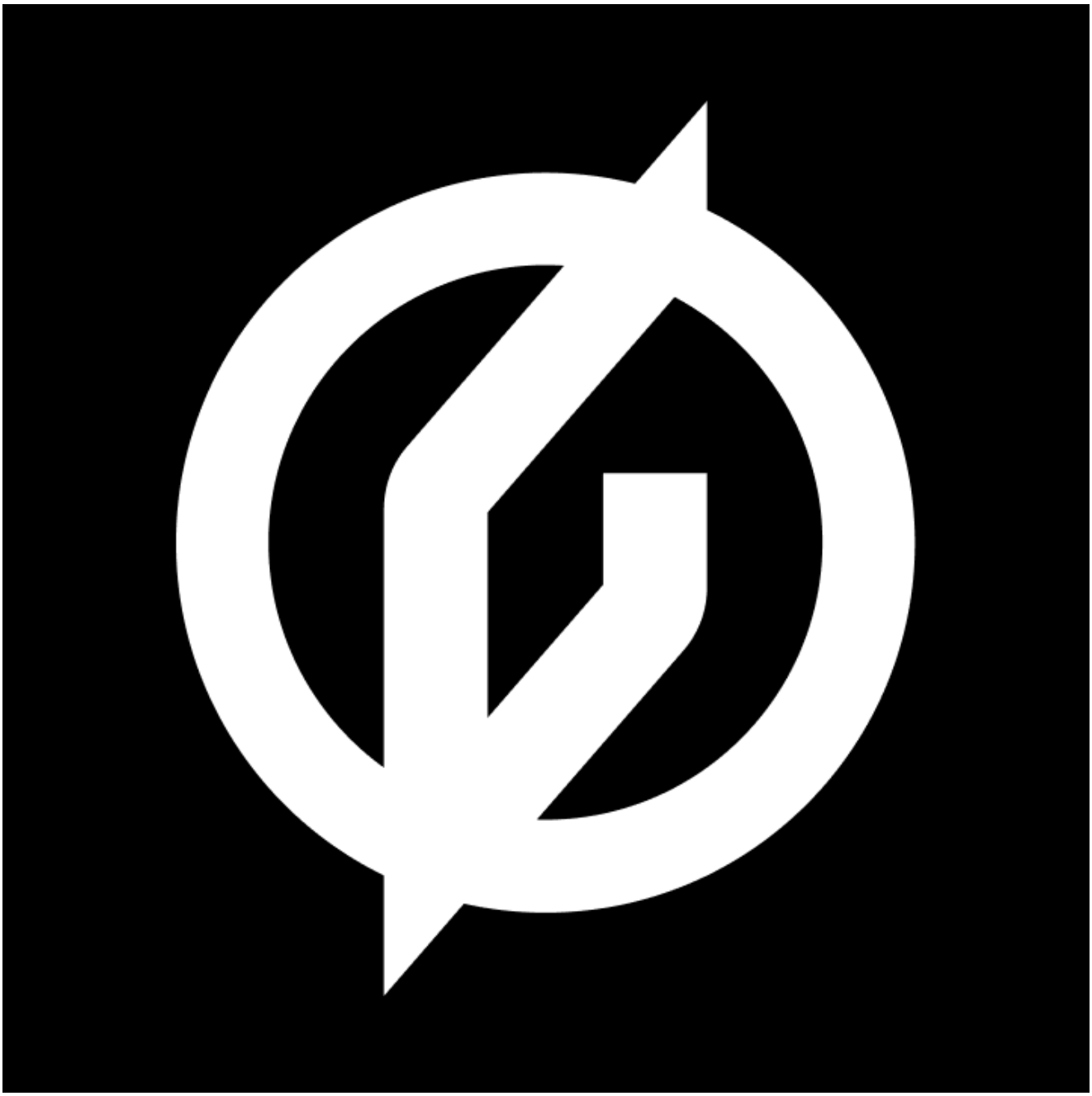
Fake investment scams in Europe

blog.group-ib.com/investment-scams-europe

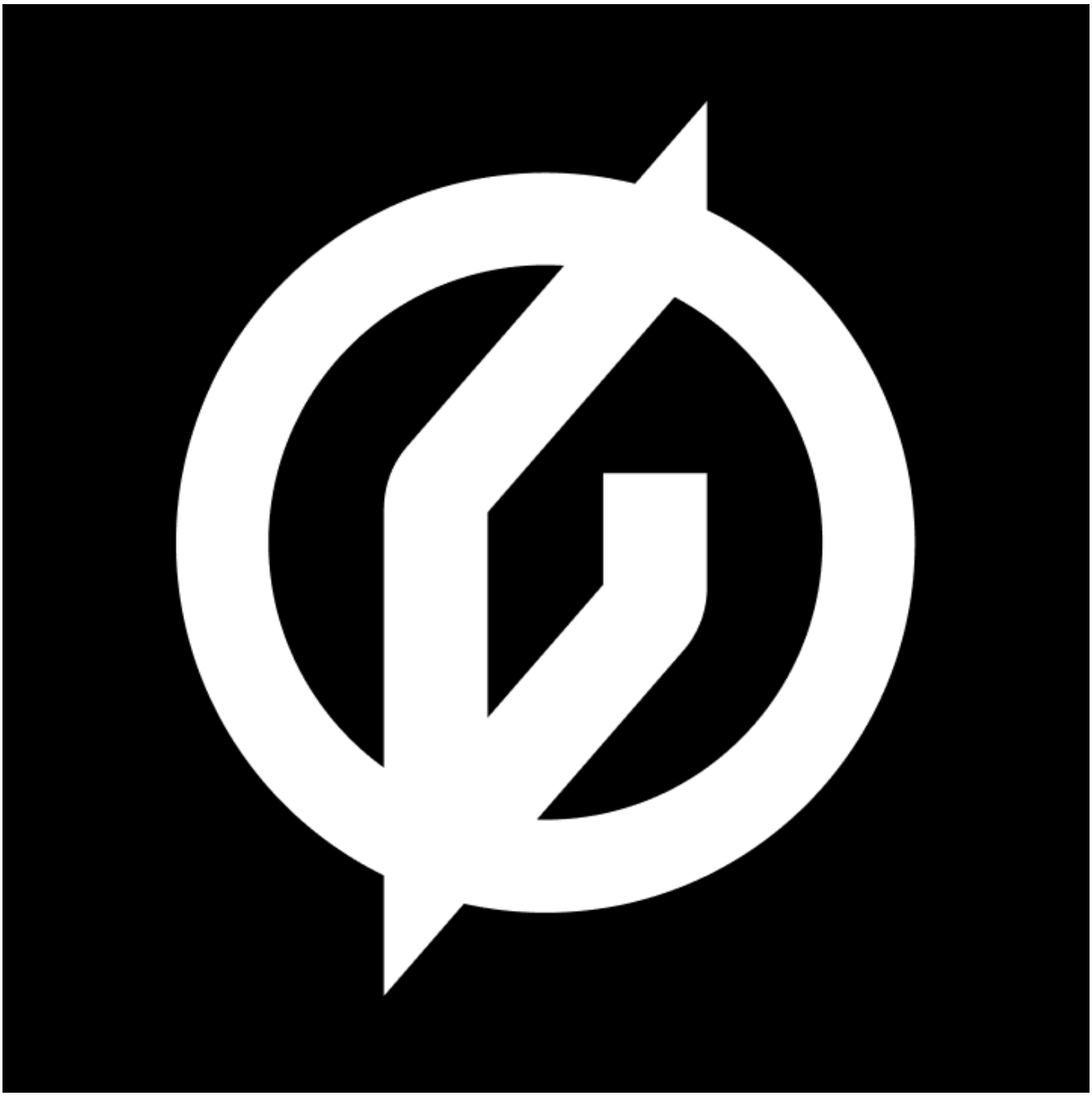
29.07.2022

How we almost got rich



Reza Rafati

Senior Analyst at Group-IB Computer Emergency Response Team (CERT-GIB) Europe



Yaroslav Kargalev

Deputy Head of the Group-IB Computer Emergency Response Team (CERT-GIB)

Fake investment scams have been around for long enough so that people could recognize them easily. For instance, in 2020, Group-IB Digital Risk Protection Team detected a massive bitcoin scam campaign in Singapore which used the names of local celebrities. Nevertheless, no matter how old the scheme is, it keeps bringing money to fraudsters.

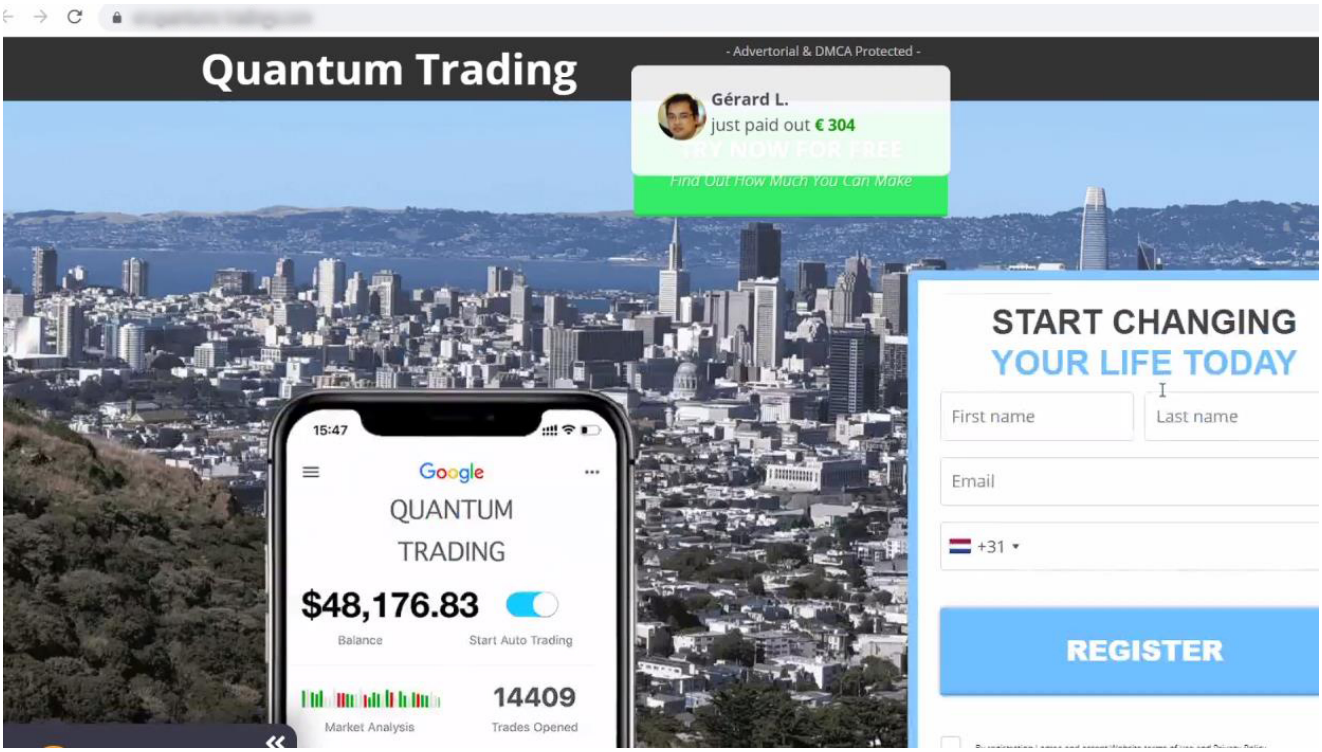
The Group-IB Computer Emergency Response Team (CERT-GIB) has been investigating several fake investment schemes which are targeting European citizens. In the course of the research, a gigantic network infrastructure was uncovered and analyzed, which contained

over **10,000** rogue resources, including similar fraudulent ones aimed at the inhabitants of the entire Eurasian continent and North America.

In our research, we noticed that the following countries are being targeted with the Fake investment scheme:

- UK
- Belgium
- Netherlands
- Germany
- Poland
- Portugal
- Norway
- Sweden
- Czech Republic

The main goal of these fake investment schemes is to convince the victims to repeatedly transfer funds to the fake investment portal. The victims are usually promised huge returns on their investments and are shown “how I got rich” stories featuring celebrities.



