

# WhatsApp Scammers

written by Mert SARICA | 7 August 2023

## Table of Contents

1. Introduction
2. How and where did they get our cell phone numbers?
3. How did they lure their victims?
4. Who owned the accounts used to transfer money?
5. From which country were they running this operation?
6. Did the fraudsters speak Turkish or did they use translation tools?
7. Conclusion

## 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



Block

Add

Today

🔒 Messages and calls are end-to-end encrypted.  
No one outside of this chat, not even WhatsApp,  
can read or listen to them. Tap to learn more.

Merhaba Tünaydın 05:52

Bugün nasılsın? 06:55

İyiym sen nasılsın ? 07:09 ✓✓

ben iyiym efendim 07:10

Tanıştığıma memnun oldum, ben Lara

07:10

Ben de. Ben Rifat. 07:11 ✓✓

Çok nazıksınız, birkaç dakikanızı alabilir miyim?

07:12

Tabii 07:12 ✓✓

Şu anda şirketimiz Türkiye'de turizm verilerinin artmasına yardımcı olmak için pazar araştırması yapıyor, yardımcı olabilir misiniz?

3 basit soruyu yanıtlayarak ve daha fazla aktivite olarak 180TL (Şimdi Öde) kazanın.

07:13

Tabii. Ödeme nasıl olacak ? 07:13 ✓✓

Efendim, şimdilik sadece banka havalesini kabul ediyoruz.

07:16

Iban vermem yeterli olacak mı ? 07:16 ✓✓

Evet 07:17

Bana yardımcı olursanız lütfen yaş aralığınızı seçer misiniz?

(bir) 20-24

(b) 25-30

(ç) 31-45

(d) 45 ve üstü

07:18

d 07:18 ✓✓

Pekala, şimdi sizden bazı pratik çalışmalar yapmanızı isteyeceğim.

07:18

Tabii 07:19 ✓✓

Soru-1: Şirketimiz size bir gezi kazansaydı hangi ülkeye gitmek isterdiniz?

(A) Japonya

(B): Avustralya

(C): diğer

Örnek (A) .Gitmek istediğiniz ülke için oy verebilirsiniz.

07:19

B 07:19 ✓✓

Güzel ülke 07:20



+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

Öyleyimidir. 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 sağlayacağından, lütfen istenen bilgileri doğru bir şekilde doldurun ve doğru olduğundan emin olun.

07:23

Ad Soyad: Rifat Ilgaz  
Banka hesap numarası: 57359646  
Bankanın adı: █████bank  
Yaş:51  
Cinsiyet:Erkek  
Mevcut iş: Muhasebe müdürü

07:26 ✓✓

Yeterli midir ? 07:26 ✓✓

Güvendiğin için teşekkürler. telgrafın var mı Şirketimiz iletişim için telegram kullandığından, eğer uygunsa, ödemenizin durumunu öğrenmek için resepsiyon görevlisiyle iletişime geçmek için telgrafı kullanabilirsiniz.

07:26

Evet var 07:27 ✓✓

İlk ödeme için kasiyer olduğu için onunla iletişime geçmelisiniz. Sana burada ödeme yapamayız.  
Telgrafınızı resepsiyon görevlisine ekleyin: @Rsp\_Nilu ([https://t.me/Rsp\\_Nilu](https://t.me/Rsp_Nilu))  
Lütfen resepsiyon görevlisine bu ödül kodunu bir mesaj gönderin: XY3171

07:27

Tamam hemen yazıyorum. 07:29 ✓✓



+60 11-6436 2947



Tamam hemen yazıyorum. 07:29 ✓✓

evet efendim 07:32

Onu telegrama ekledikten sonra, ona bu mesajı gönderin ve bana bir ekran görüntüsü gönderin, böylece sizinle daha hızlı ilgilenmesini sağlayabilirim. Bilgilerinizi tekrar kontrol edecek ve 5 dakika içerisinde ödeme işlemini tamamlayacaktır. 07:32

Ödüllerinizi almazsanız veya Resepsiyonist size cevap vermezse lütfen bana bildirin. 07:32

Yazıyor bana 07:33 ✓✓

ah! Tamam 07:33

Gönderildi, sistem ödülleri ödemek için 10-20 dakika kuyruğa giriyor. Lütfen aldığınızda bana bildirin. Satıcı veri görevleri daha iyi ödüller alabilir. 07:33 ✓✓

Size bilgi vermemi istedi 07:33 ✓✓

Gerçekten akıllısın, lütfen ödülünü bekle ve ödülünü 10 dakika içinde almazsan sana yardım edeceğim. 07:35

Tamam 07:35 ✓✓

Ödülleri beklerken bir sonraki göreve devam edebilirsiniz. 07:36

Daha fazla para kazanma fırsatı elde etmek için kayıt olmak ve çalışma grubuna girmek için resepsiyon görevlisinin talimatlarını izleyin. Bir sonraki çalışmada onunla iletişim halinde olmalısın. 07:36

Tamamdır. 07:52 ✓✓

Şirketimiz her gün çok sayıda benzer görevler yayınlamaktadır, işlemi çok basittir, günlük hayatınızı ve işinizi etkilemez, tamamlandıktan sonra size ödeme yapılır. 07:54

Katıldığınız için teşekkürler, bir sonraki çalışmada onunla iletişim halinde olmanız gerekiyor, iyi çalışmalar dilerim. 07:55



