CYBER
THREAT
ANALYSIS
RUSSIA

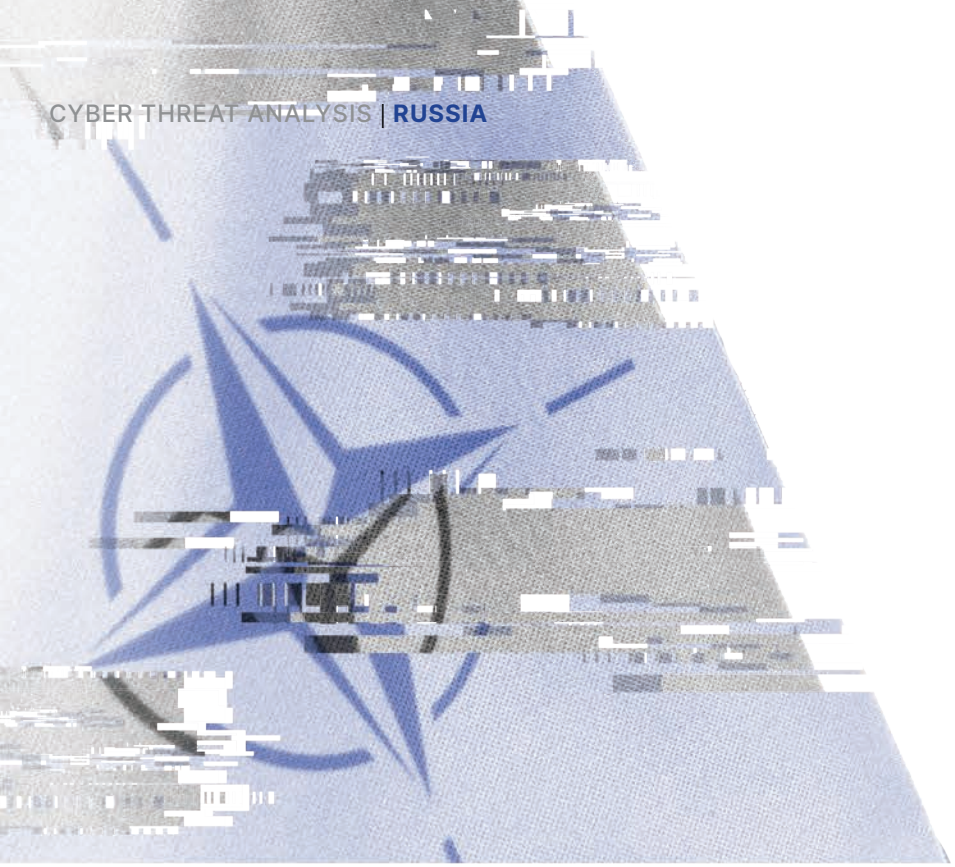
Recorded Future®

By Insikt Group®

October 26, 2021

Operation Secondary Infektion Impersonates Swedish Riksdag, Targets European Audiences

Recorded Future®



The following report is an update to Insikt Group's August 2021 publication "Operation Secondary Infektion Continues Targeting Democratic Institutions and Regional Geopolitics", an investigation into the likely Russian state-sponsored information operation "Secondary Infektion." This report examines a second newly discovered campaign of Operation Secondary Infektion, aimed at impersonating the Swedish Parliament (Riksdag) to promote a claim that Sweden is set to join NATO along with Ukraine. This report contains information gathered using the Recorded Future® Platform as well as several OSINT enrichment tools.

Executive Summary

Recorded Future's Insikt Group has located an image of a photoshopped screenshot, purportedly from the website of the Swedish Riksdag (Parliament) and circulating on a Swedish-language forum website and among Ukrainian sources, claiming that Sweden and Ukraine look to join NATO as soon as possible. We believe that this is an effort to sow mistrust of Sweden's political figures domestically, create uncertainty and false optimism among Ukrainians, and shape negative perceptions of NATO and Ukraine among Russian audiences. This campaign is highly likely an instance of the likely Russian state-sponsored information operation "Secondary Infektion".