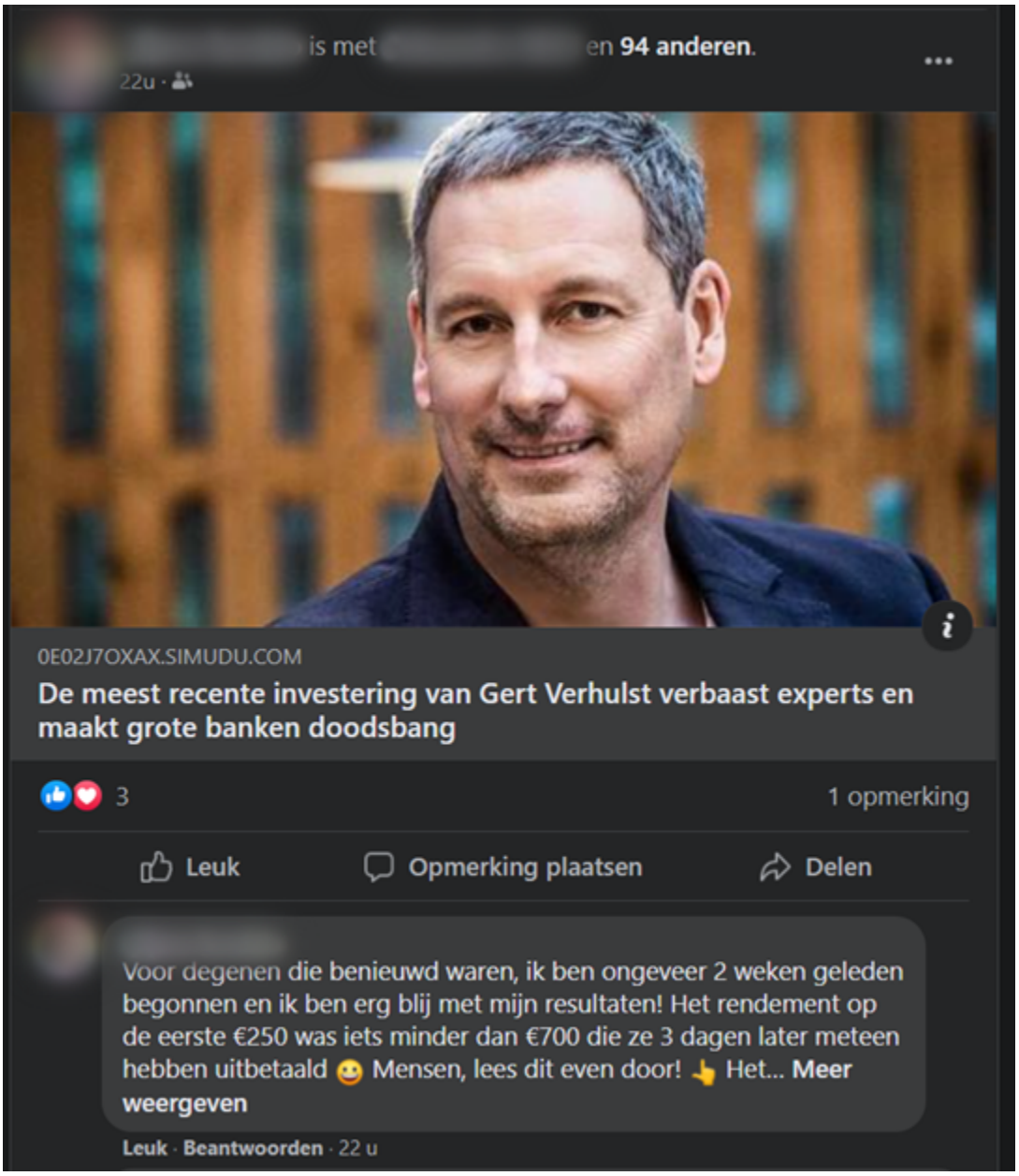
In this post, **Reza Rafati** from the Group-IB Computer Emergency Response Team (CERT-GIB) in Amsterdam will take a deeper dive into the fake investments schemes, showcase a couple of them including a conversation with the scammers that we managed to record, and provide recommendations for the users. The aim of this research is to raise awareness about the fake investment scheme and ultimately reduce the number of victims. We encourage cybersecurity researchers and the general public to join the fight against cybercrime and

share fraudulent domains with us via “Report an Incident” form at https://www.group-ib.com for further evaluation and takedown.

Fake investment schemes

Legitimate looking investment sites are popping up everywhere. We see them on various social media networks, which include the massive platforms of Youtube and Facebook.

The message displayed on those platforms makes it seem like there is a bulletproof service of making an online income. The messages state that the service is used by famous people globally. This can be from Elon Musk to local Dutch and UK celebrities. The message continues to state that it is a unique offer and that you just need a minimal deposit of 250 euros to get started.



Screenshot from a rogue Facebook profile which is sharing the scheme

The scam disseminates deceptive information as though ‘Gert Verhulst’ has surprised experts and is frightening the banks, all because he made an investment. The fake investment scheme illegally exploits the name and the image of this famous person to lure the victims to click on the link. Gert Tony Hubert Verhulst is a Belgian media entrepreneur, television producer, presenter, actor and singer. He is known in the Netherlands for his television role in the show 'Samson en Gert'.