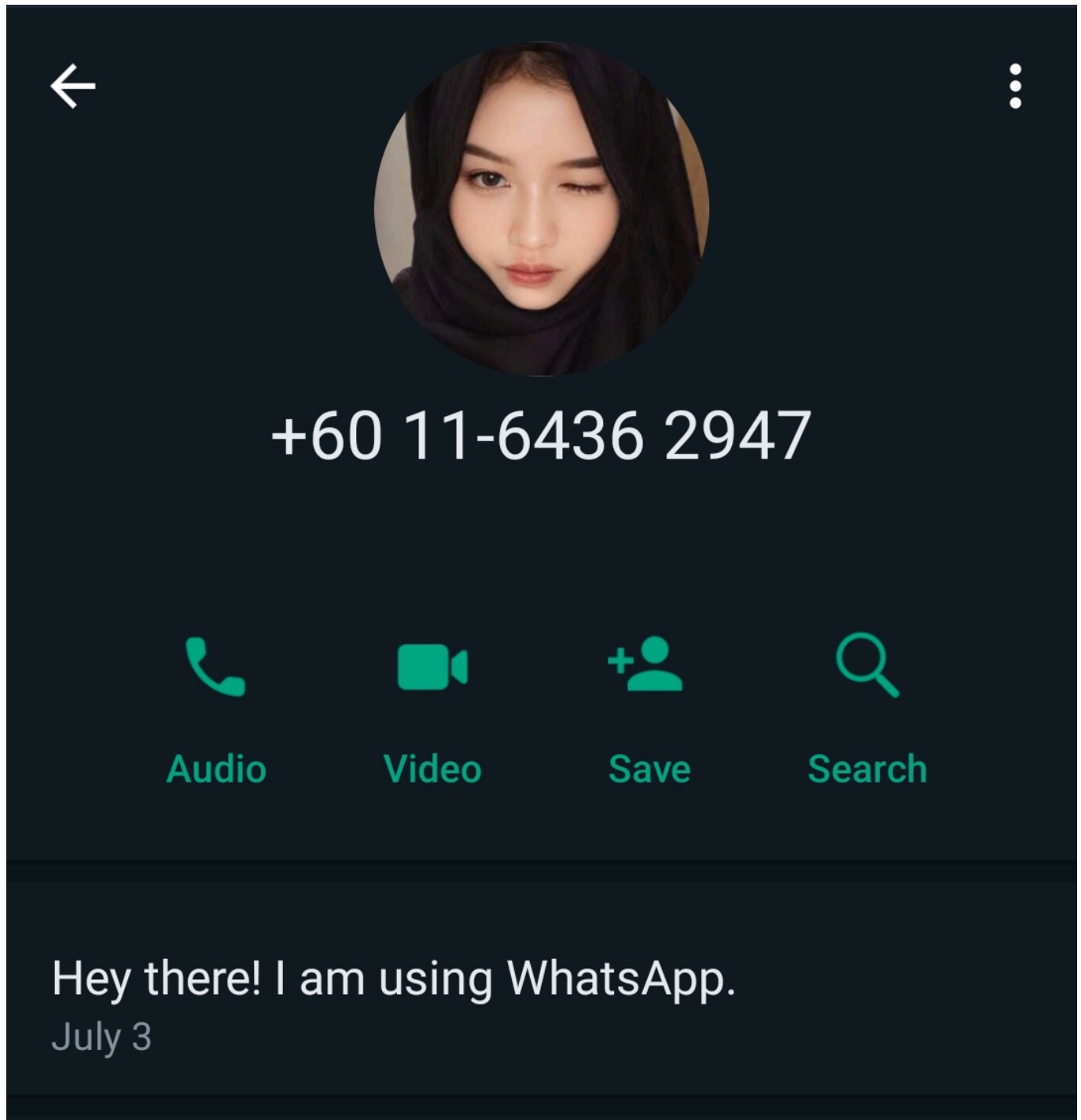
Memnuniyetle 07:55 ✓✓

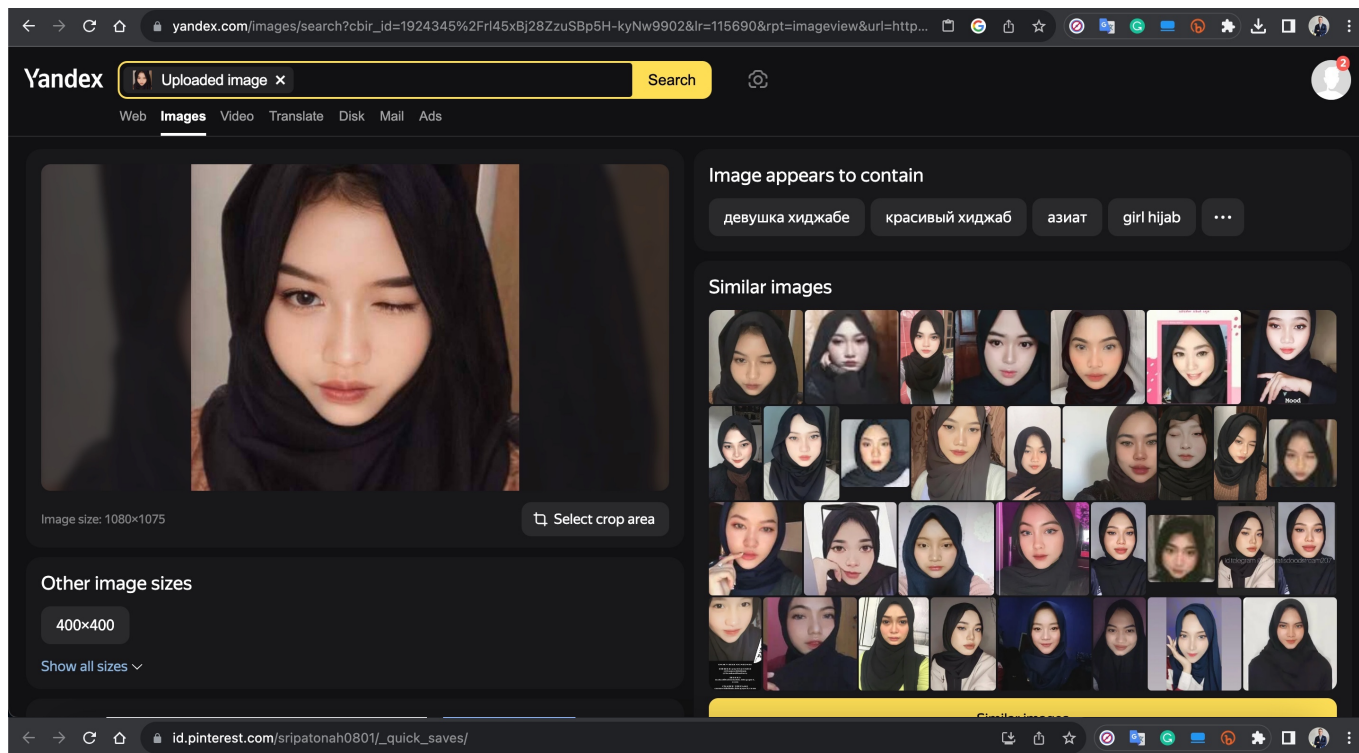
1 Unread Message



07:56

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.





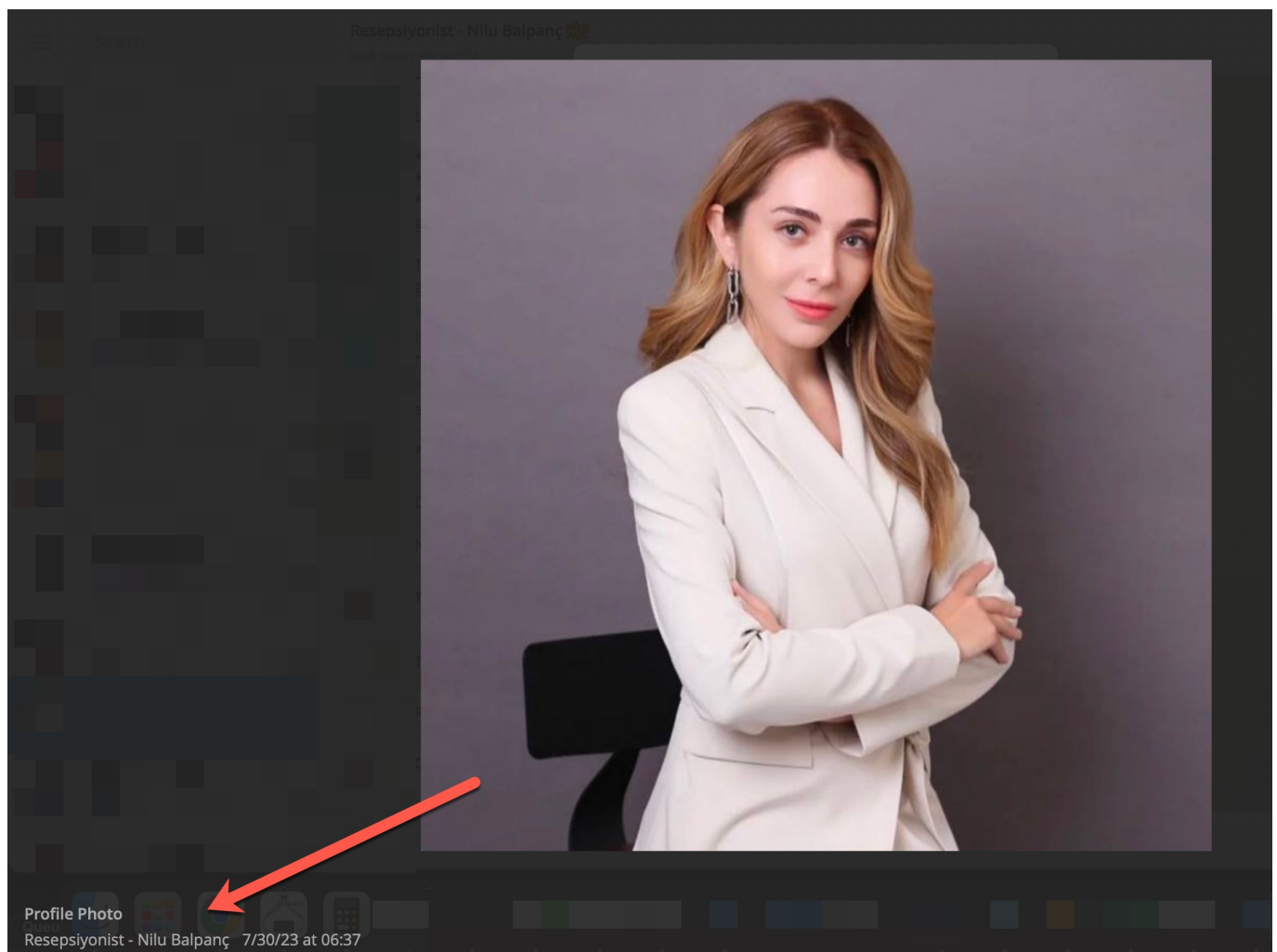
After answering all the scammer's questions, she gave me a reward code and told me to contact a person named Nilu BALPANÇ with the username Rsp\_Nilu on Telegram to pay me. When I contacted this person, who, according to Telegram Desktop, uploaded her profile photo on July 30, 2023, she told me that 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.



July 31

Merhaba. 07:28 ✓✓

Merhaba, ben resepsiyonistiniz Nilu Balpanç, ödülü almaya mı geldiniz? 07:29

Evet 07:29 ✓✓

Aramıza hoşgeldin,  
Lütfen bilgilerinizi verin, çalışmaya katılın,  
görev ve komisyon alın!

