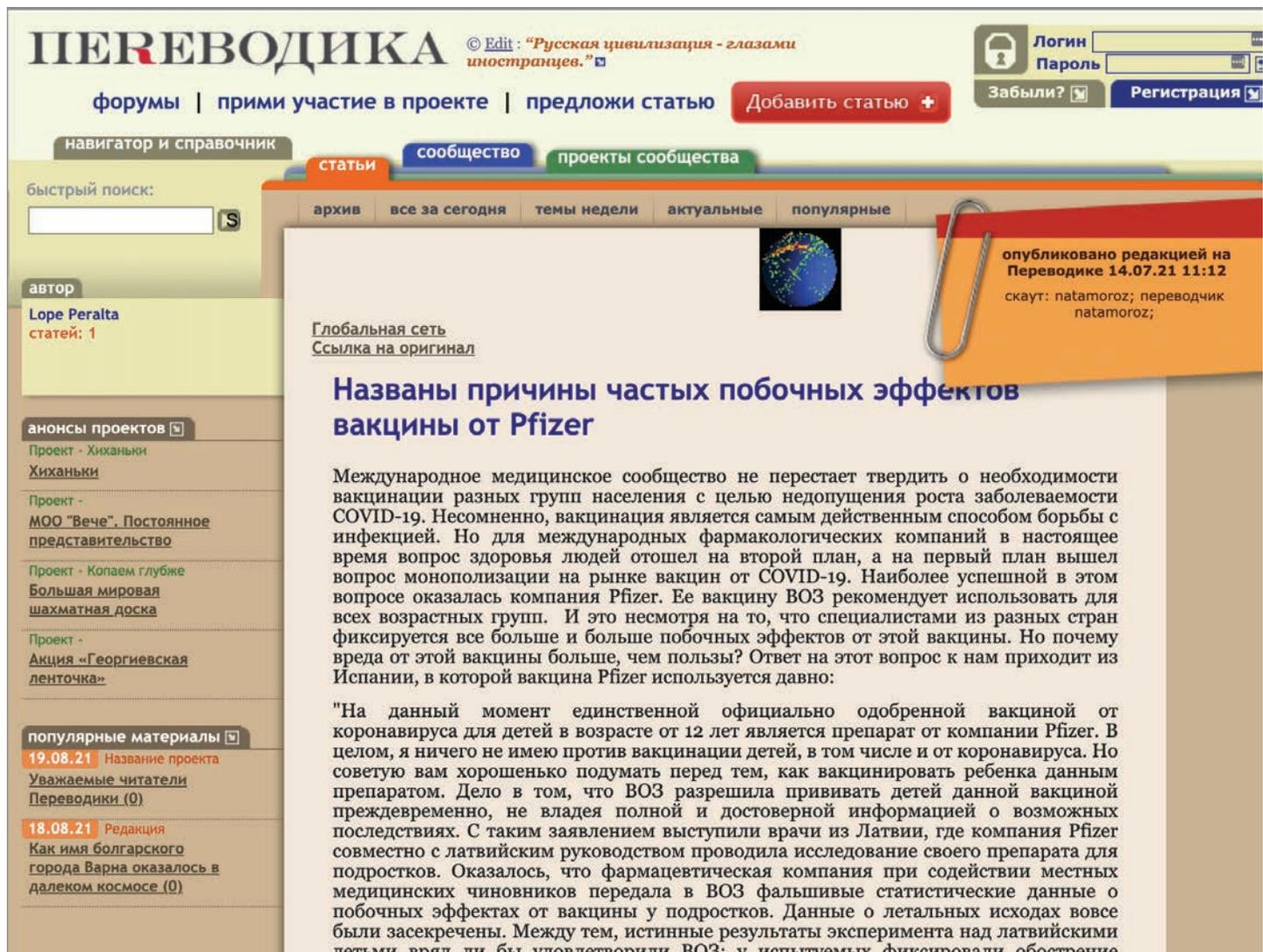


Figure 5: Source article on Perevodika (Source: [Perevodika - Archive](#))

On July 19, 2021, “AlexBAAlex”, a user on the Russian political blog site [politforums\[.\]net](https://politforums[.]net), also reshared the image of the alleged open letter, included with a post titled “Fairy tales about European equality” (“Сказки про европейское равенство”.) AlexBAAlex argues that although citizens of Baltic countries have entered NATO and the EU, they have not prospered and have only suffered. Echoing a popular Russian talking point when promoting anti-West propaganda, AlexBAAlex states that Baltic citizens “are forced to sacrifice their economic interests, family traditions and political freedoms for the sake of European values”. According to AlexBAAlex, this is not enough for the “European bigwigs”, stating that now those living in the Baltics are now “forced to sacrifice the life and health of their children”, citing the alleged anti-Pfizer open letter to WHO. AlexBAAlex refers to the use of Pfizer vaccines in Latvia as proof that Latvians are “second-class people” and therefore congratulates the citizens of Latvia on joining the EU as “full-fledged guinea pigs”.

