Facebook Hustles: The Hidden Mechanics of a Scam Machinery Impersonating News Organisations and Creators

Check First uncovered thousands of Facebook ads leading users to global counterfeit media sites including *Le Monde, BBC, Der Spiegel, Le Soir, El Mundo* ... These ads, propagated by stolen Facebook pages are all related to one another. They redirect to counterfeit media sites interconnected with thousands of other similar scam websites. Traces of these operations date back to 2019.

Table of content

Acknowledgements

CheckFirst wishes to extend their deepest gratitude to:

- Dave LaGrande, Helen Austin, Gordon Garris, Misti Dawn, and Matthias Adolsson, whose invaluable assistance and compelling testimonials have made a significant impact.

- We also appreciate the staunch support and insightful recommendations from both EDMO BELUX and the EU Disinfo Lab team; their contributions have been instrumental in the progression of our investigation.

- Our hat goes to AWO for providing their unrivalled legal expertise, sound advice, and recommendations. We would like to especially acknowledge Mathias Vermeulen and Laureline Lemoine, whose proficiency and guidance have been critical in navigating through the complexities.

- Lastly, our sincere thanks to the Meta Security teams for their prompt responsiveness in setting up a meeting and attentively considering our findings. We are grateful for your cooperation and open-mindedness.

Executive Summary

This investigation uncovered a widespread scam starting on Facebook and involving 1500+ ads leading users to counterfeit media sites. Facebook users who click on any link present on the false media websites are redirected to a personal data collection form posing as an account creation form to join a lucrative investment platform. Once the information is sent, scammers call the user's phone number to try to get them to send money through the fictional investment platform. These Facebook ads are propagated by dozens of Facebook pages of which scammers have taken control through social engineering. We estimate that the reach of the Facebook pages scammers are controlling surpasses 10 million users.

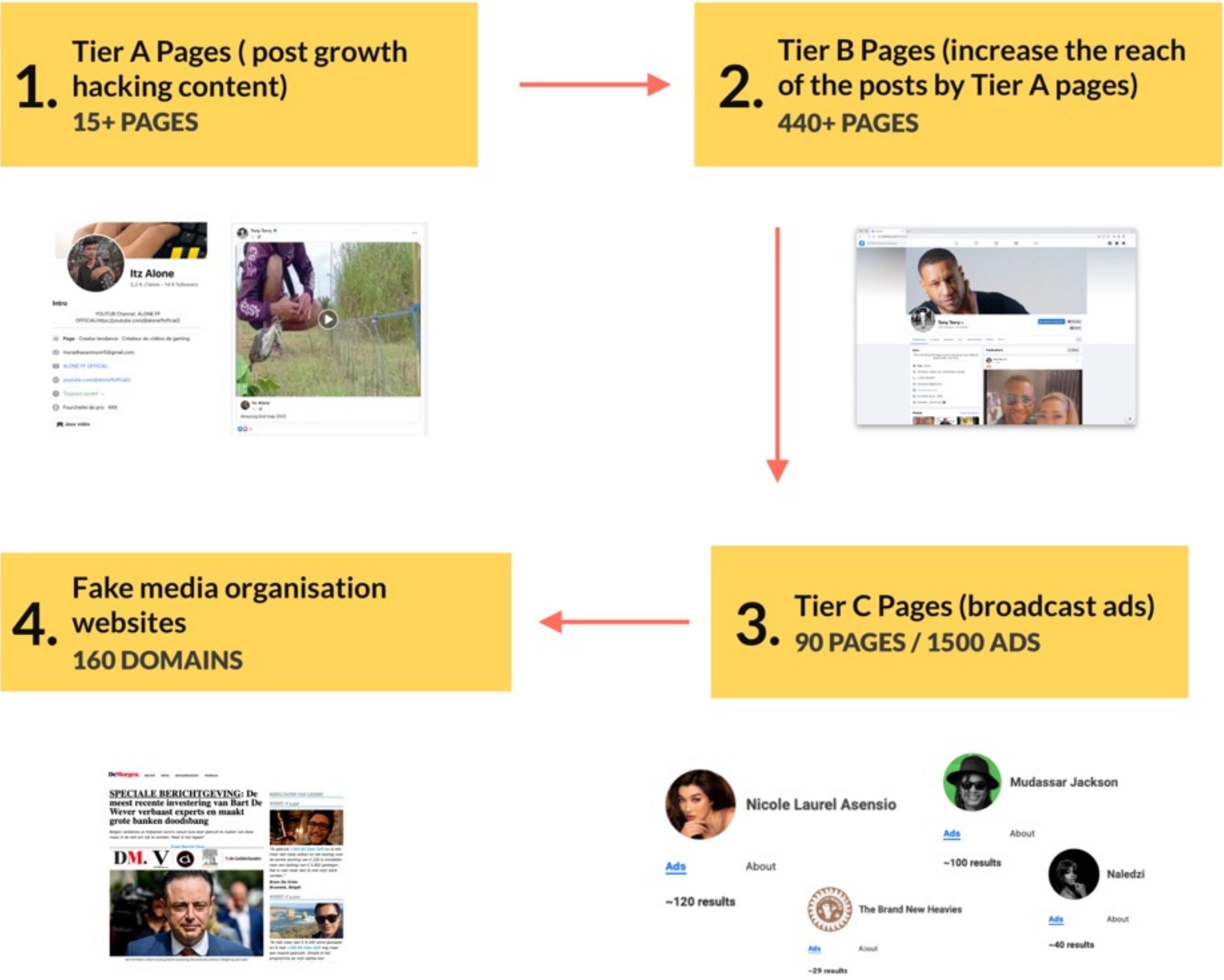
The scam primarily targets users through deceptive ads, featuring sensational language, prominent media figures, and public personalities, enticing users with clickbait titles promising quick profits or scandalous events. The common characteristics of these ads include being published from unrelated Facebook pages and redirecting users to fake media organisation websites. Political figures are also exploited in the ads, potentially influencing their public perception negatively.

The infrastructure behind the scam involves the purchase of campaigns through a network of Facebook pages controlled by the scammers themselves. Social engineering techniques are employed to gain control over these pages, as confirmed by artists and creators victimised by the scammers during what was called the "Tony Terry Scam", named after an artist's Facebook page used by scammers to lure other Facebook page owners into giving them control of their page. A case study on the "Tony Terry scam" reveals how the scammers misuse the social media accounts of well-known artists like Tony Terry. The scam involves approaching artists or creators managing Facebook pages with collaboration proposals, ultimately gaining control over their pages to run scam ads.

The scam operation relies on a complex infrastructure that includes a network of three-tier Facebook pages. The first tier consists of pages that constantly post viral content, while the second tier re-posts this content to act as recruitment pages. The third tier comprises smaller pages owned by artists or creators, who unknowingly give the scammers admin access. This intricate network allows the scammers to place scam ads and exploit the trust placed in established pages.

The support infrastructure for the scam includes forged media websites impersonating reputable news organisations like *Le Monde*, *France 24*, *Süddeutsche Zeitung* and more (we've identified 60). These websites serve as landing destinations for the scam ads displayed on Facebook, featuring clickbait articles that promote get-rich-quick schemes and fake testimonies. Additionally, forged e-commerce sites are used to bypass Facebook's verification measures.

Overall, these findings emphasise the need for user awareness and vigilance on Facebook to avoid falling victim to such scams. It highlights the importance of platform security measures and proactive detection and mitigation strategies to combat fraudulent activities.



1. Tier A Pages (post growth hacking content)
15+ PAGES

2. Tier B Pages (increase the reach of the posts by Tier A pages)
440+ PAGES

3. Tier C Pages (broadcast ads)
90 PAGES / 1500 ADS

4. Fake media organisation websites
160 DOMAINS

Figure 1: Network of the operation

Introduction

“Did he know that the camera was still rolling ? Is this the end of his career ?” The headline was written across the post, carefully designed to look like a typical popular German TV channel. Two well-known personalities shared the screen: a prominent politician and a news anchor. This is the description of an ad on the feed of a scarcely used Facebook account. Two weeks later, following clue after clue and documenting evidence as we advanced, we uncovered a large scale scam operation.

At the heart of the operation are 1500+ ads purchased from Facebook and leading users to forged media websites. Clicking any link on these websites would eventually lead victims to end up on the phone with a scammer trying to lure them into “investing” in a very lucrative venture.

During our month-long investigation, we uncovered more than 160 domains hosting meticulously counterfeit “news” websites chanting the merits of a get-rich-quick system. More than 60 media brands, mainly European, were shamelessly copied to achieve the goal of funnelling money into the scammers’ pockets. All of this in total breach of hosting companies and registrar’s terms of service. We also discovered an intricate system of more than 500 Facebook pages controlled by fraudsters to both place scam ads (and pass Meta’s verification procedures). This investigation is a journey across platforms, disinformation, social engineering traps, impersonation and even continents as scammers elaborated a convoluted network over the Americas, Europe and South Asia.

This investigation was led through open source intelligence techniques, websites’ code analysis, a series of interviews with victims of the scammers and the usage of data displayed on the Meta Ad Library. We quickly discovered that we were investigating a moving target, Facebook ads coming and going, fraudulent websites popping for a few days before being deleted.

We’ll describe in detail what ads scammers are placing on Meta’s platforms, which psychological levers they use and uncover a network of multiple hundreds of pages allowing them to place ads. We’ll explore how famous media organisations' websites are cloned and how victims are touted. We’ll go through the case study of a particular Facebook page used to social engineer other Facebook users and have them give away total control of their page. Delving deeper into the means used by fraudsters, we’ll describe the infrastructure of the scam operation spanning over Meta’s platforms, the web, call-centres, dubious investment platforms, shady companies in the Baltics and more.

The mere fact that a scam operation this size is possible, has seemingly been operating for years and still mobilises various teams of fraudsters hints at how lucrative it may be. Another conclusion of the existence of this is the dysfunction of an array of safeguards, laws, policy enforcement and verification processes. This will lead us to formulate recommendations both to potential victims, lawmakers and platforms.

1. How are users scammed?

1.1 Ads using impersonation as a way of persuasion

What are these ads?

The starting point of this investigation is the presence on Facebook of suspicious looking ads[1] usually making use of sensational language and pictures of prominent media figures and/or public personalities like politicians or entertainment celebrities. Further variations of the ad inserts use the image of global personalities like Elon Musk. Both ad types include a clickbait title promising either quick profits, or some form of disruption or scandal.

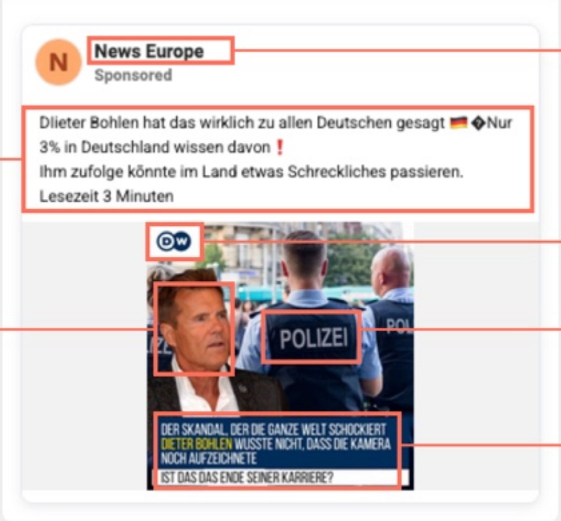
Common characteristics of these ads are:

- Published from a Facebook page unrelated to the product or event portrayed in the ad image
- Usage of public personalities
- Usage of clickbait title and body text, sometimes unrelated with the content of the ad image
- Links to a website mimicking a news outlet

[1] https://github.com/CheckFirstHQ/Facebook-Hustles/tree/main/Screenshots/Fake%20Media%20Organisation%20websites

Anatomy of scam ads

The ads either use a stock picture of a public personality or a photomontage portraying a personality having been part of a (fake) interview for a prominent media organisation.



News Europe
Sponsored

Dlieter Bohlen hat das wirklich zu allen Deutschen gesagt 🇩🇪 ◆Nur 3% in Deutschland wissen davon ❗
Ihm zufolge könnte im Land etwas Schreckliches passieren.
Lesezeit 3 Minuten

DW
POLIZEI
DER SKANDAL, DER DIE GANZE WELT SCHOCKIERT DIETER BOHLEN WUSSTE NICHT, DASS DIE KAMERA NOCH AUFZEICHNETE
IST DAS DAS ENDE SEINER KARRIERE?

Ad body text
"Dieter Bohlen really said that to all Germans 🇩🇪 Less than 3% in Germany know about it ❗ According to him, something terrible could happen in the country"

Well known personality
Dieter Bohlen is a German songwriter, producer, singer and television personality

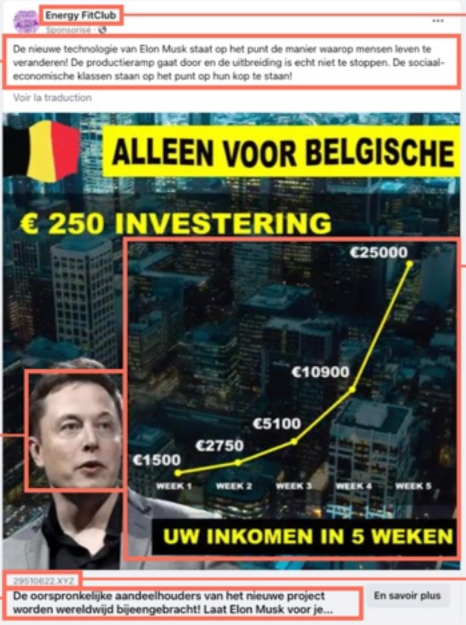
Page
Unrelated to DW

Media logo
Deutsche Welle

Drama
Involvement of the police

Clickbait title
The scandal that shocked one whole world. Is this the end of his career?

Figure 2: Anatomy of an photomontage suggesting a political scandal



Energy FitClub
Sponsorisé ·

De nieuwe technologie van Elon Musk staat op het punt de manier waarop mensen leven te veranderen! De productieramp gaat door en de uitbreiding is echt niet te stoppen. De sociaal-economische klassen staan op het punt op hun kop te staan!

Voir la traduction

29510622.XYZ
De oorspronkelijke aandeelhouders van het nieuwe project worden wereldwijd bijeengebracht! Laat Elon Musk voor je...

En savoir plus

Ad body text
"Elon Musk's new technology is about to change the way people live! The production disaster continues and the expansion is really unstoppable. The socio-economic classes are about to be turned upside down!"

Well known personality
Elon Musk is a business magnate and investor.

Link description
The original shareholders of the new project are gathered worldwide! Let Elon Musk for you...

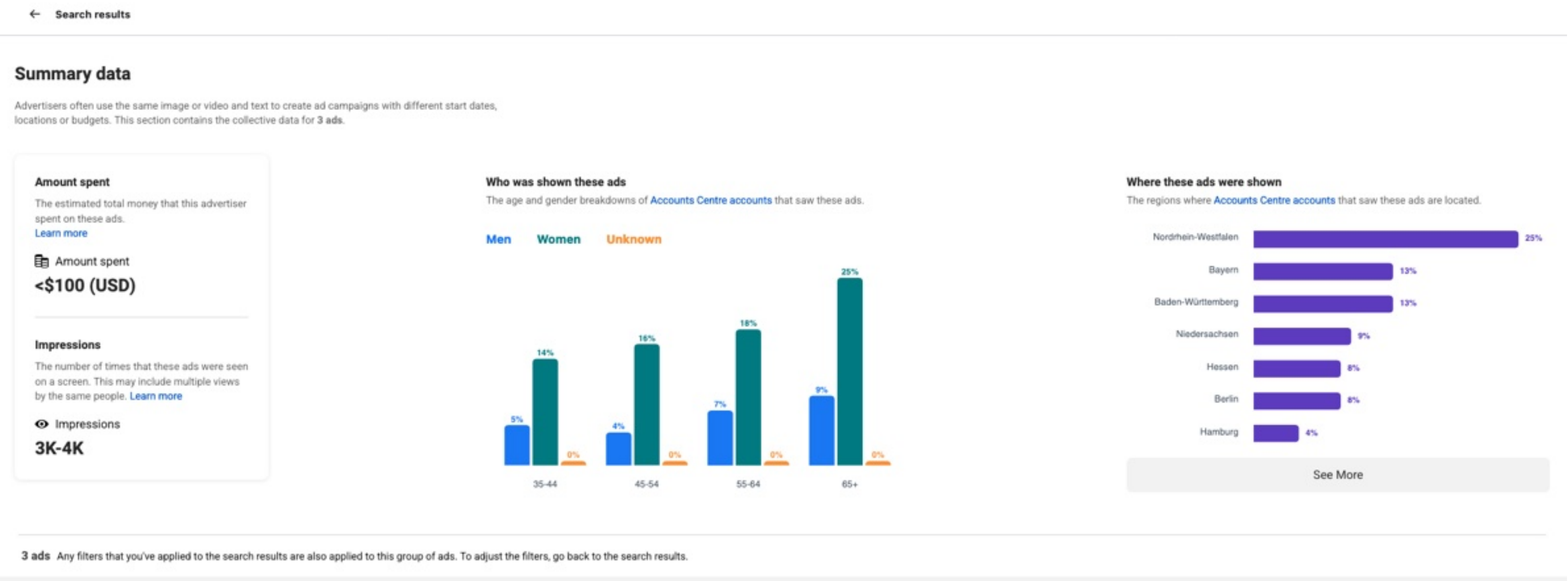
Page
Unrelated to Elon Musk or his businesses

Financial attraction
Invest 250€, get 25.000€ in 5 weeks

Domain
Unrelated to Elon Musk or his businesses

Figure 3: Anatomy of a photomontage promoting an investment, using Elon Musk's image.

