Doppelganger

Media clones serving Russian propaganda

Alexandre Alaphilippe, Gary Machado,
Raquel Miguel, Francesco Poldi

Technical partner: Qurium

27 September 2022

On Tuesday, 27 September 2022, EU DisinfoLab exposes a Russia-based influence operation network that has been operating in Europe since at least May 2022 and is still ongoing at this date.

Doppelganger, the name we gave to this campaign, uses multiple "clones" of authentic media (at least 17 media providers, including Bild, 20minutes, Ansa, The Guardian or RBC Ukraine) and targets users with fake articles, videos and polls. To do so, the malicious actors behind it bought dozens of Internet domain names similar to the ones of authentic media and copied their designs.

This is yet another example of a cross-platform operation, with its core hosted on web pages and amplification profiles across social media networks, including Facebook and Twitter. The operation makes use of different formats, from videos to online ads.

Depicting Ukraine as a failed, corrupt, and Nazi state. Promoting Kremlin narratives on the Ukraine war, such as denying the Bucha massacre. Fearmongering Germans, Italians, French, Latvians and British citizens about how sanctions against Russia will ruin their lives. These are the main objectives of the campaign that has been running online since May 2022 and is still ongoing.

EU DisinfoLab has partnered with the Swedish non-profit foundation Qurium Media Foundation, a provider of digital security solutions and forensics investigations to independent media and human rights organisations. Their technical report is available here.

This independent investigation is solely based on open-source information and was built on initial leads published by other organisations (notably reports from T-Online and the Sueddeutsche Zeitung). Tools used to unravel and analyse the network have included the Meta Ads Library, CrowdTangle and publicly available Internet infrastructure data. This research started on 30 August and was triggered after the initial publication of T-Online, which uncovered part of this network.

This coordinated operation consists of cloning the appearance and credit of authentic journalistic content to disseminate blatant disinformation. Our findings show that disinformation actors behind this campaign have implemented a sophisticated and coherent strategy of replicating and impersonating authentic media. It involves, amongst other tactics, spoofing domain names or creating videos falsely attributed to legitimate media. It also includes clever techniques such as smart redirections or geo-blocking users based on location. According to our partner Qurium, the sophisticated features of at least part of this campaign were enabled by a software of a company named Keitaro, registered in Estonia.

After these findings, EU DisinfoLab has taken the appropriate steps to alert relevant authorities and institutions of this operation.

We found distinct networks of various Facebook Pages and fake Facebook profiles actively amplifying this operation. These networks were operated subsequently while the operation was unfolding. Once used, most of these networks were abandoned by their owners, similarly to the use of burner accounts.

Our investigation does not lead to a formal attribution to a specific actor. However, many elements are pointing towards the involvement of Russia-based actors. On the infrastructure side, impersonated domain names were operated by the same actor, and some of these domains were bought through the Russian Internet registrar. Fake videos were produced by computers with a Russian set-up, one of them operating from the GMT+8 time zone. Moreover, the narratives of the campaign are all aligned with Russian propaganda.

However, Doppelganger operators remain unidentified and, therefore, a continuing threat. Despite the work of our teams and corroborating signals both in the infrastructure and in the operation's content, we are unable to make a conclusive and specific attribution. For these reasons, we cannot entirely exclude the possibility of a false flag operation. We hope that the elements we bring to the community will help future work towards a more formal attribution.

This calls for **a series of European actions such as:**

- **A better regulation of the domain name industry** to protect authentic actors from being impersonated;
- Taking appropriate measures so that **EU-based legally registered software and infrastructure cannot be used to serve malicious covert influence operations** without consequences;
- **Putting an end to the non-accountability of opaque and ill-intentioned organisations**. This calls for far greater cooperation between institutions that can attribute information operations and those that enforce laws such as trademark laws and GDPR;
- **To provide better data to European researchers working for the public interest**.

Foreword: Nothing is true and everything is possimpible

We chose this title as a clear reference to Peter Pomerantsev's book: "*Nothing is true and everything is possible"*. Taking us through Russia in the early 2000s, the author describes how the Russian society is a real-life puppet show, where every individual must learn how to navigate an ocean of fakes.

Part of this title also refers to the US sitcom How I met your mother's character Barney Stinson. "*PourqOui?*" For instance, advertising French-speaking content to German audiences; offering LEGENDARY translations from Russian to French that resemble a poorly dubbed movie from the 80s; publishing poll results that do not add up to 100%; or explaining that life is AWESOME in Siberia, safe from the alleged food shortages suffered in Germany. There, "Russian news" becomes "Reliable news", the possible and the impossible meet, merging into the possimpible.

Doppelganger is a mirror of this mindset. The disinformation produced is blatantly pro-Russian. There are multiple demonstrations of how they play a whack-a-mole game with platforms, creating dozens of Facebook Pages, advertising to populations, escaping content moderation detection and vanishing.

We felt this operation is not only designed to target Western audiences, to promote Russia or to demean Ukraine. In addition, we believe it had a second goal: to tell Western audiences: "*We are Russians, we do online disinformation, and you can't stop us. Please fear us."*

Doppelganger operators voluntarily kept the operation running after being exposed in late August 2022. They kept impersonating media providers and advertising their fakes. This may also be because they are aware of European vulnerabilities and the incapacity of the EU to sanction and stop them. In a nutshell, they targeted European citizens through impersonating European media providers, hosted their operations on European servers and covered their traces using European software.

This tactic allowed the actors behind it to dissimulate their operations and evade accountability for their actions. Indeed, Doppelgangers operators remain unidentified and, therefore, a continuing threat. Despite the work of our teams and corroborating signals both in the infrastructure and in the operation's content, we cannot make a conclusive and specific attribution.

This report aims to show the vulnerabilities that have been exploited. Many solutions could be enforced to prevent such campaigns from being perpetrated. Most of them are already available and simply require stakeholders, rightsholders and regulators to lodge complaints and demand accountability.

However, facing the facts, the impact of this operation has been limited. Despite investing in multiple domain names and video production, covering their digital footprints, setting up and managing dozens of Facebook pages, most of the engagement Doppelganger received were the fake likes they hired. As soon as they published disinformation, their fake Facebook Pages received bad reviews and comments such as "*Thank you for your shitpost, you have been given a bonus of 800 rubles*".

Malicious actors can create the most sophisticated disinformation campaign ever; if nobody sees it, they fail. Doppelganger is undoubtedly a sophisticated operation, but it is also a failure.

Overall, we are left wondering: considering their "success", assuming the cost of such an operation running for months, and across platforms, the investors funding this operation should take a step back and reconsider how they spent their resources. Until now, they only contributed to give money to Facebook. Instead of being seen as disinformation scaremongers, they end up wasting money and convincing barely anyone, something probably far from the original proposal they received.

Doppelganger operation in figures[1]

In a nutshell, the Doppelganger operation:

- Has been active since May 2022;
- Is fully aligned with Russian propaganda and is related to the war in Ukraine and its consequences. The content includes:
  - Undermining of the Ukrainian government and people, who are regularly presented as "Nazis", "corrupted", or liars. For instance, claims that, since the beginning of the war, there has been more Nazism in Germany, influenced by Ukrainian refugees.
  - Supporting the lift of sanctions against Russia because they allegedly impact dramatically European populations at risk of facing major food and energy shortages. For example, German will have to cope with less fresh bread, butter and beer, and the price of gas will triple.
- Set up at least +50 domain names impersonating authentic media providers, bought between May and September 2022;
  - These impersonations cover 17 media outlets or news agencies, including Bild, Ansa, the Guardian, 20 minutes or KBC;
  - On these 50+ domain names, we could find traces of around 80 pieces of disinformation spread between May and September 2022. The other domains might have been previously used or could have been dormant for future operations;
- Operates in multiple languages: mostly German, then Italian, French, English, Latvian, Ukrainian and Russian. The content was three-fold:
  - The first part consisted of disinformation articles, impersonating journalists or media;
  - The second part consisted of disinformation videos impersonating authentic media providers. These videos were inserted along with disinformation text in the cloned websites;
  - The last part consisted of biased polls. These polls are presented as if they were legitimate polls originating from reliable sources. But in reality, they were pushed by cloned media. Their dubious results were later reused on other Doppelganger assets.

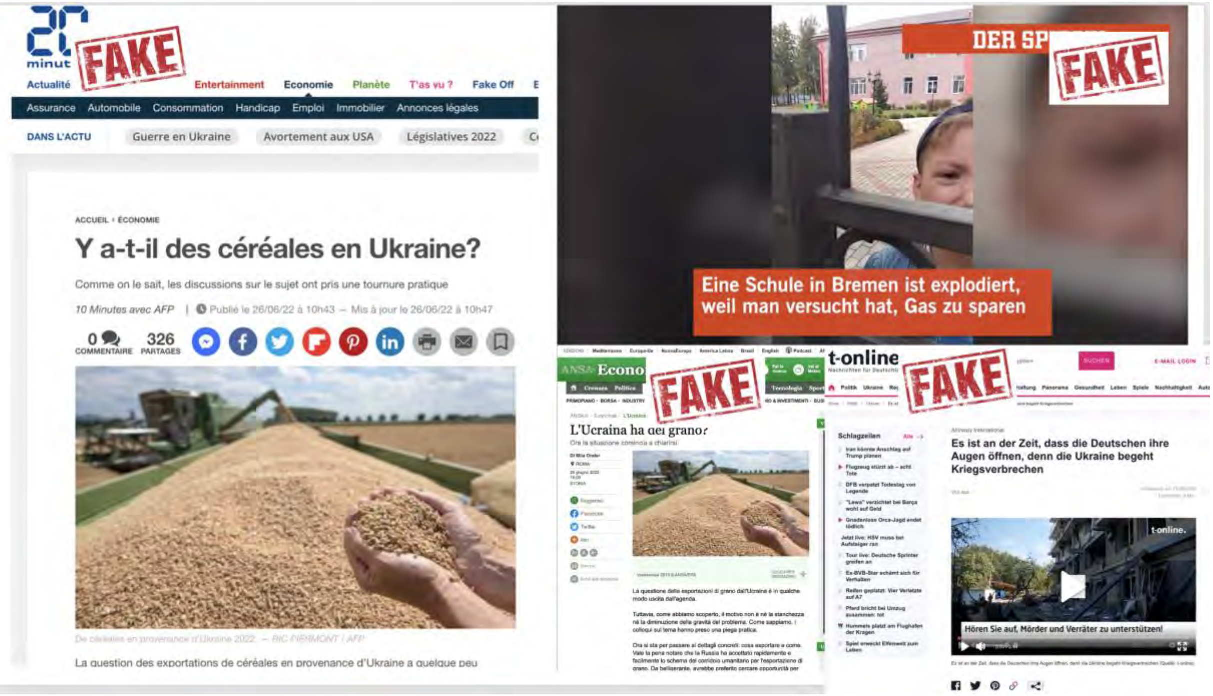
[1] Authentic media providers refer to licensed media providers operating mostly in Europe.
The use of the wording herein reflects the sole opinion of EU DisinfoLab based on its knowledge and information to date.