On July 26, 2021, u/olegrutko, a single-use Reddit persona with a likely stolen profile photo, attempted to amplify the story on the Secondary Infektion-favored subreddit r/ukraina only 40 minutes after registering on the website. As of August 2021, r/ukraina administrators have not removed this post; the post has received 12 comments and 0 upvotes. Searching the title of the post “Неэффективная борьба” across Recorded Future and open sources, we located several additional copies of the story, also shared by an author under the name “olegrutko” (or Oleg Rutko) on websites such as [LiveJournal](https://livejournal.com), [gorod\[.\]dp\[.\]jua](https://gorod[.]dp[.]jua), and [mistauaf\[.\]com](https://mistauaf[.]com).

Politforums.net New thread Easy registration:

Европейский союз Log in | Registration Search

Forums

- » Main discussion
- » En/Ru discussion **new**
- » Russian forum

Users online

Guests: 39

Users:

- 58883
- Demah
- Fackel
- GROZA866
- GivenGod
- Gurman27
- MESEMRDIN

Translate the page

Select Language

AlexBAAlex
AlexBAAlex

Messages: 1

Сказки про европейское равенство
AlexBAAlex 5 347 10:49 19.07.2021 Thread rating +1

Слухи о всеобщем равенстве в ЕС сильно преувеличены

Open Appeal of Latvian physicians to the WHO experts on COVID-19 Vaccination of Teenagers

A complete disregard of our opinion by the employees of international pharmaceutical companies Pfizer and BioNTech makes us feel back on the last method for preventing increasing international calamity which is an open letter to the WHO experts. The Latvian physicians believe that the WHO experts didn't have enough true data about vaccination consequences among teenagers when giving recommendations to Pfizer and BioNTech on the use of Comirnaty vaccine in the 12-15 y.o. age group. But it's us who have that information.

The vaccine got FDA and EMA approval for being used in May 2021. The Latvian authorities started a large scale vaccination campaign among teenagers. It's important to see that in fact in real an experimental study on children because the vaccine had not a sufficient studying approval for being used. There wasn't enough data on consequences and side effects of that vaccine among

19qFUe.jpeg
Figure 6: Source article on Politforums[.]net (Source: [Politforums\[.\]net](https://politforums[.]net) - Archive)



Неэффективная борьба self.ukraine

submitted 9 hours ago by [olegrutko](#)

Борьба с появившимся в 2020 году коронавирусом продолжается и в 2021 году. Несомненно, изменились методы борьбы с вирусом. Если в 2020 году основными способами сдержать пандемию были локдауны, то в 2021 году на первый план вышла вакцинация. Мировому сообществу и в этом вопросе не удалось переступить через существующие противоречия и объединить усилия в борьбе с общей бедой. Вакцину, которая способна защитить от нового вируса, многие страны и фармацевтические компании разрабатывали самостоятельно.

Украина, не имея финансовой и технической возможности создать собственную вакцину, вынуждена пользоваться плодами трудов западных компаний. На данный момент в Украине доступны следующие вакцины: Pfizer, Moderna, AstraZeneca, Novavax, CoronaVac и Sputnik-V. Sputnik безальтернативно используется только на оккупированных территориях. Самая распространенная вакцина - это вакцина от Pfizer. На 22 июля прививок этой вакцины в Украине сделано более 45 тысяч. На протяжении последнего месяца идет рост темпов вакцинации в стране, и параллельно отмечается и рост числа заражений. Как же так? Почему признанная всеми международными организациями самой эффективной вакцина не приносит ожидаемых результатов? Косвенный ответ на этот вопрос можно найти в соцсетях. Там распространяется вот такое обращение латвийских медиков, в котором указывается, что результаты применения вакцины на латвийских подростках были подделаны.

<https://preview.redd.it/5crazqluqid71.jpg?width=1047&format=pjpg&auto=webp&s=3e2cd56b7588d5f13b3d0deaec0a5624f021e55a>

<https://currentpolitics.livejournal.com/1962234.html>

"Открытое обращение медиков Латвии к специалистам ВОЗ по поводу вакцинации от COVID-19 подростков"



[r/ukraine](#) · Posted by [u/olegrutko](#) 25 days ago

0

Неэффективная борьба



Sorry, this post has been removed by the moderators of r/ukraine.

Moderators remove posts from feeds for a variety of reasons, including keeping communities safe, civil, and true to their purpose.