1. Tam ad:
2. Cinsiyet:
3. Meslek:
4. Yaş:
5. WhatsApp numarası:
6. Banka hesap numarası:
7. Banka adı:

07:29

1- Rifat Ilgaz  
6- 57359646  
7- [redacted] bank  
4- 51  
2- Erkek  
3- Muhasebe müdürü  
5- 07:31 ✓✓

Lütfen kodunuzu girin 07:32

XY3171 07:32 ✓✓

Gönderildi, sistem ödülleri ödemek için  
10-20 dakika kuyruğa giriyor. Lütfen  
aldığınızda bana bildirin. Satıcı veri  
görevleri daha iyi ödüller alabilir. 07:33

Şimdi sizi görev grubuna katılmaya davet  
ediyorum. Grupta her gün dağıtılan yeni  
görevler var. Para kazanmak için görevler  
yapmaya devam etmek istiyor musunuz?  
Rifat Ilgaz 07:33

Evet 07:34 ✓✓

Sağ üst köşedeki avatarıma tıkladığınızda  
"Kişilere Ekle" seçeneğini göreceksiniz.  
Beni arkadaş olarak ekledikten sonra, sizi  
daha fazla göreve katılmak için gruba  
katılmaya davet ediyorum~ 07:34

Ekledim. 07:35 ✓✓

Şimdi, lütfen [Ayarlar]'a tıklayın, [Gizlilik ve  
Güvenlik]'e tıklayın, girmek için [Davetiye  
İzinleri]'ne tıklayın, [Herkes]'e ve ardından  
Kaydet'e tıklayın 07:35

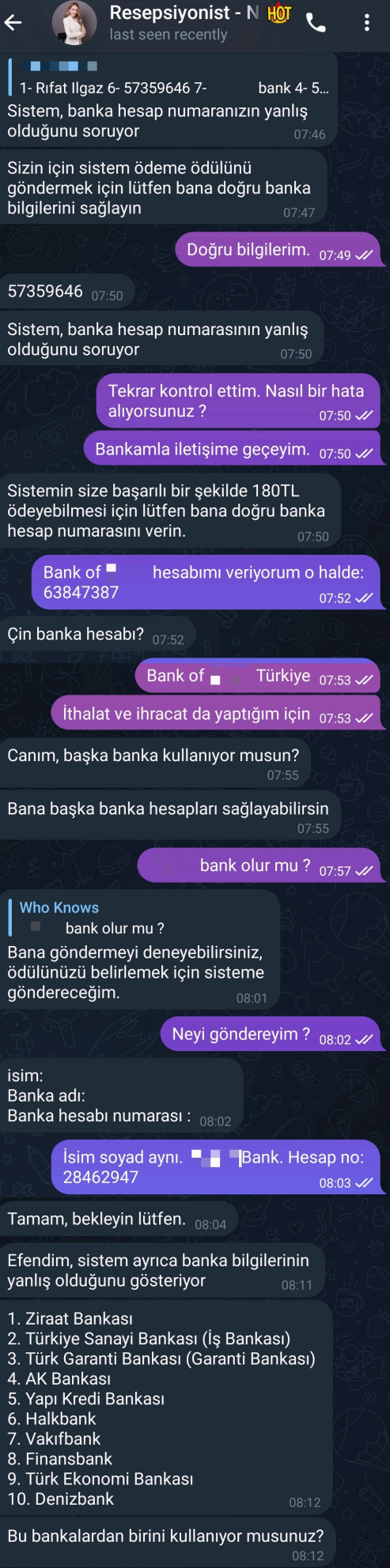
Yaptım. 07:38 ✓✓

Gruba eklendiniz ve grubun diğer üyeleriyle  
iletişim kurabilir, paylaşımda bulunabilir ve  
aynı görevleri gerçekleştirebilirsiniz. 07:39

**Yönetici Rita** ★ Admin  
【Görev 15】 YouTube abonelik görevi  
1. Adım: YouTube'u açın ve [redacted]  
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 07:43

Bir sonraki görev bırakma zamanı 15:00

Gruptaki görevler gerçek zamanlı  
görevlerdir ve kaçırılan görevler talep  
edilemez. 1 görev = 60TL, 10 görev  
tamamlamak = 600TL, ücretleri birlikte  
belirlemek için, anlıyor musunuz? 07:43



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.

Muhsin Sayıcı 09:20 ✓✓

Bir gruba eklendiniz ve grubun diğer üyeleriyle iletişim kurabilir, paylaşabilir ve aynı görevleri yerine getirebilirsiniz 09:21

【Görev 19】 YouTube abonelik görevi

1. Adım: YouTube'u açın ve 【Justin Bieber】
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 16:40 09:23

Çalışma grubu haberlerini takip edin, herkes gibi YouTube'a kemik olma görevini tamamlayın, görev numarası, ekran çıkışı bana gönderin, sizin için puan sayayım. 09:23

180 TL hesabıma gelince yapacağım. 09:24 ✓✓

Elbette 09:25

Dekontu alabilir miyim ? 09:26 ✓✓

Lütfen sabırlı olun çünkü göreve katılan çok fazla kişi var, sistem onları tek tek gönderiyor. 09:27

Efendim, ödülünüzü aldınız mı? 09:52

Hayir 09:53 ✓✓

İşlem detayı

İŞLEM ADI  
EFT BANKALAR ARASI HESABA HAVALE

GÖNDEREN  
888-0053-0157830

GÖNDEREN ADI  
SONER

ALICI  
TR78 70

ALICI ADI  
Muhsin Sayıcı

TUTAR  
180.00 TL

BANKA ADI

REFERANS NUMARASI  
7234267 KÜMÜLATİF: 180.00

TARİHİ  
31.07.2023

SAAT  
16:26:35

DEKONT NO  
000269897

AÇIKLAMA  
"TERS İŞLEM YAPILDI"

10:04

Efendim bu sistem tarafından verilen detaylar, kontrol edin 10:05

Efendim, bakabilir misiniz? 12:11

■ bank'tan mı gönderildi ? 12:30 ✓✓

Komisyon size 3. parti bir aracı kurum tarafından ödenir ve ödeme bankası sistem tarafından rastgele eşleştirilir. Her sistem eşleştirmesi farklı bir hesap olacaktır. 12:31

maaş aldınız mı 12:32

Bugünün görevi bitti, yarın sabah saat 9:00'da görev grubuna dikkat etmeye devam edebilirsiniz, iyi geceler! 13:36



## Yarı Zamanlı Görev Grub



63 members

July 31

Resepsiyonist - Nilu Balpanç added you to this group



Message





## Yarı Zamanlı Görev Grubu

64 members

### Notifications

Off



### Members



MG

Mustafa

last seen recently



Resepsiyonist - Aiyla



Admin

online



Resepsiyonist - Nilu Balpanç



Admin

online



Aysel

last seen recently



Şäljm 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

Admin

last seen recently



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

Admin

last seen recently



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



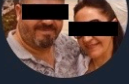
**Serdar**

last seen recently



## Yarı Zamanlı Görev Grubu

64 members



Yarı Zamanlı Görev

last seen recently



Resepsiyonist\_Hatice



Admin

last seen recently



Ceetin

last seen recently



Faruk

last seen recently



receptionist Aleyna



Admin

last seen recently



Kemal

last seen recently



Resepsiyonist- ELMAS



Admin

last seen recently



Resepsiyonist-Eylül



Admin

last seen recently



Resepsiyon-Aysegul Yerar



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.

1. How and where did they get our cell phone numbers?
2. How did they lure their victims?
3. Who owned the accounts used to transfer money?
4. From which country were they running this operation?
5. 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

yeni sunucumuz discord.gg/

Ad Soyad

June 27

Ad Şehir

TC Sorgu

Aile 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

## İNDİRİM



BOT PANEL DİSCORD



ÖZELLİKLER:



Ad Soyad



Ad şehir



Tc sorgu



Aile sorgu



Sülale sorgu



Tc-Gsm sorgu



E-okul vesika sorgu



Ehliyet Vesika sorgu



Seri no Sorgu



İban sorgu



IP sorgu



Random sorgu



Ayak no sorgu

COOL

100% müşteri memnuniyeti ✓

Aylık 150

Haftalık 100



DEVELOPER :



157 15:26



Leave a comment



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 image displays two screenshots of the SOCRadar XTI Threat Hunting interface. The top screenshot shows a search for the mobile phone number 533. The search results are displayed under the 'Exposed Raw Data' tab, showing a list of data points with columns for ID, Date, and Data. A red arrow points to the 'Data' column, which contains a URL: <https://call-center/free-40-m-gsm-tc-sql-geri-donus-hediyesi-55268.html>. The bottom screenshot shows a search for the mobile phone number 533. The search results are displayed under the 'Exposed Raw Data' tab, showing a list of data points with columns for ID, Date, and Data. A red arrow points to the 'Data' column, which contains a URL: <https://premium-database/135m-gsm-tc-to-gsm-database-74306.html>. Both screenshots show a sidebar with navigation options and a right-hand panel with 'Actions', 'Trending Keywords', and 'Recent IP Addresses'.


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.