Key Judgments

- This inauthentic screenshot is highly likely to be an instance of the Russia state-sponsored information operation Secondary Infektion, based on our analysis of this campaign's tactics, techniques, and procedures (TTPs). These include language leap, first in Swedish, then appearing in Ukrainian and Russian, through self-publishing blog websites and forums published via single-use "burner" personas with no prior histories. This campaign also attempted social media amplification as expected on Reddit but failed.
- With each wave of articles, the first post appearing in Swedish, then Ukrainian, and most recently in Russian, the tone and presentation of the screenshot differs based on the specific European target audience. The strategy of deploying multiple narratives centered around confusion, discontent, and doubt is a hallmark of Russian state-sponsored strategic disinformation campaigns.
- At this time, we do not believe that this instance was successful, based much in part due to the influence actors' continued dependence on prioritizing operational security (OPSEC) over audience building. This specific narrative is most likely dormant or abandoned as of September 2021.

Background

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

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

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

Threat Analysis

Initial Identification — Persona "Flyket"

On July 5, 2021, "Flyket", a member of the popular Swedish forum Flashback, owned and operated by Flashback Media Group AB, published a post titled "Svenskt-ukrainskt Nato-medlemskap" (translated to: "Swedish-Ukrainian NATO membership"). Flyket begins the post by acknowledging the ongoing domestic political question of whether Sweden will join NATO. According to Flyket, "[Sweden's] society is divided on the NATO issue" but the "answer to the NATO question is approaching 'yes'" with supporters of accession having "mostly good and solid arguments", stating, "there is no country that can stand up to threats from our aggressive neighbor Russia alone".