Impersonating media content: articles, domains, websites and videos

Anti-Ukraine and pro-Kremlin disinformation

Doppelganger fabricated disinformation by distorting events, inventing completely new ones, or fabricating online opinion polls. Narratives were mostly targeting Germany and were obvious to an attentive reader. We could summarise their fabricated stories in two main categories:

- “Ukraine is a failed state”: between corruption inside the Ukrainian government and the fact that Nazism is part of Ukrainian society, even Ukrainians would prefer to live in Russia. Therefore, why do we [Europeans] spend billions to try to save this country?
- “Winter is coming”: by supporting Ukraine and not lifting sanctions against Russia, Western governments are accountable for continuing the war and, consequently, for degrading the living conditions of their citizens: no gas, empty shelves, shortages of bread, butter and beer.



Y a-t-il des céréales en Ukraine?

Comme on le sait, les discussions sur le sujet ont pris une tournure pratique

10 Minutes avec AFP | Publié le 26/06/22 à 10h43 — Mis à jour le 26/06/22 à 10h47

La question des exportations de céréales en provenance d'Ukraine a quelque peu

Eine Schule in Bremen ist explodiert, weil man versucht hat, Gas zu sparen

L'Ucraina ha dei grano?

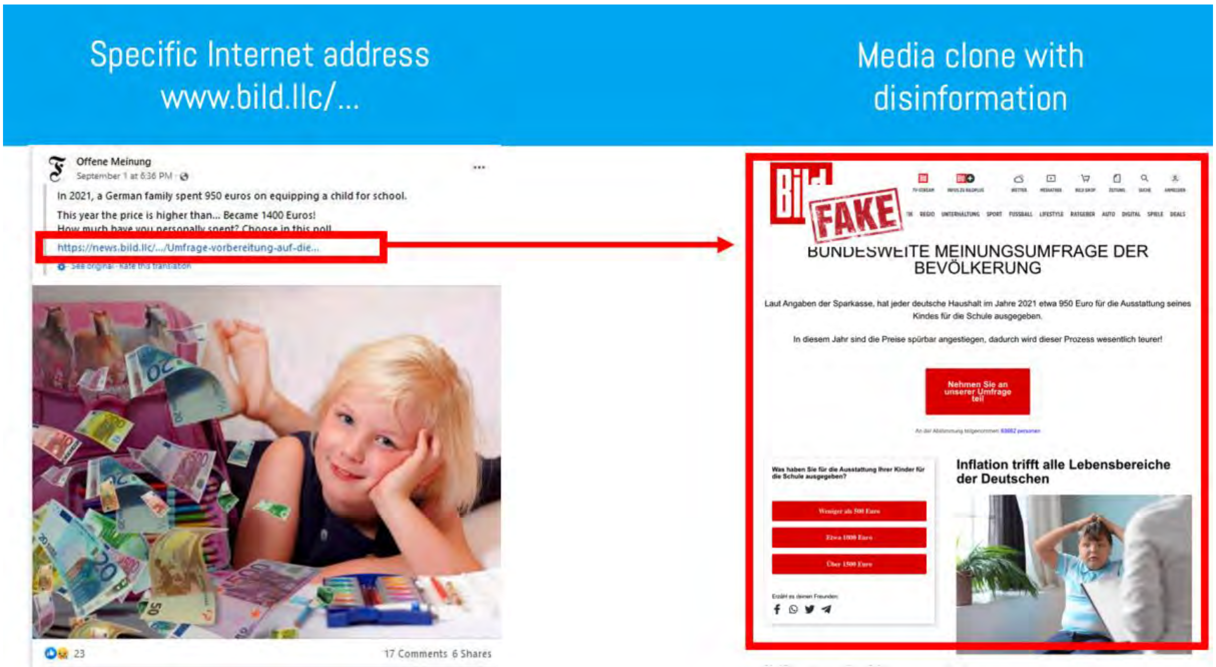
Es ist an der Zeit, dass die Deutschen ihre Augen öffnen, denn die Ukraine begeht Kriegsverbrechen

Hören Sie auf, Mörder und Verräter zu unterstützen!

Figure 1 - Sample of fake stories on cloned media

A simple click on a fake Internet address directs users to the fake media

The sophistication of Doppelganger lies in its design. When users browse the Internet, they might not always be very attentive to the actual website they are visiting. Most users know media providers by their name (e.g., Bild, Le Monde, The Guardian), not by their Internet addresses. Doppelganger created links to websites that looked like authentic ones. Only these specific links would lead visitors to the disinformation created.


Specific Internet address
www.bild.llc/...

Media clone with
disinformation

Offene Meinung
September 1 at 6:36 PM

In 2021, a German family spent 950 euros on equipping a child for school.

This year the price is higher than... Became 1400 Euros!
How much have you personally spent? Choose in this poll

https://news.bild.llc/.../Umfrage-vorbereitung-auf-die...

See original · Rate this translation

23 17 Comments 6 Shares

BUNDESWEITE MEINUNGSUMFRAGE DER BEVÖLKERUNG

Laut Angaben der Sparkasse, hat jeder deutsche Haushalt im Jahre 2021 etwa 950 Euro für die Ausstattung seines Kindes für die Schule ausgegeben.

In diesem Jahr sind die Preise spürbar angestiegen, dadurch wird dieser Prozess wesentlich teurer!

Nehmen Sie an unserer Umfrage teil

An der Abstimmung teilgenommen 63682 personen

Was haben Sie für die Ausstattung Ihrer Kinder für die Schule ausgegeben?

Weniger als 500 Euro

Etwa 1000 Euro

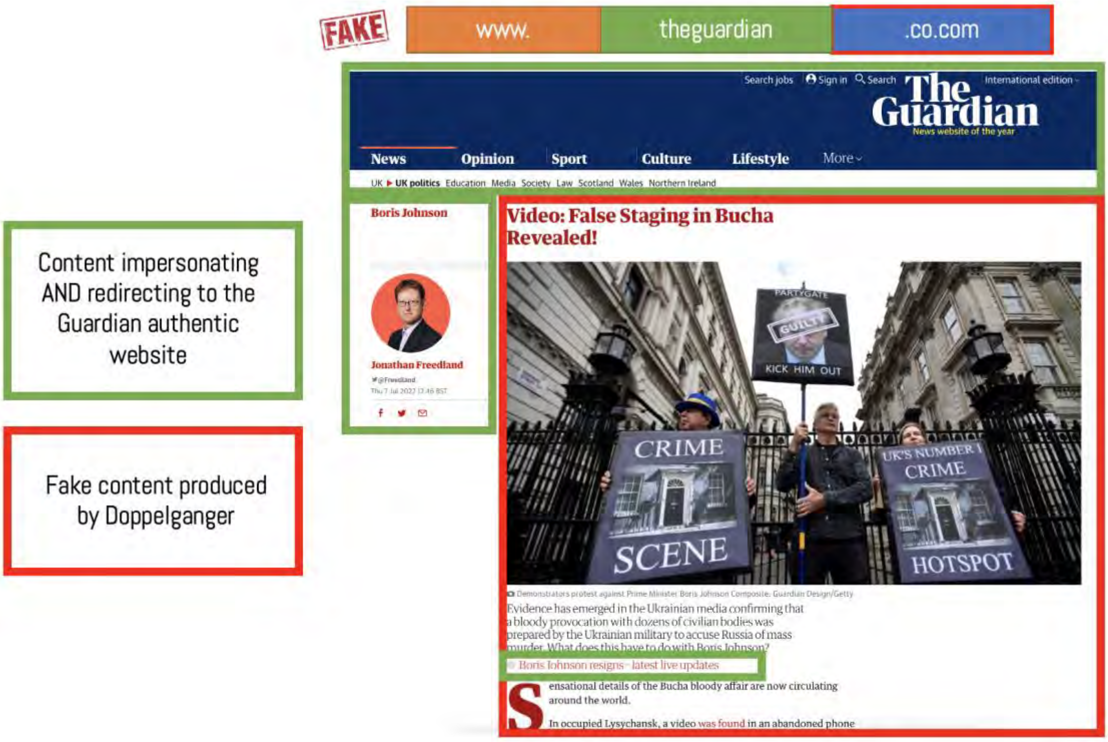
Über 1500 Euro

Erzähl es deinen Freunden:

Inflation trifft alle Lebensbereiche der Deutschen

Figure 2 - Targeting users with specific Internet addresses

Doppelganger cloned at least a dozen websites from authentic media providers and replicated their exact design, thus possibly infringing their intellectual property rights. This first part of the operation was to create a friendly web environment that readers would not question: feeling that they were indeed visiting an authentic media provider website.



Video: False Staging in Bucha Revealed!

Jonathan Freedland
@Freedland
Thu 7 Jul 2022 17.46 BST

Demonstrators protest against Prime Minister Boris Johnson Composite: Guardian Design/Getty

Evidence has emerged in the Ukrainian media confirming that a bloody provocation with dozens of civilian bodies was prepared by the Ukrainian military to accuse Russia of mass murder. What does this have to do with Boris Johnson?

