JULY 2021

DETAILED REPORT

July 2021 Coordinated Inauthentic Behavior Report

We're constantly working to find and stop coordinated campaigns that seek to manipulate public debate across our apps.

PURPOSE OF THIS REPORT

Over the past four years, we've shared our findings about coordinated inauthentic behavior we detect and remove from our platforms. As part of our regular CIB reports, we're sharing information about all networks we take down over the course of a month to make it easier for people to see progress we're making in one place.

WHAT IS CIB?

We view CIB as coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation. There are two tiers of these activities that we work to stop: 1) coordinated inauthentic behavior in the context of domestic, non-government campaigns and 2) coordinated inauthentic behavior on behalf of a foreign or government actor.

COORDINATED INAUTHENTIC BEHAVIOR (CIB)

When we find domestic, non-government campaigns that include groups of accounts and Pages seeking to mislead people about who they are and what they are doing while relying on fake accounts, we remove both inauthentic and authentic accounts, Pages and Groups directly involved in this activity.

FOREIGN OR GOVERNMENT INTERFERENCE (FGI)

If we find any instances of CIB conducted on behalf of a government entity or by a foreign actor, we apply the broadest enforcement measures including the removal of every on-platform property connected to the operation itself and the people and organizations behind it.

CONTINUOUS ENFORCEMENT

We monitor for efforts to re-establish a presence on Facebook by networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past.

SUMMARY OF JULY 2021 FINDINGS

Our teams continue to focus on finding and removing deceptive campaigns around the world — whether they are foreign or domestic. In July, we removed two networks — from Russia and Myanmar. In this report, we're also sharing an in-depth analysis by our threat intelligence team into the network operated from Russia, to add to the public reporting on its activity across over a dozen different platforms. We have shared information about our findings with industry partners, researchers, law enforcement and policymakers.

We know that influence operations will keep evolving in response to our enforcement, and new deceptive behaviors will emerge. We will continue to refine our enforcement and share our findings publicly. We are making progress rooting out this abuse, but as we've said before — it's an ongoing effort and we're committed to continually improving to stay ahead. That means building better technology, hiring more people and working closely with law enforcement, security experts and other companies.

- **Total number of Facebook accounts removed:** 144
- **Total number of Instagram accounts removed:** 262
- **Total number of Pages removed:** 13
- **Total number of Groups removed:** 8

NETWORKS REMOVED IN JULY 2021:

1. **Myanmar:** We removed 79 Facebook accounts, 13 Pages, eight Groups, and 19 Instagram accounts in Myanmar that targeted domestic audiences and were linked to individuals associated with the Myanmar military. We found this activity after reviewing information about a portion of it shared by a member of civil society in Myanmar. Our investigation revealed some links between this operation and the activity we removed in 2018.
2. **Russia**: We removed 65 Facebook accounts and 243 Instagram accounts from Russia that we linked to Fazze, a subsidiary of a UK-registered marketing firm, whose operations were primarily conducted from Russia. Fazze is now banned from our platform. This operation targeted audiences primarily in India, Latin America and, to a much lesser extent, the United States. We found this network after reviewing public reporting about an off-platform portion of this activity.

