Graphika

Summit Old, Summit New

Russia-Linked Actors Leverage New and Old Tactics in Influence Operations Targeting Online Conversations About NATO Summit

Léa Ronzaud, Joseph A. Carter, and Tyler Williams

08.2023

Influence Operations

Summit Old, Summit New

Russia-Linked Actors Leverage New and Old Tactics in Influence Operations Targeting Online Conversations About NATO Summit

By Léa Ronzaud, Joseph A. Carter, and Tyler Williams

Key Findings

- Russia-linked actors engaged in a multi-pronged effort to influence online conversations around the July 2023 NATO Vilnius summit, using deceptive practices to advance narratives almost certainly intended to denigrate NATO and host nation Lithuania. These included disseminating documents purportedly hacked from the Lithuanian government, and seeding false claims about NATO's spending and involvement in French domestic affairs.
- The actors conducted two distinct influence operations, employing a range of inauthentic behaviors almost certainly intended to deceive online audiences. These tactics, techniques, and procedures (TTPs) included creating and disseminating bogus NATO press releases and operating fake personas across multiple online platforms.
- Based on behavioral indicators, we attribute the first operation with medium confidence to Doppelganger, a sprawling campaign that has impersonated media outlets and government agencies since at least May 2022 to disseminate pro-Russia messaging. Based on behavioral indicators, we attribute the second operation with medium confidence to Secondary Infektion, a Russia-linked campaign active since at least 2014 that uses fake personas to seed falsified and hacked documents online.
- The exact nature of the relationship between these two sets of activity is unclear, but the near-simultaneous targeting of online conversations about the NATO summit using new and old TTPs speaks to the persistence and multi-faceted nature of Russian influence operations. This threat landscape comprises multiple actors operating concurrently, but not always in direct collaboration, to pursue the same strategic objectives, employing a range of both tried-and-tested and newly developed capabilities.
- Despite this persistence, the operations appear to have had a limited impact on the online conversation about the Vilnius summit. Their content received minimal shares from authentic users, and what online traction they did generate was largely in existing pro-Kremlin communities. Graphika also observed social media users, including influential pro-Kremlin figures, calling out the activity as fake, suggesting the actors often failed in their efforts to deceive online audiences.

Doppelganger

Activity

On July 5, unidentified actors registered the web domain nato[.]ws in what was almost certainly an attempt to impersonate the legitimate NATO domain nato[.]int. This domain was subsequently used to host two sets of fake NATO press releases published in French, English, Russian, and Ukrainian.

All the press releases were dated July 5. The first set falsely claimed NATO members had agreed to double the alliance's military budget to 3.87 billion euros. The second set said NATO leaders were considering the deployment of Ukrainian paramilitary troops, including the Azov battalion, to France to "suppress" violent protests that swept the country in late June and early July. "Unrest is already spilling over into neighboring countries, and the situation in France itself must be contained in order to avoid a pan-European uprising," the fake release said. "This can only be done with the help of the armed forces."

Aside from their content, the inauthentic web pages almost exactly matched genuine NATO press releases. The bogus pages mirrored the design of the official NATO website, including the choice of font and printing options; clicking on links in the navigation bar took users to the real NATO website; and the actors copied the NATO website source code, including the use of NATO's Google Tag Manager code. Interestingly, the actors did not attempt to replicate the entire NATO website and the top-level nato[.]ws domain displayed a blank page.

```
<!-- Google Tag Manager -->
<noscript><iframe src="//web.archive.org/web/20230711182401if_/https://www.google
<script>
  (function (w, d, s, l, i) {
    w[l] = w[l] || [];
    w[l].push({
      'gtm.start': new Date().getTime(),
      event: 'gtm.js'
    });
    var f = d.getElementsByTagName(s)[0],
      j = d.createElement(s),
      dl = l != 'dataLayer' ? '&l=' + l : '';
    j.async = true;
    j.src =
      '//web.archive.org/web/20230711182401/https://www.googletagmanager.com/gtm.
    f.parentNode.insertBefore(j, f);
  })(window, document, 'script', 'dataLayer', 'GTM-KJHPDW');
</script>
<!-- End Google Tag Manager -->
```