Who’s paying for the ads and what is their reach?



← Search results

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 that this advertiser spent on these ads.
Learn more

Amount spent
<$100 (USD)

Impressions

The number of times that these ads were seen on a screen. This may include multiple views by the same people. Learn more

Impressions
3K-4K

Who was shown these ads

The age and gender breakdowns of Accounts Centre accounts that saw these ads.

Where these ads were shown

The regions where Accounts Centre accounts that saw these ads are located.

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

Figure 4: Screen capture of the Meta Ad Library displaying data about a scam ad campaign categorised as a "Ads about social issues, elections or politics"

As mentioned above, certain ads created by scammers may involve politicians. This led us to the discovery of the classification by Meta of some of these ads as "Ads about social issues, elections or politics"[2], resulting in the Meta Ad Library providing additional details about the page responsible for placing said ads. This information includes an estimation of the campaign's expenditure. Examining several campaigns, we’ve established that the typical amount spent by campaign was inferior to USD100 for a number of ad impressions between 3 and 4 thousands. Based on these findings and if the same amount of money were to be used for all campaigns, a rough estimation of the total impressions of all ads discovered during our investigation would be approximately 1.5 million impressions. Notably, we couldn’t find any information for these ads categorised as “Ads about social issues, elections or politics” regarding their funding entity, which is against the commitments made by Meta as a signatory of the European Code of Practice on Disinformation[3] (see 3.2 Incompleteness of the Meta ad library).

As for the paying party, we obtained confirmation through a series of interviews with the owners of stolen Facebook pages (see section 1.2) that scammers placed the ads with funds they control themselves, although the origin of said funds is unknown. Ads are placed from once legitimate Facebook pages belonging to artists or creators who were tricked into giving admin access to their page to scammers. We call these page owners “1st level victims”. Five

[2] https://www.facebook.com/business/help/167836590566506?id=288762101909005
Ads about social issues, elections or politics are supposed to be more transparent than usual ads on Facebook. These ads show a disclaimer with the name and entity that paid for the ads and Meta gives a rough estimation of the expenditure, for example, of these ads in the Meta Ads Library.

[3] https://disinfocode.eu/

victims confirmed directly to us during interviews that they did not suffer any financial loss after the scammers seized control of their page.

What do these ads promote?

The role of these ads placed on Facebook is more oriented at getting clicks than to directly promote specific products. Some inserts are promising the users to learn more about a pseudo-scandal involving public figures, while others are displaying ways to get unrealistic returns on investments through technology products or cryptocurrencies.

Where are they published?

We found that campaigns are purchased through a network of Facebook pages. In terms of follower counts, the median value of these pages is 2500 followers, with some exceptions over 100,000 followers and one page with more than 2 million followers. Most of these pages share the characteristic of belonging to artists or creators. Control of these pages was taken through social engineering and we've identified 89 Facebook pages falling in this category.
As is offered by Meta when placing an ad, these ads are also visible on other Meta platforms: namely Instagram, Messenger and Audience Network[4].

This paper will be elaborating more on the infrastructure used to place the ads (See section 2.1).

Where do they lead to?

When clicking on the ads, users are led to forged media sites. We counted 162 counterfeit websites mimicking 60 legitimate media organisations, essentially based in Europe. These pages, hosted on a domain unrelated with the forged brand, feature articles written in a sensational tone when covering celebrities or overly enthusiastic tone when covering investment topics.

[4] https://www.facebook.com/audiencenetwork/ - Meta Audience Network Monetize your mobile game.

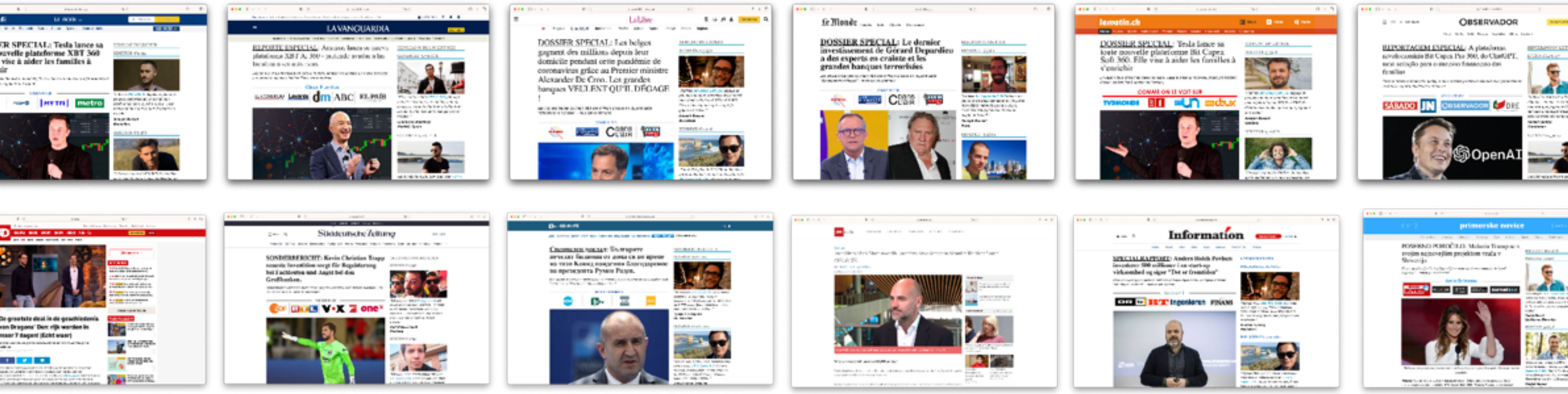


Figure 5: Screen capture of forged media sites.

Forged news websites

We've identified over 160 websites mimicking 60 media brands from 29 countries. From these impersonated media organisations, 51 are based in geographical Europe while 44 are based in the European Union. Forged websites include graphical elements, logos, page layouts and fonts typically used by the original media organisation.

A typical layout begins with a purported "Special report" header, alleging a conspiracy where a high-profile figure is accused of concealing 'truth' from the public, or is publicising an investment scheme. The website also includes a visual claiming the report to have been featured across multiple mainstream media outlets in the victim's home country, further bolstering the illusion of authenticity. This is followed by an extensive article containing links, all leading to a personal data collection form.

Additionally, the website's sidebar is populated with counterfeit testimonials from users claiming to have profited from the promoted product. Through the analysis of the source code of the websites we have identified over 50 different "products" promoted by these ads/testimonials, essentially related to investment platforms in cryptocurrencies.

Certain versions of these sites go a step further, incorporating an imitation of Facebook's comment section at the end of the page to highly praise the virtues of the advertised product.

Most notably, the bottom section of the website (hence not immediately visible by the users when browsing it) contains sections designed to collect data from users, including name, phone number and email address, all destined to the scammers. All links displayed on the page (including those in ads) point to the bottom of the page where the data collection form is located.

The ultimate objective of these counterfeit sites is two-fold: firstly, to deceive users into believing they are browsing their trusted, local news outlet, and secondly, to coax them into submitting personal information via online forms.

Some of these media were already aware that such scams existed such as RTBF[5], *Le Soir*[6], *Le Monde*[7],[8],[9], *Newtral*[10], *RTVE*[11], *Maldita*[12],[13],[14],[15],[16], *DeMorgen*[17] or *De Standaard*[18] and tried to warn their audience but, to our knowledge, no coordinated action was further pursued.

[5] https://www.rtbf.be/article/tesla-na-pas-lance-une-nouvelle-plateforme-de-cryptomonnaies-pour-aider-les-familles-a-senrichir-11109095

[6] https://www.lesoir.be/386670/article/2021-07-29/le-soir-victime-dun-plagiat-autour-des-cryptomonnaies

[7] https://www.lemonde.fr/pixels/article/2020/11/29/bitcoin-revolution-secrets-de-stars-comment-reconnaitre-les-publicites-pour-des-arnaques-aux-placements_6061565_4408996.html

[8] https://www.lemonde.fr/pixels/article/2020/11/29/revelations-sur-une-gigantesque-escroquerie-aux-cryptomonnaies_6061567_4408996.html

[9] https://www.lemonde.fr/les-decodeurs/article/2020/02/24/tout-est-faux-dans-ce-dossier-special-sur-l-investissement-miracle-de-xavier-niel_6030627_4355770.html

[10] https://www.newtral.es/estafa-elon-musk-bitcoin/20220721/

[11] https://www.rtve.es/noticias/20230202/esta-web-promociona-criptomonedas-estafa/2420569.shtml

[12] https://maldita.es/malditobulo/20230228/no-no-es-cierto-que-amancio-ortega-haya-invertido-100-millones-en-bitcoin-revolution-es-una-web-falsa/

[13] https://maldita.es/malditobulo/20200403/timo-bitcoin-risto-jordi-cruz-coronavirus-timo/

[14] https://maldita.es/malditobulo/20230427/timo-famosos-arrestados-criptomonedas/

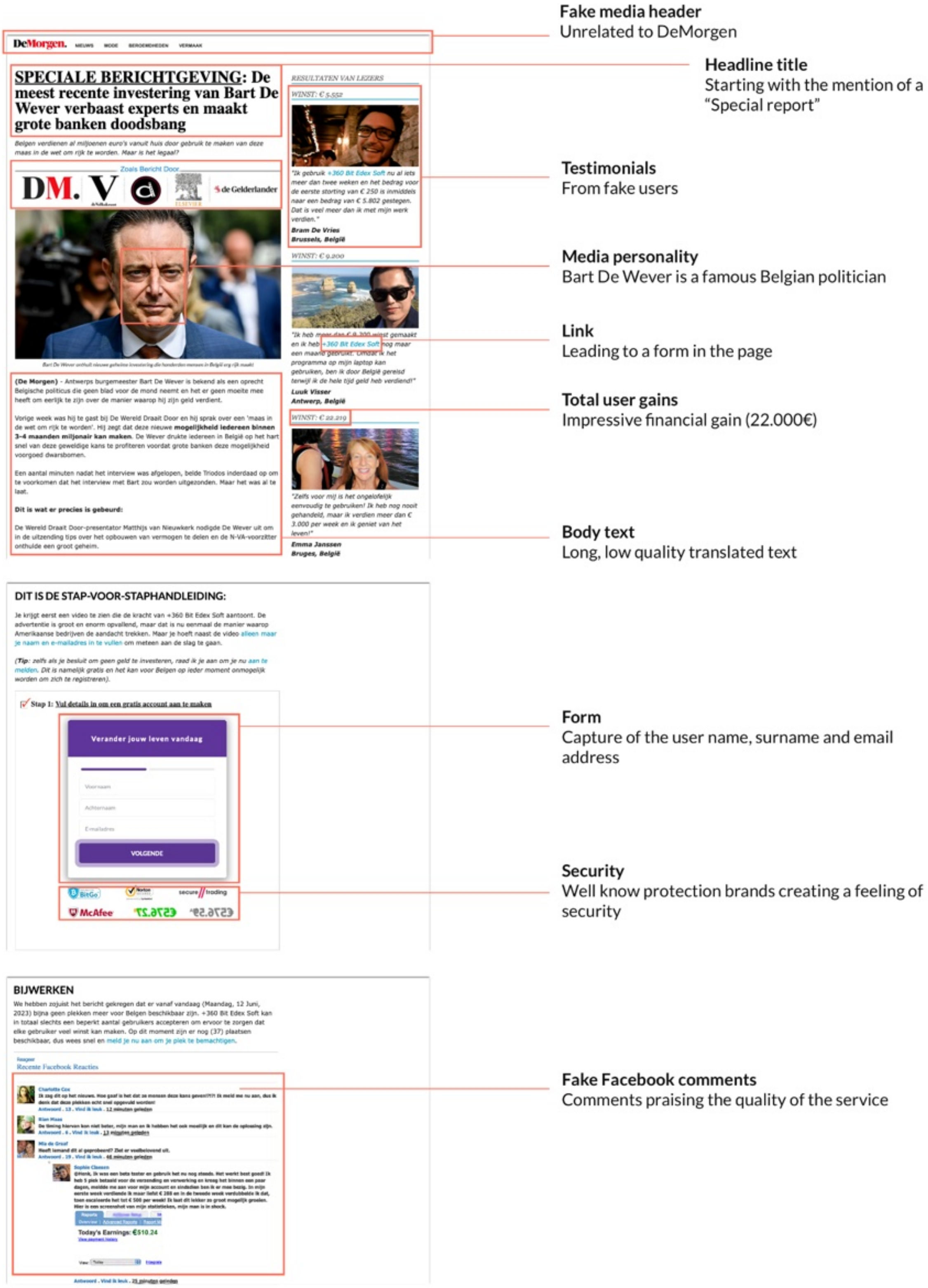
[15] https://maldita.es/timo/bulo/20230123/tinder-inversion-criptomonedas-timo/

[16] https://maldita.es/timo/bulo/20230316/wyoming-recomendar-criptomonedas-resistencia/

[17] https://www.demorgen.be/nieuws/de-morgen-waarschuwt-voor-frauduleuze-mails-over-bitcoin-investeringen~b166b7fd/

[18] https://www.standaard.be/cnt/dmf20190820_04568382

Anatomy of a scam website



DeMorgen. NIEUWS MODE BEROEMDHEDEN VERMAAK

SPECIALE BERICHTGEVING: De meest recente investering van Bart De Wever verbaast experts en maakt grote banken doodsbang

Belgen verdienen al miljoenen euro's vanuit huis door gebruik te maken van deze maas in de wet om rijk te worden. Maar is het legaal?

Zoals Bericht Door

Bart De Wever onthult nieuwe geheime investering die honderden mensen in België erg rijk maakt

(De Morgen) - Antwerps burgemeester Bart De Wever is bekend als een oprecht Belgische politicus die geen blad voor de mond neemt en het er geen moeite mee heeft om eerlijk te zijn over de manier waarop hij zijn geld verdient.

Vorige week was hij te gast bij De Wereld Draait Door en hij sprak over een 'maas in de wet om rijk te worden'. Hij zegt dat deze nieuwe **mogelijkheid iedereen binnen 3-4 maanden miljonair kan maken**. De Wever drukte iedereen in België op het hart snel van deze geweldige kans te profiteren voordat grote banken deze mogelijkheid voorgoed dwarsbomen.

Een aantal minuten nadat het interview was afgelopen, belde Triodos inderdaad op om te voorkomen dat het interview met Bart zou worden uitgezonden. Maar het was al te laat.

Dit is wat er precies is gebeurd:

De Wereld Draait Door-presentator Matthijs van Nieuwkerk nodigde De Wever uit om in de uitzending tips over het opbouwen van vermogen te delen en de N-VA-voorzitter onthulde een groot geheim.

RESULTATEN VAN LEZERS

WINST: € 5.552

"Ik gebruik +360 Bit Edex Soft nu al iets meer dan twee weken en het bedrag voor de eerste storting van € 250 is inmiddels naar een bedrag van € 5.802 gestegen. Dat is veel meer dan ik met mijn werk verdien."

Bram De Vries
Brussels, België

WINST: € 9.200

"Ik heb meer dan € 9.200 winst gemaakt en ik heb +360 Bit Edex Soft nog maar een maand gebruikt. Omdat ik het programma op mijn laptop kan gebruiken, ben ik door België gereisd terwijl ik de hele tijd geld heb verdiend!"

Luuk Visser
Antwerp, België

WINST: € 22.219

"Zelfs voor mij is het ongelofelijk eenvoudig te gebruiken! Ik heb nog nooit gehandeld, maar ik verdien meer dan € 3.000 per week en ik geniet van het leven!"

Emma Janssen
Bruges, België

DIT IS DE STAP-VOOR-STAPHANDLEIDING:

Je krijgt eerst een video te zien die de kracht van +360 Bit Edex Soft aantoont. De advertentie is groot en enorm opvallend, maar dat is nu eenmaal de manier waarop Amerikaanse bedrijven de aandacht trekken. Maar je hoeft naast de video alleen maar je naam en e-mailadres in te vullen om meteen aan de slag te gaan.