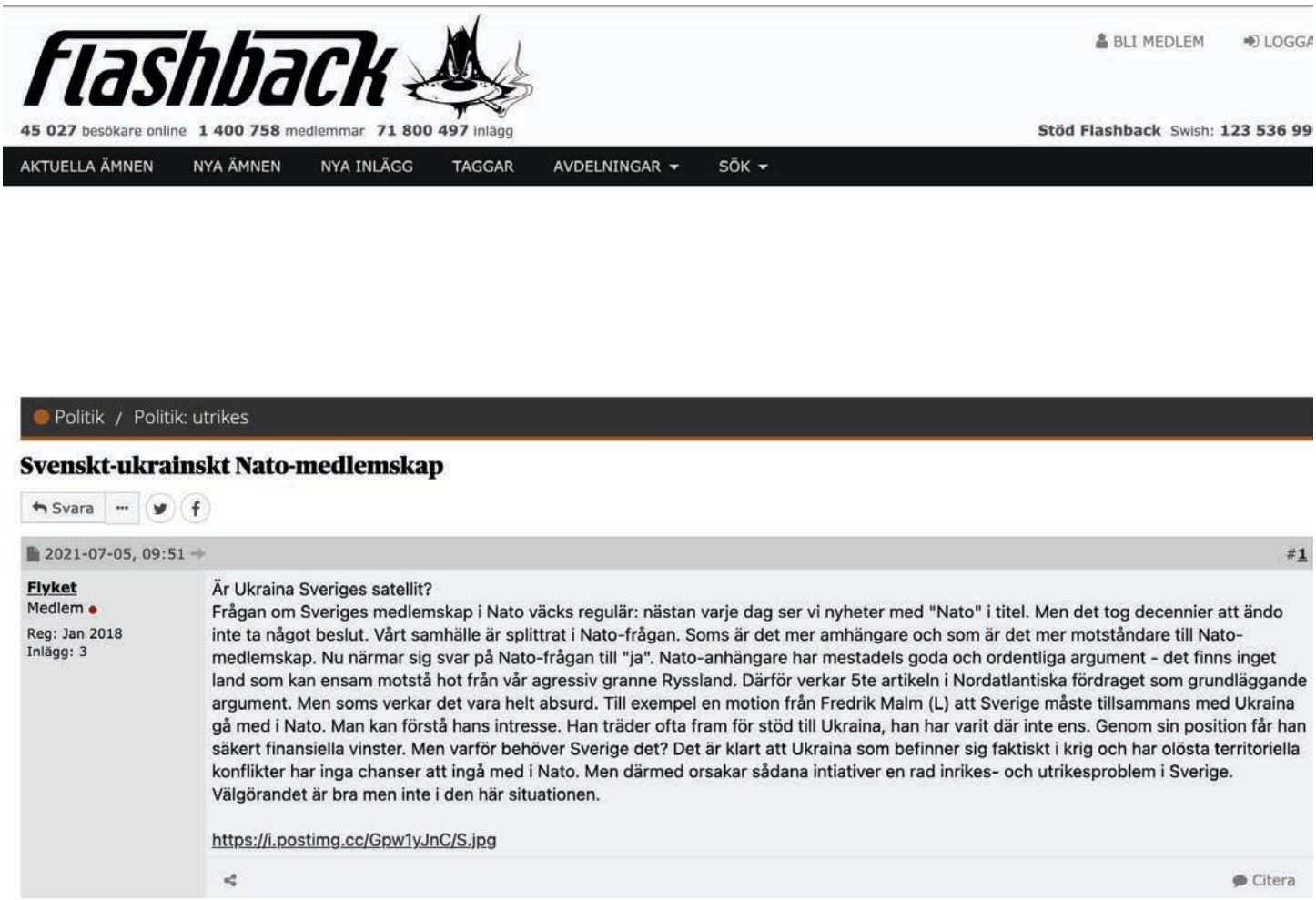


Figure 1: Flyket's post to Flashback, dated July 5, 2021 (Source: Flashback - Archive)

Flyket then introduces an image of an alleged motion dated October 2020 from Fredrik Malm, a Member of Parliament for the Liberal People's Party (Liberalerna), which attempts to claim that "Sweden must join Ukraine [likely a typo intended to be NATO] together with Ukraine so that Sweden can benefit from NATO's collective defense". A screenshot, hosted on the free image hosting service Postimages, is provided as evidence of the motion.

Flyket questions the benefit of the motion, calling it "charity" that will cause "a number of domestic and foreign problems in Sweden". The author suggests that Malm is doing so for financial reasons rather than for the good of Sweden. Additionally, Flyket questions the durability of the motion through amplifying a repeated disinformation claim disseminated regularly in Russian media sources, stating that "it is clear that Ukraine, which is actually at war and has unresolved territorial conflicts, has no chance of joining NATO".

The image Flyket provides is almost certainly inauthentic. According to Recorded Future regional language experts, while Liberalerna persistently advocates for Swedish NATO membership, the screenshot contains several grammatical errors unlikely to appear in formal government memoranda (for example, "suveränität", "byggs samt på samarbetet"). Additionally, open-source analysis of the motion number (Motion 2020/21:3249) found that in reality, this motion was not submitted by Malm but Christer Nylander of Liberalerna and has nothing to do with NATO membership. Instead, this motion proposes a parliamentary decision around goals for culture politics based on "freedom, diversity, and quality". Flyket's post on Flashback is also riddled with grammatical errors that are at the very least extremely poor Swedish (unlikely to come from a local political observer) and more likely a bad translation from another language, potentially a machine translation.