+1 (321) 359-1339



June 27, 2023

 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Hello! We (randstad) are looking for part time/full time employees - work 1-2 hours a day and earn at least CAD 1500-3000 for 5 days in a row - no experience required and can be done using mobile phone spare time. Salary is settled on the day, age must be at least 20 years old,  
Let me know if you are interested, welcome to join our team. Thanks

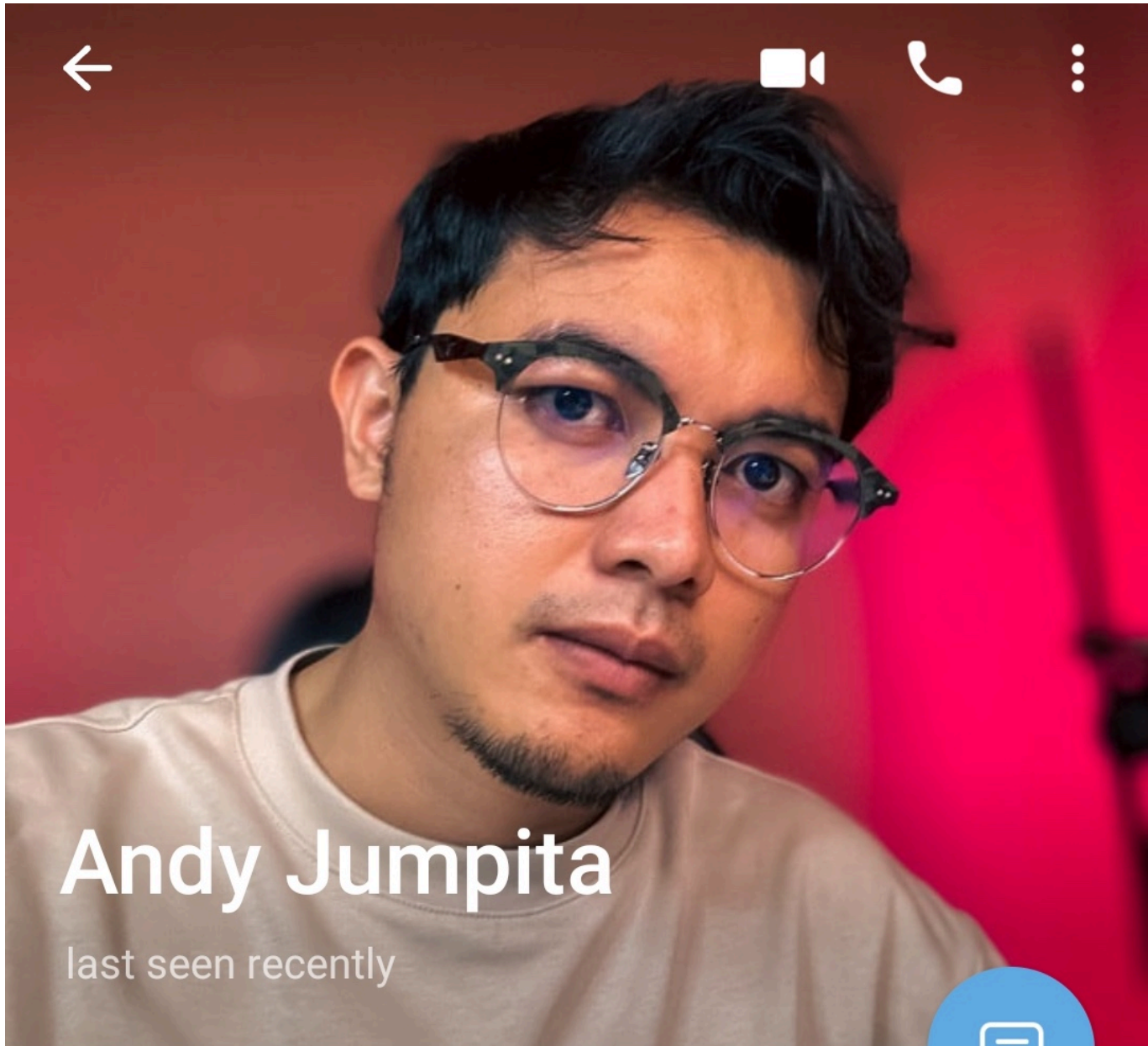
9:37 a.m.



## 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.



Andy Jumpita

last seen recently



Info

Unknown

Mobile

Notifications

On

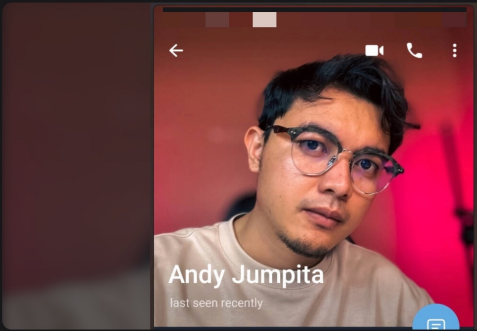


Yandex

Uploaded image x

Search

Web Images Video Translate Disk Mail Ads



Andy Jumpita  
last seen recently

Image size: 694x682

Select crop area

Other image sizes


900x900 100x100

Show all sizes v

Image appears to contain

человек анантья ананд ютубер азиат numan khan фейсбук ду...

Similar images




Similar images

YouTube


Search

Home Shorts Subscriptions Library History Your videos Watch later Liked videos Show more



IS PUNYOO RUNTHINK  
TECH REVIEW TIPS & FACTS  
FRIDAY SUNDAY 8 P M

BANGGOOD BUY




Izz Punyoo  
@izzpunyootv 22.7K subscribers 527 videos


Subscribe Join


I am izz punyoo an architect part 2 and a tech review, in this channel more ... >


HOME VIDEOS SHORTS LIVE PLAYLISTS COMMUNITY CHANNELS ABOUT


Subscriptions

 Cafe Music BGM... (4)

 The Hollywood Fix

 Pitbull

 Dr Eric Cole

 Tech Field Day

Description



I am izz punyoo an architect part 2 and a tech review, in this channel more about techy, daily life style, tutorial, tips tricks and more! stay tune with me

follow me on  
instagram : <https://www.instagram.com/izzpunyoo/>  
facebook : <https://www.facebook.com/punyootv>  
for more inquiries and review do contact our company: [runthinkstudio@gmail.com](mailto:runthinkstudio@gmail.com)  
official page runthink studio

Stats

Joined Aug 4, 2014

3,143,527 views



Yandex  Search

Web Images Video Translate Disk Mail Ads

Image size: 650x636 Reset Select crop area

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

Image appears to contain

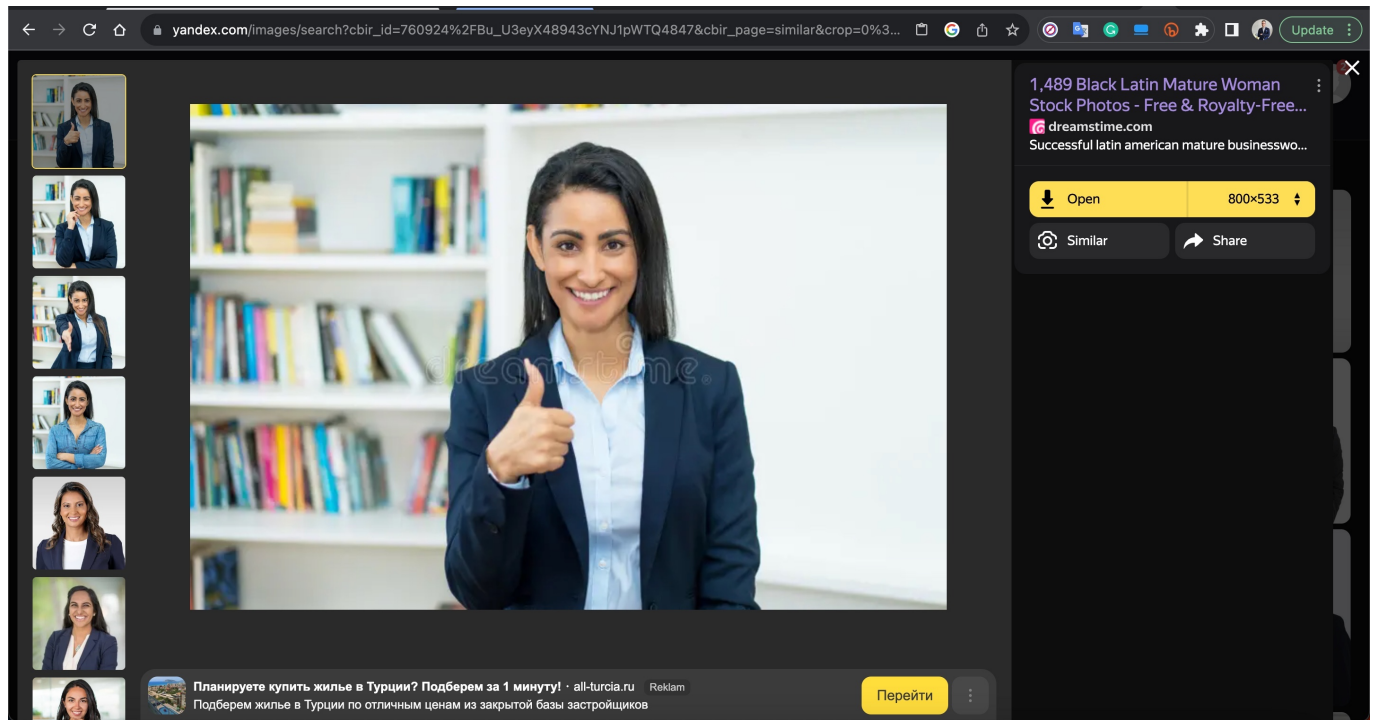
девушка женщина деловая женщина бизнесвумен ...