(***Tip***: *zelfs als je besluit om geen geld te investeren, raad ik je aan om je nu* aan te melden. *Dit is namelijk gratis en het kan voor Belgen op ieder moment onmogelijk worden om zich te registreren).*

☑ Stap 1: Vul details in om een gratis account aan te maken

Verander jouw leven vandaag

Voornaam

Achternaam

E-mailadres

VOLGENDE

BIJWERKEN

We hebben zojuist het bericht gekregen dat er vanaf vandaag (Maandag, 12 Juni, 2023) bijna geen plekken meer voor Belgen beschikbaar zijn. +360 Bit Edex Soft kan in totaal slechts een beperkt aantal gebruikers accepteren om ervoor te zorgen dat elke gebruiker veel winst kan maken. Op dit moment zijn er nog (37) plaatsen beschikbaar, dus wees snel en meld je nu aan om je plek te bemachtigen.

Reageer
Recente Facebook Reacties

Charlotte Cox
Ik zag dit op het nieuws. Hoe gaaf is het dat ze mensen deze kans geven!?!?! Ik meld me nu aan, dus ik denk dat deze plekken echt snel opgevuld worden!
Antwoord . 13 . Vind ik leuk . 12 minuten geleden

Bian Maas
De timing hiervan kon niet beter, mijn man en ik hebben het ook moeilijk en dit kan de oplossing zijn.
Antwoord . 6 . Vind ik leuk . 13 minuten geleden

Mia de Graaf
Heeft iemand dit al geprobeerd? Ziet er veelbelovend uit.
Antwoord . 19 . Vind ik leuk . 46 minuten geleden

Sophie Claesen
@Henk, Ik was een beta tester en gebruik het nu nog steeds. Het werkt best goed! Ik heb 5 piek betaald voor de verzending en verwerking en kreeg het binnen een paar dagen, meldde me aan voor mijn account en sindsdien ben ik er mee bezig. In mijn eerste week verdiende ik maar liefst € 288 en in de tweede week verdubbelde ik dat, toen escaleerde het tot € 500 per week! Ik laat dit lekker zo groot mogelijk groeien. Hier is een screenshot van mijn statistieken, mijn man is in shock.

Reports
AdSense Setup
Overview | Advanced Reports | Report M
Today's Earnings: €510.24
View payment history
View: Today

Antwoord . Vind ik leuk . 25 minuten geleden

Fake media header
Unrelated to DeMorgen

Headline title
Starting with the mention of a "Special report"

Testimonials
From fake users

Media personality
Bart De Wever is a famous Belgian politician

Link
Leading to a form in the page

Total user gains
Impressive financial gain (22.000€)

Body text
Long, low quality translated text

Form
Capture of the user name, surname and email address

Security
Well know protection brands creating a feeling of security

Fake Facebook comments
Comments praising the quality of the service

Figure 6: Anatomy of a forged website linked from the Facebook ad. Top of page: fake media article. Middle section: personal data collection form. Bottom of page: fake testimonies presented as Facebook comments

The media brands for which a forged media was found are: *7sur7, De Standaard, DeMorgen, HLN, La Libre, Le Soir, BTV, Hobnhnte, Dnevnik, N1, Ekstra Bladet, Fyens, Information, Ämppärit, iltalehti, YLE, France 24, L'internaute, Le Figaro, Le Matin, Le Monde, Der Spiegel, Nord Bayern, Online Focus, Suddeutsche Zeitung, HVG.hu, Corriere della sera, Il Gazzettino, NewsIT, Delfi, Skrastas, Gazeta, Correio, Noticias ao minuto, Observador, Stirile pro tv, Novi Cas, Primorske Novice, El Mundo, El Pais, La Vanguardia, Aftonbladet, AD, Nu, UOL, VF, A-Magasinet, Dagsavisen, La presse, BBC, The Sun, Forum, Toronto Star, Hir.ma, NZ Herald, CNA Singapore, News 24, CNN Tech, Forbes.*

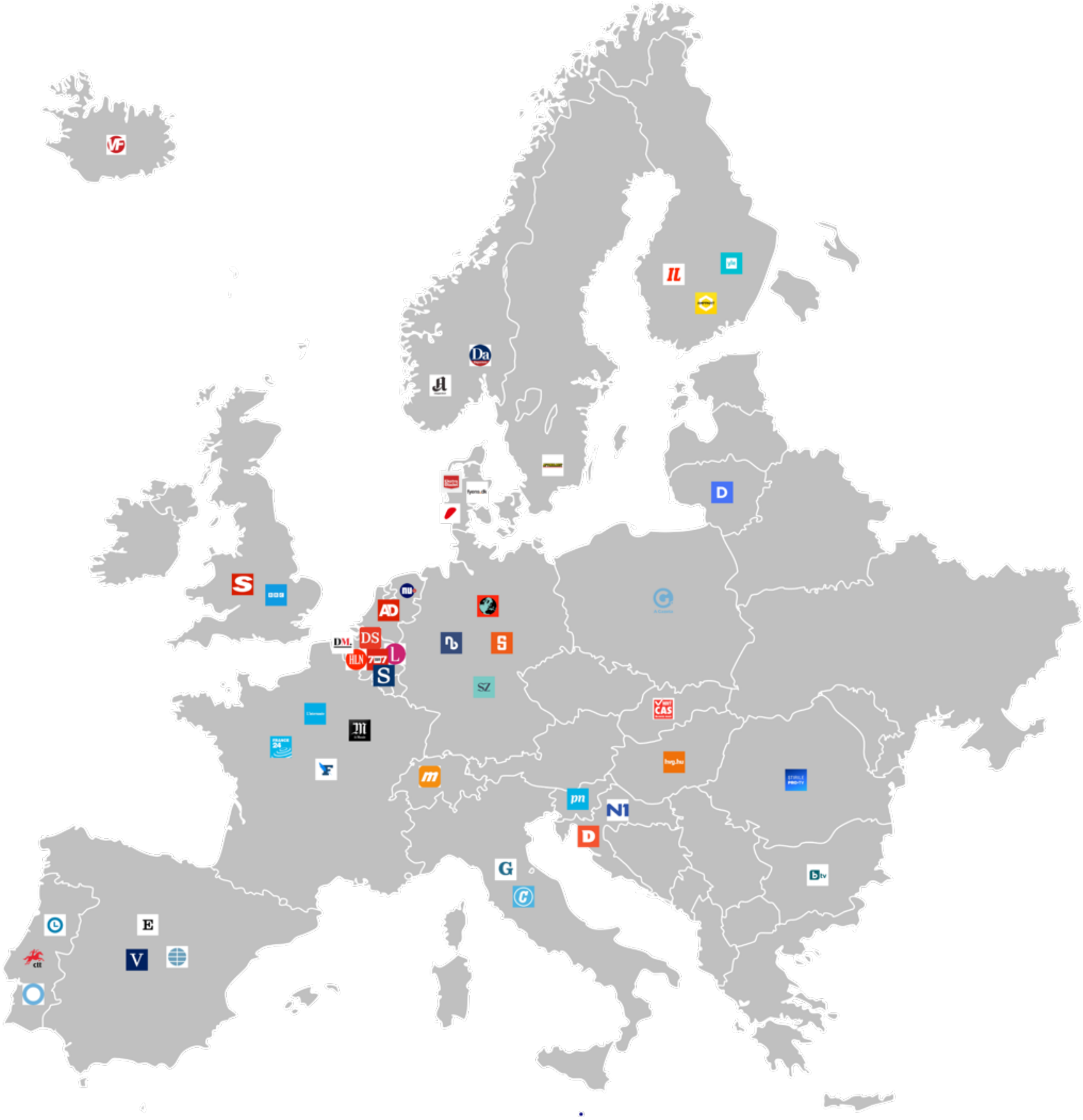


Figure 7: Indicative map of most media brands impersonated, based in continental Europe

What happens to the end victims of the scam?

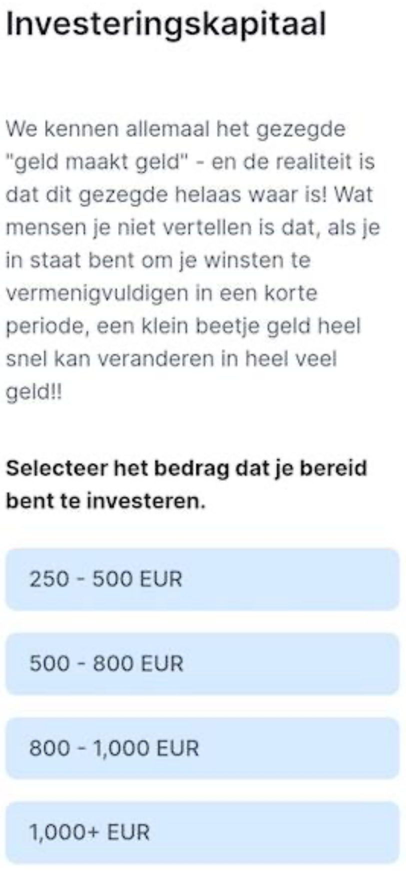
There is no way to assess for sure how each individual interaction between victims and scammers went. However, for the purpose of this investigation, we used a sock puppet to create our own experience after providing some personal data. This led us to have a phone conversation with the fraudsters where they tried to lure us into making a €999 payment by credit card, as a “first” investment to “test” their financial platform, promising between 37 and 41% interest rates.

Getting to talk to the scammers

Using a made up user profile (or “sock puppet”), we filled the personal data collection form one of the forged websites promoting crypto investment. This led us to communicate name and surname, email address and phone number. Then a short questionnaire asked about our gender, age and amount of money we were ready to invest, labelled “250-500 EUR”, “500-800 EUR”, “800-1000 EUR” and “1000+ EUR”. We clicked on the “1000+ EUR” button.

Once this data was provided, the scammers were quick to call back the phone number we had provided them. The call was placed from a number bearing a local country code.

The caller identified herself as Allison and claimed to be an account manager. She explained that she was reaching out to follow up on our registration for the financial service. Background noise suggested she was calling from a call centre or other busy room as we could hear several other phone conversations taking place.



Investeringskapitaal

We kennen allemaal het gezegde "geld maakt geld" - en de realiteit is dat dit gezegde helaas waar is! Wat mensen je niet vertellen is dat, als je in staat bent om je winsten te vermenigvuldigen in een korte periode, een klein beetje geld heel snel kan veranderen in heel veel geld!!

Selecteer het bedrag dat je bereid bent te investeren.

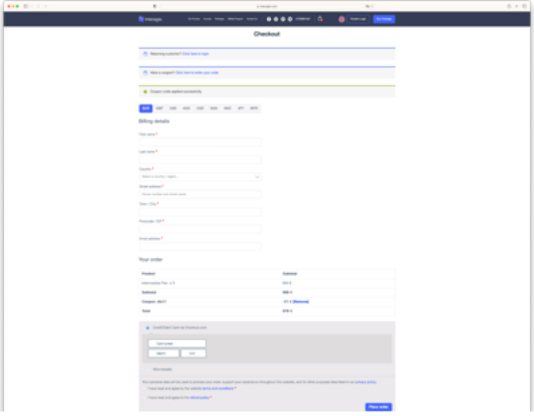
Figure 8: Screen capture of the last question asked to users on how much they are ready to invest

Yet another link, and the here comes the money trap

After some introductory words, “Allison” explained that another person will be managing our investments later. We pointed out during the conversation that we could invest for example €10,000 but the scammer carried on by saying that she wanted to give us first the opportunity to test their services: “*You’ll gonna have the chance to test out the company to see if you’re gonna like the service and be in touch with your advisor and then you will make decisions about big amounts*”.

“Allison” then wanted to carry on immediately and asked how we wanted to make our deposit, either by wire transfer, PayPal or credit or debit card. After we answered that we would pay by credit card, “Allison” sent a link via email to a checkout page hosted on interagio.com for a €999 product (see below screenshot). This page did not bear any product description. Examining this website more closely, we found that it was offering investment courses and that our credit card would be charged each month by that amount.

Still while on the phone with the scammer, “Allison” insisted on guiding us through the “registration process”. The representative put pressure and was adamant to finish this process immediately. We tried to end the conversation there but she insisted several times to complete the registration while we were on the phone, which we declined to do. She then insisted on setting a time to call us back the same day and sent a follow-up message on WhatsApp several hours after the end of the call. We have received at least two more calls from the same number during the following two days.



Checkout

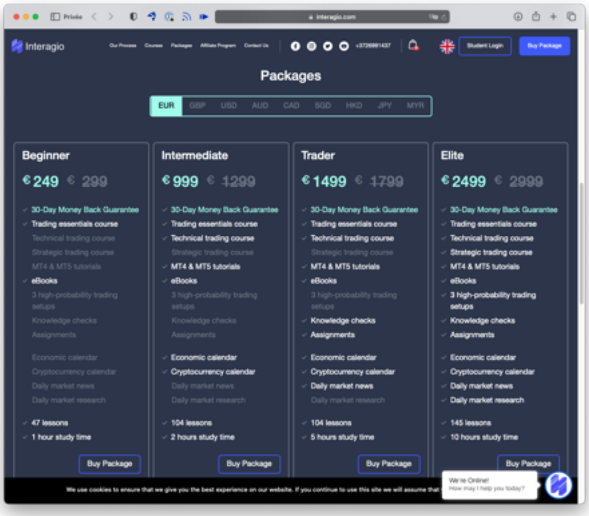
Billing details

Your order

Place order

Figure 9: Purchase page linked from an email sent by “Allison” while on the phone with our sock-puppet

Since we did not make any payment, it remains unclear if the scam ends after victims make a €999 payment or if scammers go as far as paying up 37-41% interest (or make it appear so on a trading platform) before they lure the victims into sending more money.



interagio.com

Interagio

Packages

EUR GBP USD AUD CAD SGD HKD JPY MYR

Beginner	Intermediate	Trader	Elite
€249 € ~~299~~	€999 € ~~1299~~	€1499 € ~~1799~~	€2499 € ~~2999~~
✓ 30-Day Money Back Guarantee	✓ 30-Day Money Back Guarantee	✓ 30-Day Money Back Guarantee	✓ 30-Day Money Back Guarantee
✓ Trading essentials course	✓ Trading essentials course	✓ Trading essentials course	✓ Trading essentials course
Technical trading course	✓ Technical trading course	✓ Technical trading course	✓ Technical trading course
Strategic trading course	Strategic trading course	Strategic trading course	✓ Strategic trading course
MT4 & MT5 tutorials	✓ MT4 & MT5 tutorials	✓ MT4 & MT5 tutorials	✓ MT4 & MT5 tutorials
✓ eBooks	✓ eBooks	✓ eBooks	✓ eBooks
3 high-probability trading setups	3 high-probability trading setups	3 high-probability trading setups	✓ 3 high-probability trading setups
Knowledge checks	Knowledge checks	✓ Knowledge checks	✓ Knowledge checks
Assignments	Assignments	✓ Assignments	✓ Assignments
Economic calendar	✓ Economic calendar	✓ Economic calendar	✓ Economic calendar
Cryptocurrency calendar	✓ Cryptocurrency calendar	✓ Cryptocurrency calendar	✓ Cryptocurrency calendar
Daily market news	Daily market news	✓ Daily market news	✓ Daily market news
Daily market research	Daily market research	Daily market research	✓ Daily market research
✓ 47 lessons	✓ 104 lessons	✓ 104 lessons	✓ 145 lessons
✓ 1 hour study time	✓ 2 hours study time	✓ 5 hours study time	✓ 10 hours study time
Buy Package	Buy Package	Buy Package	Buy Package

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that

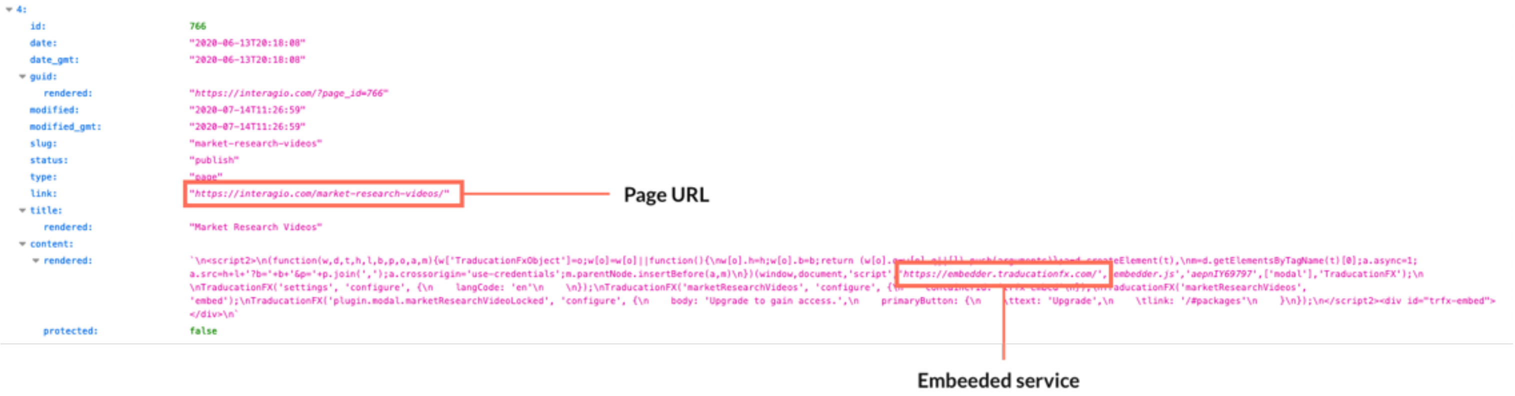
We're Online!
How may I help you today?