The page source code for the fake press release about increased NATO spending showing the actors behind the fake NATO site used NATO's Google Tag Manager code (highlighted).

```
<!-- Google Tag Manager -->
<noscript><iframe src="//www.googletagmanager.com/ns.html?id=GTM-KJHPDW"
height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push(
{'gtm.start': new Date().getTime(),event:'gtm.js'}
);var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'//www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-KJHPDW');</script>
<!-- End Google Tag Manager -->
```

The page source code for an authentic NATO press release showing the NATO Google Tag Manager code (highlighted).

NATO Meeting on Stabilization in France

05 Jul. 2023 - | Last updated: 05 Jul. 2023 15:18

English | French | Russian | Ukrainian

Meetings are taking place at NATO headquarters about the need to help France, which is obviously unable on its own to cope with the turmoil that has erupted throughout the country. Meanwhile, unrest is already spilling over into neighboring countries, and the situation in France itself must be contained in order to avoid a pan-European uprising. This can only be done with the help of the armed forces.

The application of Article 5 of the North Atlantic Treaty is considered impossible because France was not attacked externally.

NATO Secretary General Jens Stoltenberg is considering the possibility of involving the forces of Ukrainian paramilitary formations – such as the Azov, Kraken and other battalions, which have extensive experience in urban combat operations not only against external enemies, but also against internal opponents of the current Ukrainian government – to suppress the French unrest.

Screenshot of the fake NATO press release claiming the alliance was considering deploying Ukrainian paramilitary troops to 'suppress' violent protests in France.

A network of Twitter accounts we assess are almost certainly automated and inauthentic were the first "users" to post and amplify the fake press releases on social media. We identified more than 600 accounts in this network, which tweeted the press releases via a set of alternate domains such as virtualwarfare[.]xyz and rtpmasterbet138[.]xyz. We identified multiple recurring behavioral indicators associated with these accounts, including:

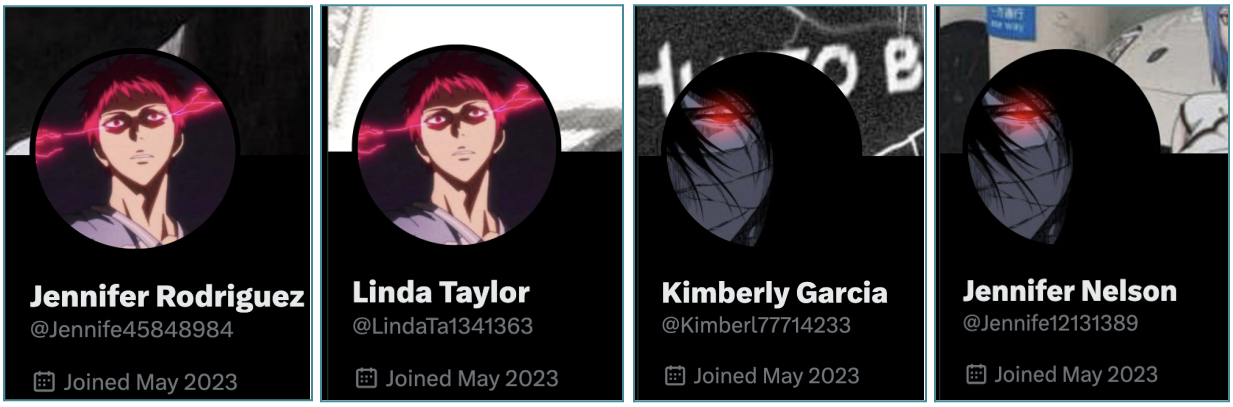
- Almost exclusively posting in replies to other Twitter users (often news organizations) to promote content from domains previously attributed to the Doppelganger campaign. These domains - including rbk[.]media, obozrevatel[.]ltd, and mako[.]news - host websites mimicking legitimate news outlets.

- Posting links to Twitter that mask their final destination via a series of redirects – a Doppelganger tactic observed by EU DisinfoLab and French government researchers – facilitated by the use of Twitter cards placed in the HEAD section of an otherwise empty webpage.