01

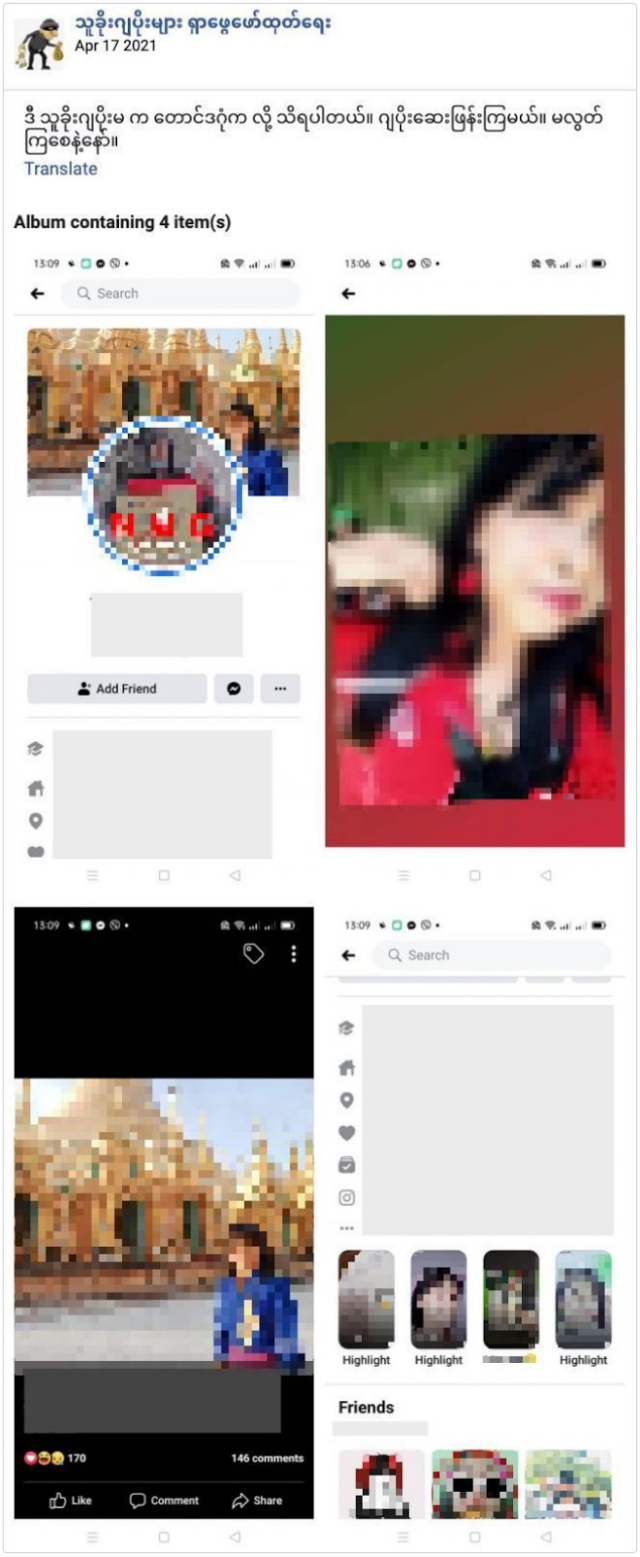
We removed 79 Facebook accounts, 13 Pages, eight Groups, and 19 Instagram accounts for violating our policy against coordinated inauthentic behavior. This network originated in Myanmar and targeted domestic audiences in that country.

The people behind this activity used duplicate and fake accounts — some of which were already detected and disabled by our automated systems — to post, comment on their own content and create Groups. Some of the accounts posed as protesters and members of the opposition and joined pro-democracy Groups, while others ran pro-military Pages that claimed to expose anti-Tatmadaw protesters. A handful of accounts used photos likely generated using machine learning techniques like generative adversarial networks (GAN). This network also amplified the content posted by Pages criticizing the National League for Democracy. They posted in Burmese about news and current events in the country, including content on both sides of the political debate in Myanmar — in support and criticism of anti-military protests, the opposition and the military coup.

We found this activity after reviewing information about a portion of it shared by a member of civil society in Myanmar. Our investigation revealed some links between this operation and the activity we removed in 2018. Although the people behind it attempted to conceal their identities and coordination, our investigation found links to individuals associated with the Myanmar military.

- *Presence on Facebook and Instagram:* 79 Facebook accounts, 13 Pages, eight Groups and 19 Instagram accounts.
- *Followers:* About 55,500 accounts followed one or more of these Pages, around 10,000 people joined one or more of these Groups, and about 1,700 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around $650 in spending for ads on Facebook and Instagram paid for primarily in US dollars.

Below is a sample of the content posted by some of these accounts and Pages.