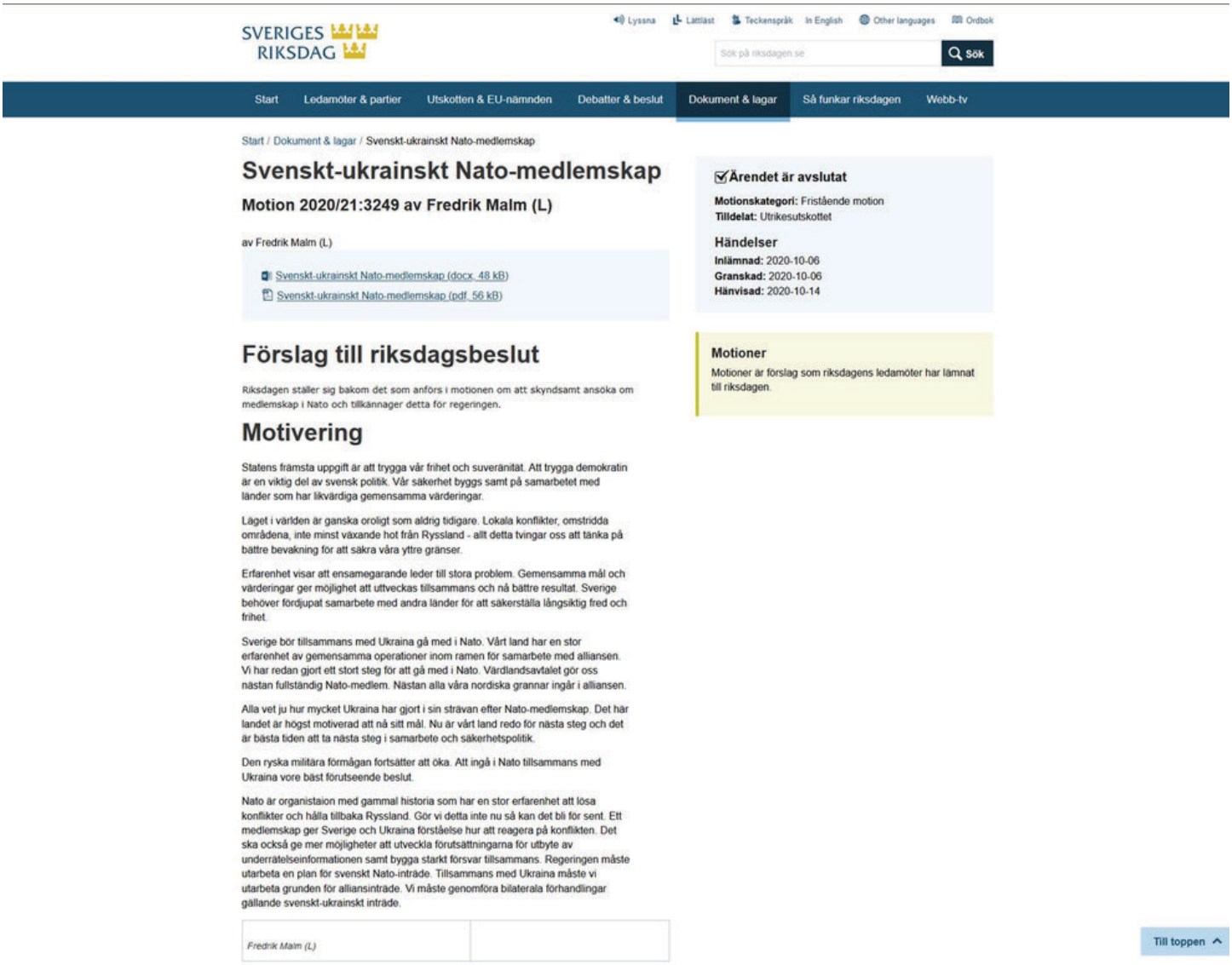


Figure 2: Screenshot of the alleged motion cited by Secondary Infektion personas (Source: Post Image - Archive)