Analysing this website further, we established that the payment she pursued was in fact a recurring fee for a training video series on investment. The website is operated by a company registered in Estonia (Educatix OÜ). Looking up the country’s business registration system, we established that the company’s general manager is an Ukrainien and Latvian citizen born in the (then) Soviet Union.

Additionally, we established that the company names used in the operation were in fact real companies which had ceased to exist since. This suggests that scammers are trying to surf on the past reputation of previously existing companies.

Figure 10: Product page of interagio.com showing different tiers of subscription to a video investment course

The website is using WordPress as its content management system and seems to resell content provided by another platform “traducationFX”.



```
▾ 4:
    id:                 766
    date:               "2020-06-13T20:18:08"
    date_gmt:           "2020-06-13T20:18:08"
  ▾ guid:
      rendered:         "https://interagio.com/?page_id=766"
    modified:           "2020-07-14T11:26:59"
    modified_gmt:       "2020-07-14T11:26:59"
    slug:               "market-research-videos"
    status:             "publish"
    type:               "page"
    link:               "https://interagio.com/market-research-videos/"
  ▾ title:
      rendered:         "Market Research Videos"
  ▾ content:
    ▾ rendered:         `\n<script2>\n(function(w,d,t,h,l,b,p,o,a,m){w['TraducationFxObject']=o;w[o]=w[o]||function(){\nw[o].h=h;w[o].b=b;return (w[o].q=w[o].q||[]).push(arguments)};a=d.createElement(t),\nm=d.getElementsByTagName(t)[0];a.async=1;
                        a.src=h+l+'?b='+b+'&p='+p.join(',');a.crossorigin='use-credentials';m.parentNode.insertBefore(a,m)\n})(window,document,'script','https://embedder.traducationfx.com/','embedder.js','aepnIY69797',['modal'],'TraducationFX');\n
                        \nTraducationFX('settings', 'configure', {\n    langCode: 'en'\n    \n});\nTraducationFX('marketResearchVideos', 'configure', {\n    containerId: 'trfx-embed'\n});\nTraducationFX('marketResearchVideos',
                        'embed');\nTraducationFX('plugin.modal.marketResearchVideoLocked', 'configure', {\n    body: 'Upgrade to gain access.',\n    primaryButton: {\n    \ttext: 'Upgrade',\n    \tlink: '/#packages'\n    }\n}});\n</script2><div id="trfx-embed">
                        </div>\n`
      protected:        false
```

Figure 11: Screengrab of a page through the WP JSON API of interagio.com showing a traductationFX product embed

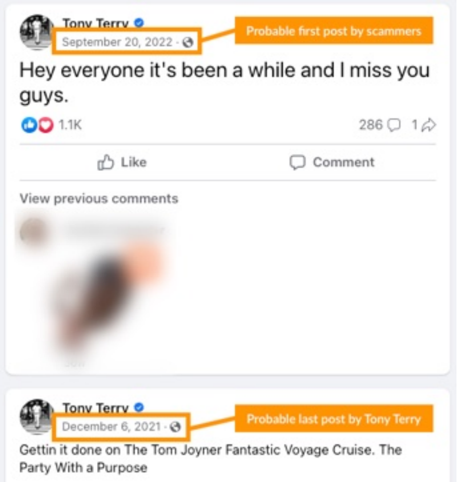
1.2 Case study: The Tony Terry scam

Tony Terry's image and Meta accounts were used as baits to take control of pages of 1st level victims. It seems like scammers pretended to be Tony Terry, proposed to take part in a podcast and ultimately gain control of the creators' pages to run fraudulent ads on it.

Who's Tony Terry?

Tony Terry is a recognised artist in the R&B genre who achieved significant popularity in the late 1980s and early 1990s. Terry's name has been associated with verified accounts on social media platforms, including Instagram and Facebook, which have been implicated in a deceptive activity. Our findings strongly suggest that Terry’s pages fell under the control of scammers.

What does the page post?



Tony Terry

September 20, 2022

Probable first post by scammers

Hey everyone it's been a while and I miss you guys.

Tony Terry

December 6, 2021

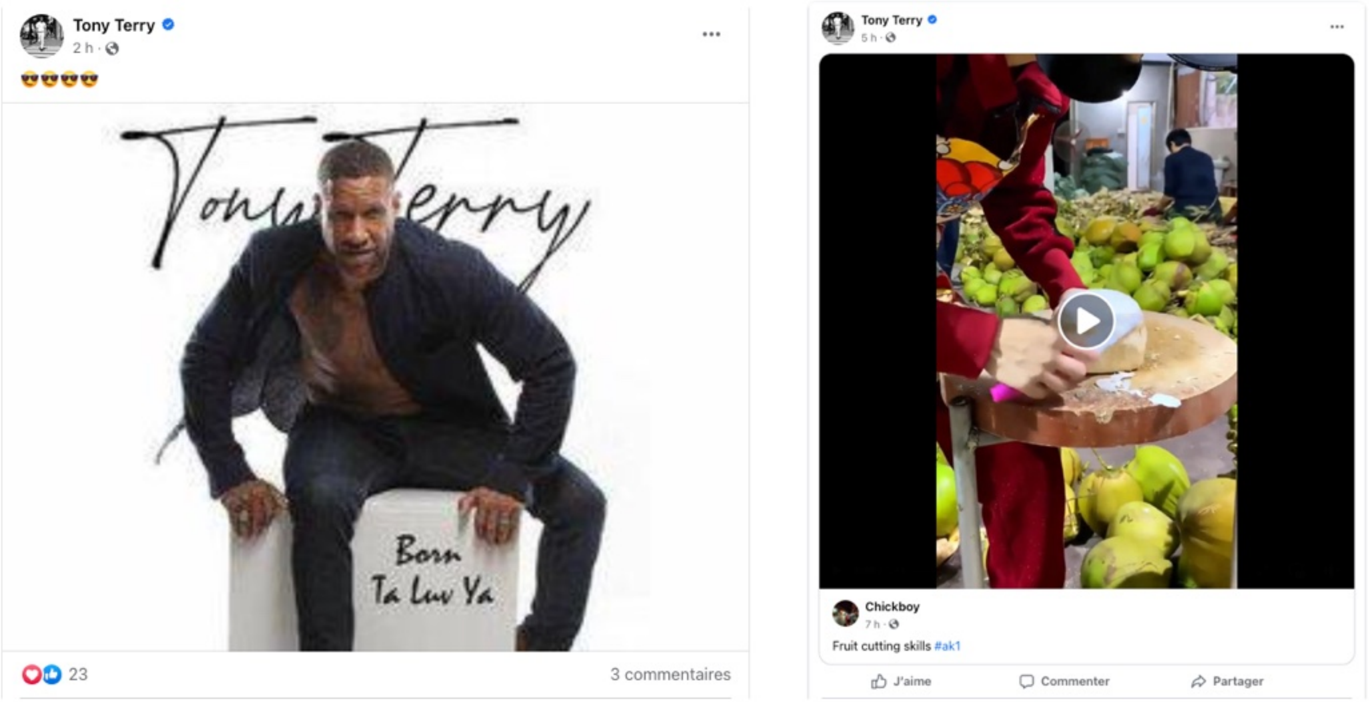
Probable last post by Tony Terry

Gettin it done on The Tom Joyner Fantastic Voyage Cruise. The Party With a Purpose

Figure 12: Last seemingly legitimate post on Tony Terry (bottom)
and first probable post by scammers (top)

Exploring the content posted on Tony Terry’s Facebook page, it seems that control was seized on September 20th 2022. The previous post before this is dated December 6th 2021 and the publishing frequency was very scarce, with only a few posts per year. After September 20th 2022 however, the page starts to post very frequently, including re-posts of other facebook pages including clickbait videos. The latter was never to be found in the page posting history before September 2022.

The content to be found on Tony Terry’s Facebook page after September 20th, 2022 can be categorised in two main categories: Photos related to himself on one hand, and re-posts of other Facebook pages’s Facebook videos on the other hand. The photos present on his page usually feature a picture of him either while performing or showing aspects of his personal life, together with emojis as the post’s text. Re-posts feature mostly unrelated Facebook videos which can be defined as candidates to go viral. These videos are re-posted from an array of pages we suspect are also controlled by the scammers. Examples of these Facebook videos can be a dog pushing a trolley, a display of “amazing skills” of a protagonist performing an unusual and spectacular action. Both kinds of publications (native posts and re-posts) are posted alternatively in relative equal proportions daily.



Tony Terry
2 h ·
😎😎😎😎

Tony Terry
5 h ·

Chickboy
7 h ·
Fruit cutting skills #ak1

Figure 13: Left: Photo post on Tony Terry's page with emojis as body text
Right: Re-publication of Facebook video from another page controlled by scammers

We interpret the purpose of re-posts as being part of a technique aiming at raising the number of followers of the page. As the scammers are using Tony Terry's page as a way to gain access to more pages through social engineering, it would make sense that the fraudsters would want to contact the 1st level victims from an account showing a significant follower count.

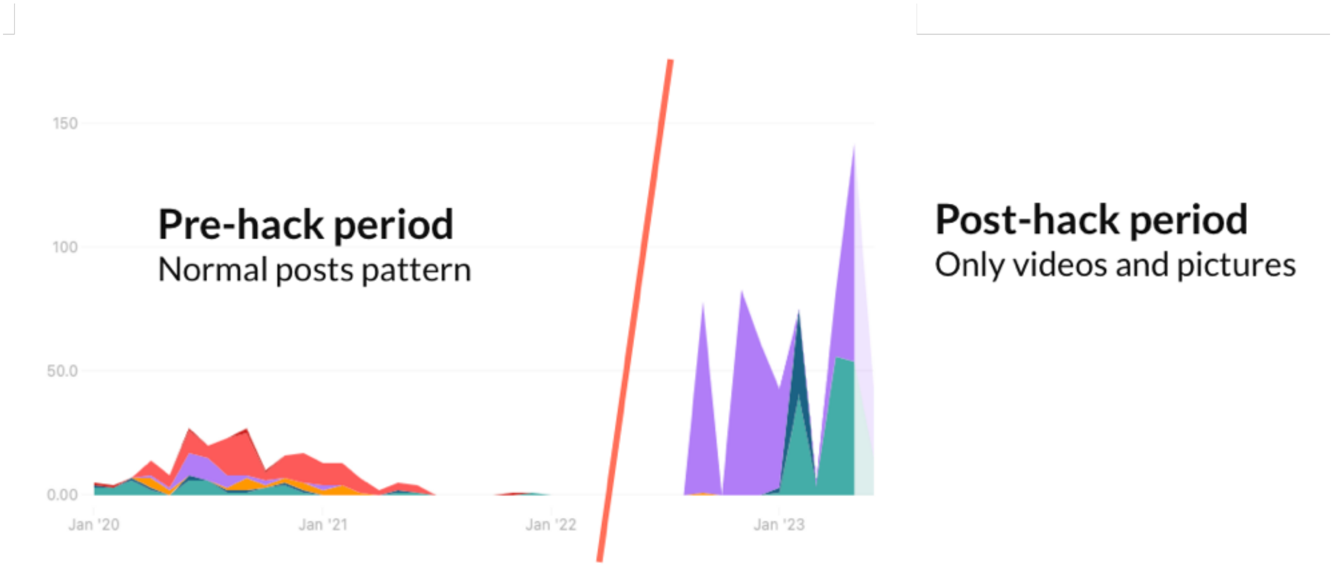


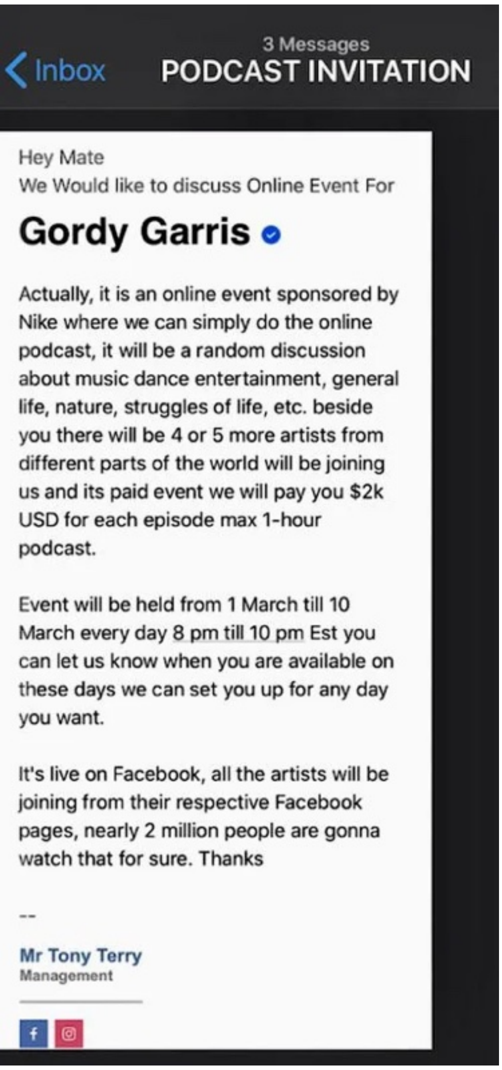
Figure 14: Tony Terry's page publication volume, type and frequence pre and post hack

How is his page used?

The scam involves the misuse of Tony Terry's social media accounts, specifically on Instagram and Facebook. The *modus operandi* of the scam is quite intricate. The scammers, posing as a member of Tony Terry's team, approach artists or creators managing a Facebook page with a proposition with the end goal to take control of their pages.

The collaboration proposals

The collaboration proposal is essentially the scam itself. It is the bait used by the scammers to lure the 1st level victims. Posing as Tony Terry or a member of his team, the scammers propose a collaboration on a podcast to artists and creators managing a Facebook page. Scammers claim that the collaboration is sponsored by Nike and offer to pay 1st level victims a significant amount (usually USD2,000) in exchange for their participation on the podcast. The following figure is a screen capture of one such email sent to a victim we have interviewed for the purpose of this investigation.



Hey Mate
We Would like to discuss Online Event For

Gordy Garris

Actually, it is an online event sponsored by Nike where we can simply do the online podcast, it will be a random discussion about music dance entertainment, general life, nature, struggles of life, etc. beside you there will be 4 or 5 more artists from different parts of the world will be joining us and its paid event we will pay you $2k USD for each episode max 1-hour podcast.

Event will be held from 1 March till 10 March every day 8 pm till 10 pm Est you can let us know when you are available on these days we can set you up for any day you want.

It's live on Facebook, all the artists will be joining from their respective Facebook pages, nearly 2 million people are gonna watch that for sure. Thanks

--

Mr Tony Terry
Management

Figure 15: Screen grab of the email sent by scammers to one of the 1st level victims (Source: Reddit, Gordon Garris)

Social engineering 101: the mechanics of taking control of a Facebook page

During our research, we conducted a series of interviews with 1st level victims. As mentioned above, they share the main characteristic of being artists or creators managing a Facebook page.

These victims would receive an email offering a paid podcast appearance in an event organised by Tony Terry. The email would have been sent from a gmail address bearing "Tony Terry"). A person pretending to work with Tony Terry would sign the email.

"Once I answered the email, I was invited to take part in a Zoom meeting to look over details" said Helen Austin, a singer from Canada who has since lost control of her Facebook page. During the Zoom call, a man described by Helen as "being quite directive" instructed her to modify some settings on her Facebook page to prepare for the podcast recording and asked her to share her screen. In this process, Helen was tricked to add another Facebook user profile "Online Events" as an admin of her own Facebook page, effectively handing control of the page to the scammers.