Translation

Page name: Discovering the thieves


February 18 2021
Listen carefully to what he said, wait for 1 years. Don't believe that he said not to protest in 1 years.
Undo
MYTEL LTE VPN 10:33 AM 63 %
Mizzima - News in Burmese
6m ·
LIVE
အမေစုကိုချစ်လို့ မုံရွာသပိတ်စစ်ကြောင်းမှာ လာရောက်ပူးပေါင်းတဲ့ ခလရ(၁၆)က တပ်ကြပ်ကြီး(စာရေး) တစ်ဦး
ရိုက်ကူး - ME
2,5K 66 Comments 647 Shares
Like Comment Share
DVB TV News
7m ·
မန္တလေးတွင် ပရဟိတအသင်းရုံးကို ရဲနှင့်စစ်တပ်က ပစ်ခတ်၊ လူငယ် ၁ ဦးဒဏ်ရာရ


added a new photo.
February 21 2021
JUSTICE FOR MYANMAR

02

IN DEPTH ANALYSIS

INFLUENCE THE INFLUENCERS: COVID VACCINE OPERATION FROM RUSSIA

By Ben Nimmo, Global IO Threat Intelligence Lead, and the IO Threat Intelligence Team

EXECUTIVE SUMMARY:

We removed 65 Facebook accounts and 243 Instagram accounts for violating our policy against foreign interference, which is coordinated inauthentic behavior on behalf of a foreign entity. This network operated across over a dozen platforms and forums but failed to build an audience. It originated in Russia and targeted audiences primarily in India, Latin America and, to a much lesser extent, the United States. Our investigation found links between this campaign and Fazze, a subsidiary of a UK-registered marketing firm, whose operations were primarily conducted from Russia. Fazze is now banned from our platform.

This campaign came in two distinct waves, separated by five months of inactivity. First, in November and December 2020, the network posted memes and comments claiming that the AstraZeneca COVID-19 vaccine would turn people into chimpanzees. Five months later, in May 2021, it questioned the safety of the Pfizer vaccine by posting an allegedly hacked and leaked AstraZeneca document. It is noteworthy that both phases coincided with periods when a number of governments, including in Latin America, India and the United States, were reportedly discussing the emergency authorizations for these respective vaccines.

This campaign functioned as a disinformation laundromat. It created misleading articles and petitions on multiple forums including Reddit, Medium, Change[.]org, and Medapply[.]co[.]uk. It then used fake accounts on social media, including Facebook and Instagram, to seed and amplify this off-platform content, using crude spammy tactics. The crux of the campaign, though, appeared to be engaging influencers with pre-existing audiences on Instagram, YouTube and TikTok to post content and use particular hashtags without disclosing the origin of the posts. This use of influencers appeared to be in line with the firm's advertised services, which included access to *"a large list of bloggers from Youtube, Instagram, and Facebook... [where] Accounts are ready to post your ads for reasonable pricing. Work with bloggers directly without any 3rd party."*

The vast majority of this campaign fell flat among the audiences it targeted, with nearly all its Instagram posts receiving zero likes. At the time of this writing, its English-language petition on Change[.]org gained only about 550 signatures, and its Hindi-language petition gained less than 900 signatures. Only the paid influencers' posts attracted some limited attention. However, this reliance on external influencers became the operation's undoing— in May, a handful of them exposed the anti-Pfizer efforts.

This continues the trend we highlighted in our recent Threat Report— influence operations increasingly target authentic influential voices to carry their messages. Through them, deceptive campaigns gain access to the influencer's ready-made audience, but it comes with a significant risk of exposure.

Another aspect of this campaign worth highlighting is its operations across multiple internet services at once, which makes it more challenging for any one platform to see the full picture and take action on the whole of the campaign. This is why a whole-of-society response to such disinformation campaigns is critical. The influencers who came forward in Germany and France played a key role in exposing the first clue to this activity. Open-source researchers and journalists were able to report on much of the operation's May activity. Our internal investigation led to uncovering the full scope of this network on our platform, including its activity in 2020, which we shared with our industry peers. Our analysis benefited from research by CNN, The Daily Beast and Graphika. This collaboration between different members of the community is vital to exposing influence operations and understanding their impact.

Still, some questions remain about aspects of this campaign — including who commissioned Fazze to run it — that would benefit from further research by the defender community. One feature of these for-hire influence operations is that they allow the ultimate beneficiary to obfuscate their involvement. Another question relates to how the "hacked and leaked" document came into Fazze's hands. As with any influence operation, understanding the motive behind leaks like these is key to putting the operation in context.