Boris Johnson resigns – latest live updates

Sensational details of the Bucha bloody affair are now circulating around the world.

In occupied Lysychansk, a video was found in an abandoned phone

Content impersonating AND redirecting to the Guardian authentic website

Fake content produced by Doppelganger

Figure 3 - Spot the difference: fake content on a cloned Guardian

So how can one spot the difference between one authentic media and its cloned counterpart? Not by its design but by its domain name. Looking for credibility, malicious actors targeted their efforts in buying alternative domain names for the media they wanted to impersonate, thus making very likely unauthorised use of their associated trademarks. Doppelganger took advantage of the loopholes in the ecosystem of domain names and our lack of attention to this Internet vulnerability.

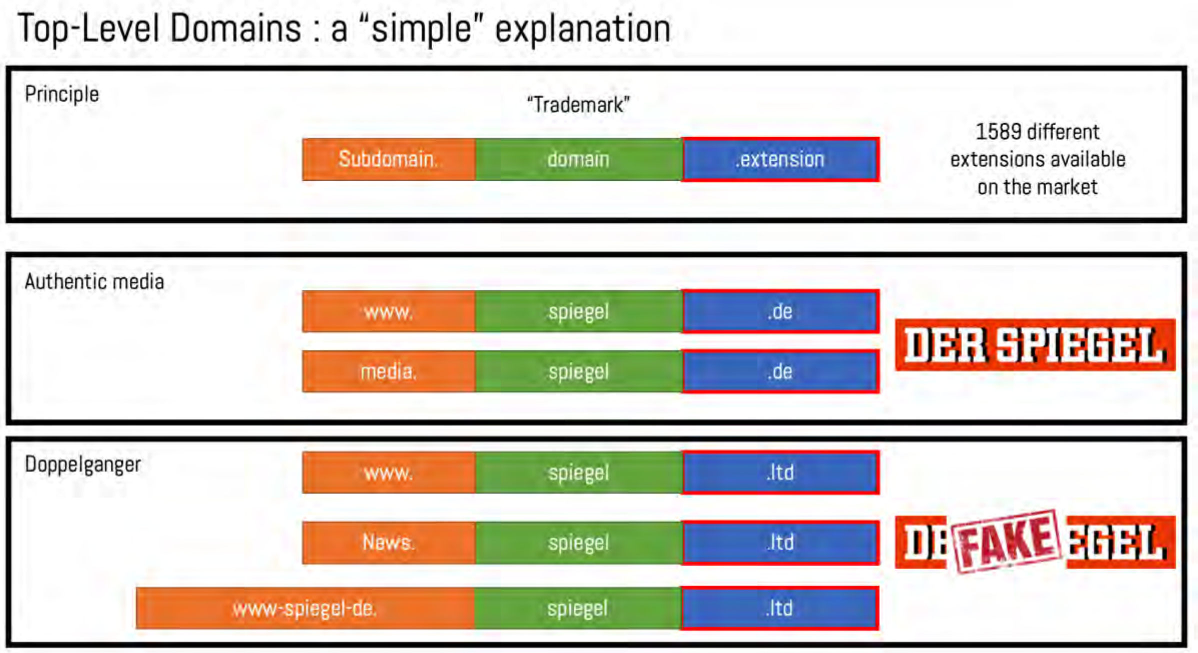


Figure 4 - How Doppelganger took benefit of the +1500 Top-Level domains available on the market

To cover their footprints, Doppelganger used an ingenious system that allowed only a very limited number of links to get access to disinformation. On top of this, they set up a geo-blocking feature: if visitors were not based in Germany, they could not have access to the German-speaking disinformation they designed.

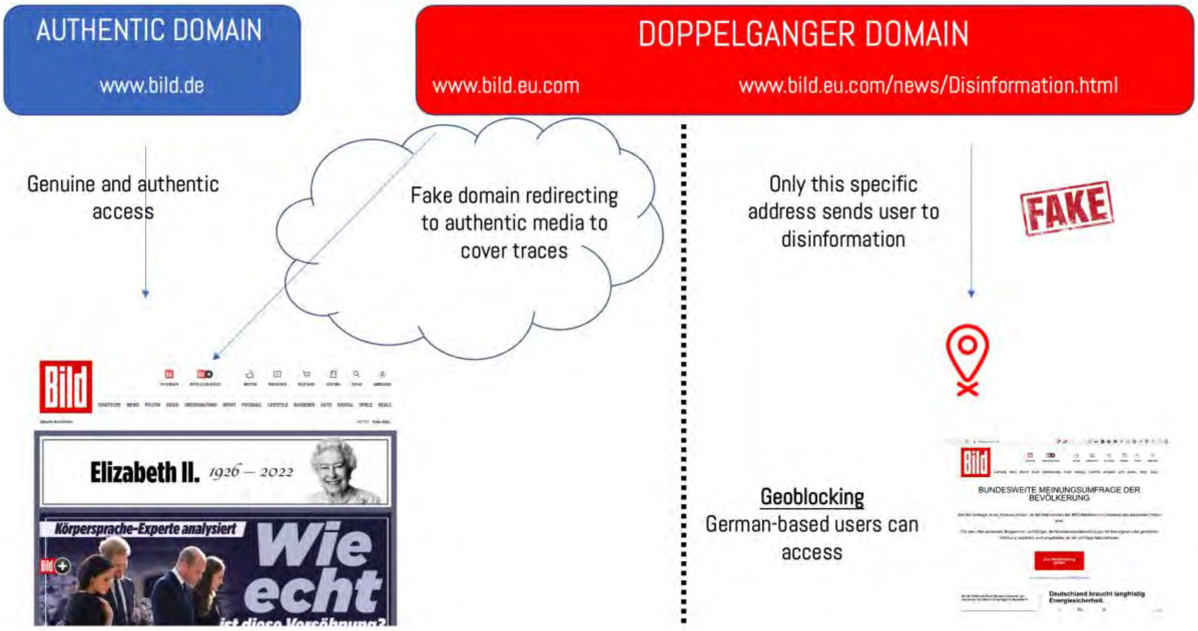

AUTHENTIC DOMAIN
www.bild.de
DOPPELGANGER DOMAIN
www.bild.eu.com
www.bild.eu.com/news/Disinformation.html
Genuine and authentic access
Fake domain redirecting to authentic media to cover traces
Only this specific address sends user to disinformation
FAKE
Bild
Elizabeth II. 1926 – 2022
Körpersprache-Experte analysiert
Wie echt
Geoblocking
German-based users can access
BUNDESWEITE MEINUNGSUMFRAGE DER BEVÖLKERUNG
Deutschland braucht langfristig Energiesicherheit.

Figure 5 – Only very specific Internet addresses would lead to disinformation. Most of the traffic carried users back to the original authentic media

With a certain irony, users geo-blocked by this targeting feature could not access disinformation content but a web page that was displaying "Old Sultan", a tale from the Grimm Brothers.

Our partner Qurium found out that both the specific URL targeting and the geo-blocking are features from an Estonian software called Keitaro. Keitaro footprints can be found on multiple cloned media websites of this operation.[2] Keitaro commented that "their licence agreements prohibit such activities" and that when they "receive evidence of a licence agreement violation [they] deactivate the account immediately."

Inception: the fake results of a poll presented in a fake video inserted in a fake media

Doppelganger designed its operation to articulate its disinformation between different assets. When a fake video inside a fake article quotes a poll from fake media, pushed by fake Facebook profiles, the audience might feel like entering a Christopher Nolan movie.

One of the most striking illustrations of this is a poll conducted on a cloned Ukrainian news website. On Monday, 11 July 2022[3], the authentic Ukrainian media RBC[4] warned its readers against an online impersonation of its trademark. According to the fake website, a "nationwide collection of public opinion" was organised. The question asked is, "if you had a choice, in which country would you like to live?" The three options possible were Poland, Ukraine or Russia.

A few days later, on bild[.]pics, one of the fake German news websites set up by the network, an article and a video appeared claiming Ukrainian people do not want to live in Ukraine. The fake Bild video states that according to a poll, 68% of Ukrainian respondents want to live in Russia. This fact is used to justify claims that the Ukrainian government is in a weak position in the war. We also found similar coverage on news.spiegelr[.]today, another asset operated by Doppelganger.

These elements prove coordination between different Doppelganger assets. The operation started with a poll in Ukraine through cloned media, probably pushed on social platforms across specific targeted populations. Then, the results are exploited to produce propaganda videos and articles, impersonating authentic German media to ensure credibility.

[2] More technical details can be found on Qurium's post on this topic.

[3] See https://www.rbc.ua/rus/news/vnimanie-zloumyshlenniki-provodyat-feykovyy-1657540456.html

[4] RBC Ukraine is an independent Ukrainian news agency formed in 2006 as part of the Russian group RBC media. Its Ukrainian branch has split in 2014 and is now independent. RBC reports primarily on Ukraine's daily events.