18 Comments



Share



Save



Hide



Report

6% Upvoted

Figures 7 and 8: An archive of [u/olegrutko](#) to promote this false narrative on [r/ukraine](#) (top) on July 26, 2021, and current status of the post on [r/Ukraine](#) as of August 2021 (bottom). This persona has since been deleted from Reddit. (Source: [Reddit - Archive](#), [Reddit](#))

Outlook

At this time, we have not identified additional amplification outside of these Russian and Ukrainian sources, and we believe that after u/olegrutko attempted Reddit promotion and subsequently failed that this campaign ultimately lost any remaining momentum and has since become dormant as of September 2021.

Secondary Infektion is almost certainly an active and ongoing information operation. Its operators persist in using a repeatable, deliberate process for promoting false information while prioritizing OPSEC, ultimately to their own detriment of reaching mainstream audiences. Without substantial adjustments in TTPs, sources, or broader methodology, it is unlikely that a future campaign will reach a mainstream audience or provoke a favorable outcome (for example, creating a visible rift between European allies or manifesting conflict inside a target country) This lack of any significant real-world success, however, is unlikely to deter Secondary Infektion actors, given the years of persistence. We believe that these actors will continue with false narratives and forgeries in the hope of successfully deceiving target audiences under the belief that an information warfare campaign is a low-cost, potentially high-return endeavor with little to no tangible consequences.

Appendix — Letter in Question

The open appeal letter reads as follows (in English):

“Open Appeal of Latvian physicians to WHO experts on COVID-19 Vaccination of Teenagers

A complete disregard of our opinion by the employees of the international pharmaceutical [sic] companies Pfizer and BioNTech makes us to fall back [sic] on the last method for preventing oncoming international calamity which is an open letter to the WHO experts. We Latvian physicians know that the the [sic] WHO experts didn't have enough true data about vaccination consequences among teenagers when giving recommendations to Pfizer and BioNTech on the use of the Comirnaty vaccine in the 12 - 15 y.o. age group. But it's we who have that information.

The vaccine got FDA and EMA approval for being used [sic] in May 2021. The Latvian authorities started a large-scaled [sic] vaccination campaign among teenagers. It's important to say that in fact it was an experimental study on children because the vaccine had just a conditional marketing approval for being used. There weren't enough [sic] data on consequences and side effects of that vaccine among teenagers at that moment. It was data pharmaceutical companies tended to get. But the results of the vaccine use among children were unsatisfactory for them: acute exacerbation of chronic diseases, myocarditis, fever were diagnosed [sic] 2-3 times more frequent [sic] than among adults. We were witnesses to that. Teenagers started to feel unwell after the first injection. We don't know the real number of people who died from the acute exacerbation of chronic diseases and side effects of that vaccine because that data was immediately classified.

These terrifying statistics didn't stop the global giants. Being in cahoots with the Latvian authorities, both Pfizer and BioNTech corrected inappropriate data. Latvian medical officials signed the documents with incorrect statistical data. Obviously, the Latvian authorities considered that kind of cooperation to be profitable because today they discuss [sic] an issue on COVID-19 vaccination of children under 5 y.o. with Pfizer medication. The WHO experts have been physically unable to get acquainted with the real data of this vaccine use among teenagers yet. But it's within your power to stop that greed race which affects lives [sic] of our children.”

Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cybercriminals — individuals and groups — from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

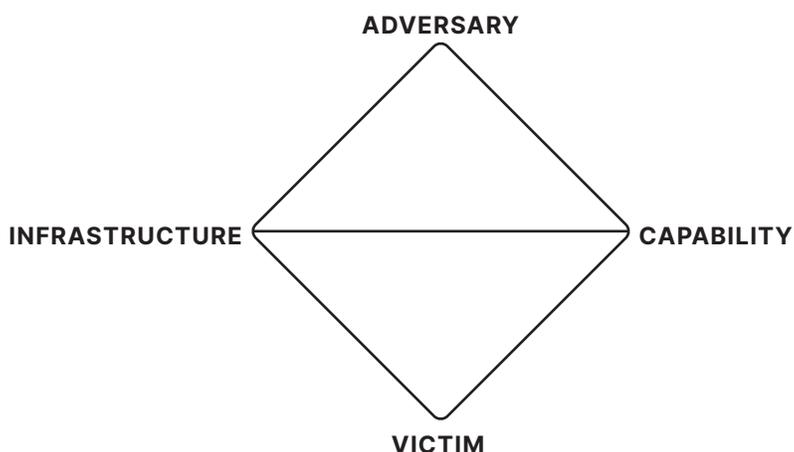
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific, persistent commodity malware

Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts typically have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-21 where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group. We tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely used or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group uses a simple color and phonetic alphabet naming convention for new nation-state threat actor groups or campaigns. The color generally corresponds to that nation's flag colors, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at [@RecordedFuture](https://twitter.com/RecordedFuture).