As part of disrupting this operation, we took down their accounts, including authentic assets of the people behind this network, and blocked domains associated with their activity. We also notified people who we believe may have been contacted by this network and shared our findings with law enforcement, independent researchers, policy-makers and our industry peers so they too can take action if they find violating activity.

TAKEDOWN BY THE NUMBERS

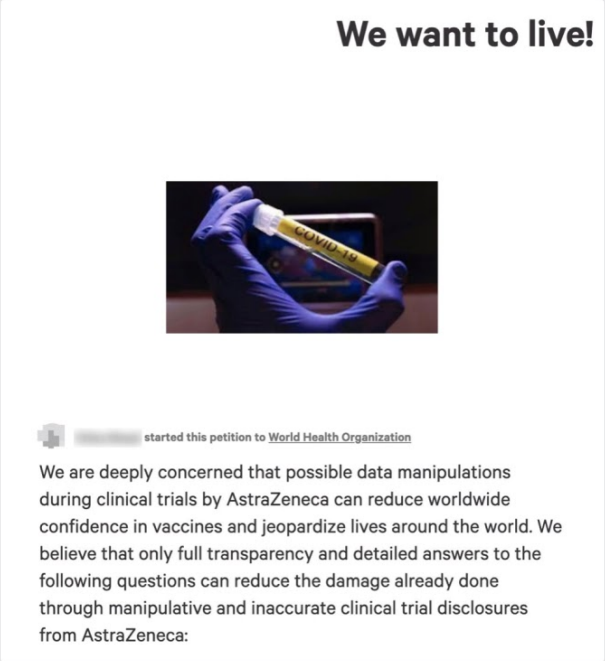
- *Presence on Facebook and Instagram:* 65 Facebook accounts and 243 Instagram accounts.
- *Followers:* About 24,000 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around $200 in spending for ads on Facebook and Instagram paid for primarily in US dollars, euros and Russian rubles. That includes the entirety of historic advertising activity by both inauthentic and authentic accounts removed as part of this network. We haven't seen ad spend associated with the vaccine-focused campaign described in this report.

NOVEMBER-DECEMBER 2020: THE ASTRAZENECA PHASE

The operation's first phase centered around the false claim that the AstraZeneca vaccine was dangerous because it was derived from a chimpanzee adenovirus. It primarily targeted audiences in India and Latin America, with sporadic and unsuccessful attempts to reach audiences in the United States. This phase of the on-platform operation has not been previously reported.

The Fazze operation began with the creation of two batches of fake Facebook accounts in late 2020, which likely originated from account farms in Bangladesh and Pakistan. They posed as being based in India.

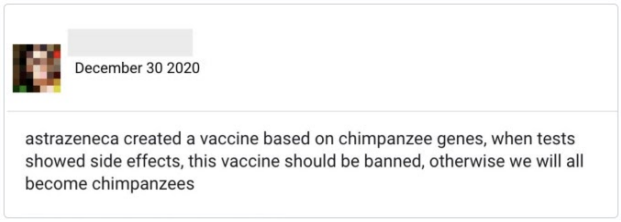
The accounts initially posted a small volume of non-covid content — typically about Indian food or Hollywood actors. In late November, however, the operation began using some of them to post on blogging platforms and petition websites, including Medium and Change[.]org. These blogs and petitions, in English and Hindi, claimed that AstraZeneca manipulated its COVID-19 vaccine trial data and used an untried technology to create the vaccine.



Image

Screenshot of a petition on Change[.]org, created by the operation and addressed to the World Health Organization on November 25, 2020.

In December, as the Indian government was discussing emergency authorization for the AstraZeneca vaccine, the operation began using fake accounts on both Facebook and Instagram to promote its blogs and petitions, together with a large stock of memes. All these memes featured the suggestion, or even the explicit claim, that the AstraZeneca vaccine would turn its subjects into chimpanzees. Many of the memes featured scenes from the 1968 movie “Planet of the Apes”.