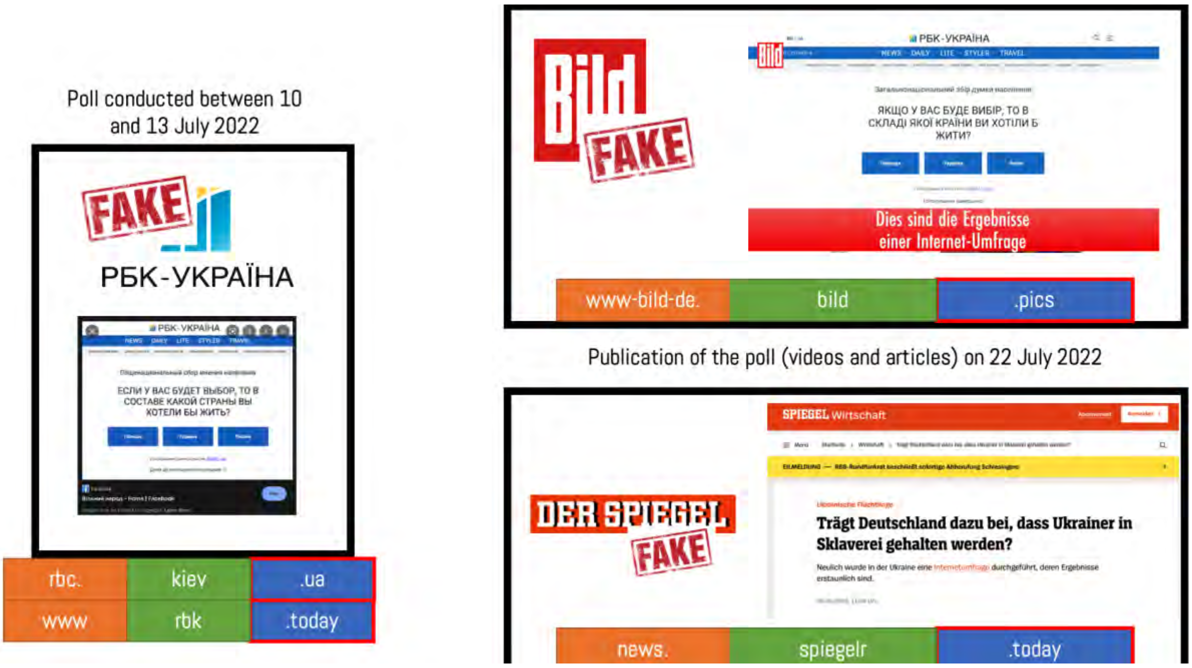

Poll conducted between 10 and 13 July 2022
FAKE
РБК-УКРАЇНА
ЕСЛИ У ВАС БУДЕТ ВЫБОР, ТО В СОСТАВЕ КАКОЙ СТРАНЫ ВЫ ХОТЕЛИ БЫ ЖИТЬ?
rbc.
kiev
.ua
www
rbk
.today
Bild
FAKE
РБК-УКРАЇНА
NEWS DAILY LITE STYLER TRAVEL
ЯКЩО У ВАС БУДЕ ВИБІР, ТО В СКЛАДІ ЯКОЇ КРАЇНИ ВИ ХОТІЛИ Б ЖИТИ?
Dies sind die Ergebnisse einer Internet-Umfrage
www-bild-de.
bild
.pics
Publication of the poll (videos and articles) on 22 July 2022
DER SPIEGEL
FAKE
SPIEGEL Wirtschaft
Trägt Deutschland dazu bei, dass Ukrainer in Sklaverei gehalten werden?
Neulich wurde in der Ukraine eine Internetumfrage durchgeführt, deren Ergebnisse erstaunlich sind.
news.
spiegelr
.today

Figure 6 – Attempt of disinformation inception by Doppelganger

At the time of our investigation, we found two similar polls hosted on one of Bild clones, bild.eu.com, similarly to the one conducted by the fake version of RBC.

- One poll asked German audiences how much they plan to spend this year for equipping their children's school equipment because of inflation[5].
- The other one is asked if people prefer to live comfortably with the Nord Stream 2 pipeline being activated or to suffer from the inconvenience of sanctions and pay higher energy bills[6].

We cannot exclude these will serve as a basis for future disinformation produced by Doppelganger in other assets.

Are results authentic?

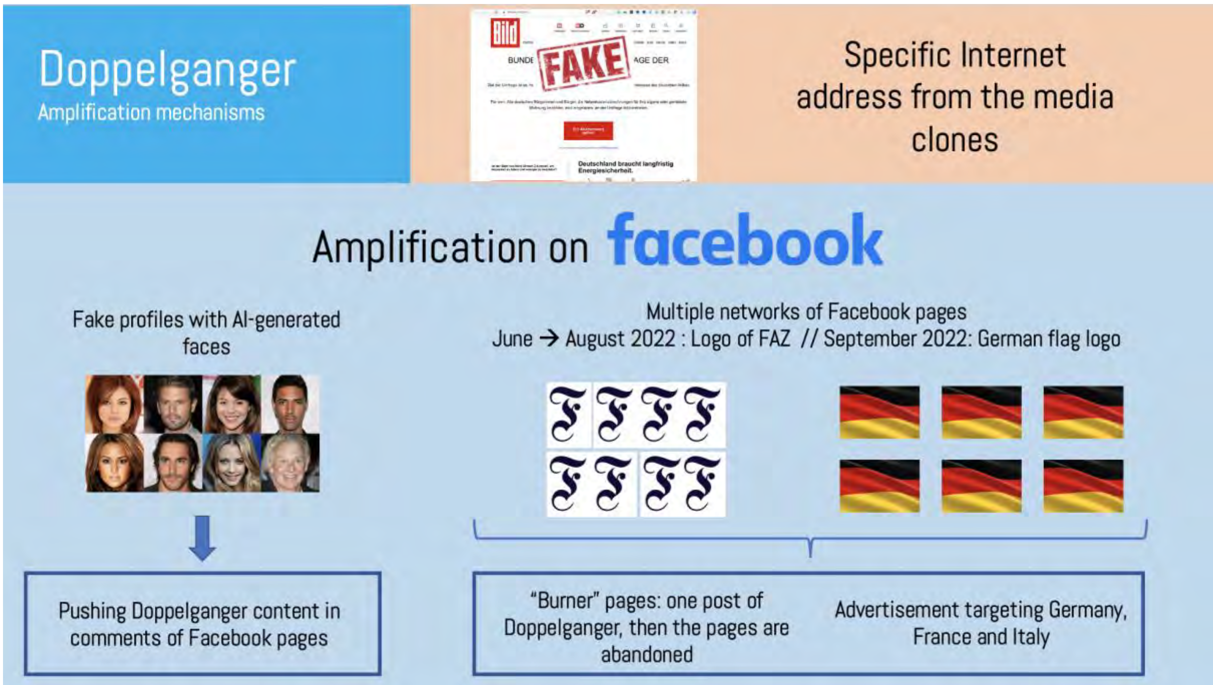
From the source code of the cloned Bild polls, we also have serious doubts about the accuracy of their results. According to our partner Qurium, the results displayed are not reflecting the accurate distribution of votes cast. When looking at the source code, we could see that before voting, results were already hardcoded in the website's source code, as if the results were decided in advance. Moreover, percentages of the results would not add up to 100 % of responses but only to 95%.

[5] See https://web.archive.org/web/20220905145817/https://www.bild.eu.com/ausland/politik-ausland/Umfrage-vorbereitung-auf-die-Schule/.

[6] See https://web.archive.org/web/20220909090650/https://www.bild.eu.com/bild/.

Burn after sharing: Disposable networks of Coordinated Inauthentic Behaviour

Looking into Doppelganger assets, we found patterns of coordinated inauthentic behaviour through profiles and Facebook pages. Like other operations, such as Secondary Infektion[7], most of these assets were like "burner" accounts. The Facebook Pages were created in bulk around certain times, activated to publish one Doppelganger campaign, and were then abandoned.



Doppelganger
Amplification mechanisms

Specific Internet address from the media clones

Amplification on facebook

Fake profiles with AI-generated faces

Pushing Doppelganger content in comments of Facebook pages

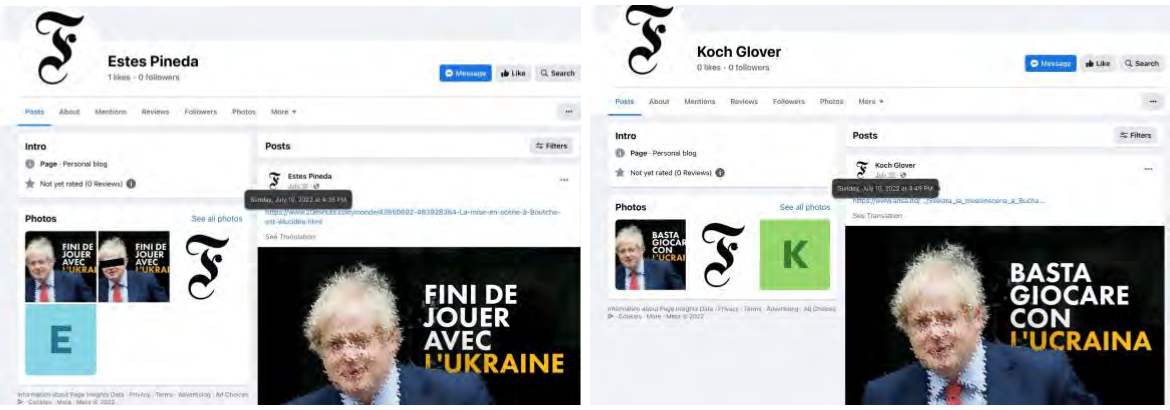
Multiple networks of Facebook pages
June → August 2022 : Logo of FAZ // September 2022: German flag logo

"Burner" pages: one post of Doppelganger, then the pages are abandoned

Advertisement targeting Germany, France and Italy

We can assume these multiple networks are coordinated as their content is very often similar in the countries they target: Germany, the United Kingdom, Italy, France, Ukraine and Latvia.

[7] See Graphika's report here https://secondaryinfektion.org/.