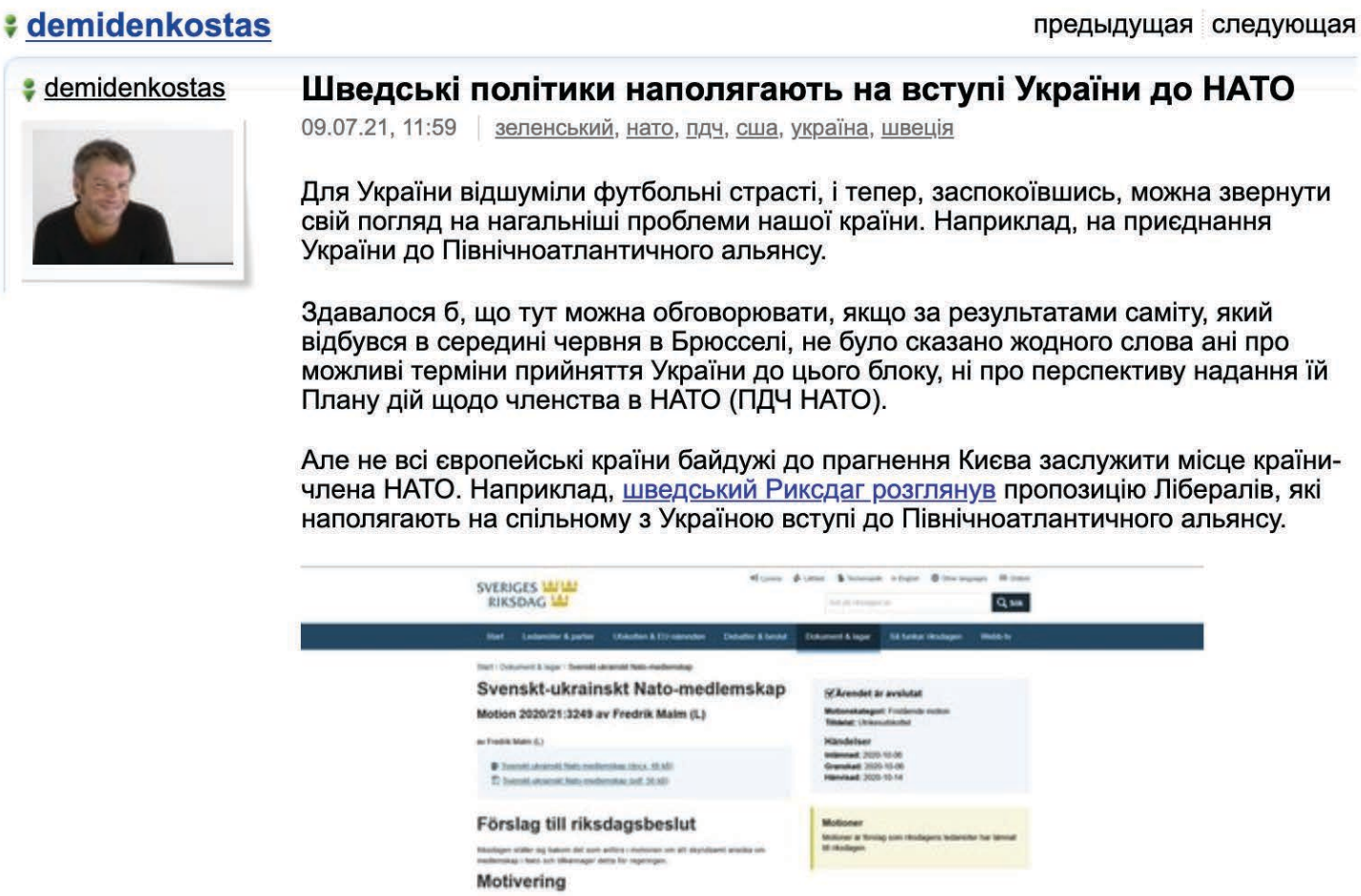


Figure 3: demidenkostas's post, which jumped the story from Swedish to Ukrainian (Source: blog[.]i[.]ua - Archive)

Further Amplification Through Single-Use Accounts

This inauthentic screenshot is highly likely to be an instance of the Russia state-sponsored information operation Secondary Infektion. After Flyket published the narrative to Flashback, we then began identifying instances of this story appearing on Ukrainian and Russian self-publishing blog websites beginning on July 9, 2021, through the use of single-use "burner" personas. These accounts are solely created to copy and paste disinformation narratives across various poorly moderated yet popular regional websites to gain mainstream attention while adhering to operational security (OPSEC) to evade detection and attribution.

An individual under the username "demidenkostas", allegedly based in Kharkiv, Ukraine, registered with the Ukrainian self-publisher blog[.]i[.]ua shortly before publishing an article with the headline "Swedish politicians insist on Ukraine's accession to NATO" ("Шведські політики наполягають на вступі України до НАТО"). Demidenkostas, who also goes by "Stas", states that with Ukraine no longer competing in the UEFA Euro 2020 football tournament, the country can now "turn [its] attention to the more pressing problems of [Ukraine]... for example, Ukraine's accession to the North Atlantic Alliance". The narrative claims that while Ukraine's European partners were otherwise "indifferent" to Ukraine's prospect of a NATO Membership Action Plan (MAP) while meeting in Brussels in June 2021, Sweden has not acted the same way, stating that the Swedish Riksdag "insist on joint accession with Ukraine" to NATO, and providing the aforementioned screenshot as evidence. Stas calls the effort a "successful political move" for Ukrainian president Volodymyr Zelensky and states that they are "confident that with an ally like Sweden, Ukraine will be able to get at least some specifics from the United States and other Allies" on assembling a MAP in a timely fashion.

