

CYBER
THREAT
ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

August 17, 2021



Operation Secondary Infektion Continues Targeting Democratic Institutions and Regional Geopolitics



The following report is an update to Insikt Group's April 2020 publication "Intent to Infekt: 'Operation Pinball' Tactics Reminiscent of 'Operation Secondary Infektion'", which investigates a long-running, Russian-linked information operation coined by the broader research community as "Operation Secondary Infektion". This report examines new findings, recent case studies, and analysis into the Tactics, Techniques, and Procedures (TTPs) as well as motivations of those responsible for this information operation against international audiences. This report contains information gathered using the Recorded Future® Platform as well as several OSINT enrichment tools.

Executive Summary

Operation Secondary Infektion is a longstanding information operation of likely Russian state-sponsored origin. First appearing as early as 2014, the campaign [received](#) its name from Operation Infektion, also known as Operation Denver by the East German Stasi in the 1980s, which was an information operation intended to convince the international community that the US military developed HIV/AIDS at a biolab research facility located in Fort Detrick, Maryland. According to Soviet KGB cables, the influence effort was to demonstrate that the biolab-developed virus [ultimately](#) "spun out of control" and was released into the wild. It was only in 1992, after the fall of the Soviet Union, that then-Foreign Intelligence Service (SVR) Director Yevgeny Primakov admitted that the Russian KGB was behind Operation Infektion.

Like Operation Infektion, Secondary Infektion relies on forgeries and fake media that attempt to enter local sources and penetrate mainstream news, typically targeting democratic governments and institutions abroad with stories intended to generate rage, confusion, and doubt in regional geopolitics. The operators behind Secondary Infektion take a keen interest in the affairs of governments operating in the former Soviet Bloc as well as those governments' domestic challenges. We believe that, with these intentions in mind, Secondary Infektion directly supports the pillars of what is known as [Russian Active Measures](#) information operations (активные мероприятия), which are commonly at the behest of Russian security services and the Kremlin.

Over the last several years, as [documented](#) by both Recorded Future and other researchers, Secondary Infektion has demonstrated persistence in its messaging and an ability to organize and repeat a process that we believe is highly likely to be manufactured by nation-state sponsored influence actors. Furthermore, the consistent narrative of other regional powers as aggressors interfering in the affairs of sovereign governments and territories supports [historical Russian state rhetoric](#) of "Russia as regional protector". This concept is manifested through diplomatic involvement and military intervention, with Russia's self-designated role as a force ensuring self-determination and justice in the "near abroad", although these objectives are often fueled by Russia's interest in countering the West.

These narratives are manufactured to achieve Russia's greater strategic and geopolitical objectives. We judge that a combination of these factors, including strategic geopolitics, interest in regional affairs, and target language(s), including Russian, point to an information operation of Russian state-sponsored origin.

Key Findings

- Operation Secondary Infektion remains an ongoing information operation in present-day 2021, though the intensity of forgeries and articles has declined from its peak of activity between 2014 and 2020. Nonetheless, we expect that these influence activities will almost certainly continue.
- We believe that it is highly unlikely that Secondary Infektion affected the 2020 US election cycle. The election did not appear to be a priority for this operation, which rather seemingly prioritized influencing regional Eastern European geopolitics. Despite this, Secondary Infektion operators used politically and socially divisive narratives found prominently in US society to advance their strategic objectives on said European audiences and populations, particularly those that speak Russian, Ukrainian, and other regional languages.
- We identified strong evidence to indicate that Secondary Infektion operators attempted to infiltrate and influence individuals associated with, or ideologically aligned to, the far right in the US in at least 1 event on 4chan, through attempting to fuel anti-Muslim sentiment and exacerbate COVID-19 disinformation.
- Though to date Secondary Infektion has exclusively used single-use personas to disseminate disinformation, we have identified at least 2 personas used more than once; 1 imitating a branch of the Anonymous collective, and the other a self-described French-speaking Armenian blogger.
- Secondary Infektion largely remains ineffective in penetrating the mainstream (including social media like Reddit, and prominent news outlets), in part due to the rigor of platform-based suspension features, the alertness of forum moderators, and the visibility of these tactics to the broader research community.
- Prominent US political figures are likely to remain unwitting subjects of attempted Secondary Infektion disinformation efforts against European audiences. Furthermore, there is little doubt that US and Western allies are, and are likely to remain, the primary focus of Secondary Infektion messaging and are likely themselves targets.
- Thus far, Secondary Infektion's tactics, techniques, and procedures (TTPs) continue to use, almost exclusively, static media, meaning "photoshopped" screenshots and images of forged documents. Although there is no evidence of their use at this time, it is possible, although unlikely, that individuals behind this operation will produce deep fakes, altered video, and edited audio.

- We strongly believe that Secondary Infektion remains a consistent but stagnated information operation, with little innovation or significant changes in its TTPs. In many ways, these repeated processes, with little change to alter their results, are representative of a concerted, organized, institutional effort.

Background

In April 2020, Insikt Group published "[Intent to Infekt: 'Operation Pinball' Tactics Reminiscent of 'Operation Secondary Infektion'](#)" following a lengthy investigation of forgeries targeting geopolitical activities in Eastern Europe and the US that appeared in sources we use to monitor international propaganda and nation-state disinformation. At the time, we determined that "Operation Pinball" (our naming classifier for this activity) was closely reminiscent of Secondary Infektion, as the two shared similar TTPs, particularly the use of self-published blogs with single-use personas, Reddit promotion, and multilingual obfuscation. Much of our knowledge of the campaign and the techniques for identifying these campaigns is credited to prior research from previous [reporting efforts](#) on Secondary Infektion from the Atlantic Council's Digital Forensic Lab (DFRLab).

After we released "Intent to Infekt", Reddit administrators [updated the community](#) on Secondary Infektion activities on the platform and independently assessed that they found "significant alignment with tactics used in Secondary Infektion that seem to uphold Recorded Future's high confidence belief that the two operations are related", giving us further confidence that the campaigns are almost certainly one and the same. Then, in June of 2020, researchers at Graphika [published](#) a comprehensive review of Secondary Infektion tactics over the last several years, which further validated our independent findings as instances of Secondary Infektion.

Based on community validation and corroborating research to date, we are certain our initial findings labeled "Operation Pinball" are case studies in the ongoing Secondary Infektion campaign. For these reasons, we will refer to this effort only under the name Secondary Infektion.

Threat Analysis

A Present-Day Update on Secondary Infektion

Based on Insikt Group's examination of Secondary Infektion TTPs from April 2020 to the present, we believe that this Russia-linked influence operation continues to be active on multi-lingual, self-publishing blog sites targeting Western institutions in Europe (such as NATO and the EU), with a particular focus on states considered to be within Russia's "near-abroad" sphere of influence. Though the volume of Secondary Infektion efforts has decreased in its intensity since the mid-2010s, this effort is still an active international influence campaign, and we expect to identify additional cases of this ongoing operation in the coming months.

We have identified sporadic but deliberate attempts to plant forged documents, biased news articles, and images in social media, online publications, and, in at least 1 case with high confidence, on the imageboard forum 4chan. With the emergence of COVID-19 in the last year and a half, Secondary Infektion handlers opportunistically repurposed traditional techniques intended to create rifts and doubt through Western institutions with malign content about the novel coronavirus, using the pandemic as a backdrop for anti-NATO and anti-US/ West disinformation material.

According to a Center for Strategic and International Studies (CSIS) [analysis](#) of Russian influence operations in the UK, the approach of Russian disinformation efforts in the country "tends to simply be to 'flood the zone' with a combination of accurate, half-true, and false information — with varying degrees of attribution — in order to introduce confusion and doubt into existing debates". Indeed, Secondary Infektion "floods" regional sources (blogs, news sites, and social media) with false information and forgeries in the hope that something catches mainstream attention. Given that many governments in Eastern Europe and Central Asia are not as transparent in domestic and foreign policy as Western European counterparts and residents of these countries frequently doubt information put forward by more mainstream media, flooding mixed-reputation regional sources with false information is potentially a very effective tactic and is likely why we identify more cases of Secondary Infektion in these regions than elsewhere.

In many cases, Recorded Future has found that Russian or Ukrainian language instances of Secondary Infektion-related documents were published on 20 or more self-publishing or pro-Russian fringe websites over a 2 to 3 week period, almost always in a "copy and paste" fashion. We concur with other [assessments](#) in the research community monitoring Secondary Infektion that this widespread dissemination approach intends to compensate

for emphasizing operational security (OPSEC) over the audience building and social media promotion that is otherwise necessary for successful information operations or influence campaigns.

While the flooding of these sources is not a suitable prescription for the downsides of strong OPSEC, the actors responsible for this effort continue to produce material with few changes in the campaign TTPs. This remains true even after Secondary Infektion was detailed in 2019 and further documented through 2020.

For example, in July 2020, NATO disclosed TTPs associated with suspected Russian information operations attempting to project COVID-19 related disinformation and propaganda as a means of advancing anti-NATO narratives. Specific case studies included:

- False claims about COVID-19 spread among NATO battlegroups in [Lithuania](#) and [Latvia](#)
- [Planted forgeries](#) emulating Polish Brigadier General Ryszard Parafianowicz on the Polish War Studies Academy website with content that was critical of the US military's presence in Poland and involvement with exercise [DEFENDER-Europe 20](#), as well as the modification of the exercises amid COVID-19

These case study examples are highly similar to campaigns observed to date in our reporting of Operation Secondary Infektion.

According to NATO, though the targets of the information operation varied, the operation was dependent on similar [disinformation techniques](#). These techniques are:

- **Forgeries** — forged letters, media, and interview
- **Fake Personas** — typically single-use "burner personas", some evidence of multi-use fake accounts
- **Falsehoods** and purposely false information
- **Amplification** — across self-publishers, rogue news sites, and other pro-Russian sources
- **Language Leap** — often including at least one European language, in addition to English
- **Outreach (in some documented cases)** — NATO states that in each of the above case studies, the administrators of the campaign used email distribution to journalists or the subjects of the campaign, intended to "provoke a response"

According to [FireEye](#), who dubbed this specific campaign “Ghostwriter”, Secondary Infektion and Ghostwriter bear a resemblance on the surface but were “two distinct activity sets given notable differences in observed behaviors and tactics”. FireEye based this conclusion on the notion that analysts have not [observed](#) the use of “traditional cyber threat activity in support of Secondary Infektion operations” and Ghostwriter’s dependence on developed personas, or impersonation of authentic individuals instead of single-use burner personas identified in Secondary Infektion.

Recorded Future considers what we previously tracked as “Operation Pinball” as an instance of Secondary Infektion, whereas Secondary Infektion is likely more accurately defined as a family of Russian-linked information operation campaigns that includes FireEye’s “Ghostwriter” campaign.

- Recorded Future assesses that these specific instances share overlaps in TTPs that further highlight a collaborative, organized effort.
- It is likely still inconclusive whether cyber threat activity, as seen with Ghostwriter and the threat actor group UNC1151, has directly supported Secondary Infektion information operations. In the case of the [NHS trade negotiation leaks](#) of 2019 — the only known case of a campaign that [strongly resembles](#) Secondary Infektion’s TTPs and successfully gained mainstream traction — the documents used in this activity were initially obtained through unknown means. However, in August 2020, new details of the campaign, [confirmed by UK authorities](#), revealed that the negotiation notes were exfiltrated following a successful breach of former UK trade secretary Liam Fox’s email account by Russian cyber threat actors. It is not yet clear how the breach, and obtained documents, was transferred to account handlers that leaked the documents on Reddit and to journalists, but the hack-and-leak was likely coordinated.
- Recorded Future has identified some degree of overlap in Operation Pinball-validated Secondary Infektion tactics and Ghostwriter’s use of real individuals’ likenesses to spread disinformation. Notably, we found this once in narratives sharing a forged letter between the Armenian National Committee of America to US Senator Bob Menendez (D-NJ). Though in this example we did not see influence actors attempting to pose as a real person, the forgery in question was [embedded](#) in a manipulated screenshot of the news outlet Kurdistan 24 with an article purported to be written by Karzan Sulaivany, a journalist for the outlet. Our examination of this campaign is provided later in this report.

- Additionally, we have uncovered at least 2 examples of incidents in which multi-use personas, albeit often in conjunction with single-use accounts, disseminated disinformation in alignment with Secondary Infektion.

So far, Secondary Infektion has not been attributed to a specific actor or group within Russia, namely in part due to the group’s emphasis on OPSEC. However, it is clear that those responsible are likely organized through nation-state means and motivated with nation-state objectives in mind.