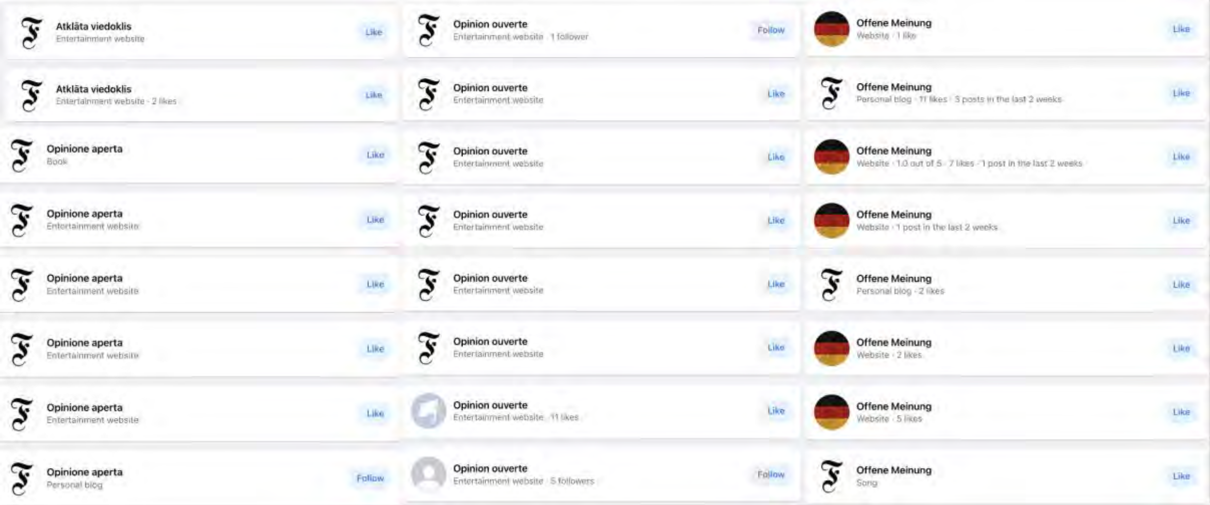


Estes Pineda
1 likes · 0 followers
Message | Like | Search
Posts | About | Mentions | Reviews | Followers | Photos | More
Intro
Page · Personal blog
Not yet rated (0 Reviews)
Photos
See all photos
Posts
Filters
Estes Pineda
Sunday, July 10, 2022 at 4:35 PM
https://www.20minutes.com/monde/43950692-483928384-La-mise-en-scène-à-Boutcha-est-élucidée.html
See Translation
Information about Page Insights Data · Privacy · Terms · Advertising · Ad Choices · Cookies · More · Meta © 2022

Koch Glover
0 likes · 0 followers
Message | Like | Search
Posts | About | Mentions | Reviews | Followers | Photos | More
Intro
Page · Personal blog
Not yet rated (0 Reviews)
Photos
See all photos
Posts
Filters
Koch Glover
Sunday, July 10, 2022 at 4:49 PM
https://www.ansa.it/.../Svelata_la_messinscena_a_Bucha...
See Translation
Information about Page Insights Data · Privacy · Terms · Advertising · Ad Choices · Cookies · More · Meta © 2022

Figure 7 –Facebook pages network shows coordination in spreading media clones

Multiple networks with large numbers of coordinated Facebook Pages were constantly created along the operation, activated, and then abandoned. For instance, we labelled one network "Open opinion", as this name was translated into multiple languages to amplify the media clones.



Atklāta viedoklis
Entertainment website
Like

Atklāta viedoklis
Entertainment website · 2 likes
Like

Opinione aperta
Book
Like

Opinione aperta
Entertainment website
Like

Opinione aperta
Entertainment website
Like

Opinione aperta
Entertainment website
Like

Opinione aperta
Entertainment website
Like

Opinione aperta
Personal blog
Follow

Opinion ouverte
Entertainment website · 1 follower
Follow

Opinion ouverte
Entertainment website
Like

Opinion ouverte
Entertainment website
Like

Opinion ouverte
Entertainment website
Like

Opinion ouverte
Entertainment website
Like

Opinion ouverte
Entertainment website
Like

Opinion ouverte
Entertainment website · 11 likes
Like

Opinion ouverte
Entertainment website · 5 followers
Follow

Offene Meinung
Website · 1 like
Like

Offene Meinung
Personal blog · 11 likes · 3 posts in the last 2 weeks
Like

Offene Meinung
Website · 1.0 out of 5 · 7 likes · 1 post in the last 2 weeks
Like

Offene Meinung
Website · 1 post in the last 2 weeks
Like

Offene Meinung
Personal blog · 2 likes
Like

Offene Meinung
Website · 2 likes
Like

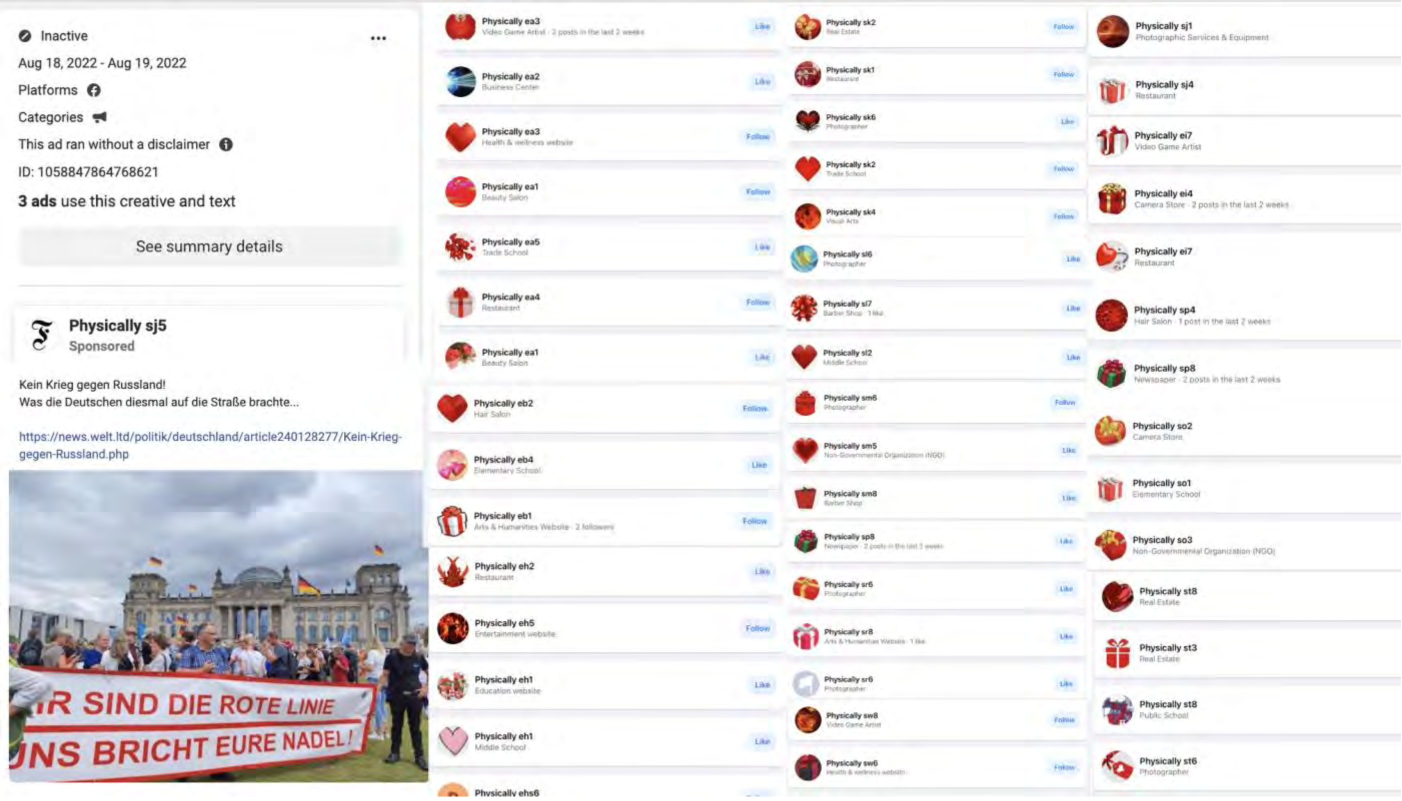
Offene Meinung
Website · 5 likes
Like

Offene Meinung
Song
Like

Figure 8 – Example of one network of Facebook pages created in bulk. All these pages are named "Open opinion", translated into German, French, Italian and Latvian.

We have been surprised by the number of Facebook Pages created and activated by this actor. At a certain point, we had to stop searching for additional assets. As we were manually querying the different keywords, we found hundreds of pages that showed coordination in the content they were posting, and we were unable to manually search every one of them.

We labelled another network, the "botiful" network because all its names were synonyms of the word "beautiful" in English. Pages that amplified Doppelganger operations were named, for instance, *physically*, *beauteous*, *fantastic*, *good-looking*, *grand as*, *pleasing,* or *winsome*.



Inactive

Aug 18, 2022 - Aug 19, 2022

Platforms

Categories

This ad ran without a disclaimer

ID: 1058847864768621

3 ads use this creative and text

See summary details

Physically sj5
Sponsored

Kein Krieg gegen Russland!
Was die Deutschen diesmal auf die Straße brachte...

https://news.welt.ltd/politik/deutschland/article240128277/Kein-Krieg-gegen-Russland.php

Physically ea3
Video Game Artist · 2 posts in the last 2 weeks
Like

Physically ea2
Business Center
Like

Physically ea3
Health & wellness website
Follow

Physically ea1
Beauty Salon
Follow

Physically ea5
Trade School
Like

Physically ea4
Restaurant
Follow

Physically ea1
Beauty Salon
Like

Physically eb2
Hair Salon
Follow

Physically eb4
Elementary School
Like

Physically eb1
Arts & Humanities Website · 2 followers
Follow

Physically eh2
Restaurant
Like

Physically eh5
Entertainment website
Follow

Physically eh1
Education website
Like

Physically eh1
Middle School
Like

Physically ehs6

Physically sk2
Real Estate
Follow

Physically sk1
Restaurant
Follow

Physically sk6
Photographer
Like

Physically sk2
Trade School
Follow

Physically sk4
Visual Arts
Follow

Physically sl6
Photographer
Like

Physically sl7
Barber Shop · 1 like
Like

Physically sl2
Middle School
Like

Physically sm6
Photographer
Follow

Physically sm5
Non-Governmental Organization (NGO)
Like

Physically sm8
Barber Shop
Like

Physically sp8
Newspaper · 2 posts in the last 2 weeks
Like

Physically sr6
Photographer
Like

Physically sr8
Arts & Humanities Website · 1 like
Like

Physically sr6
Photographer
Like

Physically sw8
Video Game Artist
Follow

Physically sw6
Health & wellness website
Follow

Physically sj1
Photographic Services & Equipment

Physically sj4
Restaurant

Physically ei7
Video Game Artist

Physically ei4
Camera Store · 2 posts in the last 2 weeks

Physically ei7
Restaurant

Physically sp4
Hair Salon · 1 post in the last 2 weeks

Physically sp8
Newspaper · 2 posts in the last 2 weeks

Physically so2
Camera Store

Physically so1
Elementary School

Physically so3
Non-Governmental Organization (NGO)

Physically st8
Real Estate

Physically st3
Real Estate

Physically st8
Public School

Physically st6
Photographer

Figure 9 – On the left, a page from the "botiful" network advertising cloned media on Facebook. On the right, we searched for similar patterns in other Facebook Pages. Only part of these pages pushed Doppelganger campaign. The rest of them were ready to be activated for potential future amplification.