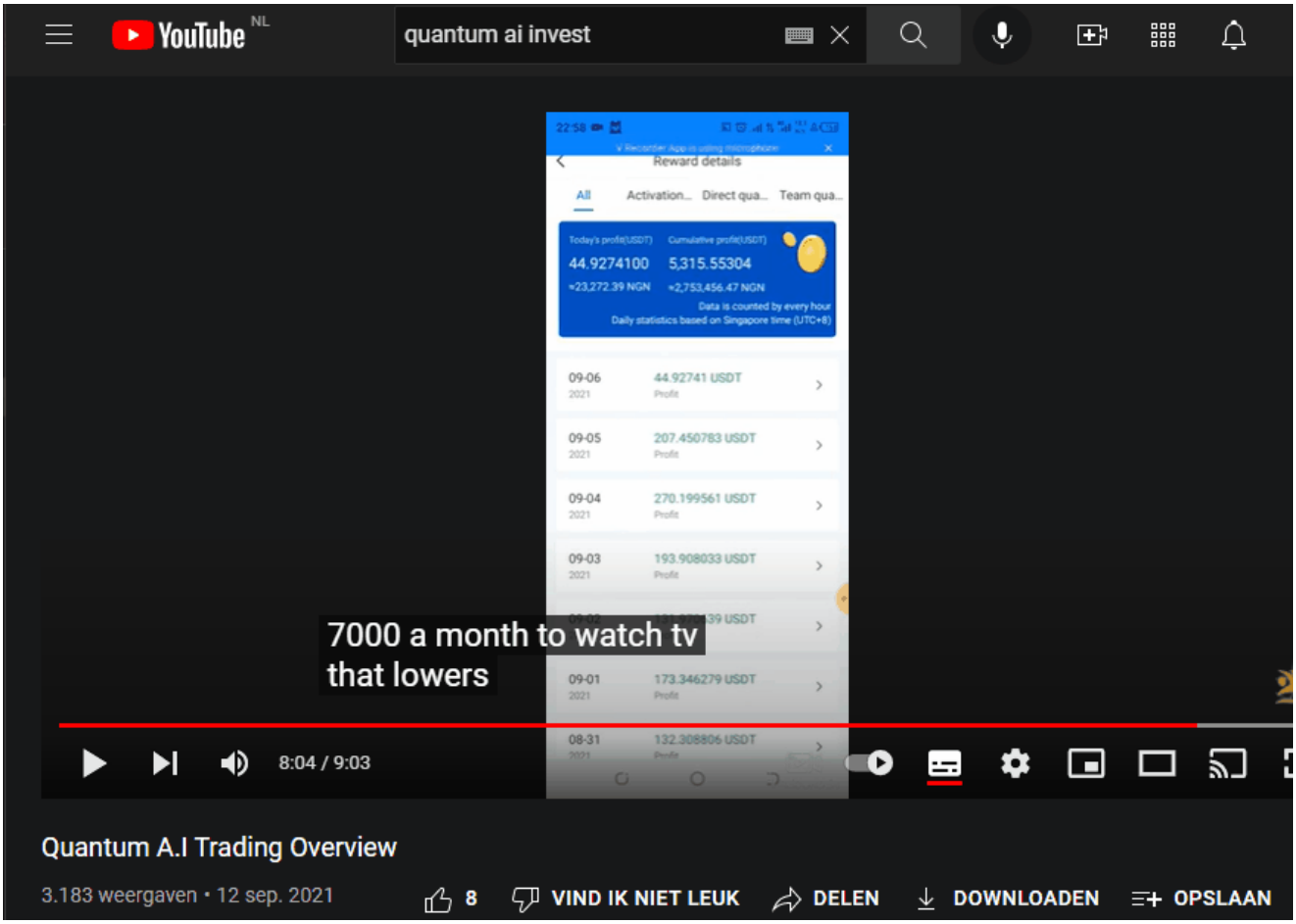
Additionally, the victim will leave a comment below the hyperlink, stating that with 250 euros the victim was able to have a profit of 700 euros in just 3 days.

In some cases, specially created rogue Facebook pages were being used to spread the fake investment scheme post via the advertisement capabilities on Facebook.

A promoted Facebook message luring victims to the fake investment schemes

The following footage is taken from Youtube, in this video the fraudster is trying to lure users to contact him. Once contacted by the victims, the scammer will assist the victims in creating the needed profile to start with the investment, and also assist in getting the initial minimal 250 euro deposit.

A video on Youtube trying to lure the viewers into contacting the actor that is participating in the fake investment schemes.



The ultimate goal is to lure the victims into visiting fake investment portals.

Your personal account manager

The scammers behind this scheme try to maximize their impact and set up the same scheme with different templates that cover specific topics. Below you can see a collection of the templates seen by CERT-GIB in the fake investment schemes.

The fake sites make use of templates that seem to be of high quality. The color palettes used and the code itself makes it look like a legitimate and trustworthy website.

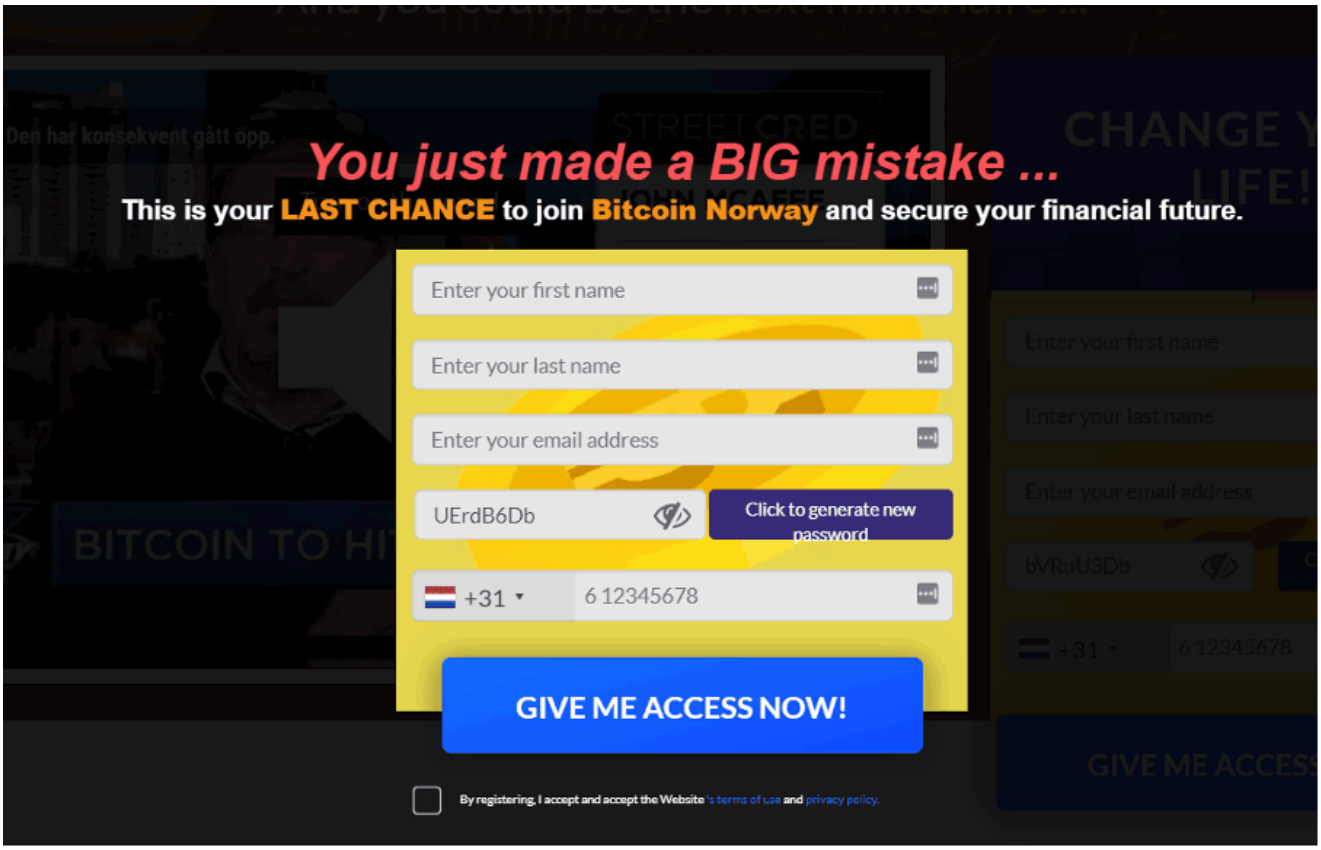
The main idea of the fake broker sites is to show content to the victims which will trigger them to:

- Register an account
- Replenish the balance on their previously made account
- Bombard the victims with success stories
- Draw fictitious stories that profit is being made via the fake broker sites

The scammers social engineer the victim into making an investment. Once the victim lands on the fake broker site, they will see various fake messages of people that have had “successful” trades and are in the process of cashing out. The fake broker site will for

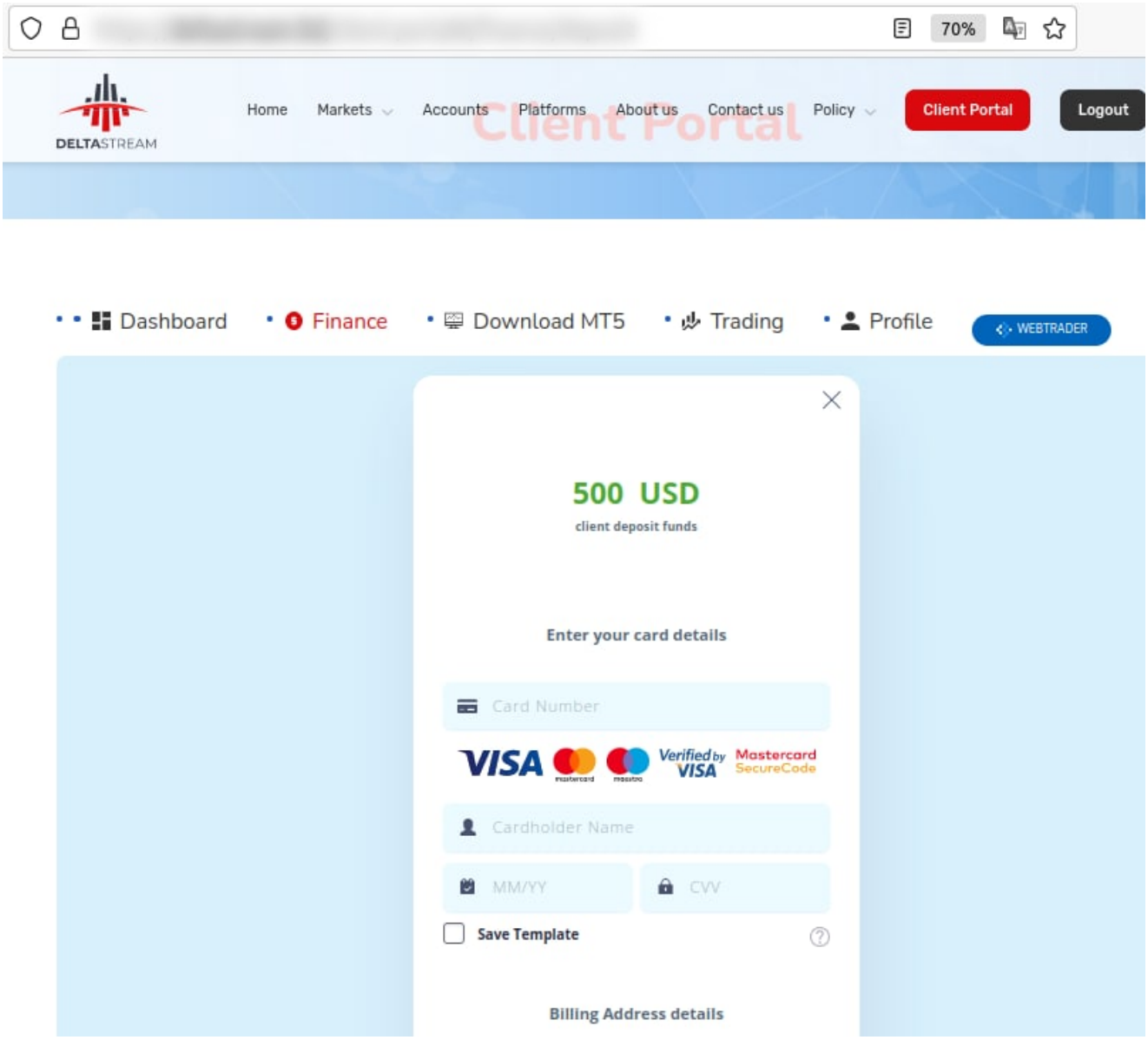
example state that a random name from your city just has withdrawn a couple of hundred euros.

The scheme is a combination of online and offline techniques. After filling out the form (shown below), the victim receives a call from scammers who provide a link to the final fraudulent invest-project with a personal account. To start trading, the victim needs to replenish the balance.



One example of a fake investment scheme form used to target Norwegian users

This “fake” account manager will assist the victim in making the right decisions on their fake investment dashboard, increasing the likelihood that the scammers can get more than 250 EUR of the victim. It also allows the fraudsters to change specific values in the dashboard so the dashboard meets the expectations of the unaware victim.



The final page where the victim is requested to perform a transaction of 250 EUR or more. It is at this stage where the credit card details are compromised and the victim loses money.

How we got scammed (on purpose)

This scheme makes use of several steps to social engineer the victim into sending out money. For research and awareness-building purposes we signed up with one of those scam websites. Shortly after signing up, we received a phone call.