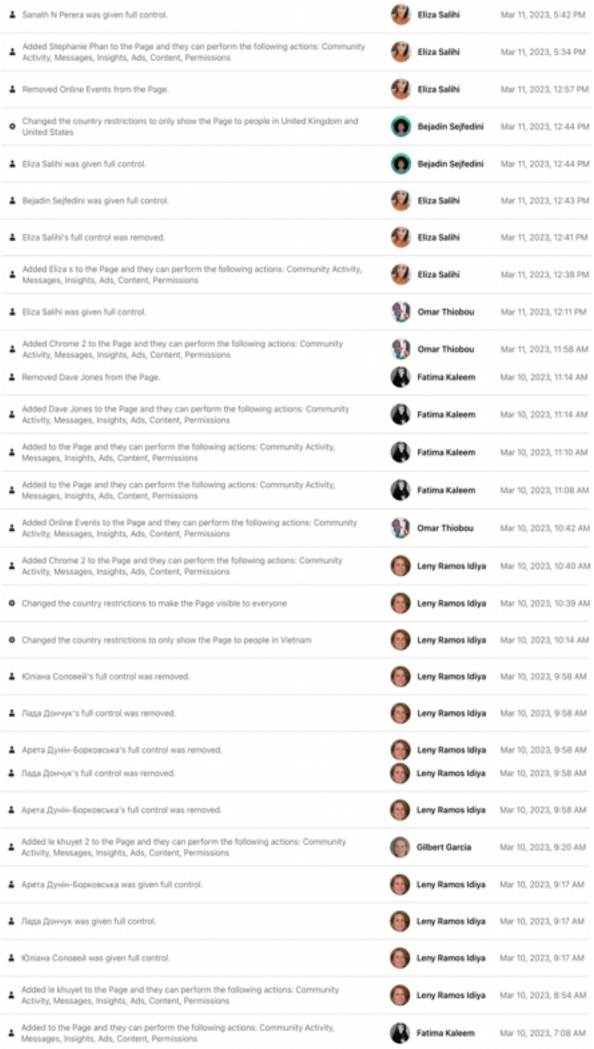
“A couple of hours later, I realised this did not feel right”, said Helen Austin, adding that she “went back to [her] computer and tried to edit the profile and couldn’t do that”. Helen still had some access to the page, but not as an admin and could see that many new administrators were being allowed to control her page. Counterfeit ad inserts were published from Helen Austin’s Facebook page shortly after these events.

A similar technique was described to us by another 1st level victim, Gordon Garris, a musician from the United States. Other accounts of victims were to be found on a Reddit topic[19] created by Meow Misti Dawn, an artist contacted by the fake Tony Terry agent. The topic gathers testimonies, including accounts of social engineering feats as recent as the end of May 2023.

Both Helen and Gordon have contacted Meta to get back control of their pages but could not obtain it at the time of writing.

Brett Raio, another victim we interviewed elaborated on the social engineering technique the scammers were using during the Zoom call. According to him, the fraudsters instruct the victim to send a verification email from Facebook to one email address the victims are not using with Meta platforms. While still seeing the victim's screen through screen sharing, the scammer asks the victim to copy the confirmation link rather than clicking it and paste the url in a browser. "When we did this, the URL wasn’t very long and the entire URL was able to be seen. So this is where they used the same exact URL sent to us via email, to intercept with their own Facebook account and give themselves access as well" explained Brett. Once scammers have the URL, they use it to gain admin access to the victim's Facebook account, subsequently reducing the victim's admin privileges and taking control of the account.

We have found other accounts [20],[21] of artists/creators publicising attempts to take control of their Facebook page through a collaboration proposal with Tony Terry.



Sanath N Perera was given full control.	Eliza Salihi	Mar 11, 2023, 5:42 PM
Added Stephanie Phan to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Eliza Salihi	Mar 11, 2023, 5:34 PM
Removed Online Events from the Page.	Eliza Salihi	Mar 11, 2023, 12:57 PM
Changed the country restrictions to only show the Page to people in United Kingdom and United States	Bejadin Sejfedini	Mar 11, 2023, 12:44 PM
Eliza Salihi was given full control.	Bejadin Sejfedini	Mar 11, 2023, 12:44 PM
Bejadin Sejfedini was given full control.	Eliza Salihi	Mar 11, 2023, 12:43 PM
Eliza Salihi's full control was removed.	Eliza Salihi	Mar 11, 2023, 12:41 PM
Added Eliza s to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Eliza Salihi	Mar 11, 2023, 12:38 PM
Eliza Salihi was given full control.	Omar Thiobou	Mar 11, 2023, 12:11 PM
Added Chrome 2 to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Omar Thiobou	Mar 11, 2023, 11:58 AM
Removed Dave Jones from the Page.	Fatima Kaleem	Mar 10, 2023, 11:14 AM
Added Dave Jones to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Fatima Kaleem	Mar 10, 2023, 11:14 AM
Added to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Fatima Kaleem	Mar 10, 2023, 11:10 AM
Added to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Fatima Kaleem	Mar 10, 2023, 11:08 AM
Added Online Events to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Omar Thiobou	Mar 10, 2023, 10:42 AM
Added Chrome 2 to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Leny Ramos Idiya	Mar 10, 2023, 10:40 AM
Changed the country restrictions to make the Page visible to everyone	Leny Ramos Idiya	Mar 10, 2023, 10:39 AM
Changed the country restrictions to only show the Page to people in Vietnam	Leny Ramos Idiya	Mar 10, 2023, 10:14 AM
Юліана Соловей's full control was removed.	Leny Ramos Idiya	Mar 10, 2023, 9:58 AM
Лада Дончук's full control was removed.	Leny Ramos Idiya	Mar 10, 2023, 9:58 AM
Арета Дунін-Борковська's full control was removed.	Leny Ramos Idiya	Mar 10, 2023, 9:58 AM
Лада Дончук's full control was removed.	Leny Ramos Idiya	Mar 10, 2023, 9:58 AM
Арета Дунін-Борковська's full control was removed.	Leny Ramos Idiya	Mar 10, 2023, 9:58 AM
Added le khuyet 2 to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Gilbert Garcia	Mar 10, 2023, 9:20 AM
Арета Дунін-Борковська was given full control.	Leny Ramos Idiya	Mar 10, 2023, 9:17 AM
Лада Дончук was given full control.	Leny Ramos Idiya	Mar 10, 2023, 9:17 AM
Юліана Соловей was given full control.	Leny Ramos Idiya	Mar 10, 2023, 9:17 AM
Added le khuyet to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Leny Ramos Idiya	Mar 10, 2023, 8:54 AM
Added to the Page and they can perform the following actions: Community Activity, Messages, Insights, Ads, Content, Permissions	Fatima Kaleem	Mar 10, 2023, 7:08 AM

Figure 16: Screenshot of the Facebook notifications of one of the victims, showing the additions of other administrators by the scammers after they had seized control of his page.

[19] https://www.reddit.com/r/facebookdisabledme/comments/11ti7wo/tony_terry_scam/
[20] https://www.tiktok.com/@sabrinabendory/video/7215299194708512046
[21] https://www.tiktok.com/@diaryofafitmommy/video/7230512584321994027

2. A complex infrastructure behind the user-facing assets

In order to attract users to their forged websites and ultimately trick them to make payments, the scammers put together a complex infrastructure involving several tiers of Facebook pages, fake media organisation websites, fake e-commerce sites, companies scattered across the globe and call centres. The following chart explores part of the infrastructure, starting from the Tony Terry case-study and depicting a successful scam operation from the moment fraudsters seize control of a 1st level victim's page to the moment where they collect money from the end victim.

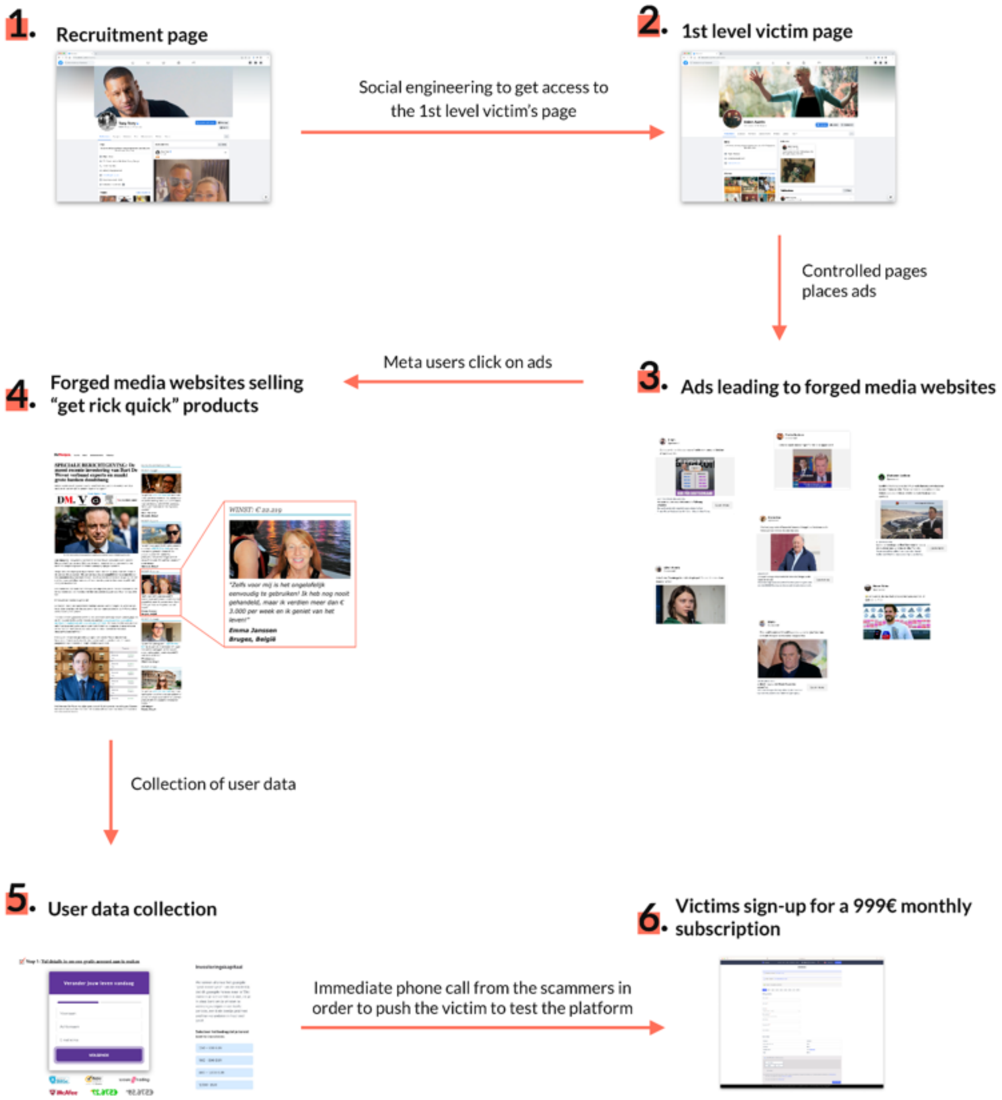

1. Recruitment page
Social engineering to get access to the 1st level victim's page
2. 1st level victim page
Controlled pages places ads
3. Ads leading to forged media websites
Meta users click on ads
4. Forged media websites selling "get rick quick" products
WINST: € 22.219
"Zelfs voor mij is het ongelofelijk eenvoudig te gebruiken! Ik heb nog nooit gehandeld, maar ik verdien meer dan € 3.000 per week en ik geniet van het leven!"
Emma Janssen
Bruges, België
Collection of user data
5. User data collection
Immediate phone call from the scammers in order to push the victim to test the platform
6. Victims sign-up for a 999€ monthly subscription

Figure 17: Chart displaying part of the scam infrastructure and mechanics from a victim's point of view

2.1 A network of three-tier Facebook pages

Let's concentrate on one side of the operation: publishing ads on Facebook. In order to lure end victims into transferring money to them, scammers have implemented an elaborate system to gain access to existing Facebook pages which they aim to take control of. We call the owners of these target pages "1st level victims".

Gaining access to an array of Facebook pages from which ads can be purchased requires the use of deception techniques. Capitalising on the online reputation of the Tony Terry page, and offering to take part in a paid event with him, scammers entice 1st level victims to book a video chat with them. The fraudsters would seize control of their Facebook pages during this conversation.

In parallel, our observations indicate that the scammers are breeding a pool of Facebook pages, i.e. attempting to raise their follower counts by posting viral videos. This breeding system involves a three-tier level of Facebook pages controlled by the scammers, categorised by role.

Tier A: Facebook pages publishing viral content (15 pages identified)

We've identified 15 Facebook pages[22] regularly posting unrelated videos to one another, which only common denominator seems to be their potential to become viral videos. These pieces of content often show spectacular or unusual events and are consistently published on the identified pages, multiple times a day. Examining the profiles of the page owners leads us to the conclusion that these pages are operated by the scammers as the owners don't seem to have a significant or credible other online presence than on Facebook. As an example of this, we noted that the Tony Terry Facebook page re-posted videos from a user called "Itz Alone". Looking up this user in CrowdTangle revealed a network of multiple hundreds of pages reposting Itz Alone's content. The user himself is presented on Facebook as a teenager. His page links to his Youtube channel where we only found unrelated gameplay videos with low view counts, whereas his Facebook videos reach multiple millions of views.

Tier B: Facebook pages re-posting content (440 pages identified)

Acting in parallel with the "tier A" pages exists another set of multiple hundreds of Facebook pages[23]. These pages mimic legitimate entities or people, often impersonating popular music personalities and other public figures to maintain an illusion of authenticity. Scammers natively post content which could have been posted by the original owner, oftentimes pictures of the

[22] https://github.com/CheckFirstHQ/Facebook-Hustles/blob/main/Data%20tables/Facebook%20pages%20Tier%20A.csv

[23] https://github.com/CheckFirstHQ/Facebook-Hustles/blob/main/Data%20tables/Facebook%20pages%20Tier%20B.csv

page owner in many cases with mere emojis as the post body. Alongside this regular native posting, scammers share clickbait videos from the “tier A” pages to bolster their credibility and follower count.

According to data shown in CrowdTangle, these “tier B” pages (approximately 440 in use) are predominantly administered from Bangladesh (96%) and Pakistan (4%). Multiple pages from this pool have posted the same content within the same timeframe.

Tier C: Facebook pages are used to publish ads (90 pages identified)

Ads are run from a set of Facebook pages originally controlled by 1st level victims. Control of these pages was taken through social engineering as described in section 1.2. We identified 90 such pages[24]. A further analysis of the original page owners shows that they mostly belong to regional level artists or creators. Once scammers seize control of the “tier C” pages, multiple dozens of page administrators are added to the Facebook control panel and ad campaigns are created. We’ve listed an array of 1500+ dubious ads being run from “tier C” pages.

A special case: recruitment pages

Looking back at the Tony Terry example, it appears that some of the “tier B” pages are used to perform social engineering deception operations in order to take control of “tier C” pages. It remains unclear if these recruitment pages were also used at some point to publish ads or not. One lead supporting this argument is the example of Bein sports reporter Ibrahim Khadra whose page was simultaneously used by scammers to publish ads and to repost videos from other pages from the scammers network of Facebook pages. One hypothesis is that once ads are blocked by Facebook or otherwise expire, such pages are recycled to repost videos.

These recruitment pages then approach smaller pages (operated by 1st level victims) with a lucrative offer to "collaborate". The page owners are lured into giving admin access to their page, enabling scammers to place ads.

Once the scammers have obtained access, they commence the second phase of their operation: posting scam ads, mainly relating to cryptocurrency or other investments presented as very lucrative. This phase seems to be persisting until the original owner reports the hacking to Facebook or the platform independently identifies and removes the scam ads.

The operation's sophistication lies in its complexity and the scammers' ability to impersonate legitimate entities convincingly. By capitalising on the trust users place in established pages and the current interest in cryptocurrency, they can exploit the platform's features to achieve their malicious goals.

[24] https://github.com/CheckFirstHQ/Facebook-Hustles/blob/main/Data%20tables/Facebook%20pages%20Tier%20C.csv

2.2 A support infrastructure for the scam to operate

Forged media website impersonating big newspapers and media organisations

An infrastructure supporting the operation of the scam consists of forged media websites[25] that impersonate well-known newspapers and media organisations. These deceptive websites are promoted through Facebook ads mimicking well-known media websites.

During our investigation, we discovered over 60 different media outlets from around the world being impersonated, with a total of 162 fake media ads identified. Among impersonated media outlets were *Le Monde*, *BBC*, *Delfi*, *Le Soir*, and others. Since the Facebook account used in this operation was located in Belgium, most of the fraudulent ads we observed were related to Belgian or French media organisations. Nevertheless, we also uncovered instances of media impersonation in various other countries, including South Africa, the United States, Finland, and Croatia using the Facebook Ads Library[26]. In total, we identified ads impersonating media organisations present in 29 countries.