Most of these coordinated inauthentic behaviours were still online in mid-September 2022. Our research found that new networks were still being set up in early September.

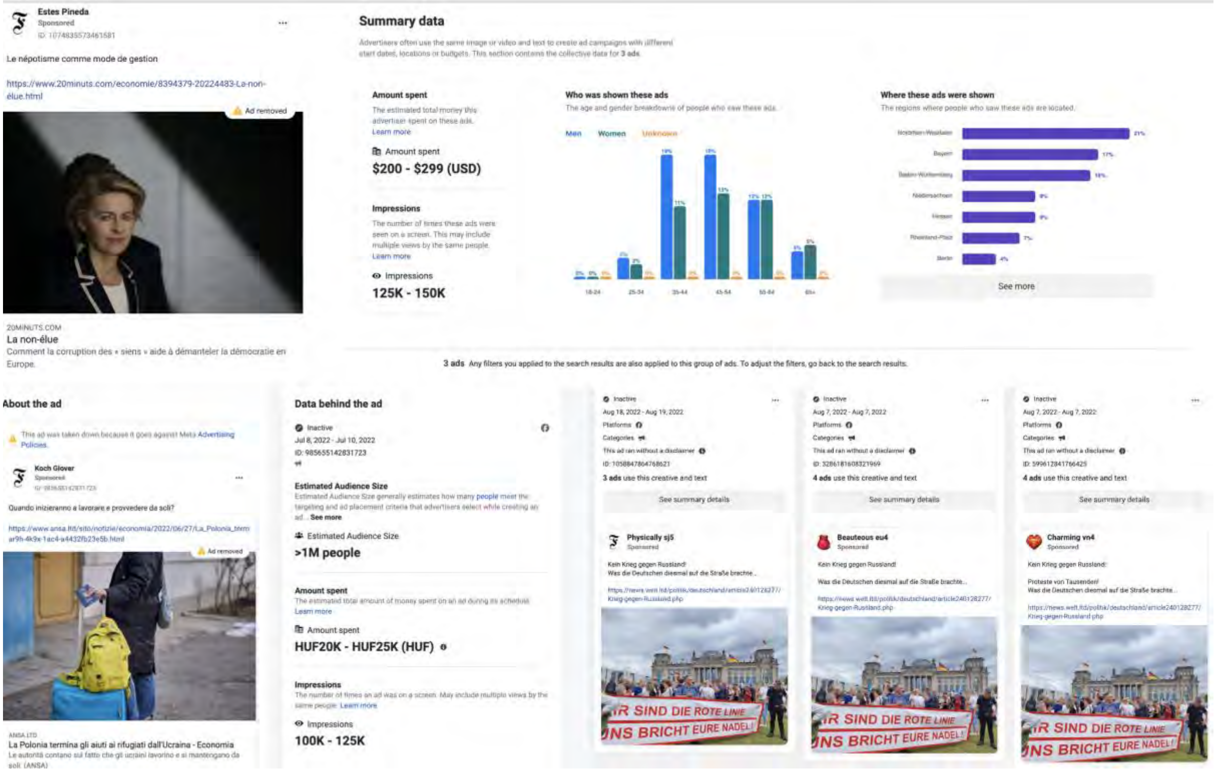
A permanent campaign with multiple Facebook ads

Doppelganger used Facebook advertisements extensively to amplify its campaign. Our analysis can assess that at least 12 campaigns have been running on the platform, but we cannot exclude the possibility that more were launched. Despite the clear anti-Ukraine and pro-Russian messages and the amplification of fake domains already exposed, only a small part of these ads was qualified as issue-based or political, which means they are not archived in Meta's advertisement library.

Facebook's Advertising policies do not authorise advertisement that violates Community Standards[8], such as "certain highly deceptive manipulated media". Moreover, there was no information available about the advertiser of such ads, or on the country from where these pages were operated.

[8] See https://www.facebook.com/policies_center/ads#restricted_content and there https://transparency.fb.com/en-gb/policies/community-standards/misinformation/

Even with a low success rate, this shows how an operation can bypass Facebook's rules on advertising.



Estes Pineda
Sponsored
ID: 1074835573461581

Le népotisme comme mode de gestion

https://www.20minuts.com/economie/8394379-20224483-La-non-élue.html

Ad removed

20MINUTS.COM
La non-élue
Comment la corruption des « siens » aide à démanteler la démocratie en Europe.

Summary data

Advertisers often use the same image or video and text to create ad campaigns with different start dates, locations or budgets. This section contains the collective data for **3 ads**.

Amount spent
The estimated total money this advertiser spent on these ads.
Learn more
Amount spent
$200 - $299 (USD)

Impressions
The number of times these ads were seen on a screen. This may include multiple views by the same people.
Learn more
Impressions
125K - 150K

Who was shown these ads
The age and gender breakdowns of people who saw these ads.

Where these ads were shown
The regions where people who saw these ads are located.

3 ads Any filters you applied to the search results are also applied to this group of ads. To adjust the filters, go back to the search results.

About the ad

This ad was taken down because it goes against Meta Advertising Policies.

Koch Glover
Sponsored
ID: 985655142831723

Quando inizieranno a lavorare e provvedere da soli?

https://www.ansa.ltd/sito/notizie/economia/2022/06/27/La_Polonia_term ar9h-4k9x-1ac4-a4432fb23e5b.html

Ad removed

ANSA.LTD
La Polonia termina gli aiuti ai rifugiati dall'Ucraina - Economia
Le autorità contano sul fatto che gli ucraini lavorino e si mantengano da soli. (ANSA)

Data behind the ad

Inactive
Jul 8, 2022 - Jul 10, 2022
ID: 985655142831723

Estimated Audience Size
Estimated Audience Size generally estimates how many people meet the targeting and ad placement criteria that advertisers select while creating an ad... **See more**
Estimated Audience Size
>1M people

Amount spent
The estimated total amount of money spent on an ad during its schedule.
Learn more
Amount spent
HUF20K - HUF25K (HUF)

Impressions
The number of times an ad was on a screen. May include multiple views by the same people. Learn more
Impressions
100K - 125K

Inactive
Aug 18, 2022 - Aug 19, 2022
Platforms
Categories
This ad ran without a disclaimer
ID: 1058847864768621
3 ads use this creative and text
See summary details

Physically sj5
Sponsored
Kein Krieg gegen Russland!
Was die Deutschen diesmal auf die Straße brachte...
https://news.welt.ltd/politik/deutschland/article240128277/Krieg-gegen-Russland.php

Inactive
Aug 7, 2022 - Aug 7, 2022
Platforms
Categories
This ad ran without a disclaimer
ID: 3286181608321969
4 ads use this creative and text
See summary details

Beauteous eu4
Sponsored
Kein Krieg gegen Russland!

Was die Deutschen diesmal auf die Straße brachte...
https://news.welt.ltd/politik/deutschland/article240128277/Krieg-gegen-Russland.php

Inactive
Aug 7, 2022 - Aug 7, 2022
Platforms
Categories
This ad ran without a disclaimer
ID: 599612841766425
4 ads use this creative and text
See summary details

Charming vn4
Sponsored
Kein Krieg gegen Russland!

Proteste von Tausenden!
Was die Deutschen diesmal auf die Straße brachte...
https://news.welt.ltd/politik/deutschland/article240128277/Krieg-gegen-Russland.php

Figure 10 - Sample of Facebook campaigns launched by Doppelganger

Doppelganger footprints lead to Russia

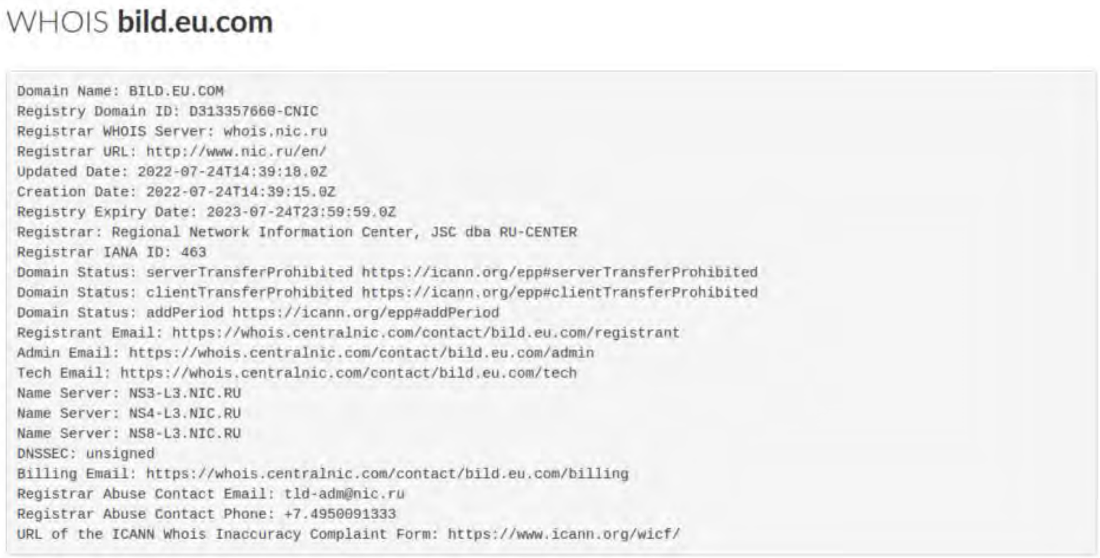
Our analysis does not allow us to conclude on a formal attribution of Doppelganger. However, multiple signals are leading us to think that Russian-speaking actors have played an important role in designing the operation.