During this phone call the scammers asked several questions that you would expect when dealing with a legitimate investment service:

- Why do you want to invest?
- How much can you invest?
- How do you make your money?

- How much time do you spend on work?

On each answer of these questions the scammer gave a positive response which led to the next step in the call. At the end of the call, the fraudster insisted on giving payment card details immediately. He was very upset when we refused. Remember, the sense or urgency that the scammers are often trying to induce is one of the red flags. Refer to the recommendations section below for more tips.

Below you can find the audio recording and the transcript of the conversation with the scam "operator" that we were able to record. *It has been partially muted for the sake of privacy.*

Transcript

A: I am calling you from [fake investment platform name]. How are you?

B: I'm good. I'm good. Thank you for calling.

A: I see you have left your details with our platform, Reza.

B: That's correct. That’s correct.

A: Is this your first-time trading?

B: Yes.

A: Okay, then you just start making profits with trading. What would you do with them? Do you have any goals?

B: Man, I think I will buy a nice car, if it goes good.

A: What kind of car you want to buy?

B: Man, you tell me what I can buy. I am interested in what type of money
I can make online.

A: It depends on you and your capital as well. Because, you understand, if your capital is big, your profits will be big as well.

B: Okay. Okay. So…

A: Let’s see. You are a beginner. So, I would like to suggest you something very simple, okay?

B: Okay, I am interested. Let me know.

A: Let's start trading with the bare minimum for a couple of days so you can check out our platform and the service we provide, check the result. And then you can make your own educated decision if you would like to continue. Okay?

B: Okay. Okay.

A: If you like it, we continue trading long term. If you don't like it, you close your account and you take out your money.

B: Sounds like a plan.

A: Sounds fair?

B: Yeah, sound fair.

A: Okay. Then speaking of money, by the way, how do you support yourself right now?

B: Man, I work full time. I work too much. I want to work less. That's why I am also investing now.

A: You work too much. What exactly is your profession?

B: I work in IT management.

A: IT Management?

B: Yeah. So, I do system repair and, you know, I have those customers like that.

A: Like administrator?

B: Yes, exactly. Exactly.

A: Working too much, so you are working over eight hours a day?

B: Man, I work around 40 to 60 hours a week. That’s too much.

A: Every day 40 to 60 hours?

B: Not every day. Every week, every week. I cannot change the hours of the day.

A: 40 to 60 hours is not much for a week.

B: For me it is man. I live in Netherlands; I shouldn’t be working so much.

A: So, you just like to spend your time with yourself, not go to the office. You want to make money online?

B: Exactly. Because my employer is not paying me too much money at this moment. And I want to make some extra money on the side. So at one moment I can tell my employer. “Ok, thank you, I will work through this”.

A: Hum, okay. You don't like to work for somebody else. You want to work for you?

B: I want to have freedom.

A: Yes. I understand why you signed up. You want to try a bit … if it is going to work for you. And let’s say after a couple of months if you build up some confidence and you see if it can be positive for you. Maybe you can achieve this financial freedom.

B: Exactly. Exactly. This is for financial freedom. You say correct.

A: Okay. Reza, so, we are going to do something like this, okay? We are going to start with a minimum. We are going to make a deposit, so we can activate the investment account. Then, you are going to have a session with your personal account manager. He is going to show you around the platform, how to use it, how to trade, okay? You will test it out for a couple of days. And then you will make your decision. Okay?

B: Okay. Sounds good, sounds good.

A: Okay. So, usually my clients from Netherlands are using a Visa or a MasterCard for the deposit. What are you using?

B: I have a Visa, but I do not have the card with me right now.

A: What is it?

B: I am at work; I don’t bring the Visa card with me. Is it possible…

A: You leave you card at home?

B: Yes, of course.

A: What do you mean “yes, of course”? Is there somebody close to your house who can help you?

B: No, no. If they go to my house, they have a big problem. No, I don’t have a Visa card with me.

A: Okay. You have a banking application on your phone?

B: Yes. Yes.

A: Usually you can check your details as well.

B: Okay. I can do that. Man, do you have option to talk to you on WhatsApp or something like that?

A: No, it is not professional to speak on WhatsApp with clients. Reza, I want to be completely professional with you and every client I speak. So, It is not serious for me to speak on WhatsApp.

B: Okay. Okay. Because…

A: My job Reza would be to remind you that once we process the transaction with your Visa card, you are going to receive an SMS on your phone. So, this is 3D security from your bank. In this SMS you are going to see a code with which you are going to approve the transaction, okay?

B: Okay. Man, I am a little bit… I am now at work also. I did not expect you to call me so quickly. Can you call me back tomorrow, so we finish this tomorrow.

A: Reza, I understand this is your first-time trading and you are not 100% sure if you want to do it.

B: No, no, no, I am. I am. But my manager is looking and he is telling me to go to work.

A: Yeah, but we are speaking only for a couple of minutes. I see you signed up recently on our web page. So,it is going to take two minutes to activate the investment account and you can make your appointment with your personal account manager for later today or tomorrow, okay?

B: We can do it…can we create the account now and I make the deposit later? Because I cannot do this right now.

A: Yes, but you understand, I need to know if you are serious about this, because I cannot keep calling the same client over and over.

B: Of course, I am serious. You just said we've been talking already for a couple of minutes. I signed up.

A: How should I know if you serious? There are many people like you telling me "Call me later, call me tomorrow".

B: Man, that I do not know.

A: Then, they do not pick up the phone!

B: Man, I will pick up the phone for you.

A: How should I be…

B: Man, if you want to be be sure, you need to call me back later because I need to go to work now. I cannot do that lke this. This is a little bit weird. if you have bad experience with some clients, I understand, It's f*** up for you. But I am interested. I want to be called back.

A: Yes, but I cannot speak with the same client over and over again. Because, you see, every day there's thousands of clients registering in our platform. So, I am constantly speaking with new clients. If I seat with clients like you who tell me “Call me later, call me tomorrow”, I will not be able to speak with new clients.

B: I understand. But I have my work here right now. I need to do my work. Yes?

A: Yes.

B: From other side, there are many, many brokers that can help me like this. And I went to you. So if you want to do business with me, you call me back tomorrow. If you don't want to do business with me, it is over.

A: How do I know if you are serious about this?

B: Man, I’m talking to you right now. Why should I not be serious?

A: Yes. How should I know?

