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

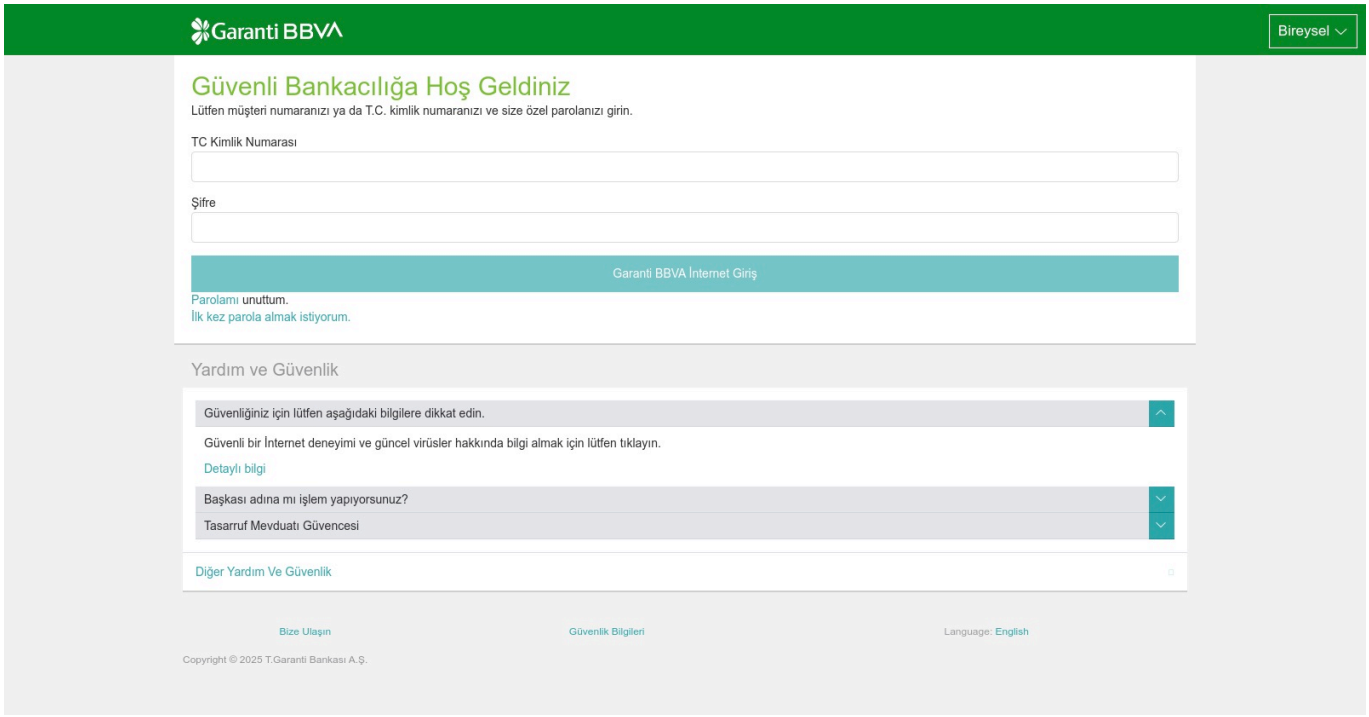
Introduction

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.

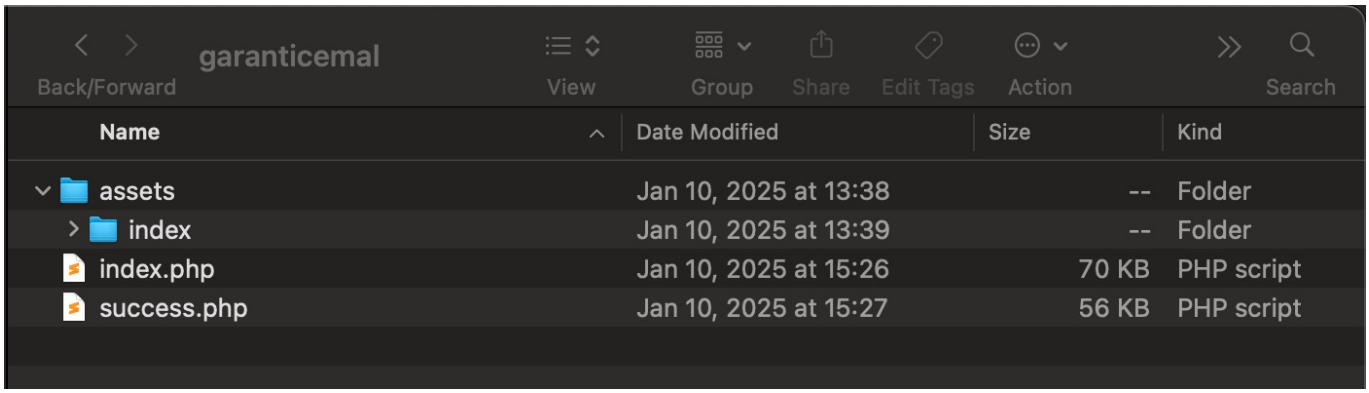
The story of this article began almost a year ago during a security research I conducted, when I encountered a threat actor who did not hesitate to use his real first and last name on phishing websites targeting Garanti BBVA customers, as well as on his Telegram profile – perhaps never considering that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