Image

Post by the network

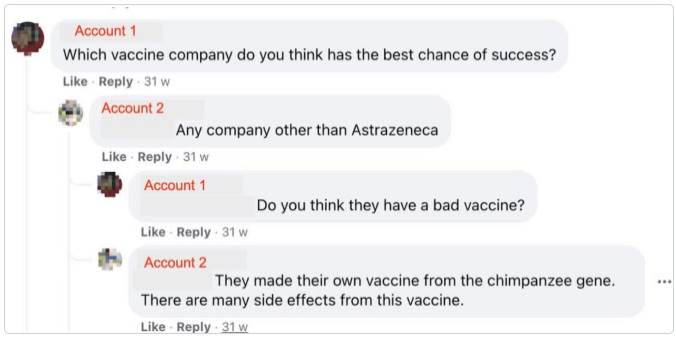
The fake Facebook accounts focused on low-volume, targeted posting: each one typically posted three to six memes, usually in Hindi, together with a link to one of the operation’s off-platform pieces of content and a brief comment in Hindi or English. These posts received few if any likes, and some were ridiculed by real people.

Image

Meme posted by this network's fake accounts, together with a link to one of the operation's petitions.

Caption

"Walter, come on over, don't hesitate! AstraZeneca's vaccine is safe! Yesterday we took the vaccine ourselves..."



Image

Conversation between two of the operation's fake accounts, responding to an unrelated post on a Page called "Texans for Vaccine Choice".

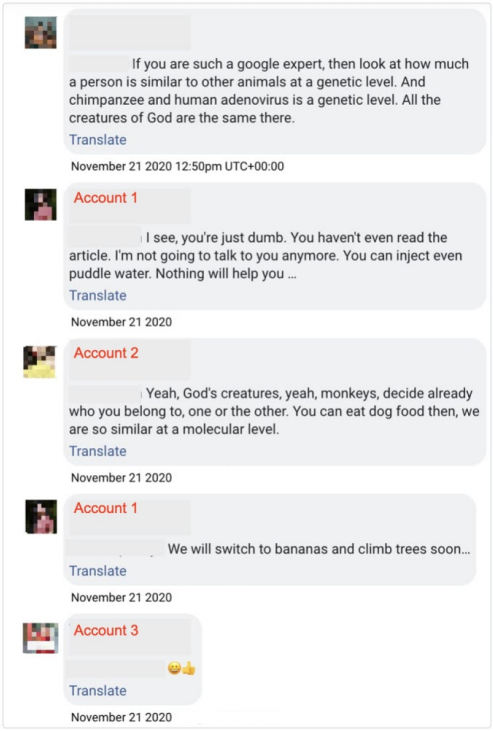


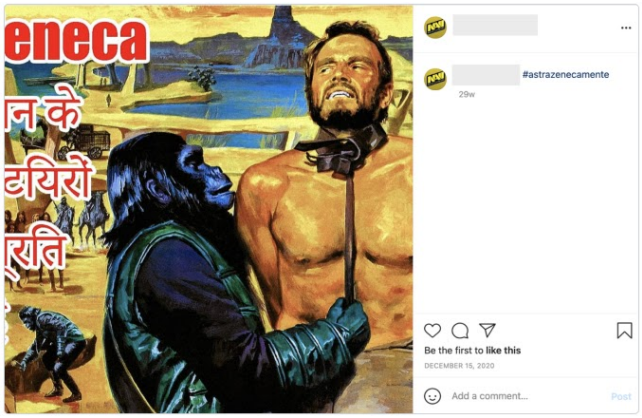
Image:

Comment from a real person mocking one of the operation's posts, followed by critical responses from three of the operation's fake accounts.

The Instagram activity was crude and spammy, and organized around a handful of hashtags. Two of them were in English: #AstraZenecakills and #AstraZenecalies, in addition to their equivalents in Portuguese: #AstraZenecamata and #AstraZenecamente. The last one was #stopAstraZeneca. The operation likely originated these hashtags: neither #astrazenecakills, #stopastrazeneca nor #astrazenecalies appeared to have been used on Instagram before. Between December 14 and December 21, about 10,000 posts that included the operation's hashtags were made, often with links to the operation's off-platform articles.

Most of the accounts posted these hashtags dozens or hundreds of times in quick succession, likely automated, with some detected and disabled by our automated systems. While the volume was high, the campaign saw minimal success. On one of the hashtags used by the operation, the top-performing post received five likes, whereas the vast majority got zero. Altogether, the operation's Instagram posts attracted around 1,000 likes combined, with most receiving zero.