B: Man, you're costing me time right now. I need to go to work. If you call me tomorrow, I will call back to you.

A: But I believe you signed up for a reason with our company. You did not sign up because you wanted to speak with me, you signed up because you wanted to start investing.

B: Exactly. Exactly. And I want to start. But I cannot talk right now. I really need to go. Yes?

A: Okay, Reza.

B: Please call me back tomorrow and we can make next steps.

A: Good luck.

B: Thank you.

“Fascinating” victim journey

In a nutshell, the scheme looks as follows:

2

The victim sees the fake investment post and is lured into clicking the post as the post claims that easy profit can be made with a minimal deposit of 250 EUR.

3

The victim clicks on the post which translates itself into two steps:

a. The victim is navigated directly to the fraudulent scheme site or an “advertisement” site which shows the “profit” famous people are making with the investment plan.
b. The victim is forwarded to an fraudulent investment site which shows successful projects and income plans.

4

The victim is shown a form which asks for contact details.

5

Once the form is filled, the victim will be contacted by phone by one of the call centers that is being used for this scheme.

6

During the call, the scammer will try to social engineer the victim into believing that the investment plan is a legitimate plan. It is also in this step that the scammer informs the victim that with a minimum of 250 euro deposit with a credit card the investment can be started.

7

Once the victim has made a deposit of 250 euro or more, the victim will get a login to a fake investment dashboard.

8

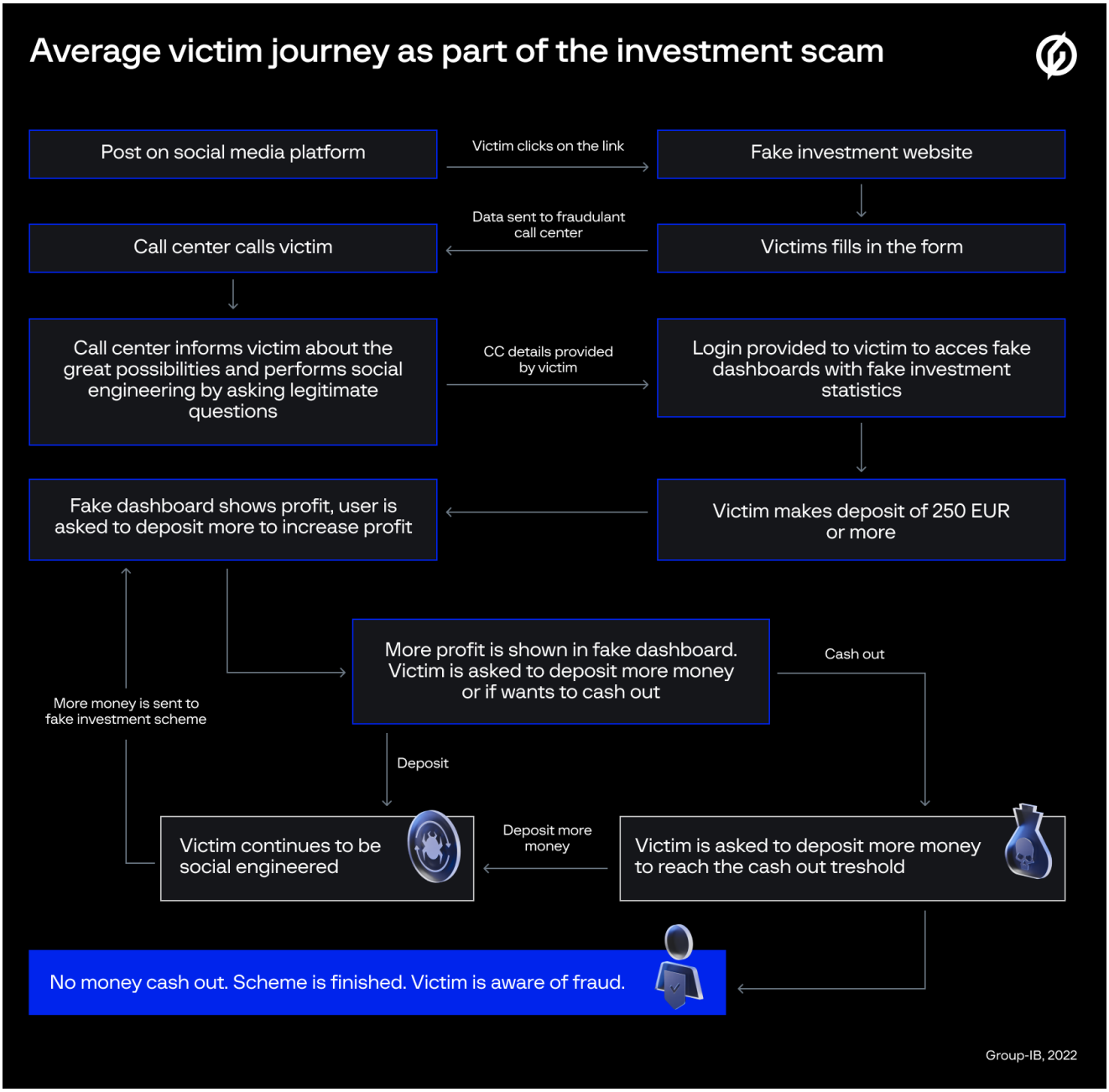
In the fake dashboard profit will be shown (while literally there is no profit as all is fake), the scammers do this to be able to ask the victim for more money, as the victim believes good profits are being made. No actual trading is taking place on the platform.

9

The scammer (fake account manager) continues to ask for more deposits so that the victim can increase their profits. If the victim agrees to deposit more, the victim will be sent back to step 8. If the victim denies, and wants to cash out, the victim will be shown step 10.