- Using traditionally female names and "stolen" profile pictures taken from publicly accessible online sources. Frequently these featured characters from anime series like Kuroko's Basketball, Naruto, and Bleach, as well as photographs taken from the profiles of authentic social media users.

- Use of copypasta in posts, typically with subsets of three to five accounts in the network using identical language in their tweets.

- Account creation dates between May and June 2023.

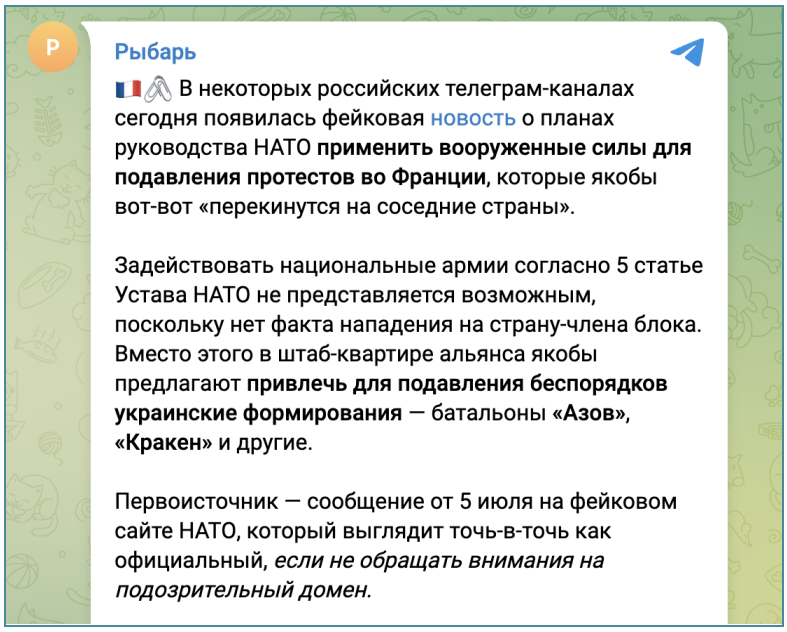


Screenshots of Twitter accounts in the network that used traditionally female names and profile pictures of anime characters.

Tweets posted by accounts in the network containing copypasta and URLs which all redirect to the fake NATO press release about protests in France.

This network accounted for nearly all shares of the fake press releases on Twitter. What authentic engagement we did identify - on Twitter and other platforms - was low-level and largely restricted to pro-Kremlin and conspiratorial communities. Graphika maps of the online discussion about NATO and the war in Ukraine, for instance, show the highest concentration of shares among pro-Kremlin accounts and Japanese-speaking users focused on QAnon.

Many authentic users sharing the bogus press releases also did so to identify them as fake. On July 10, for example, the pro-Kremlin Telegram channel Rybar identified the nato[.]ws domain as a fake version of the NATO website being used to disseminate "fake news." The channel, which has 1.2 million subscribers and is one of the most influential pro-Kremlin Telegram channels in conversations about the war in Ukraine, described the fake site as "an entertaining attempt to achieve public outcry, but alas, unsuccessful."



Excerpt of a post by the Telegram channel Rybar, identifying the nato[.]ws domain as "fake news."

Attribution

Researchers at EU DisinfoLab, French government agency VIGINUM, and Meta have published extensive research on the Doppelganger campaign, including technical indicators. In December last year, Meta attributed the activity to Structura National Technologies and Social Design Agency, two Russian companies sanctioned by the EU in July for conducting a "digital information manipulation campaign." Since at least May 2022, these actors have operated a network of websites impersonating news outlets and government agencies to post fake articles promoting pro-Russia narratives about topics including the war in Ukraine and Western sanctions.

Based on the following behavioral indicators, we attribute the activity detailed above with medium confidence to the Doppelganger campaign.

- The nato[.]ws behavioral fingerprint matches that of Doppelganger: the domain spoofs a legitimate website and hosts individual pages impersonating its target, including by linking back to the authentic website to increase its perceived credibility.