As explained in section 1.1, the ads usually share a common structure. They mimic reputable media outlets by incorporating their logos and designs; however, the associated URLs[27] do not redirect to the intended media sources. These counterfeit media websites serve as landing destinations for the ads displayed on Facebook. When users click on these ads, they are directed to websites that closely resemble the counterfeit media outlets, featuring similar logos, menu bars, and social media icons.

Often, these articles include a section titled "As Seen On" with logos of other reputable media sources, further emphasising the supposed credibility of the article. The articles frequently feature well-known figures exposing how they got rich rapidly. Phrases such as "terrorise banks" and "big banks want him out" are commonly used, often featuring pictures of individuals like Bezos, Musk, or local politicians.

The narratives of these articles are relatively consistent. A journalist is depicted as being incredulous, not believing their eyes or even wanting to censor the interviewee, a famous person. The interviewee then reveals a technique for easy wealth generation by promoting a new cryptocurrency program. The promise is to invest a small amount and earn substantial returns rapidly. The article explains the functioning of the platform and how it supposedly operates. Additional testimonies are included in the sidebar, such as stories of families in debt

[25] https://github.com/CheckFirstHQ/Facebook-Hustles/tree/main/Screenshots/Fake%20Media%20Organisation%20websites

[26] https://github.com/CheckFirstHQ/Facebook-Hustles/tree/main/Screenshots/Ads%20Examples%20from%20Ads%20Library

[27] https://github.com/CheckFirstHQ/Facebook-Hustles/blob/main/Data%20tables/Scam%20URLs.csv

or heartwarming anecdotes like a sibling gifting a car to their younger sister. The body of the article is often accompanied by stock or manipulated photos.

The fake media websites also contain additional ads, often presented as testimonies, featuring people claiming that the scam worked for them and encouraging others to invest.

Forged e-commerce sites

In addition to their other assets, scammers put together an array of fake e-commerce sites. We believe these sites exist to help bypass Facebook verification policies as scammers try to purchase ads. Having an existing, proper looking e-commerce website might help scammers purchase ads and seem to Facebook as legitimate businesses.

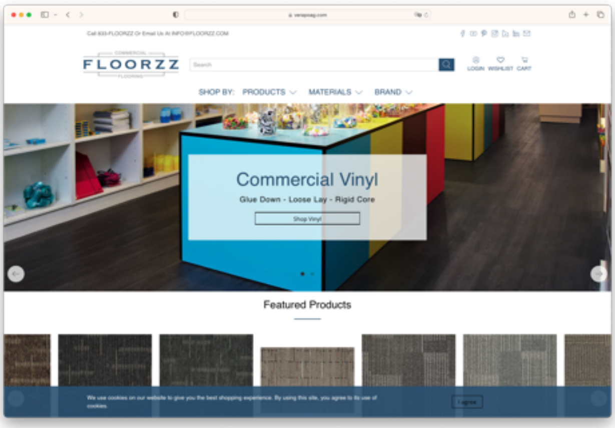


Figure 18: Screen capture of a forged e-commerce site

All false e-commerce websites we have identified mimic an existing e-commerce site, but are not entirely functional. Scammers seem to have copied the original html code of a legitimate site and re-hosted on a server they control. However, these false websites are not functional whenever a database query is necessary. For example product searches or putting a product in the cart does not work. No purchase is possible from these sites.

As regards the used domain names, their analysis shows that scammers use them to point to both forged media websites and fake e-commerce product pages. We identified the registrars linked to the domains. Our analysis shows that an array of registrars is used. However, some registrars are more used than others: 45% of the sites are using domains provided by NameSilo, followed by PDR Ltd. (29%). The following figure shows the distribution of registrars linked to 162 identified domains[28].

[28] https://github.com/CheckFirstHQ/Facebook-Hustles/blob/main/Data%20tables/Scam%20Domains.csv

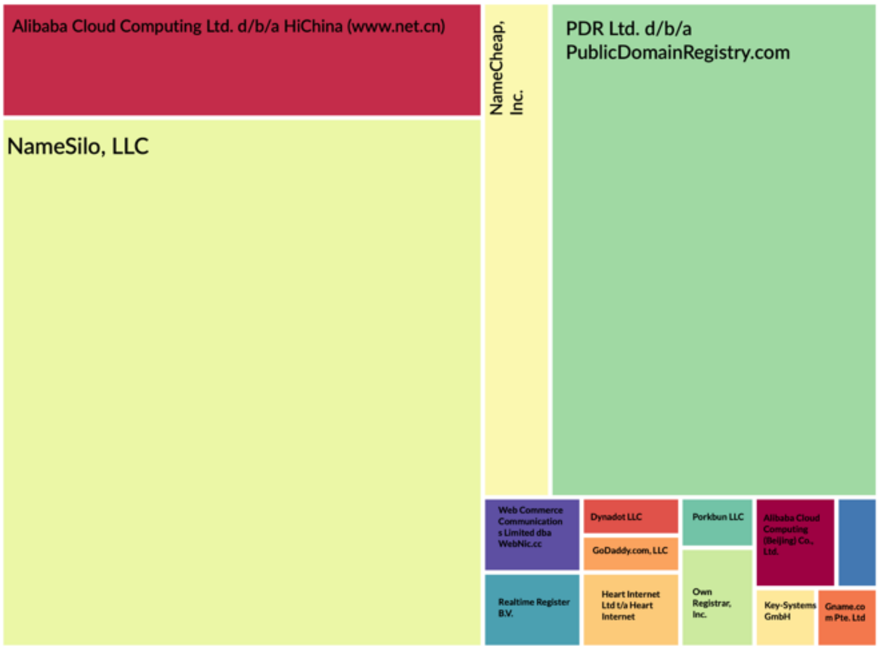


Figure 19: Distribution of registrars linked to 162 identified domains

2.3 Economics of the scam operation

Prejudice of end victims is unknown

We’ve established through the usage of a sock puppet acting as a potential victim that scammers tried to convince our fictional user to subscribe to a monthly credit card payment to a video course on investment practices described by the scammers as a first payment to test the investment platform. However, this is merely a sole example out of a probable array of payment collection methods used by the bad actors. Neither the number of victims nor the amount of money lost to scammers could be established during our investigation.

This *modus operandi* does not seem to be new, as the following testimony suggests.

“Révélations sur une gigantesque escroquerie aux cryptomonnaies” by *Le Monde*

In November 2020, the French newspaper *Le Monde* investigated a similar topic: "Révélations sur une gigantesque escroquerie aux cryptomonnaies" (*Revelations on a gigantic cryptocurrency scam*). The article features an interview of Clas Backman, a Swedish man who was a victim of a scam operation in 2019 operated by a call centre. "He invested around 20,000 euros, and ‘almost lost everything’. His complaint is still under investigation, but he has few illusions: he'll never see that money again", reports the author of the paper.

Similarly to what our findings have shown, M. Backman was firstly framed by an online ad. *Le Monde* reports that "in September 2019, he clicked on an ad for Bitcoin Trader, which advertises itself as revolutionary cryptocurrency trading software. After entering his details on the site, he is immediately called back by an 'advisor', who convinces him to invest $250 (210 euros)."

The same thing happened when we played the role of a potential victim and had a phone conversation with the scammers (see 1.1 - What happens to the end victims of the scam?).

The operation bears costs

As we have demonstrated, scammers have put in place a sizable organisation, using many domain names, hosting server space and human resources. This raises the question of the costs of this infrastructure.

As a disclaimer, we have no way of establishing how the scammers managed to pay for these services, nor if they actually paid themselves with funds they control, if these funds were stolen or if payments were fraudulent. It is for example theoretically possible, although unlikely, that scammers would seize control of other parties' accounts at registrars. As exact cost cannot be calculated (as for example hosting services which can be purchased at a wide array of prices), we merely wanted to point out some aspects of the cost structure of the scam operation.

Cost of Facebook ads

Estimating the cost spent by scammers to purchase ads is a very uncertain endeavour. The nature of Facebook campaigns, allowing advertisers to specify many audience targeting parameters, campaign objectives or campaign types does not allow to calculate a trustworthy estimation of the scammers' spending. Another factor is the lack of information available from Meta's ad library on the cost of campaigns we've uncovered. However, some information was available in the Meta Ad library about campaigns categorised as "about social issues, elections or politics". Information found about these campaigns show that scammers spent "< USD100" for all campaigns we've uncovered and found information about in the Ad Library.

Assuming that this estimated amount is true for all campaigns, which is a broad assumption, scammers would have spent up to USD150,000 in less than 15 days for the ads we've uncovered during the investigation.

Labour costs

Maintaining a network of counterfeit media websites, false e-commerce sites and multiple hundreds of Facebook pages requires some level of human labour. More interestingly, the scammers employ social engineering tactics to manipulate individuals into willingly surrendering control of their Facebook pages, which necessitates skilled individuals adept at deception and manipulation. Moreover, placing persuasive phone calls to victims also demands a team of operators. Thus, the costs incurred by scammers extend beyond financial investments, involving the allocation of human resources and specialised expertise in order to sustain their fraudulent operations, although part of these tasks may be automated.

3. Limits of platform's safeguards and enforcement of laws

3.1 The ads should not pass Facebook's scrutiny protocols

Despite Facebook's extensive advertising policies and review mechanisms[29], it is clear that certain fraudulent advertisements have managed to bypass these safeguards. This is a matter of concern as it not only undermines the trust users place in the platform but also exposes them to potential scams.

The presence of advertisements leading to counterfeit media websites promoting cryptocurrency scams on Facebook indicates a lapse in their enforcement mechanisms. It brings into question the efficacy of the automated tools employed in the ad review process. Are these tools sophisticated enough to detect such intricate scams?

Furthermore, it suggests potential inadequacies in the process described by Meta as “manual review”. Given the scope of the scam operation we’ve uncovered, a legitimate question would be to ask if Meta’s systems are fit ahead of the implementation of the DSA in the European Union.

The policies against deceptive content and unacceptable business practices should have acted as a barrier against the approval of these ads. The fact that they did not point towards a lapse in policy enforcement. This is a serious issue that warrants immediate attention.

In summary, while Facebook's advertising policies and review processes are designed to prevent fraudulent activities, the presence of these cryptocurrency scam ads indicates significant lapses in these systems. It is imperative that Facebook addresses these issues to maintain user trust and the integrity of its platform.

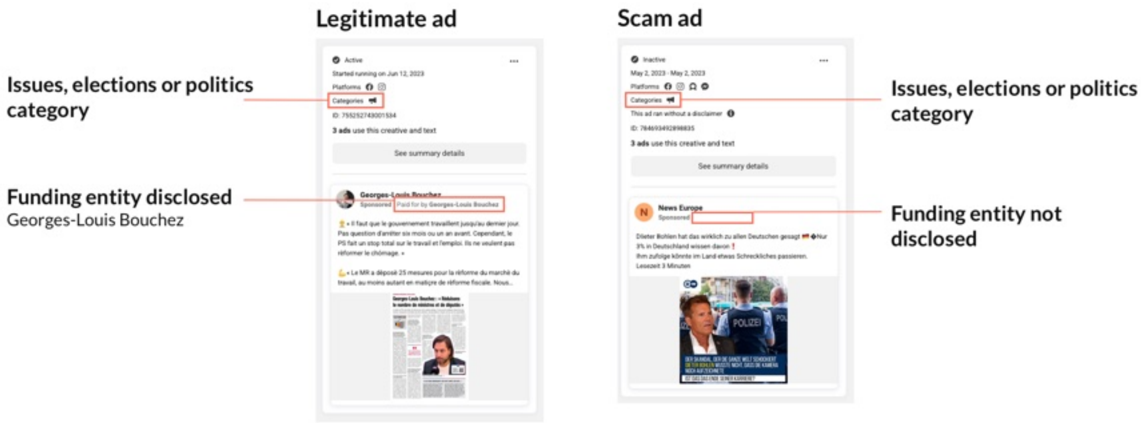
3.2 Incompleteness of the Meta Ad Library

All ads found on Facebook were not mirrored on the Ad Library. On multiple occasions, we could not find matching content in the Ad Library for an ad we had found on Facebook. Searching for the name of the page running such ads did not return any results. Furthermore, some ads were marked with the label “This ad does not respect the community standards” in the Ad Library. No further information was available on the Ad Library for these “creatives” as they were greyed out in the interface, nor did they appear on Facebook.

Additionally, when ads *were* present in the Meta Ad Library, all expected information was not present. Crucially in the case of ads labelled as “Ads about social issues, elections or politics”,

[29] https://www.facebook.com/business/help/204798856225114?id=649869995454285)

funding entities were not reported for the ads we have found. The following example shows on the left an ad categorised as such and for which the funding entity is disclosed. However, one of the ads uncovered as being part of the scam operation, while being present in the Meta Ad Library, does not show any information about the funding entity, as seen on the right. This information should be disclosed by Meta, as indicated in the Strengthened Code of Practice[30] in its Measure 6.2; a document of which Meta is signatory[31].


Legitimate ad
Scam ad
Issues, elections or politics category
Funding entity disclosed
Georges-Louis Bouchez
Issues, elections or politics category
Funding entity not disclosed

Active

Started running on Jun 12, 2023

Platforms

Categories

ID: 755252743001534

3 ads use this creative and text

See summary details

Georges-Louis Bouchez

Sponsored · Paid for by Georges-Louis Bouchez

« Il faut que le gouvernement travaillent jusqu'au dernier jour. Pas question d'arrêter six mois ou un an avant. Cependant, le PS fait un stop total sur le travail et l'emploi. Ils ne veulent pas réformer le chômage. »

« Le MR a déposé 25 mesures pour la réforme du marché du travail, au moins autant en matière de réforme fiscale. Nous...

Inactive

May 2, 2023 - May 2, 2023

Platforms

Categories

This ad ran without a disclaimer

ID: 784693492898835

3 ads use this creative and text

See summary details

News Europe

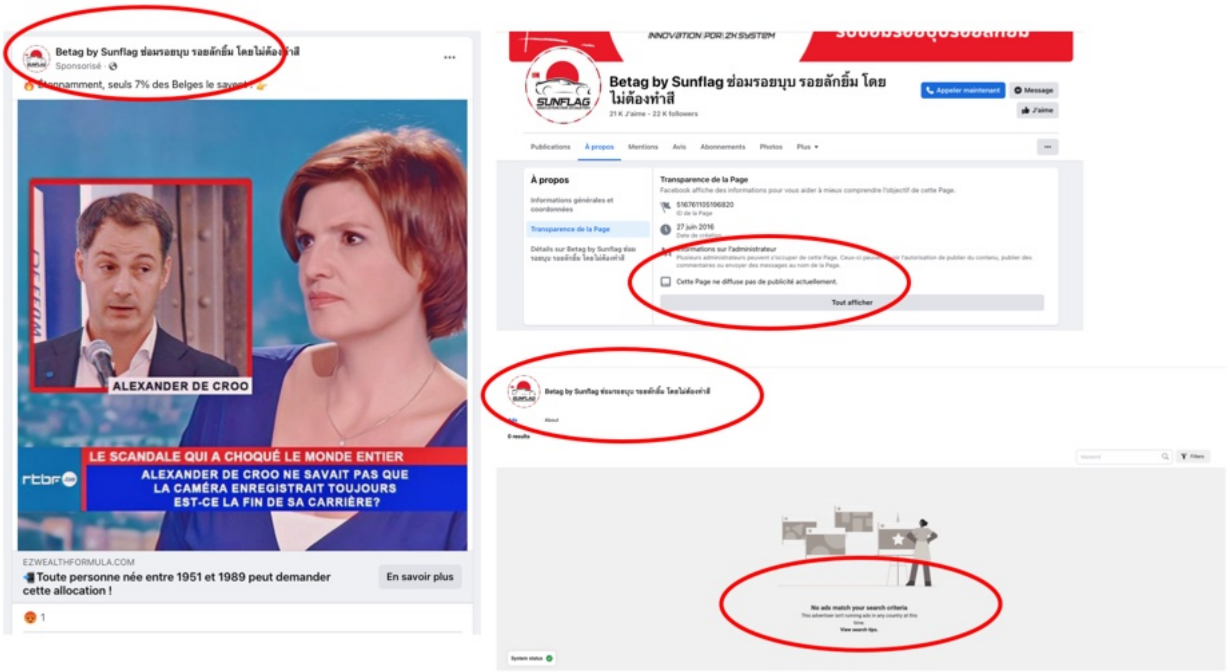
Sponsored

Dieter Bohlen hat das wirklich zu allen Deutschen gesagt 🇩🇪 Nur 3% in Deutschland wissen davon ❗
Ihm zufolge könnte im Land etwas Schreckliches passieren.
Lesezeit 3 Minuten

Figure 20: Screen captures comparing a full data disclosure on the Meta Ad Library (left) to an incomplete one (right) where the funding entity is not disclose

In the following example, in the Transparency settings of the page, we can see that the page "is currently not running any ads". If one searches for the page in Facebook Ads Library, no ads match the page. However, on the same day, we can see the ad in the Facebook feed.