Imitating Authentic Journalists With Forgeries, Fake Screenshots

While publishing “Intent to Infekt”, we continued to monitor sources that we strongly believed were conduits for promoting falsified content, namely the aforementioned self-published blogs in Eastern Europe and among the Commonwealth of Independent States (CIS), in the hope of learning more about the influence actors’ TTPs. In March 2020, we identified a forgery emulating correspondence between the Armenian National Committee of America and US Senator Bob Menendez (D-NJ). This letter attempted to generate fear of a broader conflict in Nagorno-Karabakh ahead of the March 31, 2020, Artsakh elections and was accompanied by articles presented in Russian which attempted to declare that Azerbaijan and Turkey were planning to interfere in the then-upcoming election cycle.

Like many instances of Secondary Infektion, this effort relied on a forgery to support an author’s claims. However, in this unique instance, we found that the document was planted inside an edited screenshot of a reputable news organization in Iraqi Kurdistan, using the name of an authentic journalist.



SECRETARY GENERAL
LE SECRÉTAIRE GÉNÉRAL
Jens Stoltenberg

SG(2020)0095

21 April 2020

Dear Mr. Raimundas Karoblis,

I would like to inform you about the decision to withdraw NATO troops from Lithuania in May 2020. This decision has been made due to the epidemic is now entering a more serious and complex period. The number of infected with COVID-19 NATO soldiers in Lithuania has been rising constantly.

Military medics assessed the situation in Lithuania. In accordance with the report, the situation with COVID-19 spread within the NATO enhanced Forward Presence Battle Group in Lithuania is catastrophic.

This state of affairs resulted from failure of the Lithuanian Ministry of Defence to take necessary measures to combat the spread of coronavirus. It is reported that hospitals in Lithuania are overwhelmed, short-staffed and ill-equipped as the outbreak continues.

At the moment, it is impossible to predict how widespread coronavirus will be among NATO military in Lithuania. NATO's focus is on how to save lives. So we will continue to work with Lithuania using other forms of cooperation.

I very much appreciate your attempts to restrain the spread of the COVID-19 and Lithuania's fulfillment of obligations within NATO.

Yours Sincerely,

Jens Stoltenberg

His Excellency
Mr Raimundas Karoblis
The Minister of National Defence of the Republic of Lithuania
Vilnius

North Atlantic Treaty Organization - Organisation du Traité de l'Atlantique Nord
Boulevard Léopold III - B-1110 Bruxelles - Belgique
Tel.: +32 2 707 49 17 - Fax: +32 2 707 46 66

Figure 1: NATO Secretary-General Jens Stoltenberg and Lithuanian Defence Minister Raimundas Karoblis in April 2020. Recorded Future believes that NATO's case study of the incident aligns strongly with tactics and techniques employed by Secondary Infektion.

On March 12, 2020, a Russian-language blog called, “Belarus, and not just that...” (“Беларусь и не только...”) on the website [mirtesen\[.\]ru](#) published a story titled “Military provocation to the elections in Artsakh” (Военная провокация к выборам в Арцахе). The title alludes to the Republic of Artsakh (also known as the Nagorno-Karabakh Republic (NKR)), a contested territory in the South Caucasus with a large Armenian population.

The blog post highlighted the then-upcoming change in the NKR government from a mixed presidential-parliamentary system to a presidential republic during the elections taking place later that month on March 31, 2020. The blog post stated, however, that “Baku and Ankara are going to disrupt” the elections, implying that Azerbaijan and Turkey were planning to interfere in the NKR elections. The elections in question were oddly “announced” in a forged letter from the Executive Director of the Armenian National Committee of America, Aram Hamparian (alternatively spelled “Hambaryan” by the author of the initial posting), to US Senator Bob Menendez. Both Senator Menendez and Director Hamparian were subjects of historic Secondary Infektion campaigns per Recorded Future’s “Intent to Infekt” research released in April 2020.

The forged letter makes the claim that the ANCA “[sic] has got reliable data that Azerbaijan and Turkey plan to thwart voting and disrupt the free democratic elections through the use of military force in the Republic”. Interestingly, when the blog quotes the letter in Russian, the translation is much more eloquent than the letter: “ANCA has reliable evidence that Azerbaijan and Turkey will try to interfere with the voting and disrupt democratic and free elections in the republic by using military force”, (ANCA располагает достоверными данными о том, что Азербайджан и Турция попытаются помешать проведению голосования и сорвать демократические и свободные выборы в республике путем применения военной силы). The difference in style and grammar between the initial forged letter, in English, and the quote taken from the letter and published on the blog in Russian, suggests that the forged letter was compiled manually by a non-native English speaker and the content was originally written in Russian. This is supported by the fact that a machine translation of the Russian content to English is more fluent in style than the original letter in English.

In the letter, Hamparian requests that Senator Menendez bring the matter to the US Senate to “[sic] get leverage on Turkey and Azerbaijan” as a means of ensuring that the elections take place peacefully.

The blog makes an additional claim, stating that Hamparian notes that “Azerbaijan has been actively building up firepower and replenishing its arsenal of strike systems, and now it has also secured the support of Turkey”. There is no discussion, however, of this activity in the forged letter.

A photocopy of the letter was not included within the blog itself. In this case, an image of the document was included in a screenshot of the Kurdish news outlet Kurdistan 24, with an article titled “ANCA: Azerbaijan and Turkey plan military operation during [the] election in Nagorno-Karabakh”. The article purports to be written by journalist Karzan Sulaivany.

It is almost certain that both the letter and the screenshot showing the letter on an alleged Kurdistan 24 article are fake. In an investigation of the article on the news outlet’s dedicated website, Recorded Future found no history of this article or the document in any of the outlet’s prior reporting in or around March 3, 2020, when the article was allegedly published. Furthermore, Recorded Future found no history of any such articles published by Mr. Sulaivany on this news outlet and did not identify any evidence of shared links, quotes, or discussion on open sources that would contradict our assessment that this is a fake screenshot.

Embedding a false document within a forgery of a legitimate news source was at the time a new technique that we did not previously identify. We do not believe that this demonstrated a major shift in Secondary Infektion efforts, given this technique’s rarity. Nonetheless, this example represents opportunities to further obfuscate that it is disinformation.

News

Analysis

Economy

Interviews

Opinions

Culture

Sports

Features

Kurdistan

Middle East

World

About Us | Contact Us | Apps

Q

Middle East

ANCA: Azerbaijan and Turkey plan military operation during elections in Nagorno-Karabakh

Karzan Sulaimany

March 03-2020

08:31 AM

Share

Armenian National Committee of America

NATIONAL HEADQUARTERS

February 26, 2020

The Honorable Robert Menendez

US Senator for New Jersey

528 Hart Senate Office Building

Washington, D.C. 20510

Dear Senator Menendez:

On behalf of the Armenian National Committee of America (ANCA) and the entire Armenian People I wish to extend my high appreciation and deep gratitude to you, Sir, for your tremendous contribution to the development of bilateral relations between our countries. You have provided full support to democratic evolution of Armenian State and protected Armenian interests both in the United States of America and on the international scene for many years now. Your role in advancement of the issue of the recognition of the Armenian Genocide in the U.S. Senate is particularly significant. It was ruled in our favor thanks to your long-time Herculean efforts.

Once again I am compelled to write to you in order to express concern regarding the risk of a conflict escalation in Nagorno-Karabakh during the next parliamentary and presidential elections set for March 31, 2020. ANCA has got reliable data that Azerbaijan and Turkey plan to thwart voting and disrupt the free democratic elections through the use of military force in the Republic. Similar provocations gave rise to a full-scale military conflict in April 2016, and such situation threatens to repeat.

We are sure that the USA, like Armenia, fully supports democratic aspirations of the people of Nagorno-Karabakh. They need to be able to decide their future by fair, free and transparent elections. It is therefore necessary to provide Nagorno-Karabakh voters an opportunity to exercise their voting rights and to prevent any provocations from the outside. We ask that you raise this issue in the U.S. Senate and get leverage on Turkey and Azerbaijan. Those countries reject dialogue with the government of Nagorno-Karabakh and struggle to obstruct democratic development of the Republic.

Sincerely,

Aram Hamparian

Executive Director

ANCA NATIONAL HEADQUARTERS

2000 K Street

Washington, DC 20006

PH: 202-775-2525 FAX: 202-775-7881

www.anca.org, info@anca.org

ANCA BOSTON OFFICE

200 State Street

Boston, MA 02109

PH: 617-452-0001

www.anca.org, info@anca.org

ANCA EUROPE HEADQUARTERS

40 Kingsway Road

London, UK W8 5NF

PH: +44 (0)20 7461 0141

www.anca.org, info@anca.org

Most Popular

Last 24 Hour

Last week

Last month

01 Kurdistan Region's Sulaimani records case

02 Super Tuesday: Joe Biden and the Kurds

03 UN: Turkish-backed groups carry out war

04 Masoud Barzani hails unity of Kurdistan

05 Kurdistan confirms four coronavirus cases

06 Kurdistan PM discusses bilateral ties, trade

opinion

Occupied Afrin: Learning Your

'This idyllic and lush mountainous area which had become a haven for

t f More

Sinam Sherkary Mohamad

Awat Mustafa:

Kurdistan Region: Rare opportunity for long-term

Majida Sanaan-Guharzi:

KRG Reform Bill: Legalizing early retirement for top

Shwan Hajo:

The State of Broken Promises: The current

Figure 2: The document in question was included in a screenshot of the Kurdish news outlet Kurdistan 24, with an article titled "ANCA: Azerbaijan and Turkey plan military operation during [the] election in Nagorno-Karabakh" (Source: Recorded Future)

7

CTA-RU-2021-0817

Recorded Future® | www.recordedfuture.com

Embedding the document within a doctored screenshot of a legitimate news source with the likeness of a real journalist creates the impression that both the document and the claims of Turkey and Azerbaijan interfering with the NKR elections are true.

Recorded Future identified copies of this blog post on the following Ukrainian- and Russian-language blogs and self-publishing websites: [Grodno Forum](#), [Transnistrian Social Forum](#), [PMR Forum](#), [Armenian Vardanank Forum](#), and [bramaby\[.\]com](#). The doctored screenshot was also hosted on [imgur](#), though this was likely unintentional and more because the website did not properly embed the screenshot. Except for the Armenian Vardanank Forum, each of the posts was posted by a burner persona under the username “vorsintol” (aka “Anatoly Vorsin”). For the Armenian Vardanank Forum, this identical post was made by an additional persona, “Godjii”. Interestingly, while vorsintol was registered within minutes of posting, Godjii is an older account, having registered in September 2017. Between the time of registration and posting on March 11, 2020, Godjii posted messages infrequently on the platform, mainly regarding regional politics in Eastern Europe and Central Asia. It is likely that this account was unaffiliated with Secondary Infektion and caught the story in the crossfire, resulting in an additional share.

A Second Wave of Stories Targeting NKR Elections

In or around March 6, 2020, the second series of articles referencing the screenshot was published on additional blogs and self-publishing websites, titled “Idlib - Karabakh - Donbass: Is It Time for Ukraine to Join the Russian-Turkish Conflict”.

This second set of articles initially focused more on the conflict between the Syrian Armed Forces and the Turkish army than NKR, stating, “Syrian aviation’s treacherous attack on a grouping of Turkish troops in Idlib not only provoked Ankara in a series of retaliatory strikes but also led to a critical exacerbation of the contradictions between Turkey and Russia, putting the relations of the two states on the brink of a full-scale war”.

This narrative then shifted to portraying Turkey as an aggressor, stating that Turkey “is now creating another center of tension ... another escalation of the Karabakh conflict in which Russia has traditionally supported Armenia ... together with Azerbaijan, is preparing a military demonstration in Nagorno-Karabakh to prevent the parliamentary and presidential elections in NKR from holding illegal elections in Ankara and Baku”. This narrative was also found attempting to extort diplomatic tensions between the US and Turkey.

This second wave of narratives introduced Ukraine as a possible ally for Turkey, though it framed its narrative to paint Kyiv as an aggressing force and likely was meant to convince Ukrainians that its government, not Russia’s, was responsible for the conflict in Donbas. It proposes that Ukraine could involve itself in the conflict as a possible advantageous maneuver to further distress the Kremlin as the Russian military is “stretched” in the Middle East. Furthermore, it suggests a wariness on the part of the Russian military in the face of a believed upcoming conflict in NKR, in addition to its involvement in the ongoing conflict in Ukraine. The article suggests that the Ukrainian government could use the alleged conflict between Russia, Turkey, and Syria as a way to begin “restoring sovereignty in the occupied territories”. This alludes to Crimea and a means to counter Russian activity in the Black Sea by blocking access to the Bosphorus and Dardanelles Straits for the Russian navy.