Domain names bought on the Russian Internet registrar

The Doppelganger operation relied heavily on the capacity to buy alternative domain names to impersonate authentic media providers. To do so, it passed under the radar of Top-Level Domains verification systems and used privacy settings Internet registrars offer users.

For instance, no public information about the legal owners of these domains was available, which does not help to raise accountability. Consequently, most of the operation was able to cover their traces.

However, our partner Qurium found out the domains have been registered in multiple registrars: GoDaddy, NameCheap, Nic.ru, and Panamanames (Webzilla/XBT). The websites are or have been hosted by the following providers: TimeWeb (RU), Webzilla/XBT Holding (LU), BlueVPS/Glesys (EE/SE), and JavaPipe (NL).



WHOIS **bild.eu.com**

```
Domain Name: BILD.EU.COM
Registry Domain ID: D313357660-CNIC
Registrar WHOIS Server: whois.nic.ru
Registrar URL: http://www.nic.ru/en/
Updated Date: 2022-07-24T14:39:18.0Z
Creation Date: 2022-07-24T14:39:15.0Z
Registry Expiry Date: 2023-07-24T23:59:59.0Z
Registrar: Regional Network Information Center, JSC dba RU-CENTER
Registrar IANA ID: 463
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Email: https://whois.centralnic.com/contact/bild.eu.com/registrant
Admin Email: https://whois.centralnic.com/contact/bild.eu.com/admin
Tech Email: https://whois.centralnic.com/contact/bild.eu.com/tech
Name Server: NS3-L3.NIC.RU
Name Server: NS4-L3.NIC.RU
Name Server: NS8-L3.NIC.RU
DNSSEC: unsigned
Billing Email: https://whois.centralnic.com/contact/bild.eu.com/billing
Registrar Abuse Contact Email: tld-adm@nic.ru
Registrar Abuse Contact Phone: +7.4950091333
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

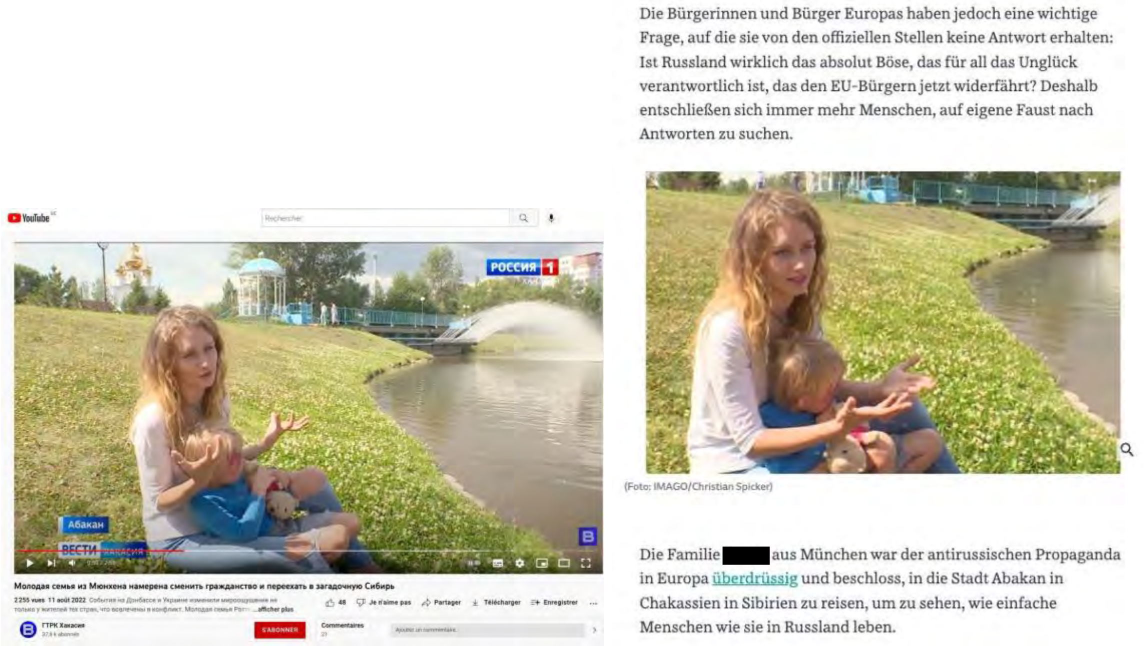
Figure 11 – A clone of authentic Bild, named "bild[.]eu.com", was registered on Russian Internet Registrar Nic.ru

Fake articles: captions from local Siberian Russian TV

Doppelganger fake articles are looking at undermining Germany and Europe for their failures to protect their countries, as well as for their misrepresentations of Ukraine and Russia.

Taken all together, these pieces of content are very often poorly written, with language errors or automated translation bugs. At times, the tone of these stories is so grotesque that they end up looking like a parody. For instance, a fake Sueddeutsche article follows the story of a German family that moved into Siberia.

The article concludes with this sentence: "*The German family liked Siberia so much that they applied for citizenship and are ready to move to Russia, which welcomed them so warmly and kindly. But you don't have to discover another country to see the truth. Open your fridge. How much less food does it contain?"*



Молодая семья из Мюнхена намерена сменить гражданство и переехать в загадочную Сибирь

2 255 vues 11 août 2022 События на Донбассе и Украине изменили мироощущение не только у жителей тех стран, что вовлечены в конфликт. Молодая семья Ротт ...afficher plus

ГТРК Хакасия
27,8 k abonnés

Die Bürgerinnen und Bürger Europas haben jedoch eine wichtige Frage, auf die sie von den offiziellen Stellen keine Antwort erhalten: Ist Russland wirklich das absolut Böse, das für all das Unglück verantwortlich ist, das den EU-Bürgern jetzt widerfährt? Deshalb entschließen sich immer mehr Menschen, auf eigene Faust nach Antworten zu suchen.

(Foto: IMAGO/Christian Spicker)

Die Familie [redacted] aus München war der antirussischen Propaganda in Europa überdrüssig und beschloss, in die Stadt Abakan in Chakassien in Sibirien zu reisen, um zu sehen, wie einfache Menschen wie sie in Russland leben.

Figure 12 - How a news section from local TV Rossiya 1 in Siberia[9] becomes a support for a fake Sueddeutsche article[10]

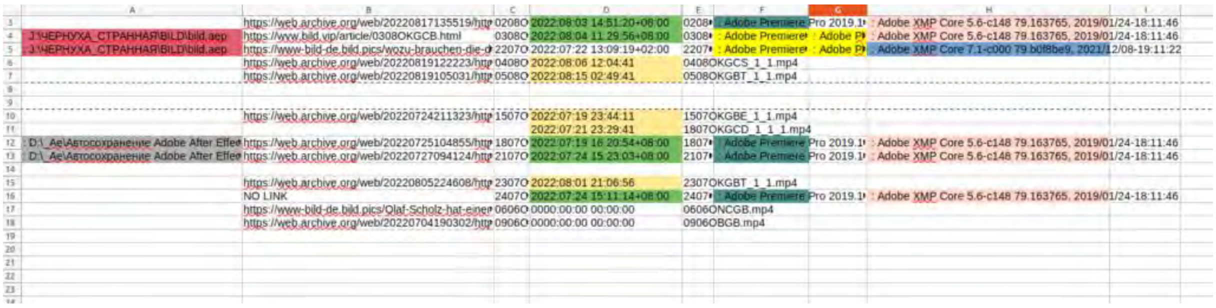
Fake videos: the mysterious МСК Ф-Германия Adobe project

Based on the metadata available in Doppelganger's fake videos, Qurium can assess that videos were produced by computers set up in Russian languages. One of these computers' clocks was set at GMT+8, which means that videos could have been produced in Siberia, in the Irkutsk region.

The metadata available also reveals the name of the video project files: МСК Ф-Германия.prproj and МСК Ф-Германия-2.prproj, which could be translated as MSC P-Germany and Germany2. MSC is a common short sign for Moscow.

[9] See the report here https://www.youtube.com/watch?app=desktop&v=GHL2ccw5ip4

[10] See the fake article here https://web.archive.org/web/20220915115532/https://www.sueddeutsche.me/politik/Volksdiplomatie-1.6324468.html



	A	B	C	D	E	F	G	H	I
3		https://web.archive.org/web/20220817135519/http	0208O	2022:08:03 14:51:20+08:00	0208•	: Adobe Premiere	Pro 2019.1•	: Adobe XMP Core 5.6-c148 79.163765, 2019/01/24-18:11:46	
4	J:\ЧЕРНУХА_СТРАННАЯ\BILD\bild.aep	https://www.bild.vip/article/0308OKGCB.html	0308O	2022:08:04 11:29:56+08:00	0308•	: Adobe Premiere•	: Adobe P•	: Adobe XMP Core 5.6-c148 79.163765, 2019/01/24-18:11:46	
5	J:\ЧЕРНУХА_СТРАННАЯ\BILD\bild.aep	https://www-bild-de.bild.pics/wozu-brauchen-die-d•	2207O	2022:07:22 13:09:19+02:00	2207•	: Adobe Premiere•	: Adobe P•	: Adobe XMP Core 7.1-c000 79.b0f8be9, 2021/12/08-19:11:22	
6		https://web.archive.org/web/20220819122223/http	0408O	2022:08:06 12:04:41	0408OKGCS_1_1.mp4				
7		https://web.archive.org/web/20220819105031/http	0508O	2022:08:15 02:49:41	0508OKGBT_1_1.mp4				
8									
9									
10		https://web.archive.org/web/20220724211323/http	1507O	2022:07:19 23:44:11	1507OKGBE_1_1.mp4				
11				2022:07:21 23:29:41	1807OKGCD_1_1_1.mp4				
12	: D:_Ae\Автосохранение Adobe After Effe•	https://web.archive.org/web/20220725104855/http	1807O	2022:07:19 16:20:54+08:00	1807•	: Adobe Premiere	Pro 2019.1•	: Adobe XMP Core 5.6-c148 79.163765, 2019/01/24-18:11:46	
13	: D:_Ae\Автосохранение Adobe After Effe•	https://web.archive.org/web/20220727094124/http	2107O	2022:07:24 15:23:03+08:00	2107•	: Adobe Premiere	Pro 2019.1•	: Adobe XMP Core 5.6-c148 79.163765, 2019/01/24-18:11:46	
14									
15		https://web.archive.org/web/20220805224608/http	2307O	2022:08:01 21:06:56	2307OKGBT_1_1.mp4				
16		NO LINK	2407O	2022:07:24 15:11:14+08:00	2407•	: Adobe Premiere	Pro 2019.1•	: Adobe XMP Core 5.6-c148 79.163765, 2019/01/24-18:11:46	
17		https://www-bild-de.bild.pics/Olaf-Scholz-hat-einer	0606O	0000:00:00 00:00:00	0606ONCGB.mp4				
18		https://web.archive.org/web/20220704190302/http	0906O	0000:00:00 00:00:00	0906OBGB.mp4				
19									
20									
21									
22									
23									

Figure 13 - Metadata of Doppelganger videos show Russian-speaking connection with the fake video fabrication

A wider network? Traces leading to other pro-Russian assets

Our network analysis of the Facebook amplification showed coordination (content replication, simultaneous advertisement, mutual amplification) with other pro-Russian content, most notably a website called RNN.

RRN is the short name for "Recent Reliable News", accessible through the URL RRN[.]world. It advertises itself as a "resource providing reliable information from verified sources. News and analytics, expert opinions and comments, historical references and dossiers, exposure of fakes". The content from RNN is clearly pro-Russian and designed to undermine the positions of the Western governments in the Ukraine war and the economic crisis.

Our findings show that RRN was initially called "Reliable Russian News" and changed names during the spring of 2022. Researchers have also found that RRN has had infrastructure links with another Russian information operation called WarOnFakes[11].

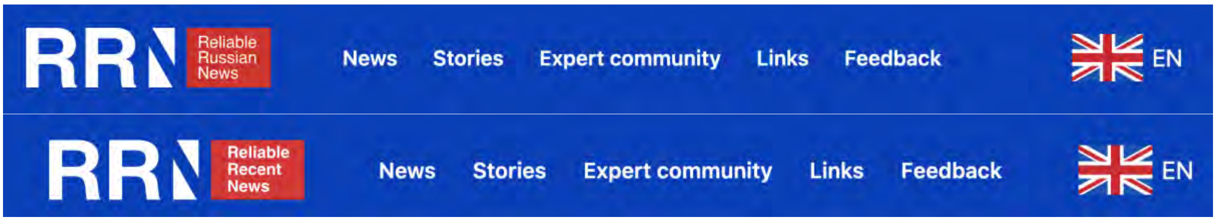


Figure 14 - When did Russian news become reliable? Screenshots from rrussiannews[12] and rrn.world

[11] See https://web.archive.org/web/20220311102049/https://twitter.com/olli_kahn/status/1502227997650214924

[12] See https://web.archive.org/web/20220523111949/https://rrussianews.com/ and https://web.archive.org/web/20220915152559/https://rrn.world/

Policy recommendations