Text in image

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

Search Translate

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

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.

08:41

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 7 8

Alıcı Bilgileri

Ad Soyad FE\*\*\*\*\* UÇ\*\*\*\*\*

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



SR

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.



Mahmut [redacted]

last seen recently



Info

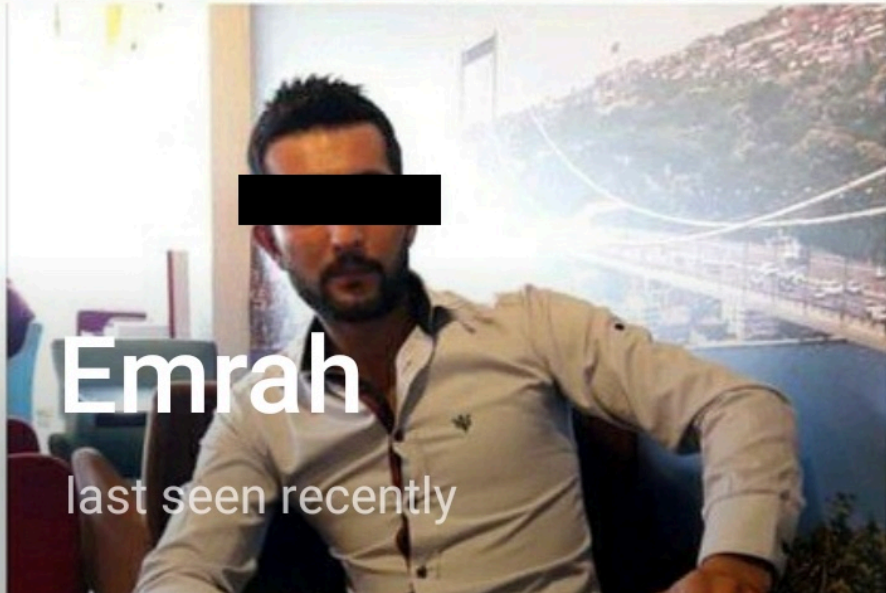
Unknown

Mobile

Notifications

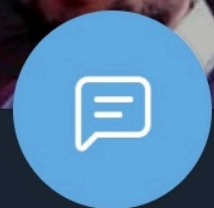
On





Emrah

last seen recently



Info

Unknown

Mobile

Notifications

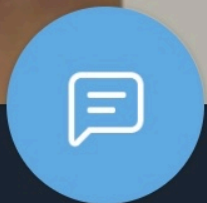
On





Musa

online



Info

@twinklesxv

Username



Notifications

On





**Dallas Balistreri**

last seen recently



**Info**

@Appointj

Username



**Notifications**

On



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 【                     



## Yari Zamanli Görev Grub

... Yönetici Rita is typing



### Pinned Message

【Görev 22】 YouTube abonelik görevi 1. Adım: Y...



**Yönetici Rita** ★

Admin

【Görev 24】 İş verileri görevi  
Gelişmiş Portföy Öğeleri (2-4 sipariş): Satıcı Onaylı: Depozito ödendi.

Tüccar bildirimi: Piyasa talebine göre, döviz spekülasyonuna yardımcı olmak için artık farklı IP'ler alıyoruz, yer sayısı sınırlıdır, lütfen ayrıntılar için resepsiyon görevlisine danışın.

VIP1 500 TL Cashback 650 TL+  
(yeni gelen avantajı)

VIP2 2000 TL Geri Ödeme 2600 TL+ (grup karı)

VIP3 3000 TL Geri Ödeme 3900 TL+ (grup karı)

VIP4 6000 TL Geri Ödeme 7800 TL+ (grup karı)

VIP5 8000 TL Cashback 10400 TL+ (grup karı)

VIP6 12000 TL Geri Ödeme 15600 TL+ (grup karı)

VIP7 18000 TL Geri Ödeme 23400 TL+ (grup karı)

VIP8 25000 TL Geri Ödeme 32500 TL+ (grup karı)

VIP9 30000 TL Geri Ödeme 39000 TL+ (grup karı)

VIP10 60000 TL Geri ödeme 78000 TL+ (grup karı)

Kontenjan sınırlıdır, önce gelen alır, kota istemek için resepsiyonistle iletişime geçin \* Ek 3000 TL ödül almak için art arda 4 iş verisi görevini tamamlayın. Bir sonraki görev bırakma zamanı 18:40

11:20



**Kelsey**

K

Bu göreve nasıl başvurulur?

← 1 11:20

**Çetin Çapraz**

**Kelsey**

Bu göreve nasıl başvurulur?

Başvurmak için resepsiyon görevlisiyle iletişime geçin

11:20

ÇE



## Yari Zamanli Görev Grub

110 members



### Pinned Message

【Görev 22】 YouTube abonelik görevi 1. Adım: Y...



UL

tamamıadım

11:27

### Unread Messages



**Aurora Raynor**

Evet kontenjana kendimiz başvurabiliriz, kendimize inanmalıyız.

11:28

AR

**Yönetici Rita** ★

Admin

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 resepsiyonist ile iletişime geçerek 3000 TL ek ödül alabilirsiniz.

11:28

İş görevleri, ek ödüller:

1. Aynı gün 30 görev tamamlayın ve ek 5000TL görev ödülü kazanın.

2. Aynı gün içinde 4 iş verisi görevini tamamlayın ve ek 3000TL görev ödülü kazanın.

Yukarıdaki ekstra görev ödülleri için lütfen resepsiyon görevlisi ile iletişime geçin.

11:28





## Yari Zamanli Görev Grub

110 members



### Pinned Message

【Görev 22】 YouTube abonelik görevi 1. Adım: Y...



B

**Boris**

%30 mu? Gerçekten mi? 2 11:09

**Yönetici Rita** ★

Admin

Bir şeyi anlamadıysanız, daha fazla ayrıntı için lütfen ilgili resepsiyon görevlisiyle iletişime geçin. 11:09

**Çetin Çapraz**

Artık fakir olmak istemiyorum. Burada çok para kazanmak istiyorum. 2 11:09

**Bennett**

Ama para kazanmak için çok çalışmalıyız, para olmadan yapamayız. 11:09

**Çetin Çapraz**

Artık fakir olmak istemiyorum. Burada... Ne kadara başvurdu? 11:10

**Sylvester Schumm**

**Boris**

%30 mu? Gerçekten mi? Tabii ki, kota başvurusunda bulunmak için resepsiyonistle iletişime geçmek için zaman ayırın. 11:10

141



Message





## 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

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.

13:15

**Hasanstoi**

harika.. görevleri bitirdim sayılır💕

13:16

**Aurora Raynor**

Son görev yayınlandı ve ödülü  
tamamladıktan sonra alabilirsiniz.