This article was spread on the following websites: [times\[.\]com.ua](#), [1zt\[.\]ua](#), [blog.meta\[.\]ua](#), [korrespondent\[.\]net](#), [mynizhyn\[.\]com](#), [gorod\[.\]dp.ua](#), and [news.vash\[.\]ua](#). Each of these posts were constructed by a false persona under the username “gavvryom” aka “Roman Havrylyuk”.



Figures 3 and 4: Identical posts by Godjii and vorsintol on March 11 and 12, 2020 (Source: Recorded Future)

Common with Secondary Infektion, the handlers attempted Reddit promotion of the story [through](#) a burner persona under the same username “gavryrom”, which connects back to the associated name Roman Havrylyuk. Recorded Future found that 1 attempted post was made to the Ukrainian-oriented subreddit r/ukraina; however, it was quickly removed by subreddit administrators. Based on the profile’s metadata, the account was registered on March 6, 2020, at 2:03 AM EST, and shortly thereafter posted to r/ukraina at approximately 2:39 AM EST. As of 2021, this account was suspended from Reddit, though copies of this campaign in other sources remain on the internet.

Ідліб - Карабах - Донбас: чи не час Україні приєднатися до російсько-турецького

6 марта 2020, 10:44

ВЛАДЕЛЕЦЬ СТРАНИЦІ
РОМАН ГАВРІЛЮК



56



Конфлікт між Росією та Туреччиною навколо ідлібського інциденту загрожує перерости в повномасштабну війну. Анкара переходить у наступ, Москва в патовому становищі. Чи не час Україні втрутитися?

Figure 5: A Roman Havrylyuk sharing the article in question on Korrespondent (Source: Recorded Future)

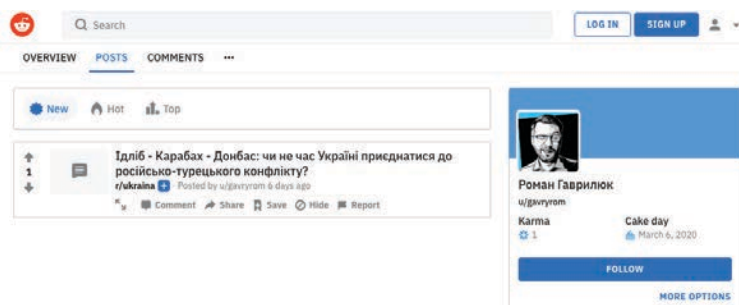


Figure 6: Gavryrom aka Roman Havrylyuk on Reddit (Source: Recorded Future)

Opportunistic Targeting — COVID-19

On multiple occasions, we found that the TTPs unique to Secondary Infektion were used opportunistically to promote disinformation regarding COVID-19, particularly in the earlier stages of the pandemic. As COVID-19 spread worldwide, many Russian domestic news outlets suggested that the US was behind the outbreak for various purposes, including bioterrorism. A EUvsDisinfo brief [published](#) on March 19, 2020, noted that one theme from Russian disinformation attempts at the time was that “coronavirus did not break out in Wuhan, China — the US is concealing its true origin, which is in fact the US or US-owned laboratories across the world”.

One source we [previously](#) identified as a go-to self-publisher, the Kazakh blog site [YVision](#), contained a report likely connected to Secondary Infektion that directly supported EUvsDisinfo’s independent findings at the time. On YVision, influence operators generated and later promoted a false narrative about US involvement in developing the COVID-19 disease in an Almaty, Kazakhstan biolab that was later released in Wuhan, Hubei Province. Insikt Group began monitoring this campaign in our data sets in mid-February 2020, and our internal findings were validated in an [independent assessment](#) in April 2020 by Adam Rawnsley of The Daily Beast.

On February 10, 2020, the group “Anonymous Kazakhstan” (Anonymous KZ), [published](#) the blog post “American Developments in the Kazakh Biolaboratory” (Американские разработки в казахской биолaborатории) claiming that COVID-19 originated from a laboratory in Almaty, Kazakhstan, which was funded by the US. The article cites a source from “among the staff of the Central Reference Laboratory (CRL) in Almaty has confirmed that the deadly coronavirus was developed in this institution”. The article alleges that the laboratory is connected to the US because it was “built with funds from the US Department of Defense”. The background of this narrative does have some elements of truth to make the overall disinformation effort more convincing: According to a 2013 Popular Science [article](#), \$103 million for building the laboratory did come from the US Department of Defense as part of the Defense Threat Reduction Agency to study dangerous pathogens. The [project](#) broke ground in 2010, and the CRL opened in September 2016.

American developments in the Kazakh biolaboratory



The activities of the Central Reference Laboratory in Almaty are closely monitored by US specialists. Further about the dangers and consequences of this cooperation.

We received confirmation of the information that was mentioned in the announcement. We think that from the previous post almost everyone guessed that it would be about coronavirus.

Our source just among the staff of the Central Reference Laboratory (TsRL) in Almaty has confirmed that the deadly coronavirus was developed in this institution. It is known that the laboratory, built with funds from the US Department of Defense, works with dangerous pathogens and is designed to "respond to possible biological threats and timely diagnose infections such as Dengue, Zika, Ebola, Merce virus and others." At the same time, only

Figure 7: The article in question, machine-translated to English (Source: Recorded Future)

Anonymous KZ claims that "the CRL in Almaty has become the main laboratory working with the diagnosis and prevention of the spread of the new coronavirus from Wuhan. In addition, contrary to media reports, of the 111 first samples received last week, according to our source, who was directly involved in testing them, there were two positive ones". Per the author's "source", these positive cases "completely coincide with the [COVID-19] strain, the study of which was started in the laboratory about two years ago and which, according to his observations, should not leave CRL all this time [sic]".

Anonymous KZ states that the analysis of COVID-19 was a joint development led by scientists from the US Centers for Disease Control and Prevention as part of a training of Kazakh epidemiologists. Per a February 2, 2020 social media [post](#) from Dr. Yelzhan Birtanov, Minister of Health of the Republic of Kazakhstan, 100 tests that passed through the CRL at that time returned negative. Furthermore, there were no reported positive cases of COVID-19 in Kazakhstan until March 13, 2020, when 3 individuals [tested positive](#) after returning from international travel.

The article blames the US as responsible for the COVID-19 outbreak, in concert with other themes in reported COVID-19 disinformation (the following quote is a machine translation):

It is worth paying attention to the fact that our reference laboratory is only part of a huge network of dual-purpose TsRLs [Central Reference Laboratory] built with Pentagon money around the world. This is a US global military biological research project outside the United States that circumvents international agreements, including the 1972 Geneva Convention for the Prohibition of the Development, Production and Stockpiling of Bacteriological Weapons, and Toxins and Their Destruction.

In support of our assumption, immediately after the news of the first victims of the new coronavirus on January 15, China signed the first phase of the shameful trade agreement with the United States, which increased spending on the purchase of completely unnecessary American goods by \$ 200 billion, and also opened the domestic market for American investment banks. Moreover, the United States upheld its duties on Chinese goods and will begin to discuss their reduction or cancellation only if China fulfills all of the above agreements.

Such agreements are concluded only in case of great pressure from one of the parties. Only the volume of commitments made by China to purchase energy and agricultural products make the United States a leading commodity export power, sweeping other suppliers, including Kazakhstan. So the strain developed by the Kazakhs undermined the Kazakh economy. Meanwhile, the Pentagon brought biological warfare to a whole new level. Now Washington is taking over global markets using biological weapons.

Like all cases of Secondary Infektion, this article had an attached document image. Unlike prior observations, this was not a forged letter among public officials. Instead, this was a well-crafted infographic titled "American Coronavirus Traced from Wuhan".



Figure 8: This infographic blames the US Department of Defense for the COVID-19 outbreak, stating that the strain constructed in CRL was released in Wuhan, China in December 2019 (Source: Recorded Future)

In total, we believe that this specific effort consisted of 3 waves, each demonstrating an emphasis of infiltrating the mainstream, albeit with little success.

- First, the original article posted by Anonymous KZ on February 10, 2020.
- Second, a significant wave throughout February 2020 consisting of one-off burner personas creating secondary narratives on Russian-speaking self-publishing websites, as well as attempted Reddit promotion.
- Finally, the third wave of activity appeared in early March 2020, albeit in far fewer numbers than the second wave.

These tactics were followed in a near-exact pattern as previously identified cases of Secondary Infection, spanning between February 10, 2020 (date of planting) to third layer summarization by around March 5, 2020. For each of the identified articles or blog posts, each referred back to the original Anonymous KZ report via hyperlink as the source.

To demonstrate the persistence of this specific campaign, Insikt Group tracked the personas and the broader narrative across 3 “waves” of activity between mid-February and early-March 2020. We note that for engagement metrics, these numbers are likely out of date for sites that are still live at the time of publication, as these statistics were recorded while the campaign was live.

First Wave (Seed)			
Title: “Американские разработки в казахской биологической лаборатории” Title: “American Developments in the Kazakh Biolaboratory”			
Date	Website (Archive)	Author	Engagement Metrics
2.10.2020	YVision.kz	Anonymous Kazakhstan	3,989 views

Second Wave			
Title: “В Алматы признались в работе над коронавирусом до эпидемии” Title: “Almaty Admitted to Work on Coronavirus Before Epidemic”			
Date	Website	Author	Engagement Metrics
2.19.2020	fishki.net	Ivan Parshin	1,410 views
2.19.2020	razumei.ru	Ivan	354 views
2.19.2020	Reddit r/liberta	u/Ivaparsh	1 upvote
2.19.2020	x-true.info	Ivaparsh	1,620 views
2.19.2020	rnbee.net	Ivaparsh	Unknown
2.19.2020	currentpolitics.livejournal.com	ivaparsh	Unknown
2.19.2020	actualno.com	Unknown	5,900 views
2.19.2020	imperianews.com	Unknown	Unknown
2.19.2020	kremlinrus.ru	Ivan Parshin	Unknown
2.19.2020	glav.su	Ivan Parshin	72 views
2.19.2020	aftershock.news	Ivaparsh	1,600 views
2.19.2020	news2.ru	Ivaparsh	Unknown
2.20.2020	mt-smi.mirtesen.ru	Unknown	4,600 views
2.20.2020	times.com.ua	Unknown	828 views
2.20.2020	Reddit r/ukraina	u/boltandy	1 upvote
2.20.2020	sluhi.com.ua	boltandy	Unknown
2.21.2020	mynizhyn.com	boltandy	61 views
2.24.2020	pero.org.ua	Andrew	Unknown
2.25.2020	mirtesen.ru	Arthur Nakhushev	4 views
2.25.2020	profi.tut.by	Arthur_Nakhushev	Unknown
2.25.2020	shock.ee	artunah (Arthur Nakhushev)	Unknown
2.25.2020	123ru.net	Unknown	13 views
2.25.2020	belarus-mt.ru	“AN”	1,000 views
2.26.2020	openarmenia.am	artunah	Unknown
2.26.2020	forumpmr.org	artunah	423 views
2.26.2020	disput.az	artunah	Unknown
2.26.2020	kavkaz.ws	artunah	Unknown

Third Wave			
Title: "Коронавирус был разработан в американской лаборатории под Алматы"			
Title: "Coronavirus was developed in an American laboratory near Almaty"			
Date	Website (Archive)	Author	Engagement Metrics
3.05.2020	paruskg.info	admin	Unknown
3.05.2020	Telegram	Остапа понесло	330 views
3.07.2020	centrasia.org	admin	Unknown

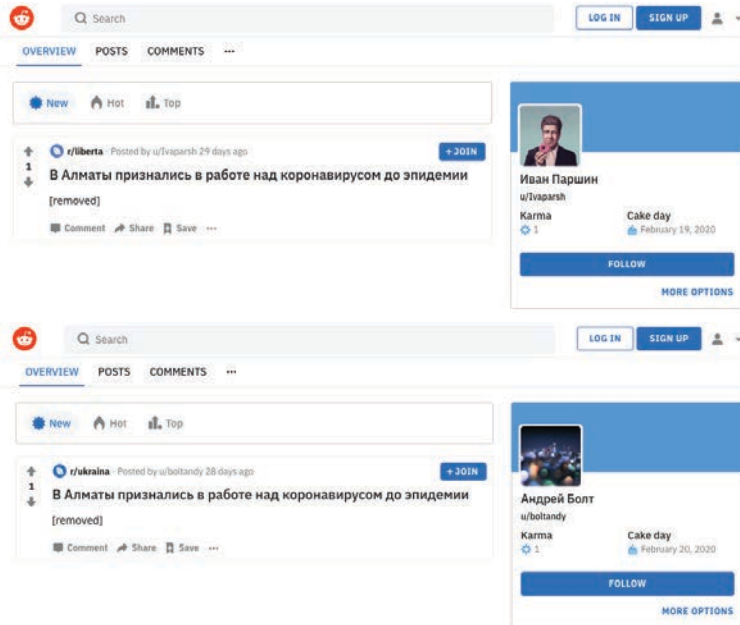
The second wave of blog posts, submitted by burner personas on known self-publishers, stated that Anonymous KZ's findings were "sensational news", linking back to the direct article on YVision. The blogs reiterate Anonymous KZ's anti-US tone, stating "this global US military biological research project allows the United States not only to circumvent international agreements on the inadmissibility of the production of bacteriological weapons but also to use viruses produced on the basis of TsRL [CRL] to put pressure on foreign policy partners". These blogs also suggest that "development of the coronavirus in Almaty [and information leaked to the press about its development] will lead to serious [economic] sanctions against Kazakhstan by China and the international community".