10

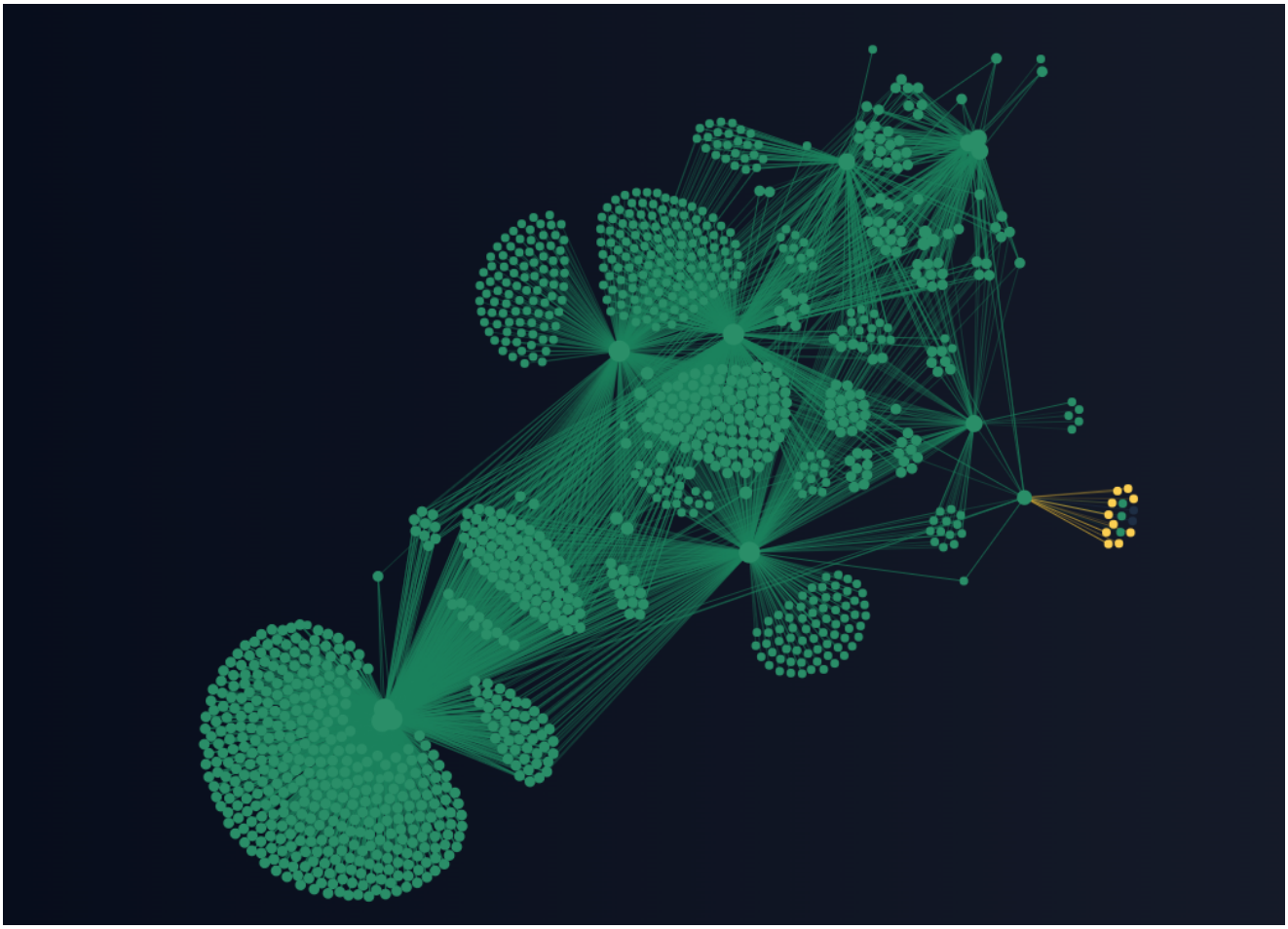
The scammer will state that the victim needs to put another deposit to meet the payout threshold. If the victim agrees to do this, they will be sent to step 8 again, if the victim refuses to deposit more, the victim will quickly realize that they have participated in a fake investment scheme and that the money has been lost.



The scale of fake investment schemes

We used our patented Graph Network Analysis tool within the Threat Intelligence system and it quickly showed us the immense size of the schemes that have been setup.
At the moment of writing, CERT-GIB tracked down **11,197** domains that were used and included in the general fraudulent infrastructure targeting Europe - this included chains of redirects and hosts of fraudulent content.

The lifetime of fraudulent sites varied from several days to several months (the more victims the site brought, the faster it went offline and its mirror was raised on another domain). At the moment of writing, from those 11,197 domains, 5,091 still remain active.



A graph view on one of the domains - leading to a massive forest of fraudulent investment scheme sites.

Source: Group-IB Threat Intelligence

The fraudsters make use of specific keywords and top level domains to trick unaware internet users into their fraudulent scheme. The keywords range from specific investment categories like Bitcoin and gold, but this is not where they stop, they continue to set up schemes that target specific countries.

In our research, we noticed that the following countries are being targeted with the Fake investment scheme:

- UK
- Belgium
- Netherlands
- Germany
- Poland

- Portugal
- Norway
- Sweden
- Czech Republic

Recommendations

The earning techniques used in the schemes abuse the trust of the victims, the scammers perform social engineering methods to keep the victim hooked.

In order to protect yourself and your surrounding against these type of threats, we have the following recommendations for you:
Investments can often be done via legitimate and established brokers. There are many sites that provide detailed information about these legitimate brokers. So don't simply click and join a site via an advertisement, do your own research online and validate that you are dealing with a legitimate broker website.

When you start with investments, you don't need to have a personal account manager telling you what to do by phone. Keep your money in your pocket and educate yourself in regards to investing.

Search for reviews - the established brokers will have reviews. These reviews can help you to get a better understanding of the service and the quality that is provided.

Often the fake broker domains have a short lifespan, this means that the domains that have been registered are quite new. You can report suspicious domains at https://www.group-ib.com via "Report an Incident" form. Our team will evaluate and take down fraudulent websites upon confirmation.
Financial organizations are recommended to use Group-IB's Fraud Protection to stop fraudulent activity even after its customers share payment details with the scammers.
Group-IB Digital Risk Protection defends the personal brand of individuals by hunting down impersonations and illegal copies of accounts.

Legal disclaimer

1. The material was prepared by Group-IB experts solely for research purposes in order to minimize the risk of further use of methods and techniques of committing illegal actions and their timely prevention.

2. The conclusions do not represent the official position of competent authorities, including law enforcement agencies, do not contain direct accusations of committing crimes or other unlawful actions, and are analytical and informative in nature.

3. All personal data including names, images, video and audio records and any other information on identified or identifiable individuals are published herein for the purposes specified above in the public interest. If you have any questions or requests concerning your personal data contained in our articles or blog posts, please address them to: privacy@group-ib.com.