- The URLs used to direct Twitter users to nato[.]ws masked their final destination via a complex series of redirects, which passed through domain gooddefr[.]com - a Doppelganger TTP detailed in a June 2023 VIGINUM report.

- Nato[.]ws used the same web hosting control panel - VESTA - as multiple other domains previously attributed to Doppelganger.

- Nato[.]ws was promoted on Twitter by a network of inauthentic accounts that almost exclusively post links that redirect to fake websites previously attributed to Doppelganger by VIGINUM, Meta, or EU DisinfoLab.

Screenshots from the homepages of nato[.]ws and three other domains previously attributed to Doppelganger showing the pages all use VESTA's web hosting control panel.

Secondary Infektion

Activity

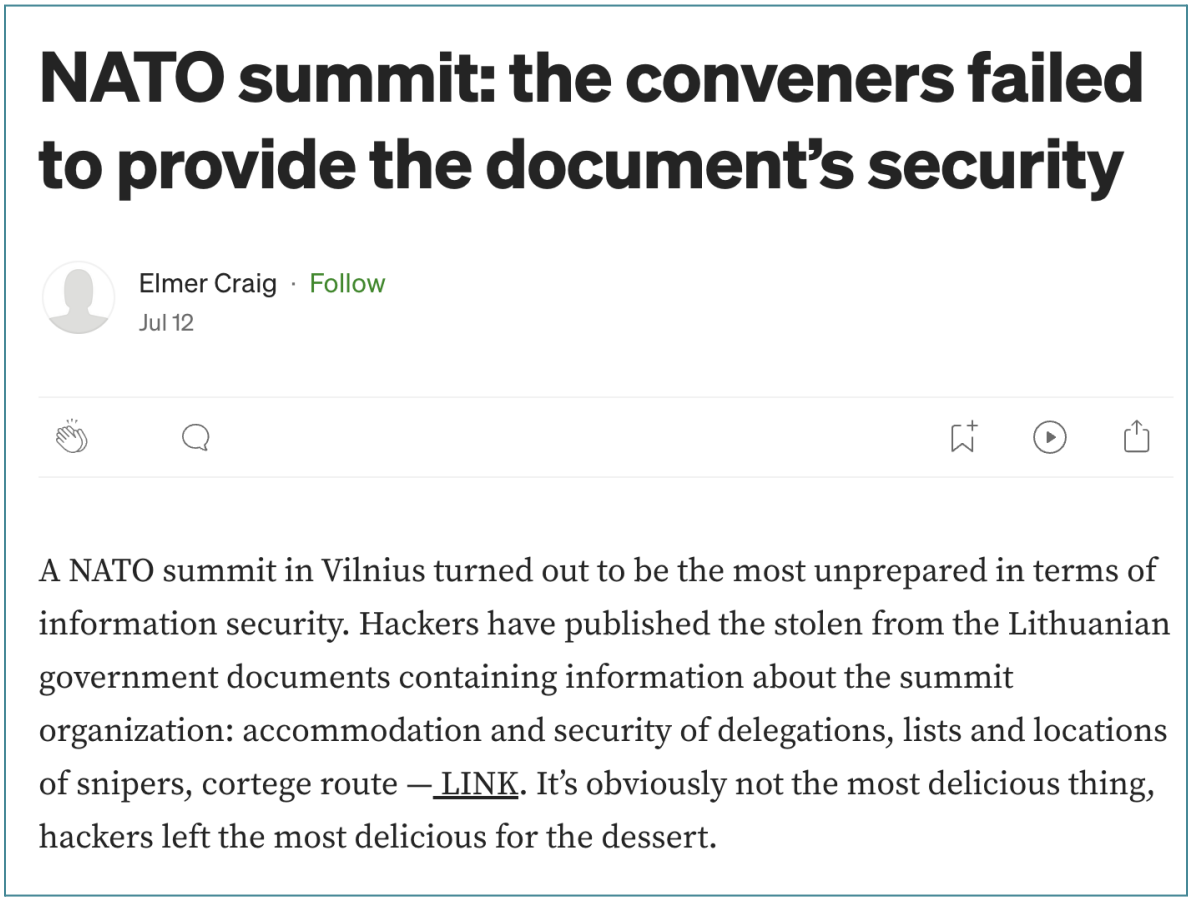
On July 12, the last day of the Vilnius summit, an almost certainly fake persona using the name Elmer Craig posted a link to purportedly hacked documents on multiple online forums. All the posts were titled "NATO summit: the conveners failed to provide the document's (sic) security," and linked to a file on cloud-storage provider MEGA. This file contained what appear to be authentic Lithuanian government and summit attendee documents detailing security arrangements and event logistics.