Almaty admitted to work on coronavirus before epidemic

Against the backdrop of the worldwide struggle against the spread of Wuhan coronavirus, [hackers from the Anonymous Kazakhstan group](#) shared sensational news. Their source from the staff of the Central Reference Laboratory in Almaty said that they developed the coronavirus, which infected more than 35 thousand people around the world. In particular, this is evidenced by the fact that two of the 111 coronavirus samples received in the CRL in recent times turned out to be positive and completely coincided with the virus strain that was developed in the laboratory a couple of years ago. Moreover, the development of this type of coronavirus was then carried out under the supervision of the US Center for Disease Control and Prevention.

Figure 9: Sample "Second Wave" article, translated to English. This example was posted by the persona "ivaparskh". (Source: Recorded Future)

As mentioned above, the influence actors attempted to promote this disinformation on Reddit but were unsuccessful, as these posts, which were submitted minutes after the accounts were registered on the website, were removed shortly after posting. As of 2021, both Reddit accounts are suspended from the platform.



Figures 10 and 11: Attempted Reddit promotion on r/liberta and r/ukraina (Source: Recorded Future)

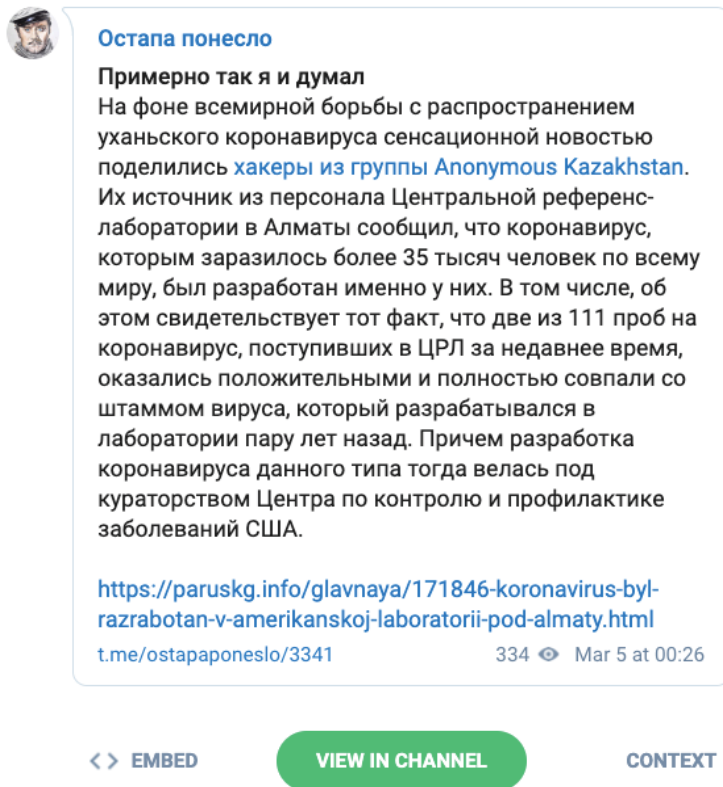


Figure 12: Promotion of the “Third Wave” via Telegram (Source: Recorded Future)

It is most likely that this information operation targeted primarily Russian-speaking audiences in Eastern Europe and among the CIS to increase suspicion and resentment towards the US. As with all other cases of Secondary Infektion, this campaign used single-use accounts on several different self-published blogs to build personas and grow audiences required for this content to go viral.

It is likely that engagement was mixed across all of these articles. Based on available data, these articles combined reached an audience of at least 20,400. Recorded Future observed [little promotion](#) across social media, with 3 known shares on mainstream social media and minimal shares on the Russian social media site VK.

It is almost certain that Anonymous Kazakhstan's post was the seed for further promotion from secondary single-use personas. Through a reverse image search of this infographic, we have identified additional reproduction of this story on over 24 websites.

We suspect that Anonymous Kazakhstan is a hacktivist front for Russian nation-state threat actors:

- Historically, APT28 has employed personas to obscure their identity both in indictments and in industry research, particularly groups under the guise of hacktivists. These personas include “CyberCaliphate”, “Anonymous Poland”, and “Fancy Bears’ Hack Team”.
- Anonymous Poland, in particular, was very likely used as a proxy to leak stolen information, as similar proxies like Guccifer 2.0 and DCLeaks were used to leak hacked data from the Democratic Congressional Campaign Committee and the Democratic National Committee. In the case of Anonymous Kazakhstan, however, there is no evidence that this is verified “leaked” information. Rather, this is false information intended to appear as a leak from a HUMINT source.

Based on Recorded Future's data set, Anonymous KZ has minimal activity history, which largely coincides with the group's fragmented and largely old post history on YVision, as well as their dedicated [social media](#) pages.

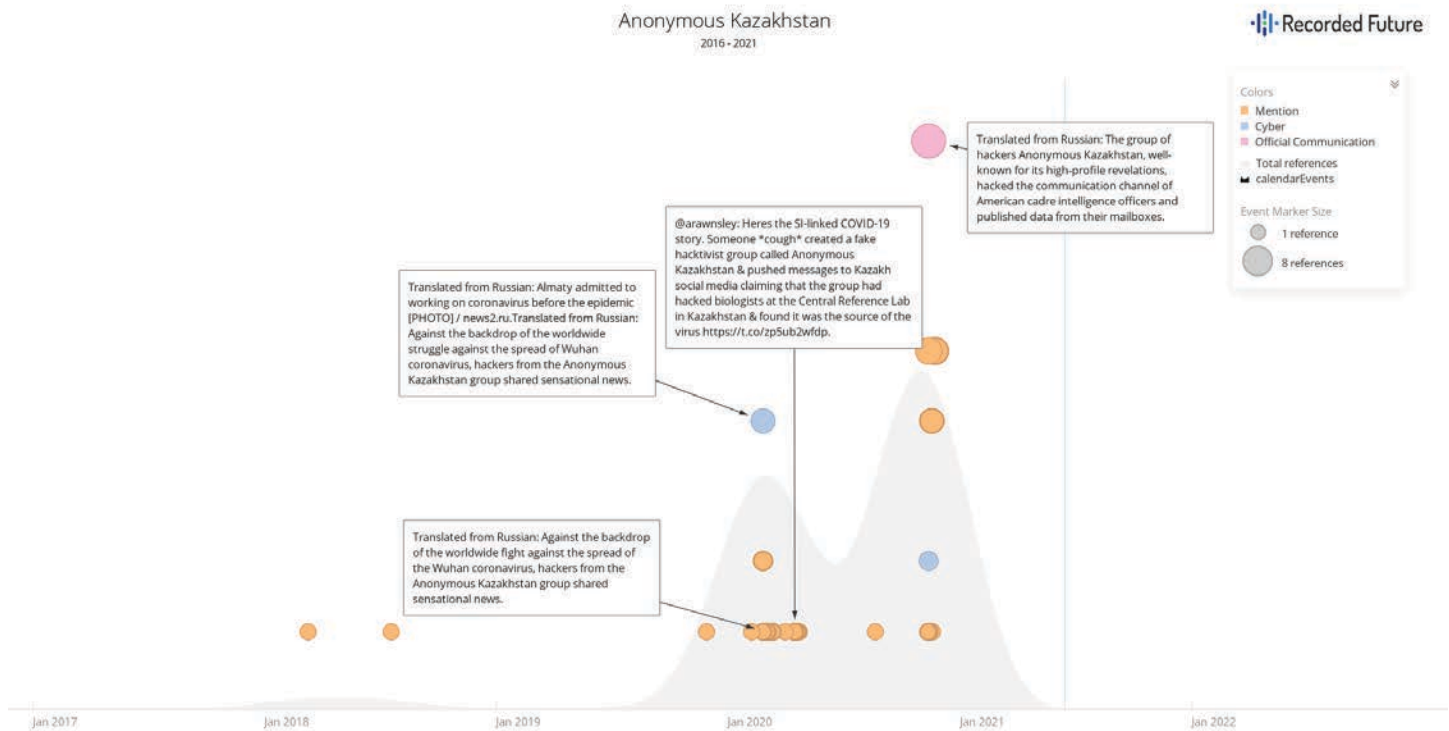


Figure 13: Recorded Future's Timeline View of mentions of Anonymous Kazakhstan (Source: Recorded Future)

From a strategic perspective, the objectives of Anonymous KZ do not align with the traditional motivations behind the hacktivist group Anonymous. Anonymous KZ takes an unusual geopolitical, nationalist stance against the US, a behavior atypical of Anonymous collective's historical standard of being anti-government or anti-establishment. Furthermore, Anonymous KZ's claims rely on an undisclosed HUMINT source rather than concrete evidence often presented in Anonymous cyber operations, such as DDoS attacks or validated leaked information from vulnerable databases.

Though the group takes on "Anonymous Kazakhstan" in name, these claims align much closer to Russian strategic objectives and ongoing overt disinformation efforts by Russian outlets. This is also coupled with the fact that Russian nation-state threat actors have been previously linked to domestic and international hacktivist organizations:

- None of Anonymous' public-facing media outlets have announced or disclosed any attacks on the CRL or leaked information. If the story about COVID-19 used as a bioweapon for economic gain were indeed true — and if there were concrete evidence of it — this would have likely reached primary Anonymous outlets and non-Russian and CIS sources.

- In reality, we observed minimal chatter of this activity outside of the aforementioned sources. This alone contradicts the accuracy of Anonymous KZ's claims as COVID-19 dominates news headlines around the world.
- The tactics of amplification through self-publishers and promotion through Reddit are identical to the tactics behind Secondary Infektion, which to date has been more closely attributed as work of Russian state-sponsored actors.
- In previous research, Recorded Future found that most of Russia's "grassroots" hacktivist organizations or operations have been [associated](#) with Russian intelligence organizations or linked to Russian government support.
- Insikt Group also found that one of the first purported hacktivism events emerging from Russia resulted in a series of DDoS attacks and other intrusions targeting Estonian government organizations in 2007. While initially attributed by researchers to domestic Russian hacktivists, some ultimately [blamed](#) the Russian state.

- In 2014, the hacking group CyberBerkut rose to [prominence](#) after they DDoSed NATO websites. While the group initially took on Ukrainian identities, technical blinks and contextual analysis provided by [Recorded Future](#) and other [organizations](#) have linked the group to the Russian state and the Russian Main Intelligence Directorate (GRU), respectively.