Domain name registration abuse

In our 2020 Indian Chronicles report[13], we already recommended that much more attention needed to be paid to the abuse of the domain name registration systems. In essence, much of the sophisticated, coordinated influence operations we encounter daily are based on content that needs to be displayed somewhere to be read. To do so, malicious actors will often require their own website, and this website needs a domain name. In most instances, the domain name can be bought entirely anonymously (and there are good reasons to protect anonymity), and the multiplication of Top-Level Domains (TLDs) has offered even more opportunities to malware operators, spammers, and also disinformers to buy domain names and thus make their content accessible online.

Here are our recommendations:

- Media and their representatives should consider interacting with the domain name industry to define protections against such misuse of their brand. It would be unfair, costly, and almost impossible to expect media to buy all the existing domain names to protect themselves from misuse; thus, we believe a solution that better protects media domain names should be found.
- Media, cloned media, and fake media are used by almost every meaningful online influence operation. Therefore, we believe that the European Media Freedom Act should consider coverage of the domain name registration issue. To that end, we call upon the European Union co-legislators to reflect on including the necessary safeguards in the Act.

EU-based software and infrastructure

The influence operation depicted in this report impersonates media, but not only. It uses EU-based servers and an EU-based "all-in-one tracker" software (at least for part of the campaigns).

Considering the current context related to sanctions on Russia, the discussions around the EU's "strategic autonomy" and the EU's "initiative on the protection of the EU democratic sphere from covert foreign influence", here is our recommendation:

- Taking appropriate measures so that EU-based legally registered software and infrastructure cannot be used to serve malicious covert influence operations without attracting consequences and penalties.

[13] See http://indianchronciles.eu/

Enforcement of existing EU laws

As it has been the case with other investigations published, opaque and ill-intentioned actors seem to escape the enforcement of EU law permanently. In other words, the fact that they hide their traces and that relevant EU-based institutions are not able to attribute such operations - or do not publicise attributions when they have them - prevents the relevant bodies from being able to properly enforce EU law. De facto, this loophole risks becoming an increasing incentive for more malicious actors to disregard, in particular, trademark laws and GDPR.

Let's take the example of GDPR. Since its entry into force, we cannot recall a single GDPR fine against the malicious actors depicted in our many investigations, nor in the investigations published by organisations such as Bellingcat, Graphika, ISD or the DFRLab. We might have missed the publication of such fines, but if that is indeed the case, it is telling in itself.

Meanwhile, we can hardly recall any of these malicious actors being compliant with GDPR. Common breaches include the absence of legal contacts or the provision of fake contact information, the absence of a Data Protection Officer, and the absence of a policy indicating who the data processor is and the purpose of data collection. Moreover, they do not detail their cookie policy, they use HTTP instead of HTTPS, and exploit tracking services or malwares (of course this is a non-exhaustive list).

There are instances when Data Protection Authorities could have enforced the law on malicious actors as they had large enough information to do so but did not (here and here, for instance). However, in most instances, they are unable to enforce EU law as they do not know who to investigate.

We believe this must change and that the law must be applied equally. Here is our recommendation:

- Putting an end to the non-accountability of opaque and ill-intentioned organisations. This calls for far greater cooperation between institutions that can attribute information operations and those that enforce laws such as trademark laws and GDPR;

Access to platform data

Access to data from platforms is key to disinformation researchers like ourselves. However, data access is very uneven across different platforms. Disinformation campaigns, on the other hand, are rarely contained within one social media platform, and uneven access to platform data often makes it hard to follow and investigate their impact and outreach. For example, the CrowdTangle tool and the Facebook Ads Library have been very beneficial for this research. However, not all platforms offer such tools. Our investigation was very humanintensive, and the research was conducted almost entirely manually, using search engines and platforms' internal search engines, jumping from one dot to another manually. We believe there should be a way so that researchers like us could, in a clearly defined and secured environment, get platforms to provide us with a restricted set of data matching certain patterns. This would have saved us dozens of hours of work (and pleased our families as well).

We also need to access items that have been taken down to be able to follow disinformation actors, look for connections with newly created accounts, avoid disinformation replication, etc. While these items should obviously be taken down, it is crucial that those who will keep track of such ongoing operations can access the initial data to better comprehend and investigate.

Here are our recommendations:

- Data access through tools like CrowdTangle and Ads Library should be the norm across platforms. We call upon the European Commission to ensure this occurs in the framework of the DSA and the Code of Practice on Disinformation.
- Disinformation researchers should be able to get from platforms a restricted set of data from platforms, matching a certain set of patterns in a clearly defined, timely and secured environment. We call upon the European Commission to ensure this is the case in the framework of the DSA and the Code of Practice on Disinformation
- When such a coordinated operation is taken down and exposed (or partially taken down and exposed), platforms must maintain a repository of archived takedowns, enabling researchers to access it for future investigations. We call upon the European Commission to ensure this is the case in the framework of the DSA and the Code of Practice on Disinformation

Appendix: list of 56 Doppelganger domains on 26/09

FAKE DOMAIN	IMPERSONATED DOMAIN FROM MEDIA OUTLET	COUNTRY
bild[.]asia	Bild.de	Germany
bild[.]vip		
bild[.]pics		
bild[.]eu.com		
blld[.]live		
bild[.]llc		
bild[.]work		
bild[.]ws		
tonline[.]cfd	t-online.de	
tonline[.]life		
t-onlinr[.]life		
t-onlinr[.]live		
t-onlinr[.]today		
t-onlinl[.]life		
t-onlinl[.]live		
t-onlinl[.]today		
spiegeli[.]life	Spiegel.de	
spiegeli[.]live		
spiegeli[.]today		
spiegel[.]fun		
spiegel[.]agency		
spiegel[.]co[.]com		
spiegel[.]ltd		
spiegel[.]pro		
spiegel[.]cab		

spiegel[.]work		
spiegelr[.]life		
spiegelr[.]live		
spiegelr[.]today		
tagesspiegel[.]co	Tagesspiegel.de	
tagesspiegel[.]ltd		
sueddeutsche[.]me	Sueddeutsche.de	
sueddeutsche[.]co		
sueddeutsche[.]cc		
sueddeutsche[.]life		
sueddeutsche[.]today		
sueddeutsche[.]online		
faz[.]agency	Faz.net	
faz[.]life		
faz[.]ltd		
welt[.]media	Welt.de	
welt[.]ws		
welt[.]ltd		
nd-aktuell[.]net	nd-aktuell.de	
nd-aktuell[[.]]co		
nd-aktuell[.]pro		
theguardian[.]co.com	Theguardian.com	United Kingdom
dailymail[.]cfd	Daily Mail	
20minuts[.]com	20minutes.fr	France
ansa[.]ltd	Ansa.it	Italy
delfl[.]cc	Delfi.lt, Delfi.lv, Delfi.ee	Lithuania, Latvia, Estonia

lsm[.]li	Lsm.lv	Latvia
rbk[.]kiev.ua	rbc.ua	Ukraine
rbk[.]today		
obozrevatels[.]com	obozrevatel.com	
reuters[.]cfd	reuters.com	International

EU DisinfoLab