13:16

AR

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	Alacaklı Hesap No	: TR69 0006 4000 0014 3930 2547 08
Borçlu Hesap No	: 888-0444-0098968		Karşı Şube	: 0952 - HAZ. VE SER. PİY. OPR. BÖL.
Müşteri No	: 0016276708		VKN/Vergi Dairesi	:
VKN/Vergi Dairesi	: 22787607470		Adı Soyadı/Unvan	: Fatma
Adı Soyadı/Unvan	: BEYTULLAH		Adres	:
Adres	: KORDI İPLİK ÇAKILLI KASABASI KIRKLARELİ			
TR77000460044488800098968				
<b>TUTAR BİLGİLERİ</b>				
MEVDUAT	5008.03 TL		0.00 TL	
ŞEH	0.00 TL		5000.00 TL	
GECEFT KOMİSYON	0.00 TL		7.65 TL	
GECEFT BSMV	0.00 TL		0.38 TL	
TOPLAM			5008.03 TL	
YALNIZ BEŞBİN SEKİZ 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 zamanı

19:20

★ 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

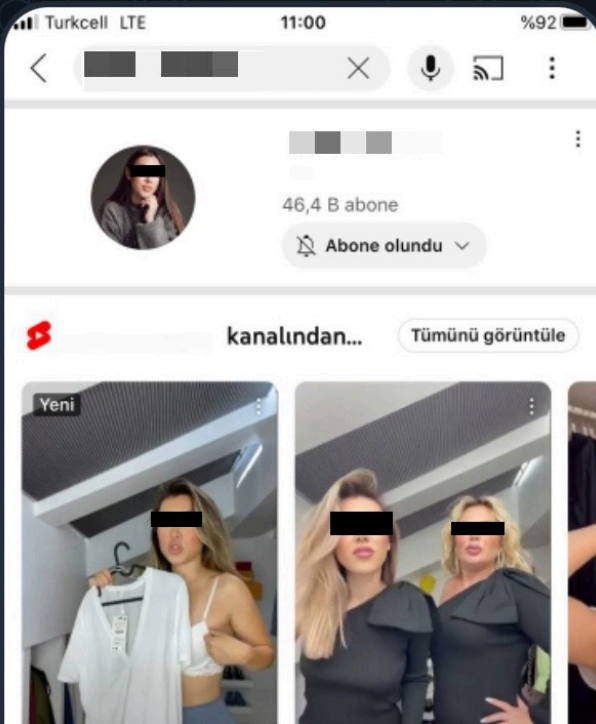
1. Adım: YouTube'u açın ve 【】  
arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.



Bir sonraki görev bırakma zamanı  
11:20

04:00

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



HT

286





## Yari Zamanli Görev Grub

109 members

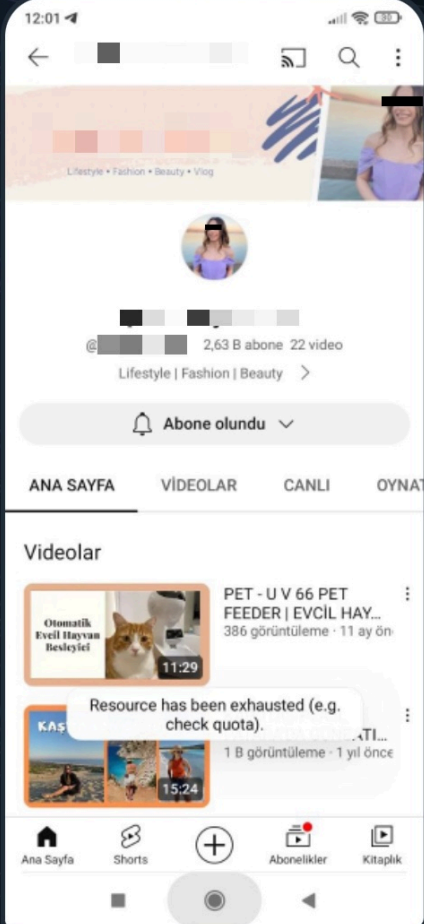


Abonelik eklendi

AA

G8

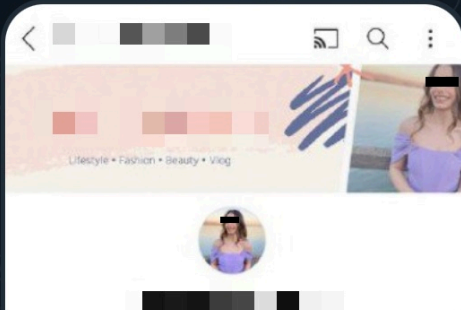
05:01



K

G8

05:01



A

206



Message





## Yari Zamanli Görev Grub

109 members



### Pinned Message


【Görev 13】 YouTube abonelik görevi 1. Adım: Y...



**Yönetici Rita** ★

Admin

### 【Görev 9】 YouTube abonelik görevi

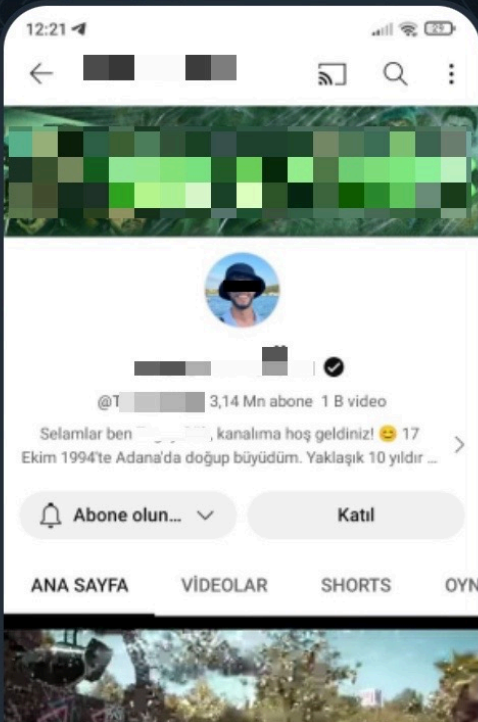
1. Adım: YouTube'u açın ve  arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.



Bir sonraki görev bırakma zamanı  
12:40

05:21

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



K

183



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  
[Banka Adı]

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

Düzenleyen Şube : 7777 - K DİREKT MOBİL CEP  
Borçlu Hesap No : 888-0444-0098968  
Müşteri No : 0016276708  
VKN/Vergi Dairesi : 22787607470  
Adı Soyadı/Unvan : BEYTULLAH  
Adres : KORD İPLİK ÇAKILLI KASABASI KIRKLARELİ

ALICI BİLGİLERİ

Alacaklı Hesap No : TR89 0006 4000 0014 3930 2547 08  
Karşı Şube : 0952 - HAZ. VE SER. PİY. OPR. BÖL.  
VKN/Vergi Dairesi :  
Adı Soyadı/Unvan :  
Adres :

TR77000460044488000098968

TUTAR BİLGİLERİ

MEVDUAT	3008.03 TL	0.00 TL
ŞCH	0.00 TL	3000.00 TL
GECEFT KOMİSYON	0.00 TL	7.65 TL
GECEFT BSMV	0.00 TL	0.38 TL

TOPLAM  
YALNIZ ÜÇBİN 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



Şubersiz 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	MASRAFI 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.



## Yarı Zamanlı Görev Grub

... Esra Sayın Karaöz is typing



### Pinned Message

【Görev 18】 İş verileri görevi Gelişmiş Portföy Ö...



önceden iletişime geçmediğim için.

08:58

### Unread Messages



Esra !

Anaparayı ve kârı çoktan aldım.

← 2 09:00



Umut

Esra

Anaparayı ve kârı çoktan aldım.

Gerçekten iadeyi yapıyorlar mı? 09:01

1903 basaran 1903

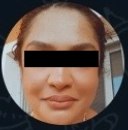
Ya sacmalamayın :) 09:01

Yaparlar mı 09:01

Kandiriyorlar 09:01



Cikin 09:01



Esra

Umut Bal

Gerçekten iadeyi yapıyorlar mı?

Daha yapmadın mı? 09:01



Umut

Ben inanmadığım için yapmadım

09:01

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.

14:02



Alarm, Wi-Fi, 4G, and battery level %85.



Normal telefonda  
kamera boşluğu  
olmaz.



Kim o posta yöneticinizden sesli  
diyafonunuzu hemen Audio görüntülü

0:06

Türkçe bilen biri videolar için  
altyazı genelde açmaz.

tv ar



emi

Ailenizin Güvenliği İçin Sesli Diafonları Değiştirme  
Zamanı

**Reklam** • Audio Elektronik A.Ş.

[Siteye git](#)



3,49 B abone

Abone olundu

Telefonda bu  
kaydırma çubuğu  
görünmez.

ndan en yeniler



Ana Sayfa

Shorts



Abonelikler

Kitaplık



14:21

3G 11



3G ?



@ 1,85 B abone 37 video

Merhabalar Arkadaşlar Bu Kanalda Oyun,Film,Dizi Vb. Birsürü Şey Olucak.İsmimiz Gibi Daha Ne Olsun

Abone olundu

Ana Sayfa Videolar Oynatma Listeleri Topluluk

## FİMLERİN GİZLİ KAHRAMANLARI



FİMLERİN GİZLİ KAHRAMANLARI / 150 DUBLAJ SANATÇISI / SESLENDİRİCİLER /...

82 B görüntüleme · 3 yıl önce

Abonelik eklendi



Turk Telekom



14:01

%88



3,49 B abone 224 video

MERHABA

TV KANALIMIZA HOŞ  
GELDİNİZ



Abone olundu



ANA SAYFA

VIDEOLAR

SHORTS

Videolar



Gidilesi,...  
Kardele...