Minor Use of Established Personas in Secondary Infektion

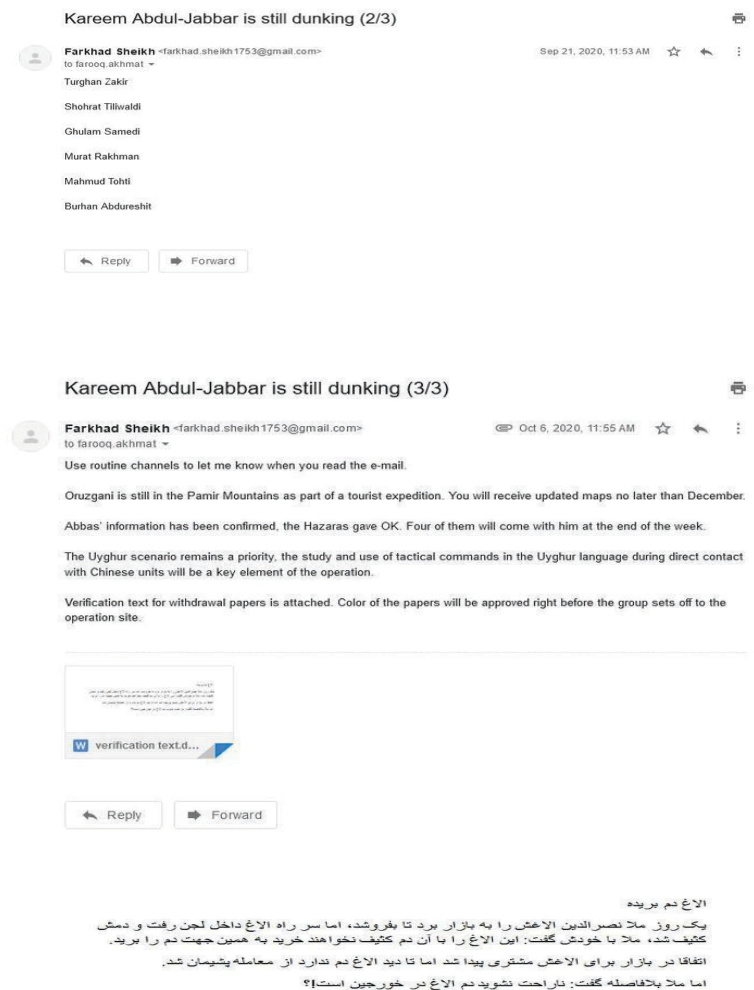
To date, one of the hallmark TTPs of Secondary Infektion has been the application of single-use personas to disseminate disinformation narratives. The largest drawback of this approach is the lack of a wide audience or strong following of these accounts. A significant audience of 1 account or 1 persona is not a requirement, but in situations where an influence operator uses a burner account, it is less likely that the account (or accounts across multiple sources) will receive the traction necessary to popularize a particular narrative.

In our analysis of Secondary Infektion sources in the past year, we have found 2 examples of Secondary Infektion influence operators using a multiple-use persona: the first is Anonymous KZ, and the other is a mysterious French-language persona that goes by the blog handle “SargArs”. These personas attempt to establish a reputation for disseminating content, and likely in the process hope to grow an audience through reputation, all while amplified through single-use accounts. In each of these following examples, however, their posting behaviors are highly irregular and do not in themselves establish a pattern of behavior.

Revisiting Anonymous Kazakhstan

Anonymous KZ, outside of claims that the novel coronavirus that spurred COVID-19 originated from a Kazakh-based US defense-funded laboratory, is an established persona, first appearing in mid-July 2019 as part of a campaign that claimed that the US and the EU planned to provoke violence in Kazakhstan (Of note, the campaign also called out Russia and China as being responsible). Three weeks after going live, Anonymous KZ went dormant until February 2020, when it reappeared with the Almaty biolab narrative. Creatively, Anonymous KZ attempts to appear authentic to the Anonymous collective, using branding and stylistic behavior of previous Anonymous operations and going so far as to filter fake images of text messages in a crafted video set to the tune of “[за волком и соколом](#)” by Holdaar for dramatic effect.

Following the Kazakh biolaboratory narrative it pushed in February and March 2020, Anonymous KZ [resurfaced](#) in late October 2020, claiming that it had breached communication networks of CIA intelligence officers and assets in Central Asia, exfiltrating alleged emails between these assets that seem to prove plans for a terrorist attack against the PLA units located in the Wakhan corridor along the border of Tajikistan and Afghanistan. In September 2016, China and Tajikistan [agreed](#) to a contract for the construction of border outposts in the region, allowing for the Chinese construction of up to 11 Tajik-staffed outposts as well as a training center for border guards.



Figures 14, 15, and 16: Anonymous KZ email forgeries. (Source: Recorded Future)

НА ТАДЖИККО-АФГАНСКОЙ ГРАНИЦЕ ГОТОВЯТСЯ МАСШТАБНЫЕ ПРОВОКАЦИИ

Нападение на китайских военнослужащих в Памире может серьезно дестабилизировать ситуацию в регионе и явно не останется незамеченным в мире событием. С одной стороны, может усугубиться положение уйгуров в Китае, с другой, КНР точно не оставит без внимания информацию о причастности к возможному инциденту США.

<https://picua.org/images/2020/11/16/2e850e09cf0bccbdc72e77a99afd7220.jpg>

Несмотря на то, что Таджикистан испытывает серьезные экономические трудности и является далеко не самым влиятельным геополитическим игроком в Центральной Азии, особое географическое положение страны привлекает к ней немало внимания. Ключевой проблемой для Душанбе остается приграничная зона с Афганистаном, на которой регулярно устраивают провокации террористы и давно обосновались наркоторговцы. Таджикистан пытается бороться с этими явлениями и для обеспечения безопасности на границе регулярно обращается за помощью к международным партнерам, самым активным из которых в последние годы стал Китай. Именно между КНР и Таджикистаном был подписан контракт на строительство пограничных застав в регионе еще в начале октября 2016 года. Благодаря помощи китайских специалистов на таджикско-афганской границе помимо пяти застав были построены три комендатуры, пять пограничных постов и один учебный центр.

Подобная активность китайских инженеров и военнослужащих в Таджикистане не прошла незамеченной в США. Вашингтон, который также наращивает активность в странах Центральной Азии и конкурирует за влияние в регионе с Китаем и Россией одновременно, почти сразу обвинил Пекин в создании военной базы на территории Таджикистана. И даже после официального опровержения данной информации США не смирились с присутствием китайских военных на границе с Афганистаном и решили не ограничиваться только дипломатическим противостоянием. Достаточно известная своими громкими разоблачениями группа хакеров Anonymous Kazakhstan взломала канал связи американских кадровых разведчиков и опубликовала данные с их почтовых ящиков <https://yvision.kz/post/869593>.

<https://picua.org/images/2020/11/16/025ce92c3c52797ef68981de85ac0430.jpg>

<https://picua.org/images/2020/11/16/af0d74b633d7a821f5ed714be25786f2.jpg>

Согласно обнародованной информации, в Памире уже работает завербованная ЦРУ группа и под видом туристов собирает разведданные. Затем эти сведения будут переданы конкретным исполнителям планируемых против подразделений ИОАК терактов - хазарейцам. Те, в свою очередь, будут обязаны при тактических командах использовать уйгурский язык и после совершенных нападений скроются в Афганистане, где при остановке патрулями предъявят листки следующего содержания.

<https://picua.org/images/2020/11/16/7eb3568bea490d7bd68b7731695b7b57.jpg>

Безусловно, нападение на китайских военнослужащих может серьезно дестабилизировать ситуацию в регионе и явно не останется незамеченным в мире событием. С одной стороны, может усугубиться положение уйгуров в Китае, с другой, КНР точно не оставит без внимания информацию о причастности к возможному инциденту США. Таким образом, попытка Вашингтона провокациями в Таджикистане нивелировать неудачу в Казахстане, где местная ЦРЛ в этом году публично отказалась от сотрудничества с американскими военными (в том числе из-за проведения ими незаконных исследований по COVID-19) может теперь обернуться еще более серьезным геополитическим провалом <https://delo.kg/?p=56453>. При этом для самого Таджикистана и Центральной Азии диверсии с участием иностранных спецслужб на границе с Афганистаном могут стать очень серьезным испытанием в плане безопасности, и грозят превратить регион в настоящий плацдарм для более масштабных вооруженных столкновений между Китаем и США в будущем.

Источник (<https://semey.city/blogi/narodnye-novosti/40903/>)

Figure 17: One of the first versions of the story appearing on the blog site [Semey City](https://semey.city/). The blog failed to load the images intended to be embedded, showing raw URLs of where copies were hosted. (Source: Recorded Future)

Anonymous KZ claims that the CIA, under the guise of tourists, are working with local assets to conduct preliminary reconnaissance of the border area, allegedly with the help of an asset named “Abbas” who is supported by individuals tied to the Hazaras Shia Muslim minority ethnic group that primarily resides in Central Afghanistan.

According to Anonymous KZ's analysis of the emails and attached document, Abbas's Hazaras group, under the command of US intelligence and disguised as Uyghurs and using Uyghur-language tactical commands, were directed to launch an attack on the PLA at the border. The motivation of this narrative is not entirely clear, and could lead to a few possibilities, including stoking ethnic tensions among local Afghan groups, spurring distrust about the US and CIA's footprint in Afghanistan, and potentially even attempting to stoke fears among Chinese political and military officials with possible Uyghur separatist attacks on PLA units in the area.

As expected, influence operators [attempted](#) to use Russian/CIS-based self-publishers to spread these images, as well as attempted language leap into English on the forum “[House of Politics](#)”, [Medium](#), and a purported US-news website called “[USA News Today](#)”. Regardless of language, each author presented these alleged findings under the pretext that, if successful, the operation would likely turn the region into a springboard for future larger-scale conflict between China and the US.

The attached image, shown in figure 16, above, which was instructed to be used by operatives crossing the Tajikistan-Afghanistan border, makes little sense on the surface. The note, written in Farsi, is likely a play on a well-known Islamic folk tale known as “Mullah Nasruddin And His Donkey”, and is perhaps intended to serve as a code of sorts. The text is otherwise random and out of place.

The translated text reads as follows:

“One day, Mullah Nasruddin took his donkey to the market to sell it, but the donkey fell into the mud and got his tail dirty. The Mullah said to himself “this donkey won't sell with a dirty tail” so he cut it off. It just so happened that he found a customer for the donkey, but once they saw the donkey had no tail, they were uninterested. The mullah said at once, don't worry — the tail is in the saddlebag!”



Русский Демидур

На таджикско-афганской границе готовятся масштабные провокации

Несмотря на то, что Таджикистан испытывает серьезные экономические трудности и является далеко не самым влиятельным геополитическим игроком в Центральной Азии, особое географическое положение страны привлекает к ней немало внимания. Ключевой проблемой для Душанбе остается приграничная зона с Афганистаном, на которой регулярно устраивают провокации

Figure 18: A Russian [Telegram account](#) with an audience of 16,000 subscribers in 2021, attempted to amplify this story a week after Anonymous KZ published its “findings”; approximately 4,000 subscribers have viewed this post since November 6, 2020. (Source: Recorded Future)

The Russian Telegram account (name translated to “Russian Demiurge”) shown above was likely this story's best chance of success in reaching mainstream sources. Shortly after Russian Demiurge posted the story on Telegram, it was featured on the Russian-language mirror for News Front, a Crimea-based disinformation and propaganda multimedia outlet believed to be under the direction of the Russian Security Service (FSB)

according to the US State Department. In this case, however, the article did not receive any substantial additional engagement.

At this time, we consider News Front's sharing of this specific story to be more of a coincidence than a concrete link between Secondary Infektion and Russian intelligence. In our monitoring of this outlet, News Front regularly cites and republishes content in the areas of military news and geopolitics, often within the bounds of the Russian strategic viewpoint. This content often originates from suspect or otherwise non-vetted sources, like obscure Telegram channels with no direct or otherwise visible relation to News Front.

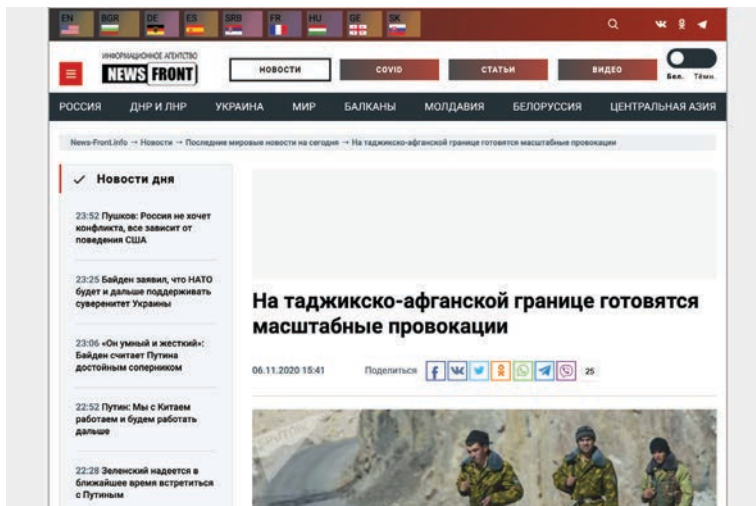


Figure 19: Story from Anonymous KZ reaching feeds on FSB-linked News Front (Source: Recorded Future)

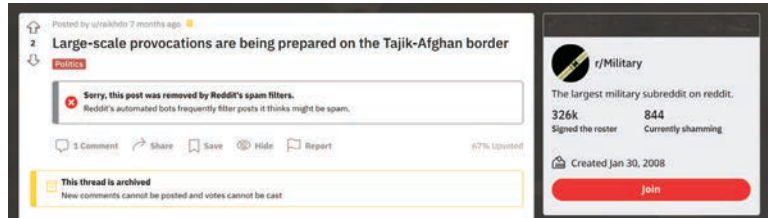


Figure 21: "raikhdo" also attempted Reddit promotion, but failed. Reddit's spam filters successfully countered this post before it gained any notable traction, and u/raikhdo is suspended from Reddit as of 2021. (Source: Recorded Future)