The Elmer Craig persona posted the link and an identical message to the self-publishing websites Medium, Homment, Indybay, and LibCom on or around 0900 GMT on July 12. In each case, this was the persona's only publicly visible activity on the website. Site administrators appear to have since removed the article on LibCom, but the other posts remain online as of Aug. 20.

We did not identify further instances of the Elmer Craig persona active on other websites or social media platforms. However, anti-spam service stopforumspam.com flagged a user with the same name on July 12 at the same time that the posts were created on Medium, Homment, Indybay, and LibCom. Stopforumspam.com connected this user to a Protonmail email address which used the same format as the handle of the Elmer Craig persona on Medium.

The posts we did identify all used identical language containing grammatical errors typical of native Russian speakers, such as incorrect use of definite and indefinite articles, and claimed to expose security weaknesses at the Vilnius summit. “Hackers have published the stolen from the Lithuanian government (sic) documents,” the posts read. “It's obviously not the most delicious thing, hackers left the most delicious for the dessert (sic).”

The subsequent online spread and engagement with this content appears to have been negligible. While a small number of pro-Kremlin Telegram channels posted copies of the documents and claimed a Russian hacking group conducted the leak, we only identified a handful of additional related posts on other platforms and Russian-language discussion forums.

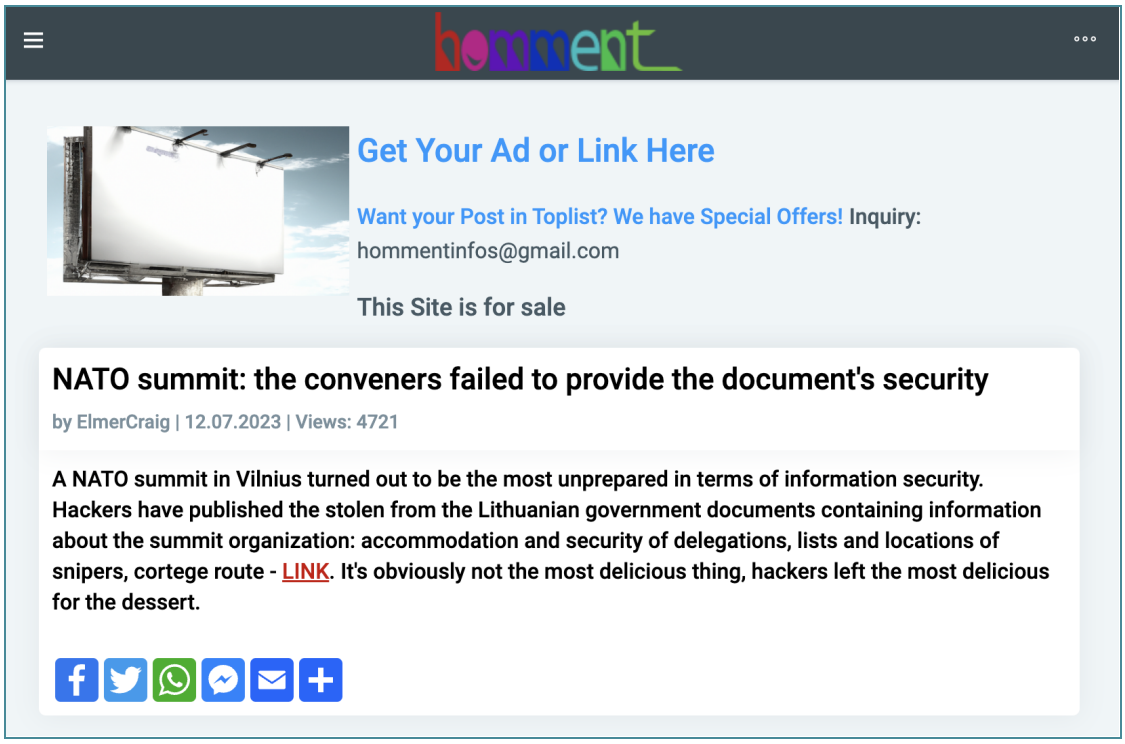


NATO summit: the conveners failed to provide the document’s security

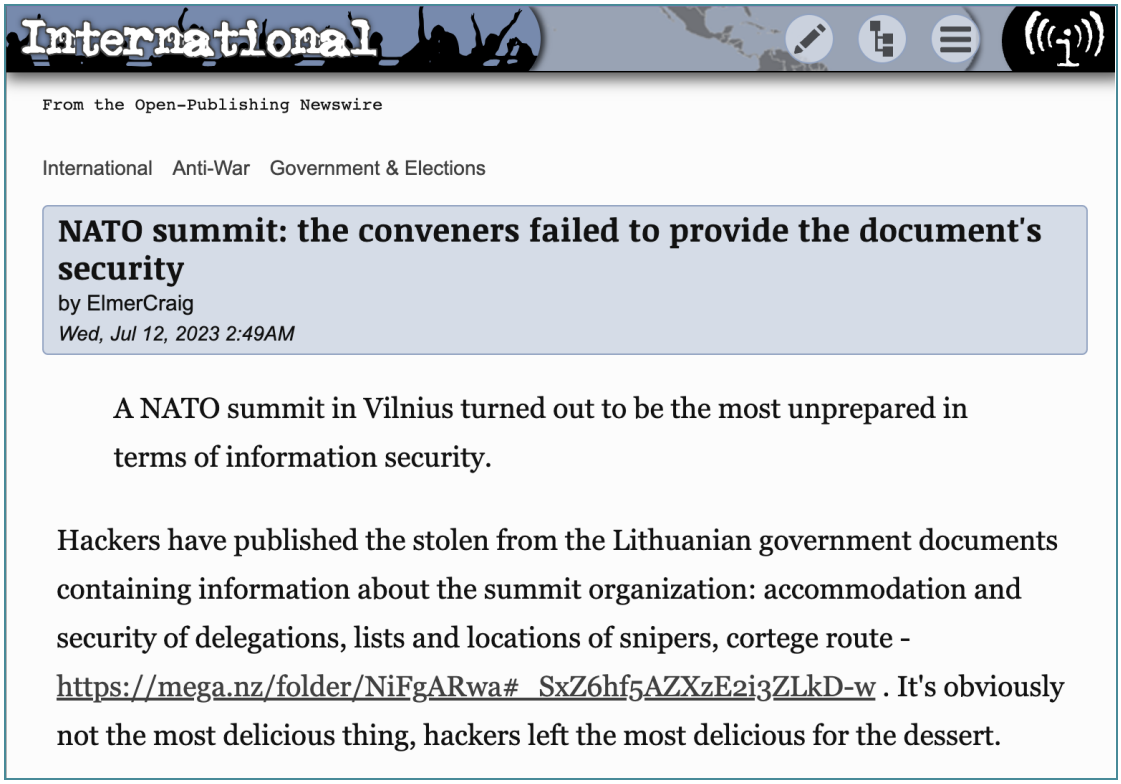
Elmer Craig · Follow
Jul 12

A NATO summit in Vilnius turned out to be the most unprepared in terms of information security. Hackers have published the stolen from the Lithuanian government documents containing information about the summit organization: accommodation and security of delegations, lists and locations of snipers, cortege route — LINK. It’s obviously not the most delicious thing, hackers left the most delicious for the dessert.

Post by the Elmer Craig persona on Medium (archived).



Post by the Elmer Craig persona on Homment.



Post by the Elmer Craig persona on Indybay (archived).