Ana Sayfa



Shorts



Abonelikler



Kitaplık



tv



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

19:41



Kelimelik • şimdi

**Kelimelik**

Bey@z Zambak ile yeni oyun açıldı

MUZIK grubu



@

23,5 B abone



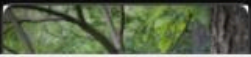
Abone olundu



Mix -

YouTube

## Müzik albümleri



Abonelik eklendi



Kismet 1. Bölüm



İzlemeye devam...



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

OYNATILAN

## Videolar



10:03

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

Abonelik eklendi





@PUSKEVIT 3,73 B abone 96 video

PUSKEVİT İÇİN ABONE OL! >

Abone olu... ▾

Katıl

ANA SAYFA

VİDEOLAR

SHORTS

DYK



WHATSAPP Kişiler Görünmüyor?  
(Dual WhatsApp)



Ana Sayfa



Shorts



+



Aboneiler



Kitaplık



Yari Zamanli Görev Grub

109 members

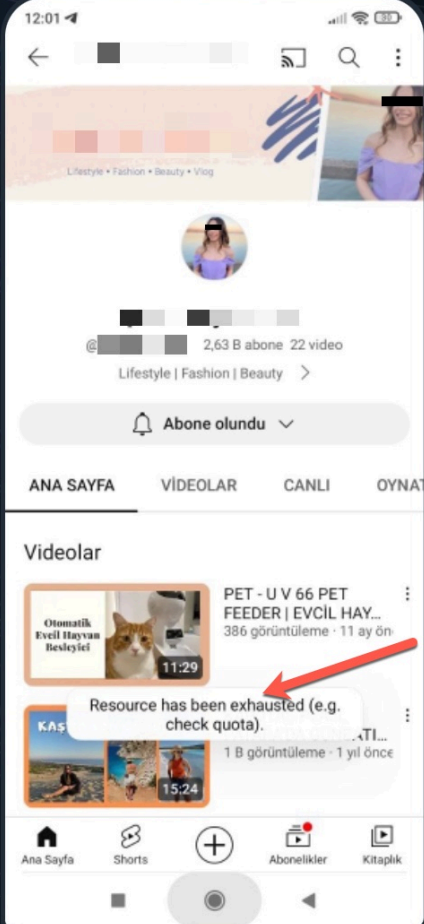


Abonelik eklendi

AA

G8

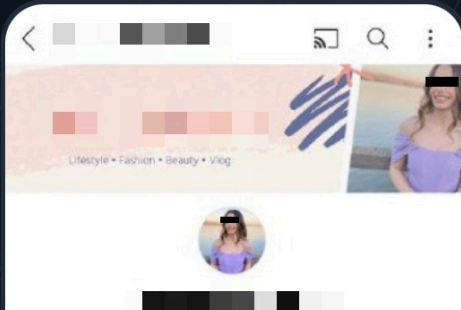
05:01



K

G8

05:01



A

206



Message



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.

last seen recently

vip kanalına alır mısın ?

Dört tüccar görevini tamamladıktan sonra  
VIP kanalına katılabilirsiniz. 13:23

tamamladım zaten 13:23 ✓✓

Bu abonelik görevidir 13:24

Grupta her gün dört tüccar görevi  
yayınlanacak 13:24

fark etmedin mi 13:24

satın mı almam lazım ? 13:26 ✓✓

Evet 13:27

almak istiyorum o halde 13:27 ✓✓

Bugünün görevi bitti 13:27

satın almanın yolu yok 13:27

Yarın sabah 9:00'da görev grubunu takip  
edebilir ve katılabilirsiniz. 13:28

satın almak için ödemeyi nasıl  
yapabiliyorum ? Ona göre hazırlayayım  
yarın için. 13:28 ✓✓

Ön ödeme tutarına bağlı olarak, gelirin  
değişecektir. Geri ödemeler 30 dakika  
içinde yapılabilir. Ne kadar çok ön ödeme  
yaparsanız, o kadar çok komisyon  
kazanırsınız 13:29

Gelişmiş Portföy Öğeleri (2-4 sipariş):  
Satıcı Onaylı: Depozito ödendi.  
Tüccar bildirimi: Piyasa talebine göre,  
döviz spekülasyonuna yardımcı olması için  
artık farklı IP'ler alıyoruz, yer sayısı sınırlıdır,  
lütfen ayrıntılar için resepsiyon görevlisine  
danışın.

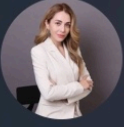
VIP1 500 TL Cashback 650 TL+ (yeni gelen  
avantajı)  
VIP2 2000 TL Geri Ödeme 2600 TL+ (grup  
karı)  
VIP3 3000 TL Geri Ödeme 3900 TL+ (grup  
karı)  
VIP4 6000 TL Geri Ödeme 7800 TL+ (grup  
karı)  
VIP5 8000 TL Cashback 10400 TL+ (grup  
karı)  
VIP6 12000 TL Geri Ödeme 15600 TL+  
(grup karı)  
VIP7 18000 TL Geri Ödeme 23400 TL+  
(grup karı)  
VIP8 25000 TL Geri Ödeme 32500 TL+  
(grup karı)  
VIP9 30000 TL Geri Ödeme 39000 TL+  
(grup karı)  
VIP10 60000 TL Geri ödeme 78000 TL+  
(grup karı) 13:29

bunlar yetki şartlarıdır 13:29

ödemeyi kredi kartı ile mi yapabiliyorum ?  
13:29 ✓✓

Geçici olarak kredi kartı ödemesi kabul  
edilmemektedir, sadece banka ödemesi  
13:30

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. :)



Resepsiyonist - N **HOT**

... typing



Nasıl ödeme yapabilirim ? 06:49 ✓✓

Önemli değil, ne kadar miktarı seçersiniz?

06:52

Giriş olan 500 TL 06:55 ✓✓

500 TL yatırıncı ne kadar kazanabilirim ?

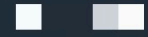
06:56 ✓✓

500 650 kazanabilir 07:11

Tamam 07:12 ✓✓

Ödeme bilgilerini alabilir miyim ? 07:17 ✓✓

Lütfen bekleyin, sizin için getiriliyor 07:20



TR39 [redacted] 03  
Osman [redacted]

07:21

transfer miktarı:500

\*Ödeme seçimi HIZLI havale, EFT seçimi geçersiz

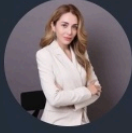
\*Yorum yapmaya gerek yok

\*Havaleyi tamamladıktan sonra, lütfen havalenin ekran görüntüsünü ve ödeyenin adını sağlayın

07:21

Transferi 15 dakika içinde tamamlamak için, süresi dolmuş ve geçersiz, tutar daha fazla veya daha az olamaz

07:21



Resepsiyonist - N **HOT**

last seen recently



08:14 ✓✓

kullanabilirsiniz 08:17

Denedim olmadı ikisinde de. Sizin hesapta problem var.

08:18 ✓✓

lütfen bana ekran görüntüsü sağlayın 08:20

Ne öneriyor? 08:20

Diğer herkes aktarımı normal şekilde tamamlayabilir 08:20

Çağrı merkezini arayın diyor, ekran görüntüsü aldirtmıyor uygulama. 08:20 ✓✓

Her iki banka da aynı mı? 08:20

Evet. 08:20 ✓✓

"Güvenlik politikası gereği ekran görüntüsü alınmamaktadır." diyor. 08:21 ✓✓

Tamam, senin için yeni bir sistem hesabı almaya çalışacağım 08:21

■ bank  
Handan ■ ■  
TR57 ( ■ ■ ■ ■ ■

90 08:23

Bu bankaya 500 ödemeyi deneyin 08:23

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;

6. They contact the victim using a foreign number on WhatsApp and take them to a Telegram group.
7. 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.
8. 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.
9. The scammers use accounts opened in more than one bank for money transfers.
10. 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.

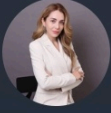
## From which country were they running this operation?

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.



Resepsiyonist - N **HOT**

last seen recently



hangi banka ? 09:55 ✓✓

■ bankası 10:14

■ ■ i bankası uygulaması şu hatayı veriyor, sebebi konusunda fikriniz var mı ?  
[bit.ly/123456789](https://bit.ly/123456789) 10:15 ✓✓

Hiçbir fikrim yok 10:16

Sizin için kontrol edebilmem için bana bir ekran görüntüsü göndermeniz gerekiyor

10:17

ekran görüntüsünü buradan gönderemedim, güvenlik politikası hatası veriyor o nedenle image sitesine yükledim.

10:17 ✓✓

Benim için fotoğraf çekmek için diğer cep telefonlarını kullanabilirsiniz.

10:19

Başka telefonum yok, [bit.ly/123456789](https://bit.ly/123456789) buradan bakıp söyleyebilir misiniz ?