Figure 22: A "Fact-checked" English-language copy of the story on USA News Today, written by a "Sandra Brown" (Source: Recorded Future)

SargArs's Attempts to Provoke Revolution in Armenia

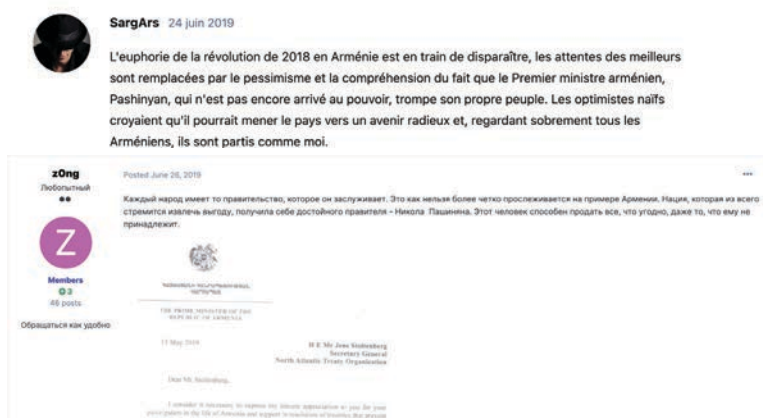
The likely Secondary Infektion persona "SargArs", who also goes by the alias "Sargise Arshakuni", is a French-speaking Armenian expatriate with a keen interest in Armenian political affairs and a particular disdain for Armenian Prime Minister Nikol Pashinyan. Based on the account's post history, this account first appeared in June 2019 with the article "Le destin du Haut-Karabakh est résolu" (translated: "Nagorno-Karabakh's fate is determined") alongside a likely forgery (available in the Appendix) emulating correspondence between Prime Minister Pashinyan and NATO Secretary-General Jens Stoltenberg.



Figure 20: "raikhdo" sharing an English version of the claim on House of Politics. It is likely that raikhdo is the same author as "Donald Raikh" on Medium. (Source: Recorded Future)

Broadly speaking, the fake document, along with a blog article, attempted to convey a message that, under the direction of the US and partially motivated by the “business interests” of the so-described “Pashinyan Mafia”, Armenia is likely to join the NATO alliance at a great loss to its citizens, including the alleged impending surrender of over 50% of Nagorno-Karabakh to Azerbaijan, foiled economic opportunity, and the country’s loss of standing with other regional nations. SargArs seemingly attempted to provoke unrest in Armenia against the current government with the statement at the end of their post, indicating, “I would like to hope that Armenians can avoid the fate of silent slaves, not succumb to provocations and regain their independence and the right to a normal life, albeit at the cost of a new revolution”.

Le destin du Haut-Karabakh est résolu



Figures 23 and 24: Attempted language leap from French to Russian, with little traction (Source: Recorded Future)

In early July 2019, Armenian information security expert Samvel Martirosyan [alerted followers](#) to the fake document, and Armenian outlet [Panorama](#) asked the prime minister’s office for comment on the fake. According to Vladimir Karapetyan, Spokesperson for Prime Minister Pashinyan, “it is evident for all [that] the document is nothing but absurdity”.

For over a year between June 2019 and November 2020, SargArs was silent, mirroring the myriad of one-off burner personas that periodically demonstrate TTPs strongly similar to those linked to Secondary Infektion. On November 26, 2020, the persona resurfaced with a new blog post titled “Pachinian: la trahison et ses conséquences” (translated: “Pachinian [sic]: treason (or betrayal) and his consequences”) with another fake letter, again targeting Armenian audiences with anti-Pashinyan content, calling the prime minister a “traitor” and actor who has “tormented” the “unhappy Republic of Armenia”.

Pachinian: la trahison et ses conséquences



SargArs 26 nov. 2020 Modifié

2020 ne cesse d'étonner. Épidémie, guerres, politique sale - tout cela est tombé en 2020, trop, trop. Je voudrais m'arrêter plus en détail sur les événements fatidiques qui se déroulent en Arménie.

Tous ces procès sont tombés au sort de la malheureuse République d'Arménie, tourmentée par la politique du traître Pachinian. En conséquence, les Arméniens ont perdu leur territoire ancestral, le

Figure 25: SargArs reappearing on his blog page, November 2020 (Source: Recorded Future)

SargArs’s grievances against the Armenian government include “the virus, the economic crisis, [and] corruption”, as well as “the refugee problem and the historic pain of the loss of historic land” most likely alluding to Nagorno-Karabakh. SargArs references back to their June 2019 letter between Pashinyan and Stoltenberg and pleads with their audience, hoping that “everyone will have the tact not to ask me where I got this information from, but at the same time, they will be smart enough to believe in the truth of this information, since now events are unfolding exactly according to the scenario described”, stating “Pachinian [sic] showed perseverance and the Armenians lost Nagorno-Karabakh”.

SargArs, citing a fake letter again between Pashinyan and Stoltenberg (available in the Appendix), states that Pachinyan “continues to work for the United States more than Armenia” and assesses that “he [Pashinyan] is ready, at the cost of the Armenian army ... to help strengthen Turkey in the South Caucasus region”. Using the document as evidence, SargArs hopes that [Pachinyan] “will face not only resignation and evacuation to Washington but well-deserved punishment under the laws of war. For my part, I [SargArs] have done my best for this”.

Less than one week later, as late as December 1, 2020, copies of this forgery began appearing on Russian-language open-source forums, such as [grodno\[.\]net](#), from a persona under the name “tigranramazyan”. The level of dissemination was minimal, only appearing on a handful of Russian-language websites, with no real additional amplification.

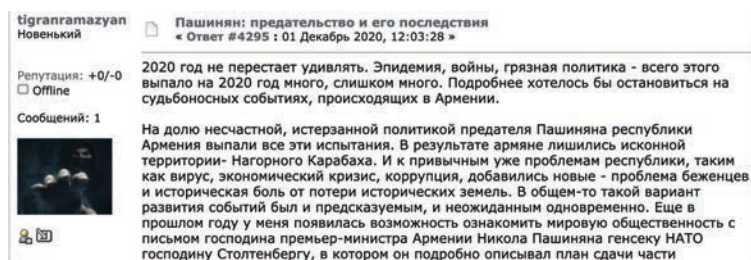


Figure 26: “Tigranramazyan” on grodno[.]net (Source: Recorded Future)



Тигран Рамазян

01.12.2020 в 3:25

Политика

Пашинян: предательство и его последствия

После проигрыша в Нагорном Карабахе Пашинян готовит новую авантюру. 2020 год не перестает удивлять. Эпидемия, войны, грязная политика - всего этого выпало на 2020 год много, слишком много. Подробнее хотелось бы остановиться на судьбоносных событиях, происходящих в Армении. [Читать далее](#)

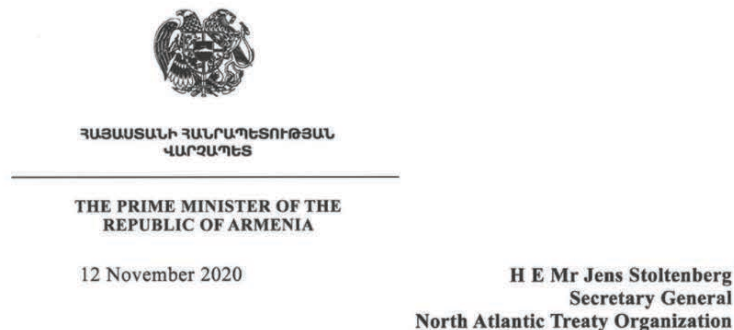


Figure 27: "Tigran Ramazyan" copying content over to mirtesen.ru (Source: Recorded Future)

Labeling a Forgery a Fake to Generate Additional Confusion

Throughout our monitoring period, Insikt Group observed Secondary Infektion influence operators pushing forgeries and other fakes with blog articles and website posts under the assumption that the crafted document, webpage, or claim was entirely true. Though an otherwise consistent tactic, in July 2020 we found these operators called out one forgery as a fake in an attempt to give validity to their disinformation narratives and likely generate additional confusion and discord among their targets. This specific case [sought](#) to strain relationships between the Republic of Georgia and Ukraine by using 2 copies of the same forgery document, with 1 copy promoted in CIS sources as authentic, and a later copy circulating other CIS-based sources with a stamp labeled as "fake".

This specific campaign attempted to exploit an alleged rift between former Georgian President Mikheil Saakashvili and Ukrainian Minister of Internal Affairs Arsen Avakov. The first forged [document](#), the crux of the disinformation effort overall, claimed that the "ex-head of the Odessa Regional State Administration" [Saakashvili] asserts the need for [Arsen] Avakov's resignation (to be replaced with Gia Lordkipanidze) and threatens negative consequences for a number of ministers, deputies, and even the president (of Ukraine)".



NATIONAL REFORMS COUNCIL
НАЦІОНАЛЬНА РАДА РЕФОРМ

Вих. №30062020-02 від 30 червня 2020 року

Голова Виконавчого комітету реформ Національної Ради України
Саакашвілі М. Н.

Прем'єр-міністру України
Шмигалью Д. А.

Шановний Денисе Анатолійовичу!

Реформування Міністерства внутрішніх справ вимагає кардинального перегляду кадрової політики на найвищому рівні. На жаль, спроба відставки міністра Авакова не мала успіху, в тому числі й через Вашу позицію. Між іншим, збереження за Аваковим посади Міністра внутрішніх справ загрожуватиме Україні серйозною політичною кризою, бо концентрування в руках голови МВС владних повноважень та політичного впливу, які підкріплені багатотисячними підрозділами добре озброєних бойових формувань, може негативно позначитися на перспективах України як демократичної держави. Більш того, як показує практика, Аваков має схильність вирішувати політичні та інші розбіжності, використовуючи весь спектр ресурсів, які йому доступні, і тому існує реальна загроза для всіх політичних сил, які, на його думку, беруть участь у тиску на МВС і особисто на нього. Отже, в небезпеці перебувають не тільки демократичні цінності, але й політична система України в особі низки міністрів, депутатських груп у Верховній Раді та самого Президента.

Крім того, твердження про незамінність Авакова на посаді голови МВС я вважаю в корені невірним. В Україні достатньо спеціалістів високого рівня, які здатні реформувати правову систему та створити для МВС образ некорумпованого, відкритого та сумлінно працюючого міністерства. Зокрема, це завдання готовий вирішити Гія Лордкіпанідзе, який має величезний досвід роботи на відповідних посадах, як у Грузії, так і в Україні. Як голова Виконавчого комітету Національної ради реформ України, запевняю Вас, що реформування правової системи країни можливо лише шляхом залучення відповідальних та професійних кадрів замість посадовців, які дискредитували себе численними корупційними скандалами.

Хотілося б підкреслити, що жодні демократичні реформи в Україні неможливі, поки злочинці та корупціонери на вищих посадах відстоюють свої особисті інтереси, маючи при цьому досить серйозні повноваження та вплив. Це ставить хрест не тільки на перспективах євроатлантичної інтеграції України, але й на її функціонуванні, як вільної та правової держави.

З повагою,

Head of the Reforms Executive Committee of the National Reforms Council of Ukraine
MIKHEIL SAKASHVILI

Голова Виконавчого Комітету Реформ Національної Ради Реформ
МИХЕЛІ НІКОЛОЗОВИЧ СААКАШВІЛІ



NATIONAL REFORMS COUNCIL
НАЦІОНАЛЬНА РАДА РЕФОРМ

Вих. №30062020-02 від 30 червня 2020 року

Голова Виконавчого комітету реформ Національної Ради України
Саакашвілі М. Н.

Прем'єр-міністру України
Шмигалью Д. А.

Шановний Денисе Анатолійовичу!

Реформування Міністерства внутрішніх справ вимагає кардинального перегляду кадрової політики на найвищому рівні. На жаль, спроба відставки міністра Авакова не мала успіху, в тому числі й через Вашу позицію. Між іншим, збереження за Аваковим посади Міністра внутрішніх справ загрожуватиме Україні серйозною політичною кризою, бо концентрування в руках голови МВС владних повноважень та політичного впливу, які підкріплені багатотисячними підрозділами добре озброєних бойових формувань, може негативно позначитися на перспективах України як демократичної держави. Більш того, як показує практика, Аваков має схильність вирішувати політичні та інші розбіжності, використовуючи весь спектр ресурсів, які йому доступні, і тому існує реальна загроза для всіх політичних сил, які, на його думку, беруть участь у тиску на МВС і особисто на нього. Отже, в небезпеці перебувають не тільки демократичні цінності, але й політична система України в особі низки міністрів, депутатських груп у Верховній Раді та самого Президента.