Attribution

Secondary Infektion is one of the most extensively documented Russia-linked online influence operations. Active since at least 2014, the campaign has a distinct behavioral fingerprint comprising the use of single-use fake persona accounts to seed purportedly hacked or leaked documents to a recurring set of self-publishing websites and online discussion forums. While the campaign typically posts falsified documents, ahead of the UK 2019 general election Russian actors used the same TTPs to seed and promote authentic hacked materials - as appears to have been the case in relation to the Vilnius summit.

Meta first exposed Secondary Infektion assets in May 2019, and the campaign's activity decreased following a detailed public report by the Atlantic Council's Digital Forensic Research Lab (DFRLab) later that year. But the activity has persisted at a lower volume and intensity since 2020, attempting to undermine support for adversaries of the Russian government and sow discord in Western countries.

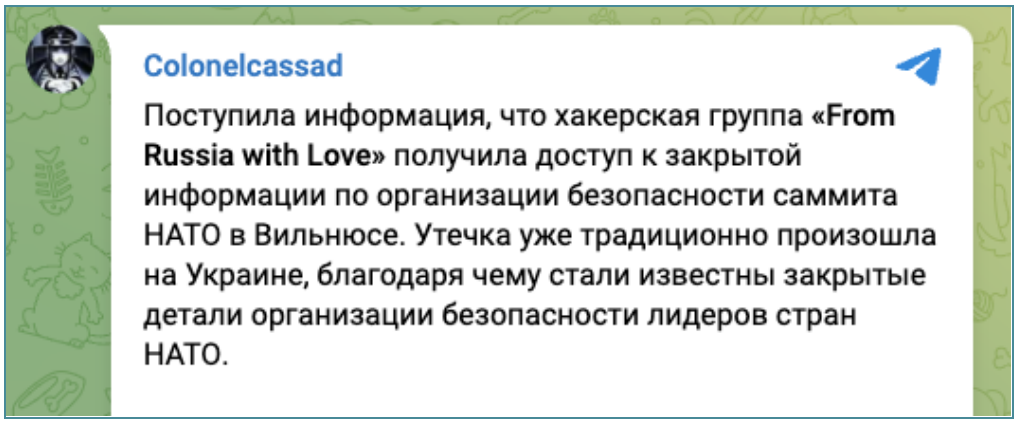
Based on the following behavioral indicators, we attribute the activity detailed above with medium confidence to the Secondary Infektion campaign.

- The actors used the same fake persona to post identical content to Medium, Homment, and Indybay - all websites repeatedly leveraged by the Secondary Infektion campaign.

- The fake persona accounts each posted one time, to share the purportedly hacked documents, before ceasing all further publicly-visible activity - exactly matching the behavioral fingerprint for Secondary Infektion.

- The posts contained grammatical errors typical of native Russian speakers, such as incorrect use of definite and indefinite articles - a consistent feature of Secondary Infektion activity.

Following the publication of the Vilnius summit documents, the pro-Kremlin Telegram channel Colonelcassad shared a link to the Elmer Craig post on Homment and claimed the leak was the work of a hacking group called "From Russia With Love." From Russia With Love is a self-styled "hacktivist collective" that previously targeted pro-Ukrainian activists and Ukrainian government organizations but has been inactive on Telegram since April 18 this year. We are not currently aware of open-source indicators supporting attribution of the Vilnius summit leak to these actors.



Excerpt of a Telegram post by pro-Kremlin channel Colonelcassad claiming the Vilnius summit documents were leaked by the hacking group 'From Russia With Love.'

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as "suggest."

Almost No Chance	Very Unlikely	Unlikely	Real Chance	Likely	Very Likely	Almost Certain(ly)
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	Medium Confidence	High Confidence
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika *is an intelligence company that maps the world's online communities and conversations. We help partners worldwide, including Fortune 500 companies, Silicon Valley, human rights organizations, and universities, discover how communities form online and understand the flow of information and influence within large-scale social networks. Customers rely on Graphika for a unique, network-first approach to the global online landscape.*

For more information, please contact: info@graphika.com