10:19 ✓✓

Para transferi esnasında bu hatayı veriyor.

10:19 ✓✓

Lütfen henüz ödeme yapmayın 10:20

Tamam 10:20 ✓✓

Sistem hesabı kotası dolu 10:21

Hazır olduğunuzu onayladıktan sonra, en son hesaba yeniden başvurmak için benimle iletişime geçin.

10:21

grep [REDACTED].jpeg access.log

```
171.102.239.190 - - [05/Aug/2023:14:19:45 +0000] "GET /images/_..jpeg HTTP/1.1" 200 30764 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gec
ko) 007scrm/4.58.8 Chrome/108.0.5359.215 Electron/22.3.18 Safari/537.36"
```

socradar.io/labs/ioc-radar/171.102.239.190

Company Partners Contact Free Access

# SOCradar LABS

Dark Web Report

IOC Radar

Country Threat Landscape Report

Industry Threat Landscape Report

## IOC Radar

Search on the IOC Radar. Enter domain, ip address or hash...

171.102.239.190

Tags: -

Risk Rating: [Progress Bar]

ASN Name: 38082

ASN Description: IIT-TIG-AS-AP True International Gateway Co., Ltd., TH

ASN Subnet: 171.102.239.0/24

ASN Raw: 171.102.0.0 - 171.102.255.255 true-cor...

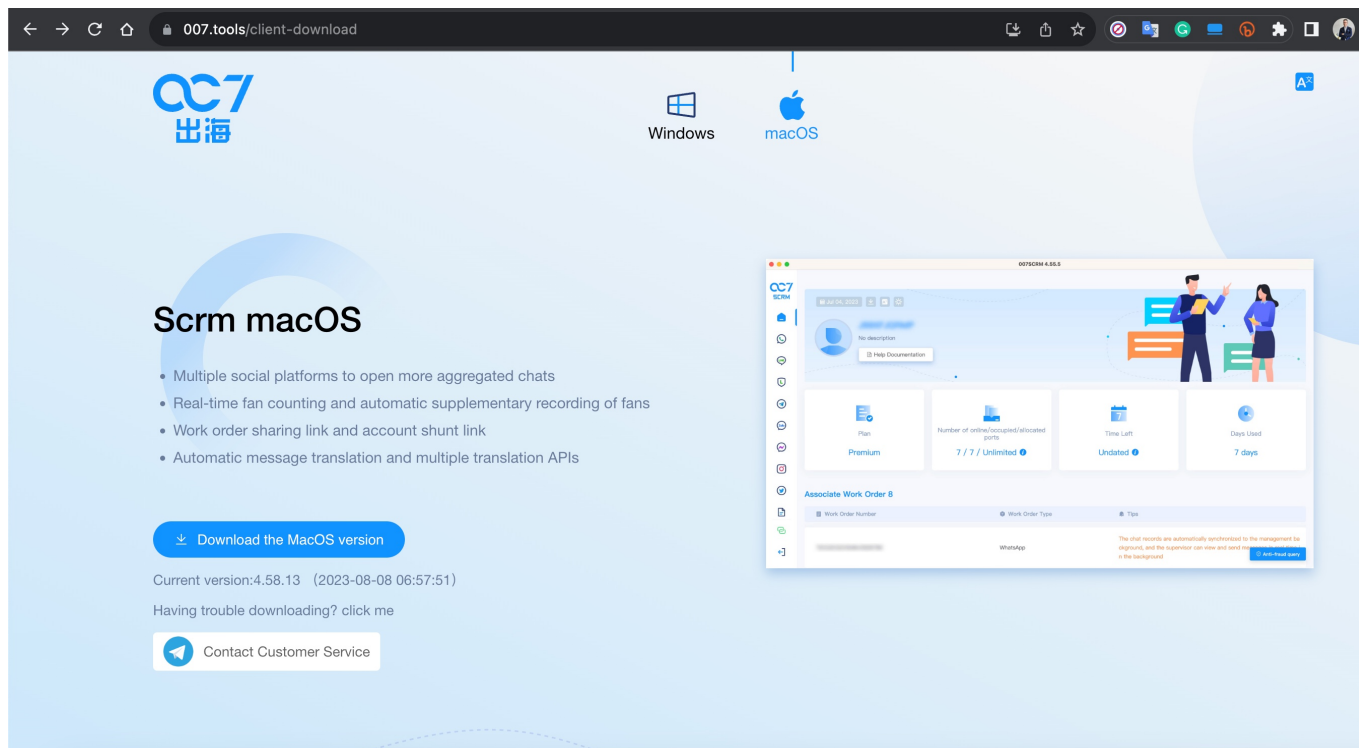
Latitude: 16.71667 Longitude: 98.56667

Country Code: TH Region Name: Tak

Feed Source Finding Dark Web Finding Penalty Reason Recent References

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. :)



Karakalpak

last seen recently



August 4

Selam 11:31 ✓✓

Merhaba 11:38

Nasılsın ? 11:38 ✓✓

İyiyim 11:38

Yarın zamnanlı görev grubundaki görevini tamamladın mı ? 11:40 ✓✓

4 tüccar görevini tamamladım 11:41

Nagadar gazandın ? 11:41 ✓✓

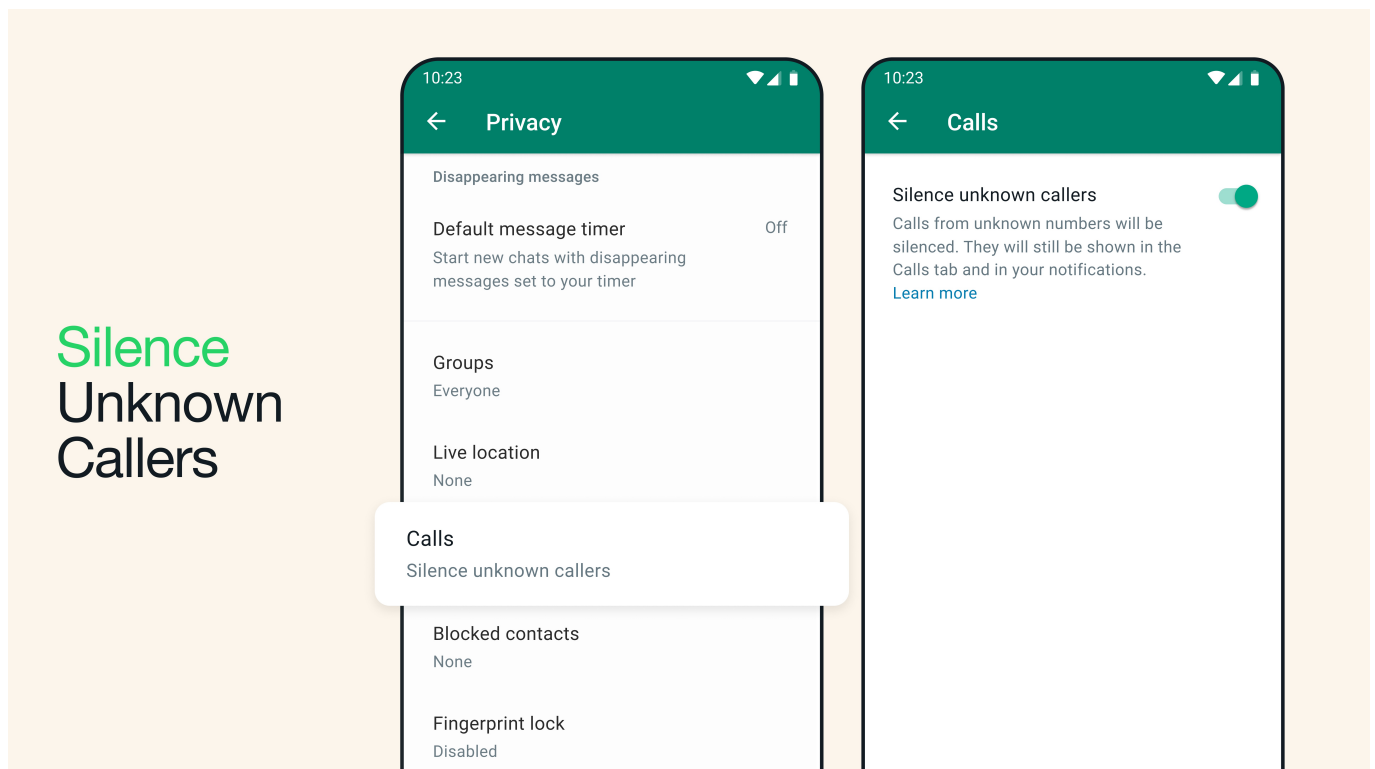
Evet 11:46

Nagadar ? 11:50 ✓✓

# 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.