Крім того, твердження про незамінність Авакова на посаді голови МВС я вважаю в корені невірним. В Україні достатньо спеціалістів високого рівня, які здатні реформувати правову систему та створити для МВС образ некорумпованого, відкритого та сумлінно працюючого міністерства. Зокрема, це завдання готовий вирішити Гія Лордкіпанідзе, який має величезний досвід роботи на відповідних посадах, як у Грузії, так і в Україні. Як голова Виконавчого комітету Національної ради реформ України, запевняю Вас, що реформування правової системи країни можливо лише шляхом залучення відповідальних та професійних кадрів замість посадовців, які дискредитували себе численними корупційними скандалами.

Хотілося б підкреслити, що жодні демократичні реформи в Україні неможливі, поки злочинці та корупціонери на вищих посадах відстоюють свої особисті інтереси, маючи при цьому досить серйозні повноваження та вплив. Це ставить хрест не тільки на перспективах євроатлантичної інтеграції України, але й на її функціонуванні, як вільної та правової держави.

З повагою,

Head of the Reforms Executive Committee of the National Reforms Council of Ukraine
MIKHEIL SAKASHVILI

Голова Виконавчого Комітету Реформ Національної Ради Реформ
МИХЕЛІ НІКОЛОЗОВИЧ СААКАШВІЛІ

Figures 28 and 29: July 2020 examples of [Secondary Infection](#). Two copies of a forged document emulating correspondence between former Georgia President Mikheil Saakashvili and Ukrainian Prime Minister Denys Shmyhal. Left: The original fake document spread on blog sites and self-publishers, and Right: a rebuttal forgery, which calls out the forgery as a fake. This is most likely to create additional doubt and confusion. (Source: Recorded Future)

We have included each copy of the document below both of which were included with a corresponding editorial article appearing on multiple Russian and Ukrainian self-publishers:

This campaign continued through mid-July 2020 before going dormant, appearing in 3 distinct waves, principally through the expected amplification and Reddit promotion via the Ukrainian subreddit r/Ukraina. We believe that this campaign, though deliberate and persistent in its efforts to break through to mainstream sources, was unsuccessful. The 3 waves were:

- Wave 1: Initial introduction of the forgery via blog sites, self-publishers, and rogue news websites in Eastern Europe.
- Wave 2: A rebuttal piece to the initial forgery document, representing the document with the label “FAKE” across the document, accusing individuals of the Ministry of Internal Affairs for spreading the forgery.
- Wave 3: Presentation of both documents, capping off by further proposing that the “purpose of the information attack was discrediting Saakashvili in the eyes of Ukrainians and the political elite, and the authors of the forgery are the employees of the Ministry of Internal Affairs”.

There are 2 underpinning issues that have made Ukraine and Georgia attractive targets for similar disinformation campaigns:

Georgia and Ukraine both once hoped to join NATO (pre-2008). Both countries have significant Russian-speaking populations, and both have significant ethnic Russian populations. Vladimir Putin in particular has long lamented NATO’s eastward encroachment towards Russian borders. Both nations have now each suffered very bloody wars at the hands of Russia. It is likely that this is a recent example of Russian efforts to drive a wedge between the two allies and their close strategic and diplomatic relations.

- Vladimir Putin has stated (and this is now enshrined in the new constitutional amendment) that he is willing to try to unite all Russian-speaking peoples and ethnic Russians in the near abroad; this is largely a ploy to reclaim land lost as a result of the fall of the Soviet Union, which he has [lamented](#) as the “greatest geopolitical disaster of the [20th] century”. The war in Georgia, ostensibly as viewed in Russia, was to “protect” the Russian-speaking peoples of South Ossetia, which is part of Georgia and falls under its sovereignty entirely; immediately after the war, Vladimir Putin granted a Russian passport to anyone in South Ossetia who sought one. This allows Vladimir Putin to act on “protecting” Russian interests in the area but also obtain a certain level of control over the territory. Similar situations apply to Crimea, the Donbas region of Ukraine, and other potential hotspots for future destabilizing efforts in the Baltics (most likely Estonia and Latvia).

Secondary Infektion Operators Infiltrate Far-Right Favored 4chan

As discussed earlier, we noted that Secondary Infektion operators attempted to capitalize on the substantial mis- and disinformation over COVID-19 in the earliest months of the pandemic. As part of this effort, we uncovered evidence of likely Secondary Infektion influence operators infiltrating 4chan’s /pol/ board, a forum notable for frequent far-right extremist posts, in a probable attempt to stir both anti-Muslim sentiment amid COVID-19 and drive pandemic disinformation narratives. At the same time, as narratives of this event appeared in primarily Russian-language sources, the influence operators likely viewed this campaign as an opportunity to also promote anti-US sentiment among domestic audiences within the CIS. We believe this information operation is highly likely to be a case of Secondary Infektion, based on the repeated pattern of behavior reflected in other Secondary Infektion campaigns (to reiterate, the recurrent use of single-use personas, the copy-and-paste nature of divisive narratives on self-publishing sources, and target audience).

On March 26, 2020, we located an anonymously posted article published on the self-publishing website [Perevodika](#), promoting a narrative that far-right Americans are actively blaming the Muslim population for the spread of COVID-19. The article, titled “The American Ultra-Right Accuse Muslims of Making Pleas to Spread Coronavirus” (Russian: “Американские ультраправые обвиняют мусульман в призывах распространять коронавирус”) was what we determined at the time to be the seed source for promotion on other CIS-based self-publishing sites. Further investigation into other sites uncovered multiple, single-use false author personas, a regularly demonstrated and persistent TTP associated with Secondary Infektion efforts.

The article published on Perevodika cites a post on 4chan’s /pol/ board, referring to the forum as a source of “a huge number of representatives of ultra-right white supremacists of the USA”. The story notes that “an entertaining picture surfaced with an alleged appeal to Muslims to spread the coronavirus around the world”, posted by an anonymous 4chan ID “cQjPLDKk” in a thread on /pol/ that was discussing the Christchurch, New Zealand mosque shootings on March 15, 2019.



Figure 30: The post and image in question identified on 4chan (Source: Recorded Future)

Per the post, the text within the image, written in Arabic, is addressed to Muslims who are puzzled by COVID-19 and do not know what to do to protect themselves from the virus. This image states that COVID-19 is punishment for Europeans, and Muslim biological immunity is supposedly stronger than that of the Europeans and they are therefore safe, despite reports of infections. Further, the blog posts suggest that followers were chosen to spread COVID-19 abroad “until the complete victory of Islam and the elimination of all obstacles to the resettlement of Muslims to Europe”.

The post states that the image presents a series of phrases “that could come from the mouth of the radical”, but admits the translation is poor, writing, “But the trouble is: the text in the picture is an obvious and inept translation”. In consultation with native Arabic speakers, Insikt Group confirmed that this text contained multiple grammatical, stylistic (such as punctuation marks and links between sentences), and contextual errors (lack of reference to context within the Quran, for example) that are most likely to be made by a non-native speaker or non-specialized person (meaning someone unlikely to be a religious extremist).

The blog posts conclude that the message is a beneficial citation to 4chan’s ultra-right audience “to justify their prejudice against all who are not members of the white race”, stating at the end that “at a time when we all need solidarity and unity, unfortunately, there are forces trying to strengthen the chaos reigning in the world”.

Recorded Future investigated the screenshot in the Perevodika article and verified that this post was [authentic](#). In prior cases of Secondary Infektion, we identified that operatives disseminated forged screenshots within Russian-speaking blog posts, though this was not the case here.

The prominence of this screenshot on Russian-language blog sites, which Recorded Future found reposted across more than 20 self-publishing websites primarily from Russia and Ukraine, is unusual. Furthermore, based on timestamps of the 4chan post and the seed article on Perevodika, Recorded Future found that this article was drafted and published approximately 5 hours after the post was made on 4chan; we believe that the short turnaround suggests an association and likely coordination between the seed article and the 4chan user. Like most prior cases of Secondary Infektion, with the exception of the two multi-use personas detailed in this report, one-off author personas were relied upon to promote these posts. In this case, we identified individuals under the name “[Mikhail Potapov](#)” and the username “[mihpotach](#)”, as well as attempted Reddit promotion under the username “[u/paartchuk](#)”, which we linked to the one-off persona “[Artyum Parchuk](#)”.

Based on this 4chan discussion’s suspicious appearance on sources regularly featured in Secondary Infektion, as well as the convergence of multi-wave article postings synonymous with this information operation, it is very likely that the image of Arabic text is a forgery. Though we do know that extremist groups, such as the Islamic State, initially [attempted](#) to capitalize

on the pandemic as a backdrop to conduct attacks in cities hardest hit by COVID-19, the organization [specifically directed](#) followers not to spread the virus abroad, as well as adhere to strict hygiene standards for their personal wellbeing. If our assessment is accurate, this most recent observation provides further evidence that likely Russian-speaking operatives can and do have a presence on forums with fringe audiences such as 4chan. This example specifically also indicates that these operatives are actively attempting to exhibit prejudices of the ultra-right, consistent with historical targeting of societal divisions in the US.

Fake Social Media Post Purportedly From Texas Governor Greg Abbott About Biden Administration and Ukraine

In our initial April 2020 analysis, we anticipated that Secondary Infektion influence actors were likely capable of using this campaign's well-documented TTPs to engage in public influence ahead of the 2020 US presidential election cycle, just as closely mirrored TTPs had before the UK elections of 2019. Part of this assessment was based on these actors' previous use of emulating correspondence among and between high-profile US officials and international organizations and other policymakers, as well as the clear anti-US and overall anti-West sentiment across all of the examples of Secondary Infektion cases. Ultimately, Secondary Infektion, to the best of our knowledge and tracking, did not specifically target the 2020 presidential cycle, but we do know that actors engaging with this campaign were aware of hot-button issues surrounding the election.

In tracking Secondary Infektion's repeated patterns of behavior, we specifically, in at least 1 example, found influence actors responsible for this campaign attempting to draw from political discussions of President Joe Biden's political and family affairs in Ukraine. Using a social media forgery, likely Secondary Infektion influence operators repurposed these narratives to target Eastern European audiences with the goal of generating discontent and doubt into US commitments to regional security.

On March 31, 2021, Insikt Group [identified](#) a Ukrainian self-publishing website disseminating disinformation about the Biden administration's policy toward Ukraine. From late March to early April 2021, this self-publisher and others disseminated copies and versions of an article titled "Biden-Poroshenko. How does Ukraine influence US policy?" (Ukrainian: Байден-Порошенко. Яким чином Україна впливає на політику США?) circulating in Ukrainian and Russian, authored by individuals using the aliases "[andrimelnic](#)" or "Andriy Melnyk" (Андрій Мельник), a "[naisvladislav](#)" aka "vladiknice" or "Vladislav Nice" (Владислав

Найс), and an "[andreysimon](#)", or "[Andrey Simon](#)". We consider the post of the article identified on the self-publisher website gurt.org[.]ua as the seed for this campaign, based on additional websites reposting these articles referencing this website as the original source of the story, many of which are still available to view.

The article asserts that the (at the time of publication) new Biden administration was hesitant to communicate with Ukrainian President Volodymyr Zelensky and claims, falsely, that the Biden Administration "does not regard Ukraine as its key ally". In another [version](#) of the story, published by "naisvladislav", an additional author's note suggests that former President Petro Poroshenko "has some compromising evidence on the Biden family" and has extorted this information to guarantee himself as the next prime minister of Ukraine. The article predicts that if Poroshenko becomes prime minister, it is sufficient evidence to support allegations of corruption against President Biden, which were among the leading US political discussion topics leading up to the 2020 US presidential election.

The article includes a screenshot of a post purportedly from Texas Governor Greg Abbott's verified social media profile. The text from the post reads as follows:

"Biden's [sic] is the first Admin. in US history forced to pander to a Third World Country.

Can't wait for the public disclosure.

Foreign policy crisis caused by the Biden Admin. is just beginning & will get far worse.

Btw how is Hunter [Biden] doing?"

The post includes a photo of President Biden (as vice president) meeting with former Ukrainian President Petro Poroshenko taken during their meeting in Washington on December 7, 2015.