In another sign of the sloppy nature of this campaign, most of the posts that used Portuguese-language hashtags between December 14 and December 16 attached them to Hindi-language memes. From December 17 onwards, they accompanied the hashtags with the same memes, but translated into Spanish. ("AstraZeneca mata", "AstraZeneca kills", is the same in Spanish and Portuguese, whereas "AstraZeneca lies" is "AstraZeneca mente" in Portuguese, but "AstraZeneca miente" in Spanish.) Perhaps not surprisingly, this spammy amplification also failed to attract attention.



Image

Meme posted by one of the Instagram accounts on December 15, 2020. The meme was in Hindi, but the account had an English name. It was operated from Russia, and it used a Portuguese hashtag.

Image

Two posts by the same fake account on December 14 and December 30, showing the same meme in Hindi and then in Spanish. The Hindi meme came with an English comment, the Spanish meme with a Hindi comment. Neither post gained reactions.

Upper post caption: "Now it's your turn to get vaccinated with AstraZeneca".

Lower post text: "The vaccine was based on a chimpanzee gene from the company AstraZeneca."

Lower post caption: "OK, it's your turn for the AstraZeneca vaccine."

While this spammy campaign was still running, a handful of health and wellbeing influencers posted Instagram stories that used the same hashtags, referenced the fact that the AstraZeneca vaccine was derived from chimpanzee adenovirus and shared links to the petitions that the Fazze operation had created. While possible, it appears highly unlikely that these influencers shared the operation's work organically. Given the public reporting about this network's engagement with influencers in May, it is likely that the operation used similar tactics in December 2020 and asked unwitting people to amplify this campaign against AstraZeneca across social media platforms.

The Instagram spam activity ended on December 21. The Facebook accounts continued posting at a very low level — roughly a post a week — into early January. Between December 30 and January 18, the Argentinian, Indian, and Brazilian governments granted emergency authorization to the AstraZeneca vaccine. On January 6, the operation stopped posting.

MAY 2021: THE PFIZER PHASE

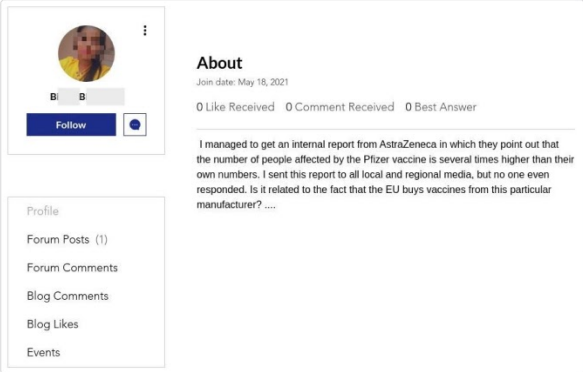
After months of inactivity, the operation resumed in May 2021 to claim that Pfizer's COVID-19 vaccine had caused a much higher "casualty rate" than other vaccines. This time, the on-platform activity appeared to be limited to a few dozen Facebook posts in English that primarily targeted Pages and Groups in the United States, which received almost no reaction, and a single post by an influencer in Brazil. Open-source reporting confirms that Fazze also sent emails to influencers in France and Germany, who ultimately exposed it, and likely recruited a YouTube influencer in India. We did not see evidence of this phase of the operation targeting India, France and Germany on our platform.

This phase of the operation coincided roughly with a period when the European Medicines Agency and Brazil were discussing approving the Pfizer vaccine for adolescents, and came just after the US Food and Drug Agency approved it for adolescents on May 10. Pfizer was also reportedly in talks with the Indian regulator in early May over an "expedited approval pathway" for its vaccine.

At the core of this second phase of the operation was a 12-page document comparing the efficacy of different COVID-19 vaccines. The operation claimed that it had been hacked and leaked from AstraZeneca. It included a table which purported to show that the Pfizer vaccine caused a much higher casualty rate than other vaccines; the table has since been described by BBC investigative journalists as "cobbled together from different sources and taken out of context". It has not been confirmed how the document made it into this operation's hands.