[30] https://ec.europa.eu/newsroom/dae/redirection/document/87585
[31] https://ec.europa.eu/newsroom/dae/redirection/document/87559



Betag by Sunflag ซ่อมรอยบุบ รอยลักยิ้ม โดยไม่ต้องทำสี
Sponsorisé

Étonnamment, seuls 7% des Belges le savent !

ALEXANDER DE CROO

LE SCANDALE QUI A CHOQUÉ LE MONDE ENTIER

ALEXANDER DE CROO NE SAVAIT PAS QUE LA CAMÉRA ENREGISTRAIT TOUJOURS EST-CE LA FIN DE SA CARRIÈRE?

EZWEALTHFORMULA.COM

Toute personne née entre 1951 et 1989 peut demander cette allocation !

Betag by Sunflag ซ่อมรอยบุบ รอยลักยิ้ม โดยไม่ต้องทำสี
21 K J'aime · 22 K followers

Transparence de la Page

Facebook affiche des informations pour vous aider à mieux comprendre l'objectif de cette Page.

516761105196820
ID de la Page

27 juin 2016
Date de création

Informations sur l'administrateur

Plusieurs administrateurs peuvent s'occuper de cette Page. Ceux-ci peuvent avoir l'autorisation de publier du contenu, publier des commentaires ou envoyer des messages au nom de la Page.

Cette Page ne diffuse pas de publicité actuellement.

Betag by Sunflag ซ่อมรอยบุบ รอยลักยิ้ม โดยไม่ต้องทำสี

0 results

No ads match your search criteria

This advertiser isn't running ads in any country at this time.

View search tips.

Figure 21: Screen captures from a fraudulent ad (left), publishing facebook page about section (top right) and screen capture of the results page on the Meta Ad Library after a search for identified Facebook page where running ads were not found (bottom right)

3.3 Legal implications - Terms of Service

Meta's terms of service

According to Meta's policy[32] those ads should not be available on the platform as they are breaking several of their measures:

"**Unacceptable Business Practices**: Advertisers must not promote products, services, schemes, or offers using deceptive or misleading practices, including those intended to scam people out of money or personal information. This would include running a campaign using a hacked page, as it involves deceptive practices and potentially infringes on personal information.

Misleading Claims: Ads must not contain claims that are debunked by third-party fact checkers or, in certain circumstances, claims that are misleading or false. This would apply to any claims made on a hacked page that are not true or are misleading.

Community Standards: Ads must not violate Facebook's Community Standards. Unauthorised access to a user's account (hacking) is a violation of these standards.

[32] https://www.facebook.com/business/help/488043719226449?id=434838534925385

Circumventing Systems: Ads must not use tactics that are intended to circumvent Facebook's ad review process or other enforcement systems. This includes techniques that attempt to disguise the ad's content or destination page.

Policy Enforcement: Facebook uses a combination of automated and manual review to ensure policy compliance. In addition to reviewing individual ads, they monitor and investigate advertiser behaviour and apply restrictions to advertiser accounts that violate their Advertising Policies, Community Standards, or other Facebook policies and terms."

In summary, running those campaigns should not be allowed because it involves deceptive practices, potentially infringes on personal information, violates community standards, and attempts to circumvent Facebook's ad review process.

Registrars' terms of service

We compiled a list of all associated domains. Pertinent details such as the registrar of the domain, the date of purchase, and the associated name servers were gleaned from WHOIS data. 45% of the identified domains were obtained from the registrar NameSilo LLC, while of said domains were registered with 29% PDR Ltd.

According to NameSilo's Terms of Service[33], any form of impersonation of a recognized media outlet with the intent to deceive users is explicitly forbidden. Section 5(a)(vi) and (vii) state that users bear the sole responsibility for their content and must ensure it doesn't infringe upon any third party rights, including copyrights, trademarks, patents, trade secrets, moral rights, privacy rights, rights of publicity, or any other intellectual property or proprietary right. Consequently, creating a mimic website, which likely involves copyright infringement, is clearly prohibited.

Furthermore, section 4(b)(I) stipulates that the user's content must not infringe, violate, or misappropriate any third-party rights. This provision also dictates that user content must not implicate NameSilo in violating any laws, regulations, rules, or rights of third parties. Thus, creating a mimic website, particularly with the intent to deceive users, would likely contravene these stipulations.

Lastly, section 4(c)(V) explicitly prohibits the use of their services for any illegal activities, which would include the creation of a website with the intent to deceive and scam users. This would be a clear violation of their terms and could lead to the suspension or termination of the services.

[33] https://www.namesilo.com/support/v2/articles/general-terms/terms-and-conditions

Hosting providers terms of service

The name servers of the domains provide valuable insights into where the domain is managed. It was noted that the majority of these domains are managed via CloudFlare, which unfortunately, does not provide much information due to its inherent anonymity.

However, some domains, like “dumplita.com”, deviate from this trend and are managed by Digital Ocean instead of CloudFlare. Notably, the content on these websites remains consistent with the others, thereby suggesting that some of the counterfeit websites could be hosted on DigitalOcean's servers. This revelation is significant as it opens a potential avenue for action against these websites based on violations of Digital Ocean's Terms of Service.

According to Digital Ocean's Terms of Service[34], any form of impersonation of an established media outlet with the intent to deceive users is explicitly prohibited. Section 3.4[35] of their terms states that users bear the sole responsibility for their content and must ensure it doesn't infringe upon any third party rights, including copyrights, trademarks, patents, trade secrets, moral rights, privacy rights, rights of publicity, or any other intellectual property or proprietary right. Consequently, replicating a website, which likely involves copyright infringement, is clearly disallowed.

Furthermore, section 4.5[36] of their terms stipulates that the user's Services Content must not infringe, violate, or misappropriate any third-party rights. This provision also dictates that user content must not implicate Digital Ocean in violating any laws, regulations, rules, or rights of third parties. Thus, replicating a website, particularly with the intent to deceive users, would likely contravene these stipulations.

4. Possible actions

4.1 First level victims

The affected user can visit the official Meta Support Center or Help Center website in order to consult the section related to hacked or compromised accounts/pages and follow the instructions provided.

Another option is to submit a report through the Facebook Help Center's reporting feature, specifically flagging the issue as a "Hacked or Fake Account" or "Impersonation" to bring attention to the page takeover. This report is supposed to alert Meta's support team to investigate the matter and take appropriate action.

It's advisable for the affected user to provide as much relevant information and evidence as possible, including details about the page, any suspicious activities or changes observed, and

[34] https://www.digitalocean.com/legal/terms-of-service-agreement
[35] https://www.digitalocean.com/legal/terms-of-service-agreement#3-do-community-user-content
[36] https://www.digitalocean.com/legal/terms-of-service-agreement#4-services-content

any communication received from the scammers. This will assist Meta in comprehensively understanding the situation and taking appropriate measures to regain control of the page.

While contacting Meta directly does not guarantee an immediate resolution, it is an essential step to alert them about the issue, raising Meta's awareness on current scam operations while avoiding further utilisation of the victim's brand assets as well as reputation.

4.2 Impersonated media

In the aftermath of scammers counterfeiting websites by utilising the brand assets of impersonated media brands, the affected entities can undertake certain actions to address this infringement. One recommended course of action is to file copyright claims with the hosting companies involved. It is worth noting that the terms of service employed by the majority of hosting companies explicitly prohibit impersonation.

By submitting copyright claims, the impersonated media brands can assert their intellectual property rights and request the removal or suspension of the fraudulent websites. This proactive measure serves as a legal recourse for the affected brands to protect their brand identity and combat the unauthorised use of their assets. By leveraging the provisions outlined in the hosting companies' terms of service, the impersonated media brands can effectively affect a key part of the scammers' infrastructure.

4.3 Impersonated personalities

Public figures of which the image and reputation was used in the ads can consider legal actions. We've listed at least one case of this dating back in 2018 when the British journalist Martin Lewis took Facebook inc. to court[37] after he noticed his image was used in scam ads. Lewis eventually dropped the charges after Facebook agreed to cover his legal costs, make a GBP 3 million donation to a charity to work on a anti-scam programme and implement an UK-specific one-click reporting tool for scam ads.

[37] https://fullfact.org/online/martin-lewis-crypto-fake/

5. Disclosure Timeline

25 May 2023
Contacted 1st level victims to inform them about the misuse of their pages and collect testimonies, Conducted 1st level victims interview.

05 June 2023
All media organisations for which we’ve found a forged website were contacted.

06 June 2023
Contacted Meta.

06-07 June 2023
Conducted additional 1st level victims interviews.

08 June 2023
Shared findings with Meta and provided them with datasets collected during the investigation. The company representatives required that our conversation remained “off the record”.

14 June 2023
Contacted Meta, Cloudflare, NameSilo and PDR Ltd team with our findings and the data related to their respective services asking for comments.

Conclusion

Before concluding, the authors would like to remind that this investigation was led over the course of a month and data were collected in 10 days. Still, in this short amount of time, we uncovered a significant amount of forged websites, 1500+ dubious ads on Facebook, an array of over 500 Facebook pages controlled by scammers and came to uncover parts of the mechanics of the operation. However impressive, these numbers are probably just the tip of a massive iceberg. The more leads we followed, the more of the operation we could see. We decided to contain our efforts within a short period as our findings and understanding seem appealing enough to call out a number of actors and show some extent of their malfunctioning policies, safeguards and procedures.

This case is particularly interesting to us as it aggregates many deception techniques and psychological triggers commonly found in disinformation campaigns. It is particularly notable that scammers felt the need to mimic reputable media organisations and use their visual identity and logo to produce false content, luring citizens into sharing their personal information and ultimately attempting to steal from them.

The fact that the scammers' infrastructure can run at all, recurring to an array of products and services obtained from major companies is a serious concern (non withstanding the fact that these providers collect money in the process through sales). Namely, the enforcement of the terms of service of Meta and multiple registrars and hosting companies is clearly problematic. No part of this scam operation could exist if existing terms were observed. The mere fact that we found traces of similar operations dating back in 2019 is even more concerning.

Looking at this through the lens of the soon to be implemented Digital Services Act across the European Union leaves the authors sceptical about the ability of mentioned companies to comply with the new regulations. We are however hopeful that disclosures like this investigation will help to trigger conversations among responsible stakeholders and take the issue event more seriously.

The fitness of the legal arsenal also deserves scrutiny. We've established through our contacts with media organisations that some of them had started legal actions in their respective countries several years ago, with no results to date and a sense of helplessness on their part to prevent further impersonation of their brand assets.

Online crime and fraud have been serious concerns for decades. This investigation shows, once again, that scammers are ready to create intricate operations spanning all over the planet, taking advantage of the decentralised nature of the internet. Targeting European victims through a network of Facebook pages seemingly owned by Americans while being managed from Bangladesh to collect money in the Baltics is a perfect illustration of an organisation betting on the inability of law enforcement services to cooperate across borders.

Methodology

Comprehensive Analysis of Advertisements

Our research methodology began with a non-conventional and practical approach, which involved the use of a dormant Facebook account registered as a Belgian user. This user has demonstrated a sporadic pattern of Facebook activity over the years, mainly due to not using the Facebook or Instagram applications on their mobile devices. Additionally, their interaction with content has been minimal in recent years, indicating a subdued presence on the platform.

While studying the account's scrolling behaviour, we were particularly interested in the array of advertisements that spotlighted well-known Belgian public figures. These ads, which immediately caught our attention, prompted us to dig deeper. To facilitate a comprehensive examination of these ads, we implemented the following steps:

- Our first action was to meticulously catalogue all pages that were disseminating ads. Our focus was specifically on ads that were linked to a seemingly counterfeit news organisation website and were being displayed to our test user.
- Next, we turned our attention to the textual content of these ads. Using the Facebook Ads Library we were able to uncover new pages and ads.

These carefully structured measures bore fruitful results, enabling us to enumerate more than 1,500 advertisements and identify over 90 unique pages during the relatively short period between May 15 and May 26.

In-Depth Analysis of Pages

An interesting observation that surfaced during this inspection was that certain pages were reposting content that seemed unrelated to their usual postings. This prompted us to further investigate these pages, especially in terms of their activities and motivations behind such reposting.

To efficiently analyse these page activities, we employed Crowdtangle[38]. We examined the activities of pages that were reposted by the misappropriated pages, aiming to draw patterns and insights.

Next, we compiled a list of pages that were sharing content similar to those reposted by the hijacked pages. We then processed this list to remove any redundancies, deduplicating the page names and identifiers to ensure that each page on our list was unique and that we had a comprehensive overview of all relevant pages.

This process of analysis and cross-verification led us to an exhaustive list of more than 440 distinct pages.

[38] https://apps.crowdtangle.com/

Investigation of the Counterfeit News Organisation Website

To comprehend the objectives of these advertisements and the counterfeit news organisation website, we initiated a thorough investigation into the site's source code in an attempt to understand both the structure of the website and their authors' intent.

Upon detailed inspection of the code, we found significant commonalities that indicated a coordinated operation. Firstly, the structural similarities across the ads suggested they were all part of the same campaign. Secondly, we noticed a recurrent pattern with data loaded from external sources, which consistently originated from the same set of domains. This recurring theme in the structure and data sourcing was indicative of a singular operation.

Moreover, we observed that the content forms present on these pages were also configured to be submitted to this same collection of domains. This consistency of form submissions further supported our inference of a unified operation.

These findings, derived from examination of the website's source code, offered substantial evidence to conclude that the ads and the fake news organisation website were part of an overarching, coordinated operation. This understanding significantly enhances our comprehension of the nature and potential goals of these entities, and forms a crucial aspect of our investigation.

Unravelling the Scam

To grasp the implications of this operation, we decided to engage directly with the perpetrators. We created a 'sock puppet', to communicate with the scammers under the guise of a potential victim. This involved using a SIM card which could not be traced to the investigators, placing it in a fully reset and new android device. The phone was then used to create a Google account with fictitious personal information, including fake names, address and profile pictures, providing us with an email address to communicate to the scammers. Similarly, we used the phone number attached to the SIM card to create a WhatsApp account, anticipating that scammers would want to contact the sock puppet through this platform.

Review process

This document has been reviewed following Check First's process[39] including the review of the final document by two internal employees and two external reviewers qualified in the field of the research. The process assessment grid used by the reviewers is available here[40].

The external reviewers for this document are :

- Researcher in disinformation in an NGO
- Senior Researcher & OSINT expert

This document has scored 94 out of 100 after review.

Archiving

All the investigation data captured by CheckFirst between May 15 and May 26 are available on Github.

The choice of screenshots as an archiving system was made because fraudulent websites and Facebook pages could be archived on archive.today or web.archive.org.

[39] https://checkfirst.network/about-us/our-review-process-for-osint-operations/

[40] https://docs.google.com/spreadsheets/d/1ka2rcMAmiUgDKIiTxXNS5cB0poax8C-GCC2Gl1_sRmY/edit?usp=sharing

Annexes

All research documentation is available in a public GitHub repository.