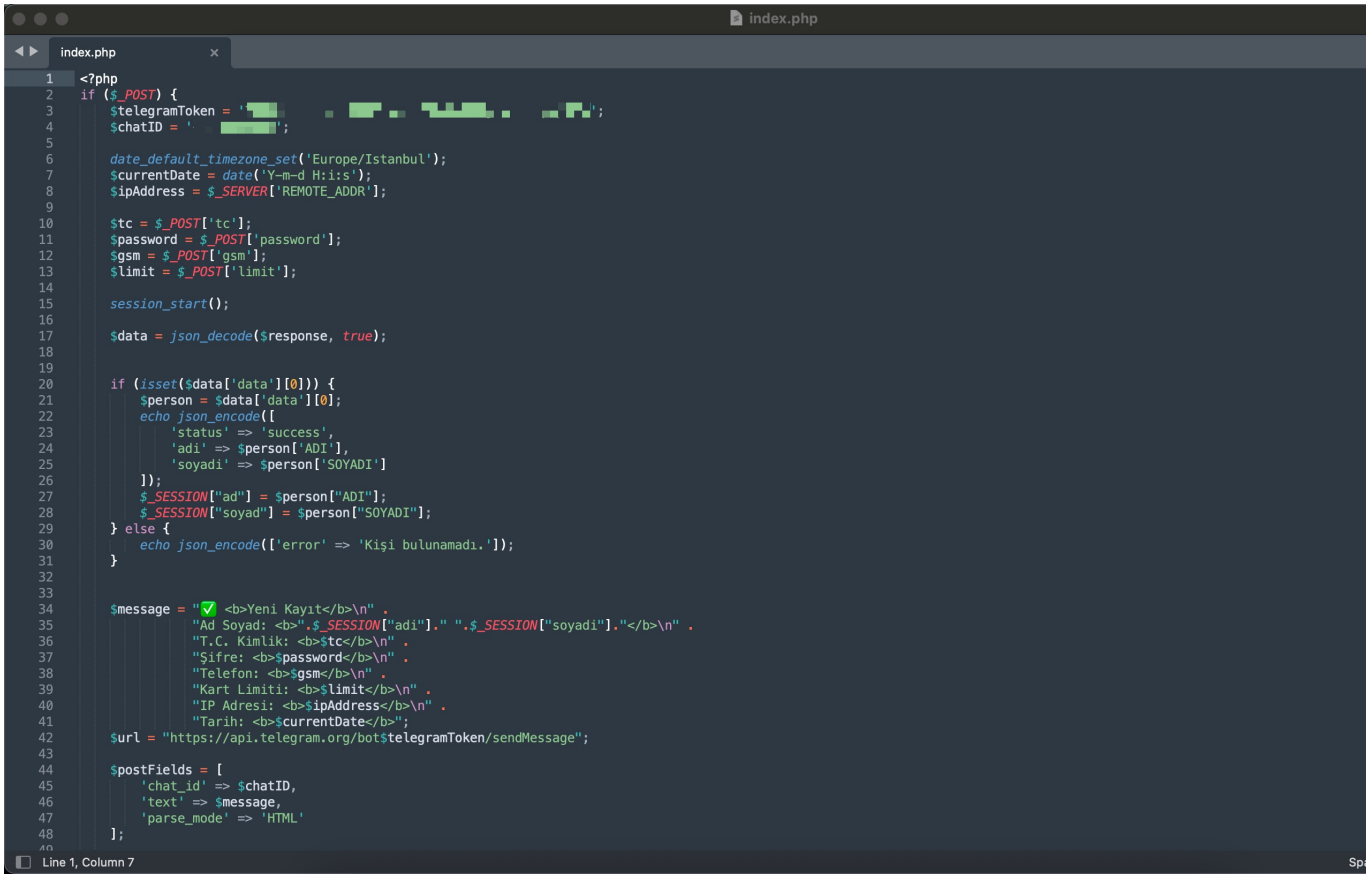
Threat Hunting

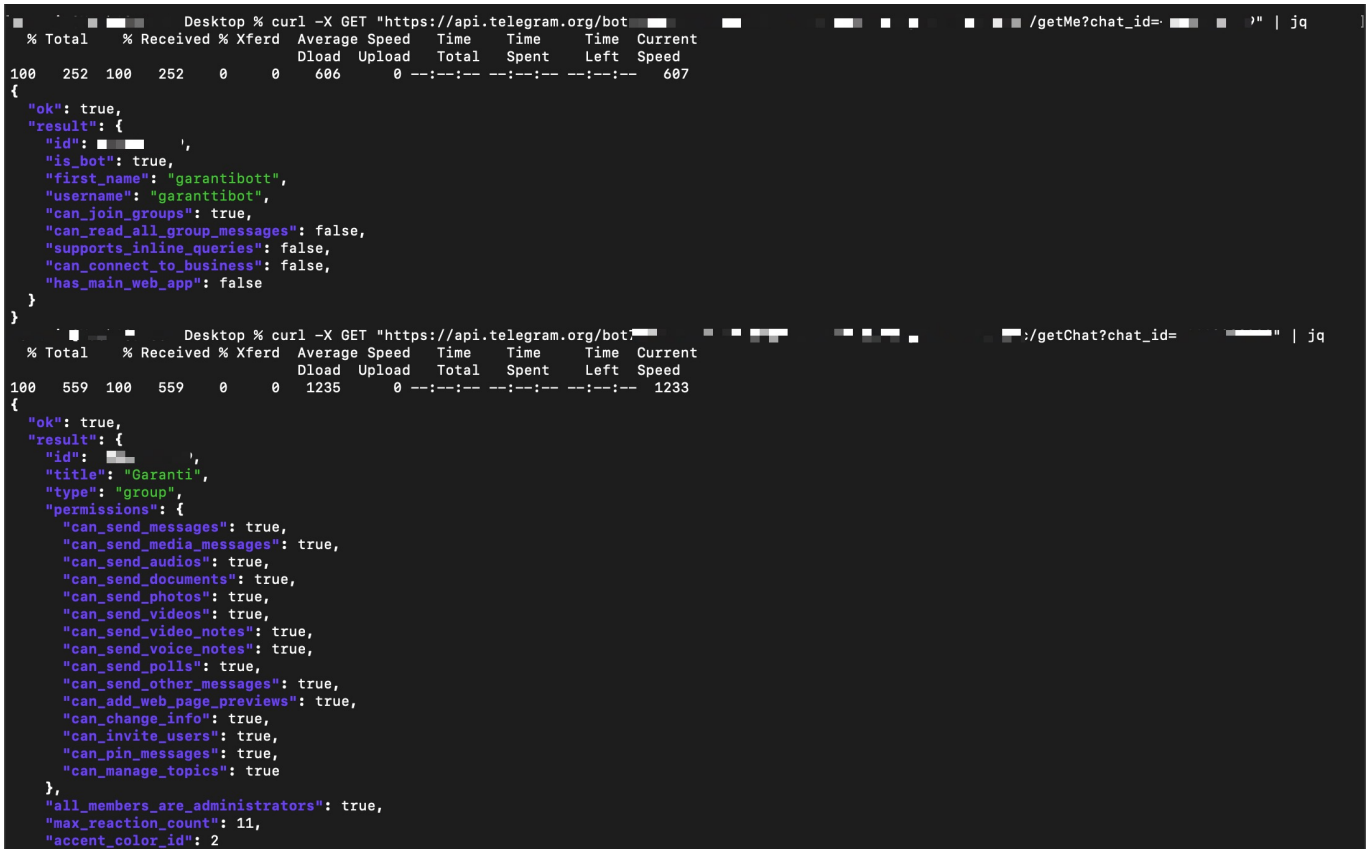
While conducting threat hunting on phishing sites detected on the SOCRadar Cyber Threat Intelligence Platform, three