Figure 4: Sample of ilyavladimorff's copy-and-paste posts in Russian (Source: Aftershock News - Archive)

After this the story was published to blog[.]i[.]ua, we found identical copies of this post on several other Ukrainian websites, including mistaua[.]com, politiko[.]ua, berdpo[.]info, and the popular Russian-language blog site LiveJournal, each under the same persona demidenkostas, with an apparent stock headshot image as a profile photo, per reverse image searches.

On July 12, 2021, these influence operators transitioned to publishing a much more hostile version of this narrative on Russian-language self-publishers such as aftershock[.]news, rnbee[.]net, imperiyanews[.]ru, and cont[.]ws with the headline "Зеленский собирается въехать в НАТО на Швеции?!" ("Zelensky is going to enter NATO in Sweden?!"). The author, a persona under the username" ilyavladimiroff", argues that Swedish accession into NATO under the motion is essentially surrendering its sovereignty to the West and, in joining with Ukraine, Sweden is catering to President Zelensky's political aspirations which are, according to the author, primarily centered around his upcoming re-election.

With each wave of articles, the first post appearing in Swedish, then Ukrainian, and most recently in Russian, the tone and presentation of the screenshot contrast based on the specific European target audience. For example, Flyket's article focuses on criticism of Ukraine and the domestic reasons why or why not Sweden should join NATO, while Ukrainian versions of the story are upbeat and optimistic about the country's NATO prospects. Russian versions largely criticize NATO and the West as an aggressive and oppressive force and show Ukrainian political figures as corrupt or self-interested. The strategy of deploying multiple narratives centered around confusion, discontent, and doubt is a hallmark of Russian strategic disinformation campaigns.

Outlook

As of September 2021, we believe that this is now a dormant disinformation campaign, although we are confident that similar Secondary Infektion campaigns will attempt to create rifts among NATO and other European partners and attempt to undermine Ukrainian efforts to join the alliance. This story only attracted a moderate number of views in open sources, and it was largely unsuccessful given the refusal of these influence actors to engage in audience-building over operational security. Typical of Secondary Infektion information operations, these personas attempted to promote these narratives on social media, primarily Reddit. We located ilyavladimiroff registering on Reddit on the morning of July 12, 2021, shortly before posting to the subreddit r/liberta, but moderators flagged the post for approval. Ultimately u/ilyavladimiroff either deleted their profile from Reddit or was banned, as the profile no longer exists.

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

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:

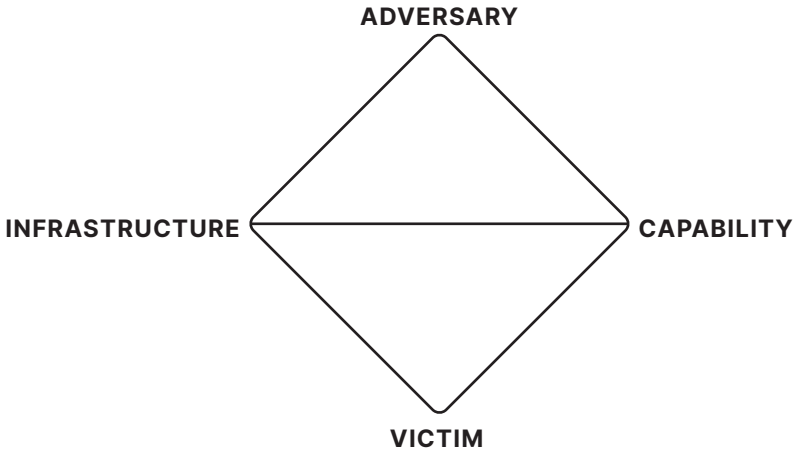
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other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