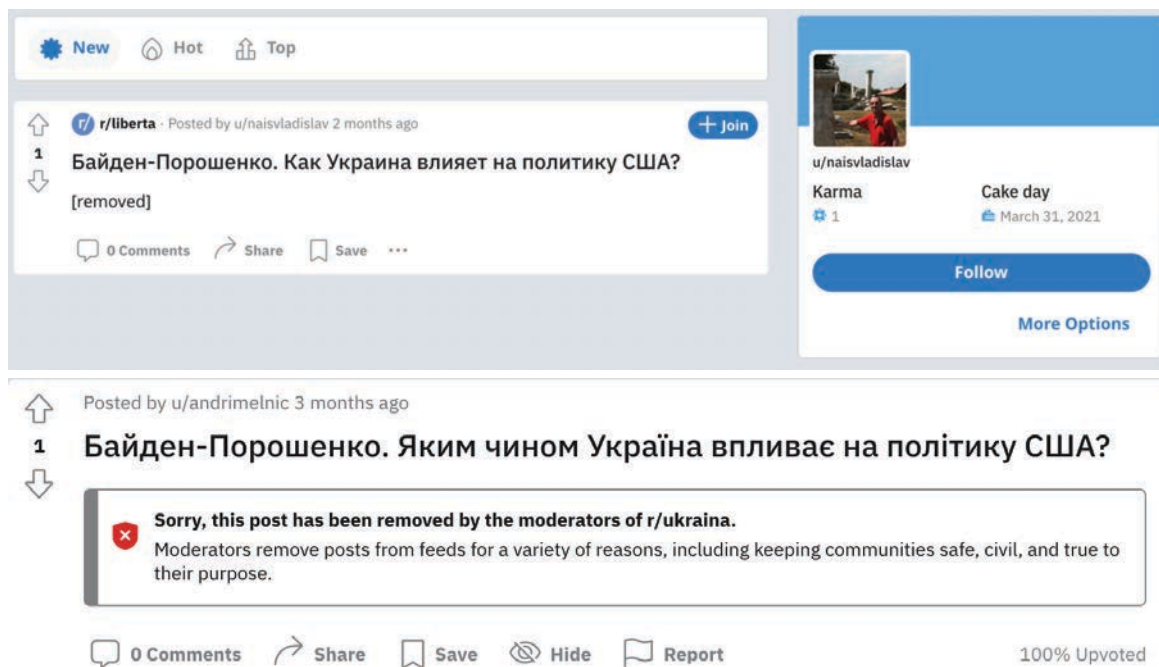
Figure 31: The fake post purportedly from the social media account of Texas Governor Greg Abbott (Source: Recorded Future, [Archive](#))

The screenshot is almost certainly a forgery, likely generated through off-the-shelf editing tools. Our judgment is further validated in an error level analysis (ELA) of the source image, which suggests at least some digital modification. There is no documented history of Governor Abbott posting this message. In addition to this, we consider the subject matter (a US state governor combatively discussing foreign affairs on social media) suspicious, not to mention blatant errors in grammar, atypical of a formal government account.

Insikt Group considers the authors of these posts as inauthentic single-use personas created solely to further disseminate these articles across blogs and websites with negligible moderation policies. These accounts, like most others we have linked with Secondary Infektion, had a short life span, publishing only 1 article per website, and they were created shortly before posting. After posting the article, these accounts, like most others we have tracked, were abandoned.

As expected, influence operators attempted social media and Reddit promotion with newly registered Reddit users [u/andrimelnic](#) and [u/naisvladislav](#) publishing this story on [r/ukraina](#) and [r/liberta](#). This activity on Reddit further indicates that this incident is likely both linked.

To improve the account's OPSEC, these accounts frequently attempt to pose as legitimate individuals by using authentic headshots; in this case, we have found in an open-source investigation that the photos of Andriy Melnyk and Andrey Simon are highly likely to have been stolen from Russian and other CIS-based dating websites, based on reverse image searches of the profile photos. We believe that Secondary Infektion operators frequent regional dating sites as a source for obtaining a believable profile photo to add authenticity to their profiles. Similar dating websites, personal blog pages, and at times social media, provide easy-to-obtain — albeit voluntarily provided — personal details (like a photograph) which are likely to be of use when developing a burner persona that attempts to balance authenticity with OPSEC.



Figures 32 and 33: [u/naisvladislav](#) attempts to post on [r/liberta](#) were ultimately unsuccessful. The user [u/andrimelnic](#) has since been [deleted](#). (Source: Recorded Future)

Сайты с информацией про изображение




169x300

Scott, Мужчина из США, Scottsdale

Cuteonly.ru

Scott,38-1



100x150

Go to image page

Cuteonly.ru

Самые популярные 34 - 42 лет



56x99

Блоги - I.UA

Blog.i.ua

andrimelnic

Сайты с информацией про изображение



100x100

Utilizatorii site-ului

Dosug.md

Utilizatorii site-ului



100x100

Андрей

Dosug.md

Свадьба (0). Места развлечений (0). Форумы (0). Фильмы (0). Работа (0).




100x100

Непрочитанное - КАЗАХСТАНСКИЙ ЮРИДИЧЕСКИЙ ФОРУМ

Forum.zakon.kz

Перейти в профиль пользователя andreysimon. andreysimon.




300x533

Хочу познакомиться. Dmitri из Белоруссии, Минск, 36

Cuteonly.ru

Dmitri,36-1




300x533

Мужчины возрастом от 34 до 37 лет рыбы

Cuteonly.ru

Мужчины возрастом от 34 до 37 лет рыбы

Figures 34 and 35: Profile photos for both Andriy Melnyk and Andrey Simon, stolen from Russian dating websites, most notably cuteonly[.]ru (Source: Recorded Future)




31 МАРТА 11:23

0 комментариев 0 просмотров за сутки

Владислав Найс, 31 марта 11:23

2 фотографии





Andrew Poulter (Patron of Honour of the DANUBIUS Project)

- Archaeology
- Emeritus Professor / Research Professor
- University of Nottingham / University of Birmingham (United Kingdom)

Figures 36 and 37: Vladislav Nice's profile photo appears to be likely stolen from this profile of UK-based professor Andrew Poulter (Source: Recorded Future)

Outlook

Secondary Infektion is almost certainly an ongoing information operation and regularly demonstrates its persistence in promoting false narratives with minimal adjustments in TTPs, sources, or broader methodology. Though not directly included in this report, we have identified and documented several other examples of mainly Eastern European-centered Secondary Infektion campaigns in the past year, including:

- The [targeting](#) of Turkmen political affairs, [suggesting](#) that Turkmenistan will join the Collective Security Treaty Organization (CSTO)
- Attempts to [undermine](#) the Moldovian government and its ability to support its citizens
- Attempts to [exacerbate](#) European tensions and hostilities towards refugees and refugee camps
- The creation of political rifts in Sweden through an [active campaign](#) to emulate the Swedish parliament with a declaration that Sweden and Ukraine together will join NATO

Sources we identify as linked with Secondary Infektion information operations are regularly tracked, and validated instances of these information operations are available for further investigation for existing Recorded Future clients.

In many ways, these efforts are seemingly regimented and are strongly reflective of organizational behavior that is hesitant to change, such as formal government. Almost exclusively, we have found that these operators use static media and imagery to promote their campaigns, so far shying away from significantly manipulated or machine-generated disinformation, such as deepfake photos and video.

Researchers have attempted to link this information operation with suspected Russian military intelligence, however, given that Secondary Infektion places a large emphasis on OPSEC, attribution is an incredibly difficult task. That said, we remain confident that this is a coordinated and methodical operation perpetrated by Russian state-sponsored actors and the tactics demonstrated throughout the history of Secondary Infektion broadly remain strongly reminiscent of Active Measures campaigns most commonly conducted through Soviet and Russian security services.

Appendix — Letters Published via SargArs



ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱՊԵՏ

THE PRIME MINISTER OF THE
REPUBLIC OF ARMENIA

13 May 2019

H E Mr Jens Stoltenberg
Secretary General
North Atlantic Treaty Organization

Dear Mr. Stoltenberg,

I consider it necessary to express my sincere appreciation to you for your participation in the life of Armenia and support in resolution of troubles that prevent extending of cooperation with NATO. Understanding your deep concern with the role Armenia plays for security in the region, I am in a hurry to inform you that the agreements we reached earlier, the reliability of which you confirmed during a personal meeting in January of this year, are close to be implemented by us. The main obstacle to the rapprochement of Armenia with NATO – the presence of Armenian troops on the territories disputed with Azerbaijan – is to be eliminated within a year. In the framework of the plan on withdrawal of the Armenian troops from the conflict zone and transfer of control over the disputed territories to Azerbaijan, a question on desirability of further support of Nagorno-Karabakh by Yerevan will be submitted to a national referendum. No doubt, such an initiative will cause a negative response from the most of the Armenian nation, and the special groups controlled by us will provoke protests to make an illusion of destabilization of the domestic situation and create a convincing pretext to move the troops from Nagorno-Karabakh inside the country.

In turn, I ask you for assistance to be sure Azerbaijan secures the commitments under which its control will be re-established exactly over 50 percent of Nagorno-Karabakh. Wherein I affirm the leadership of Armenia agrees the rest of Nagorno-Karabakh will be a neutral gray area with a possibility of obtaining autonomy. I reckon on you to control Azerbaijani actions setting out prevention of the violation of existing agreements as well.

I hope that mutually beneficial respect of the interests contributes to the development of cooperation between NATO and Armenia, and guarantees peace and stability in the entire South Caucasus region as well.


NIKOL PASHINYAN



ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱԴԵՏ

THE PRIME MINISTER OF THE
REPUBLIC OF ARMENIA

12 November 2020

H E Mr Jens Stoltenberg
Secretary General
North Atlantic Treaty Organization

Dear Mr. Stoltenberg,

Being your sincere follower and loyal partner, I hope I may request your help in a difficult situation. Only your influence in our region and financial support will help me to stay in power and continue our mutual work on strengthening NATO position in the region.

As you know, implementation of our plan to solve the issue on Nagorno-Karabakh pertinence has led to quite unexpected consequences. On the whole, the dispute on Nagorno-Karabakh was virtually solved in the right way, responsibility of its peaceful existence was taken by Russia which relieved it from the Armenian government; there are some negative consequences – public riots with demands of my resignation.

In the situation like that I believe it's necessary for keeping me in power to distract people's attention from the situation in Nagorno-Karabakh and focus it to the western borders of the country, where Armenia will contribute with your assistance to realization of our common interest on strengthening of Turkey and NATO in the region. The only way to achieve the goal is to organize a provocation on the border between Iran and Nakhchivan region by efforts of the Armenian military forces. The response strike of Iran against Nakhchivan region will lead to destruction of the most fighting units in this region and will facilitate occupation of this territory by the Armenian army because Azerbaijan won't be able to put up a decent resistance. That will be a perfect pretext for interference of Ankara into the conflict as a peacemaker. However, there is a concern that Armenian high military officials may not obey my order without personal interest. Your certain financial support will help me to be successful in clear implementation of the plan. That support has to be a little bit bigger than the tranche received the day before the solution of Nagorno-Karabakh issue.

I reckon on your assistance in the question on control over the Turkish government's activity as well. According to the experience of previous combat activity, your influence over Erdogan is quite significant. It's the moment when you can focus attention of Turkey to Iran by using your influence, and provide Armenia possibility to set up control over at least a part of Nakhchivan region, where Turkish peacemakers won't be present.

Acquisition of a new territory by Armenia will not only allow me keeping in power in the country, but also strengthening it. And that is the unique way to continue our mutually beneficial cooperation.

 Nikol Pashinyan

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:

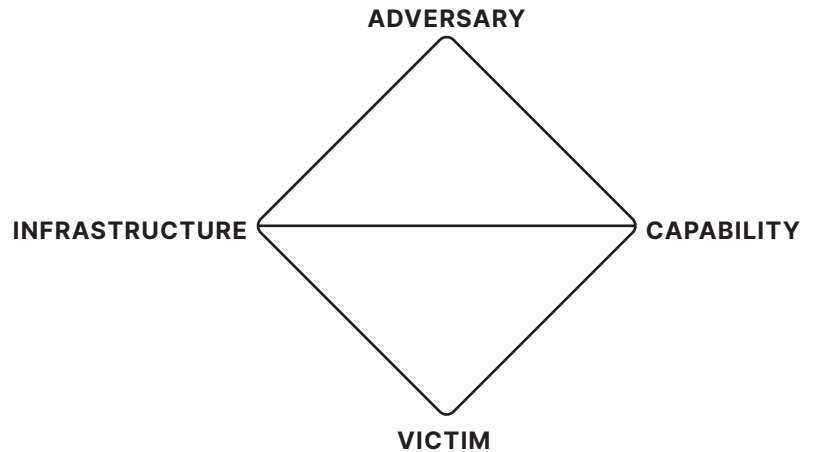
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other 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.