Spoiled media list

Country	Media organisation
Belgium	7sur7
	De Standaard
	DeMorgen
	HLN
	La Libre
	Le Soir
Brazil	Forum
	UOL
Bulgaria	BTV
	Hobnhnte
Canada	Toronto Star
Croatia	Dnevnik
	N1
Denmark	Ekstra Bladet
	Fyens
	Information
Finland	Ämppärit
	iltalehti
	YLE
France	France 24
	L'internaute
	Le Figaro
	Le Monde
Germany	Der Spiegel
	Nord Bayern
	Online Focus
	Suddeutsche Zeitung
Hungary	HVG.hu
Iceland	VF
Italy	Corriere della sera

	Il Gazzettino
	NewsIT
Lithuania	Delfi
	Skrastas
Morocco	Hir.ma
New Zealand	NZ Herald
Norway	A-Magasinet
	Dagsavisen
Poland	Gazeta
Portugal	Correio
	Noticias ao minuto
	Observador
Romania	Stirile pro tv
Singapore	CNA Singapore
Slovakia	Novi Cas
Slovenia	Primorske Novice
South Africa	News 24
Spain	El Mundo
	El Pais
	La Vanguardia
Sweden	Aftonbladet
Switzerland	Le Matin
The Netherlands	AD
	Nu
United Kingdom	BBC
	The Sun
United States	CNN Tech
	Forbes

Identified pages

Pages advertising for fake news media websites (Tier C)

Page name
Fred e Gustavo
Nicole Laurel Asensio
Ibrahim Khadra
Zona Gallos
Tom "Conman" Connors
Rob Woodcox Photography
Selección Nacional de Guatemala
Young Paris
Naomi Raine
Morgan Maassen
Naledzi
Mattias Adolfsson
Alfonso Portillo
Clear Soul Forces
Marc Vedo
The Brand New Heavies
Alycia Dias
Mudassar Jackson
Andrew Myers Art
Fame on Fire
GT
Pham Công Lâm
Linda Purl
Betag by Sunflag ซ่อมรอยบุบ รอยลักยิ้ม โดยไม่ต้องทำสี
Anshuman Jha
Dre Baldwin
Rasd Maroc
Sarıçam Belediyesi
Bilal Afridi
HD Lighting
Kristine W
Smile12i
Edwin Rivera
Gil Joe

So Nyeo Shi Dae S9 VNFanpage
Akarid Trade
PT. LIGA INDONESIA
Anshuman Jha
The Akarin Protection Agency
Bruno
BiancaColour
El Suri cato
Bob Peters
Instituto de Ciencias Administrativas, Económicas y Contables
DEATH CLIPS
Radio Bicester
SBA Imagen y Estilo
Loma Verde Camping
Piscovende
Loma Verde Camping
Boutique MoGa
Associazione Culturale Extramoenia
Mangalore Africa Mission
Natación Coto Brus
I wanna stay up all night-one direction
Xioczana Canales
Faig Store
Union-Vecinal Mar del Plata
Núcleo de Choro y Samba BA
Adrian Gostick
Muhammad Saadat khan usafzai
SM Informática
Universal Group
Stefannewspodcast
News Europe
Valyushka
Smart Shop
Mabel Nash
Sparkler
Dreaming a new life
Snoopydawg
Future is now
Bisayang tisoy
Jasperdizon

Halvord
Großer Skandal
The finance
A path to dream
Don Pablo Rp
BeWanted Colombia
Idagussurya
Ym_zerotea
Фудбалска Репрезентација на Македонија
I Wish : Faites Un Vœu
Mahdi Baccouch
Michael McCrudden
Meep Sincero
Materiales Educativos
Shulls 2.0

Growth hacking pages (Tier A)

Page name
Viral videos
Itz alone
Videos story
وصفات سحرية مايا 2
Refrigeración DYE
Colglobal News
Gubuk'sloter
Titip Untuk Mereka
Beauty & Wellness by Marynette Gamboa
DJ Mario Valentino
Shatrudhan
เสน สุรินทร์ร็อค surin rock man
Conviviendo Con Thomas
Raffaele Castiglione
Zai
EyesfromHeavencandles Llc

Domains hosting fake media website

Domain	Registrar
29510622.xyz	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
aboutinvestmentbanker.com	NameSilo, LLC
accuseswitchrampbarely.online	Namecheap
adtostore.xyz	NameSilo, LLC
aglenetion.com	NameCheap, Inc.
ahdjsy.com	NameSilo, LLC
aiaigame.top	NameSilo,LLC
angelcomm30.shop	Alibaba Cloud Computing Ltd.
aseantogel.club	NameSilo, LLC
asetqq.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
avlxrnd.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
balu8754.shop	Alibaba Cloud Computing Ltd.
beginstyle.top	NameSilo,LLC
bespread.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
birtutambilim.top	NameSilo,LLC
bitpromo.club	NameSilo, LLC
blowascope.com	Web Commerce Communications Limited dba WebNic.cc
bluesatoshi.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
bowlcome.top	NameSilo,LLC
bussound.top	NameSilo,LLC
camwomen.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
carcloud.top	NameSilo,LLC
censuscd.top	NameSilo,LLC
chattalk.top	NameSilo,LLC
chulaalumni.com	Realtime Register B.V.
corteecostura.top	NameSilo,LLC
coshame.club	NameSilo,LLC
cryptomax.live	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
customfind.top	NameSilo,LLC
dakepigomu.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
devcommit.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
dnewz.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
donnorth.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
drugbush.top	NameSilo,LLC
dumplitua.com	NameCheap, Inc.

dwaqws.top	PDR Ltd
elccloud.com	NameSilo, LLC
eugenesutherlin.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
ezinenakliyat.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
ezwealthformula.com	NameSilo, LLC
faultdutchcinnamonpalace.online	Namecheap
fedromate.com	NameCheap, Inc.
fiatlove.com	NameSilo, LLC
fivebook.top	PDR Ltd
foreclosureavoidancepro.com	NameSilo, LLC
fricky.xyz	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
friv2019.live	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
funnybacara.shop	Alibaba Cloud Computing Ltd.
goldpornmovies.top	NameSilo,LLC
goodguygetit.com	NameSilo,LLC
guhdsg.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
imaloce.com	NameCheap, Inc.
imtruman.top	PDR Ltd
investmenttodepositratio.com	NameSilo, LLC
investmentwithchase.com	NameSilo, LLC
itacow.top	PDR Ltd
jbqfgx.xyz	Dynadot LLC
joslynbarket.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
joslynbarket.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
kabizlik.life	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
khfash.top	PDR Ltd
kjhtech.com	NameSilo, LLC
kunhaimaoyi.com	GoDaddy.com, LLC
legitsol.club	NameSilo, LLC
londonescorts.top	NameSilo,LLC
lowpricepandora.top	NameSilo, LLC
mafed.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
mail-ikubinfo.com	NameSilo, LLC
margaritabrand.com/	NameSilo, LLC
marketingware.co.uk	Heart Internet Ltd t/a Heart Internet
matt-lambert.co.uk	Heart Internet Ltd t/a Heart Internet
mduffvn.shop	NameSilo, LLC
mediaprintcopy.com	NameSilo, LLC
medslistusamen.com	NameCheap, Inc.
minchin.top	PDR Ltd

minebeehive.top	NameSilo, LLC
mjghf.com	NameSilo, LLC
moneycircle.top	NameSilo,LLC
montleger.com	Porkbun LLC
moonlaner.top	NameSilo,LLC
musedemuse.com	OwnRegistrar, Inc.
mycuesac.top	PDR Ltd
myjingshui.com	Alibaba Cloud Computing (Beijing) Co., Ltd.
myjingshui.com	Alibaba Cloud Computing (Beijing) Co., Ltd.
nanningzx.top	NameSilo,LLC
neeqe.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
onlineimigran.top	PDR Ltd
oyundanhaber.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
pauladiloka.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
pesonaindonesia.top	PDR Ltd
phonemarket.top	PDR Ltd
plqjasm.top	NameSilo,LLC
ppshop.top	NameSilo,LLC
presleynet.com	OwnRegistrar, Inc.
quchao.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
raikeurope.com	Web Commerce Communications Limited dba WebNic.cc
ratitudefor.top	PDR Ltd
rbhotsale.top	NameSilo,LLC
roinmklpvee.digital	NameSilo, LLC
rotubo.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
rtfabstore.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
sacredportal.shop	Alibaba Cloud Computing Ltd.
saglikverileri.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
sc994.com	NameSilo, LLC
sdxtswkj.com	NameSilo, LLC
sellbitcoins.top	NameSilo, LLC
seocrawlerrank.com	NameSilo,LLC
surprisefacts.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
tamplmediax.com	Key-Systems GmbH
texansjerseyvip.top	PDR Ltd
textloans.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
thebenefactor.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
thevonline.com	NameSilo, LLC
tnccheap.top	NameSilo,LLC
totalinsurance.top	NameSilo,LLC

tracquisitions.com	NameSilo, LLC
trufflesque.xyz	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
trustrollup.com	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
tsxxswzny.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
tuantai.top	PDR Ltd
ueitayxy.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
ukhemp.top	NameSilo,LLC
verapoag.com	Gname.com Pte. Ltd
videostreams.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
wgjbtvki.com	Realtime Register B.V.
wizardcrack.xyz	NameSilo, LLC
wnrncn.top	NameSilo,LLC
worstdoctor.top	NameSilo,LLC
z6trax.com	NameSilo,LLC
zayessiver.com	NameCheap, Inc.
hqbdsmtube.com	NameSilo, LLC
postinvestmentholdup.com	NameSilo, LLC
tuixuexi3.com	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
marquis-rents.com	NameSilo, LLC
rolluptrust.com	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
juaraqq.life	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
025bmw.com	NameSilo, LLC
portemondiale.xyz	NameSilo, LLC
cheapprilosec.top	NameSilo,LLC
creatlab.xyz	NameSilo, LLC
flyskyoo.top	NameSilo,LLC
baldberry.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
magicos.top	NameSilo,LLC
jfmjyo.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
pauladiloka.xyz	PDR Ltd. d/b/a PublicDomainRegistry.com
londonescorts.top	NameSilo,LLC
temablogspot.xyz	NameSilo, LLC
commonbacara.shop	Alibaba Cloud Computing Ltd.
cocinafacil.xyz	NameSilo, LLC
mjghf.com	NameSilo, LLC
slarposed.space	Namecheap
simanfashion.top	NameSilo,LLC

Disclosure communications

Names have been removed for privacy concerns. Some communications including sharing private information with victims or on-going legal actions are not disclosed.

Email sent to the news organisations

June 5 2023 from CheckFirst >

Dear [xxx] team,

I hope this message finds you well.

I'm writing on the behalf of Check First, a Finland-based software and methodologies company focused on helping the fight against disinformation.

My purpose for writing today is to urgently bring your attention to a growing concern involving your media organization's image and name being exploited in various scams. Just to make things clear, we're not seeking to sell you anything but merely are eager to expose the scammers, their mechanics and prevent further people from falling victim to impersonation and becoming part of a large scale scam operation.

Our team has discovered a troubling trend where thousands of Facebook advertisements are being used to direct unsuspecting users to counterfeit media sites worldwide, including one that illegitimately bears your organization's name and likeness. The source of these deceptive ads are hijacked pages with followers ranging from a few individuals to as many as 2 million.

The scams have been found to originate from a network of websites associated with a single domain, which further redirects users to fraudulent cryptocurrency websites. This interconnected web of scam websites is vast, with roots tracing back to 2019, causing potential substantial financial losses to innocent victims.

We understand the importance of brand integrity and the trust your audience places in you, which is why we're determined to help you confront this extensive fraudulent operation. You have the possibility to takedown these websites by invoking copyright infringements on the services used by the scammers. By leveraging your copyright rights, we aim to coordinate a global action against the service providers hosting these websites, seeking their immediate takedown.

Your participation and support in this initiative would be invaluable. Could we schedule a conversation at your earliest convenience to discuss how we can collaboratively combat this issue and protect your brand's image?

For your information, we plan on publishing our investigation around June 22th.

We look forward to your positive response and stand ready to assist in every way possible.

Kind regards,

Communication with NameSilo LTD

June 14 2023 from CheckFirst >

Dear NameSilo Team,

I hope this message finds you well.

I am [xxx] of CheckFirst, a Finnish software and methodologies company that aims at providing solutions to stakeholders tackling disinformation.

We have recently concluded an in-depth investigation into a complex and widespread scam operation. This operation, which involved thousands of Facebook ads redirecting users to counterfeit media sites, has been found to leverage services from various domain registrars - your platform, NameSilo LLC, included.

Remarkably, 45% of the identified domains associated with this operation were registered through your platform. Our findings suggest that this operation contravenes various sections of your Terms of Service, specifically those concerning user content and prohibitions against infringement of third party rights and engaging in illegal activities.

As we prepare to publish our investigation's findings, we are committed to ensuring a comprehensive and balanced report. Therefore, we are reaching out to request your comments on the following:

- How does NameSilo respond to reported violations of your Terms of Service?
- What measures does NameSilo currently have in place or plan to implement, to prevent misuse of your services?

Your responses will provide our readers with a crucial perspective on this matter and the steps being taken to rectify it.

We appreciate your prompt attention to this request and look forward to your response by 19 June, as we aim to publish the investigation report shortly thereafter.

Should you wish to discuss these matters further, please feel free to contact me.

Thank you in advance for your cooperation.

Best regards,

June 14 from NameSilo >

Hi,

The short story is that we take bad domains down as they are reported and confirmed to be bad. If you have a specific domain in question, we can search to see if it was indeed reported and what actions we took

Communication with PublicDomainRegistry LTD

June 14 2023 from CheckFirst >

Dear PDR Team,

I hope this message finds you well.

I am [xxx] of CheckFirst, a Finnish software and methodologies company that aims at providing solutions to stakeholders tackling disinformation.

We have recently concluded an in-depth investigation into a complex and widespread scam operation. This operation, which involved thousands of Facebook ads redirecting users to counterfeit media sites, has been found to leverage services from various domain registrars - your platform, PDR Ltd, included.

Remarkably, 29% of the identified domains associated with this operation were registered through your platform. Our findings suggest that this operation contravenes various sections of your Terms of Service, specifically those concerning user content and prohibitions against infringement of third party rights and engaging in illegal activities.

As we prepare to publish our investigation's findings, we are committed to ensuring a comprehensive and balanced report. Therefore, we are reaching out to request your comments on the following:

- How does PDR respond to reported violations of your Terms of Service?
- What measures does PDR currently have in place or plan to implement, to prevent misuse of your services?

Your responses will provide our readers with a crucial perspective on this matter and the steps being taken to rectify it.

We appreciate your prompt attention to this request and look forward to your response by 19 June, as we aim to publish the investigation report shortly thereafter.

Should you wish to discuss these matters further, please feel free to contact me.

Thank you in advance for your cooperation.

Best regards,

Communication with CloudFlare

June 14 2023 from CheckFirst >

Dear Cloudflare Team,

I hope this message finds you well.

I am [xxx] of CheckFirst, a Finnish software and methodologies company that aims at providing solutions to stakeholders tackling disinformation.

We have recently completed an extensive investigation into a complex and widespread scam operation. This operation involved a multitude of Facebook ads that redirected users to counterfeit news sites. Throughout our investigation, we have identified several key entities, including Cloudflare, who may have been unknowingly implicated in this elaborate scam.

Our investigation traced the name servers of the involved domains and discovered that a number of domains (97%) are managed via Cloudflare. The content on these websites aligns with the pattern of the fraudulent operation, suggesting that some of the counterfeit news websites may be using Cloudflare's services.

According to the Terms of Use of Cloudflare, any form of impersonation of an established news outlet with the intent to deceive users is explicitly prohibited. Your terms state that users are solely responsible for their content and must ensure it doesn't infringe upon any third-party rights, including copyrights, trademarks, patents, trade secrets, moral rights, privacy rights, rights of publicity, or any other intellectual property or proprietary right.

As we finalize our report, we believe it is crucial to include your perspective. Could you provide a comment on the following:

- How does Cloudflare respond to reported violations of your Terms of Use?
- What measures does Cloudflare currently have in place or plan to implement to prevent such misuse of your services?

We kindly request your response by 19 June, as we aim to publish our investigation report shortly thereafter.

Should you wish to discuss these matters further, please feel free to contact me.

Thank you in advance for your cooperation.

Best regards,

Communication with Meta

June 14 2023 from CheckFirst >

Dear [xxx],

Following our meeting on June 8th, I am writing to request additional information and comments regarding our findings. We hope the data we shared so far has been useful.

To augment our report, we would really appreciate if you could answer the following:

1. Can you provide additional details regarding the network we've uncovered? We're particularly interested in its scale, duration, outreach, and the total amount expended on advertisements across Meta by the implicated parties.

2. Could you kindly elaborate on the actions you've taken or intend to take in response to the discovery of these deceptive pages?

3. What measures are currently in place, or will be implemented, to prevent similar fraudulent operations from occurring in the future?

4. Our inquiry has shed light on the two-tiered moderation process for ads on Meta, revealing its vulnerability. While the automated first tier may need technical adjustment, we'd like your insight on why the human verification tier failed in this instance.

5. Our team found the Meta Ads Library to be a powerful resource during our investigation, and we commend your efforts in creating it. Nevertheless, we've identified instances of ads appearing on user feeds that do not seem to be catalogued in the library. Could you provide an explanation for this?

6. We've observed that advertisements categorised under "Issues, elections, or politics" lack information about their funding entities. While privacy laws may prohibit such disclosure in some instances, our examples primarily target European audiences, a region where this information is recommended under the European Code of Practice against Disinformation Measure 6.2, to which Meta is a signatory. Could you clarify why this data is absent?

7. The following articles from Le Soir, RTBF and FullFact report about similar cases dating back 2021 and 2022. The FullFact article reports about Martin Lewis having sued (then) Facebook Inc and later dropped charges after the company had made promises to take action against scam ads. Which actions have Meta taken since then?

We value your cooperation and look forward to your response. Your insights will not only enhance our report but also facilitate our collective pursuit of transparency and accuracy.

Thank you once again.

Check First is an ally in the fight against disinformation. We gathered skills and knowledge to build a company that is at a cornerstone of the fact-checking world.

We are an accelerator. We provide fact-checkers, researchers and policy makers tools, methodologies and solutions to gather their forces in the fight against fake-news.

https://checkfirst.netwok
info@checkfirst.network