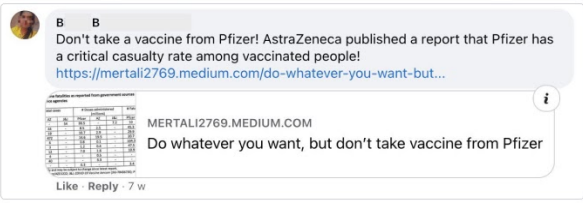
The Pfizer-focused phase of the operation began on May 14 with three articles on Medium, Reddit and ethicalhacker[.]org, posted within roughly 90 minutes. Each article claimed that AstraZeneca had been hacked, and shared a low-quality screenshot of the "casualty rate" table.

As before, the operation did not immediately promote these fake articles on our platform. Instead, on May 18, one of its Facebook accounts was used to create an account on a UK-based medical forum for students, and posted the entire "hacked" document there. The next day, a second wave of articles appeared on third-party websites to promote the "Pfizer casualty rate" narrative, referencing the first wave of articles as a source. The operation then used its Facebook accounts to post the links to these articles in different health- and news-related Groups and Pages. This time, all the posts were in English, and they primarily focused on US-based audiences, but the volume of posting remained very low, typically two-four posts per account, which received almost no reaction.



Image

Screenshot of the post on the British medical forum claiming to leak the full AstraZeneca document, May 18.



Image

Screenshot of a comment by the same fake Facebook account, responding to a local news story in Florida on 20 May, 2021. The account shared a link to one of the operation's early articles.

According to French investigative publication Fact & Furious, the operation sent influencers on YouTube, Instagram and TikTok a detailed briefing containing the campaign arguments, articles, and instructions to add links in the influencers' bios. Interestingly, unlike in December, the operation itself did not rely on spammy tactics nor used any hashtags. However, it reportedly instructed the influencers to use generic hashtags, such as #corona and #covid19, likely in an attempt to inject their content into the mainstream pandemic-related conversation online.


EN

TASK FOR THE INTEGRATION:

YOUTUBE/ INSTAGRAM/TIKTOK:

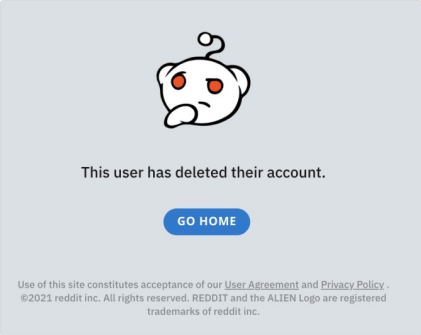
1. Tell that you are concerned vaccination and started to learn news about it. Because this topic is important for each person.
2. Explain that Astrazeneca's report has leaked. It shows the **mortality rates among the vaccinated population**.
   FOR ALL COUNTRIES:
   Tell that this info was publicated in famous French publication called Le Monde
   IF YOU **ARE FROM FRANCE**, TELL AND **SHOW** ARTICLE IN LEMONDE
   Link

   FOR ALL COUNTIRIES EXCEPT FRANCE:
   Show the table (you can show screenshots of articles / article titles on the screen) - YOU CAN FIND THEM BELOW
3. **Make the main conclusion** from the table. Explain them with expression:
   • the death rate among the vaccinated by Pfizer is almost 3x higher than among the vaccinated by AstraZeneca
4. Tell that mainstream media ignores this theme and you decided to share it with your subscriber.
5. Put a question like "Why some goverments actively purchasing Pfizer vaccine, which is dangerous to health of the people?

Image

Part of the tasking that the Fazze campaign was reported to have sent to influencers. (Source: factandfurious.com).

The attempt to reach influencers proved to be the operation's undoing. Rather than taking Fazze's money (reportedly 2,000 euros), one French and one German influencer exposed the campaign. This triggered a wave of open-source research that identified Fazze's corporate ownership and the influencers they targeted. In response, Fazze appears to have deleted most of its fake articles by the end of May, and its staff removed the references to Fazze from their social media bios. According to public reporting, when journalists approached the influencers in Brazil and India, they, too, deleted their content.



Image

Screenshot of the profile of one of the accounts run by the operation, subsequent to its exposure in May 2021.