domain names starting with grnt- caught my attention: grnt-avantaj1.xyz, grnt-avantaj2.xyz, and grnt-avantaj4.xyz.



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.



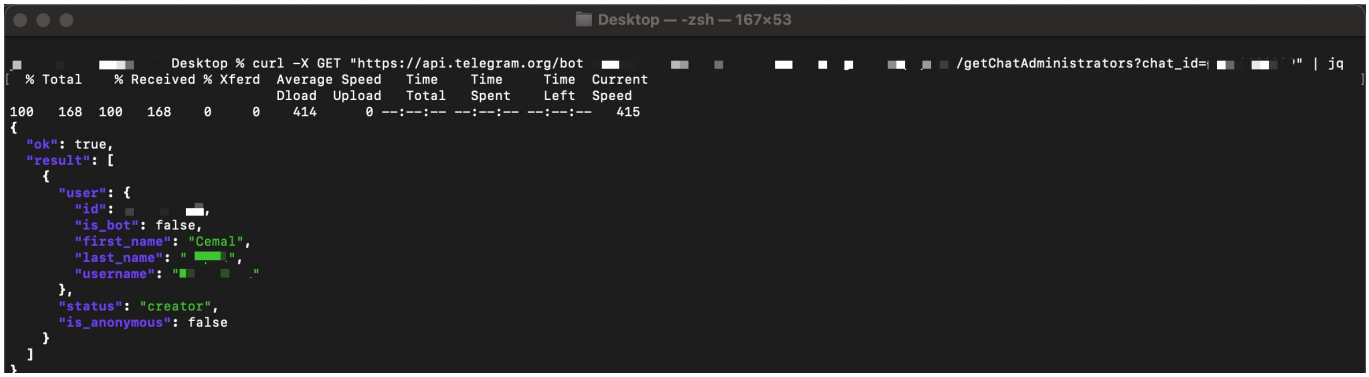


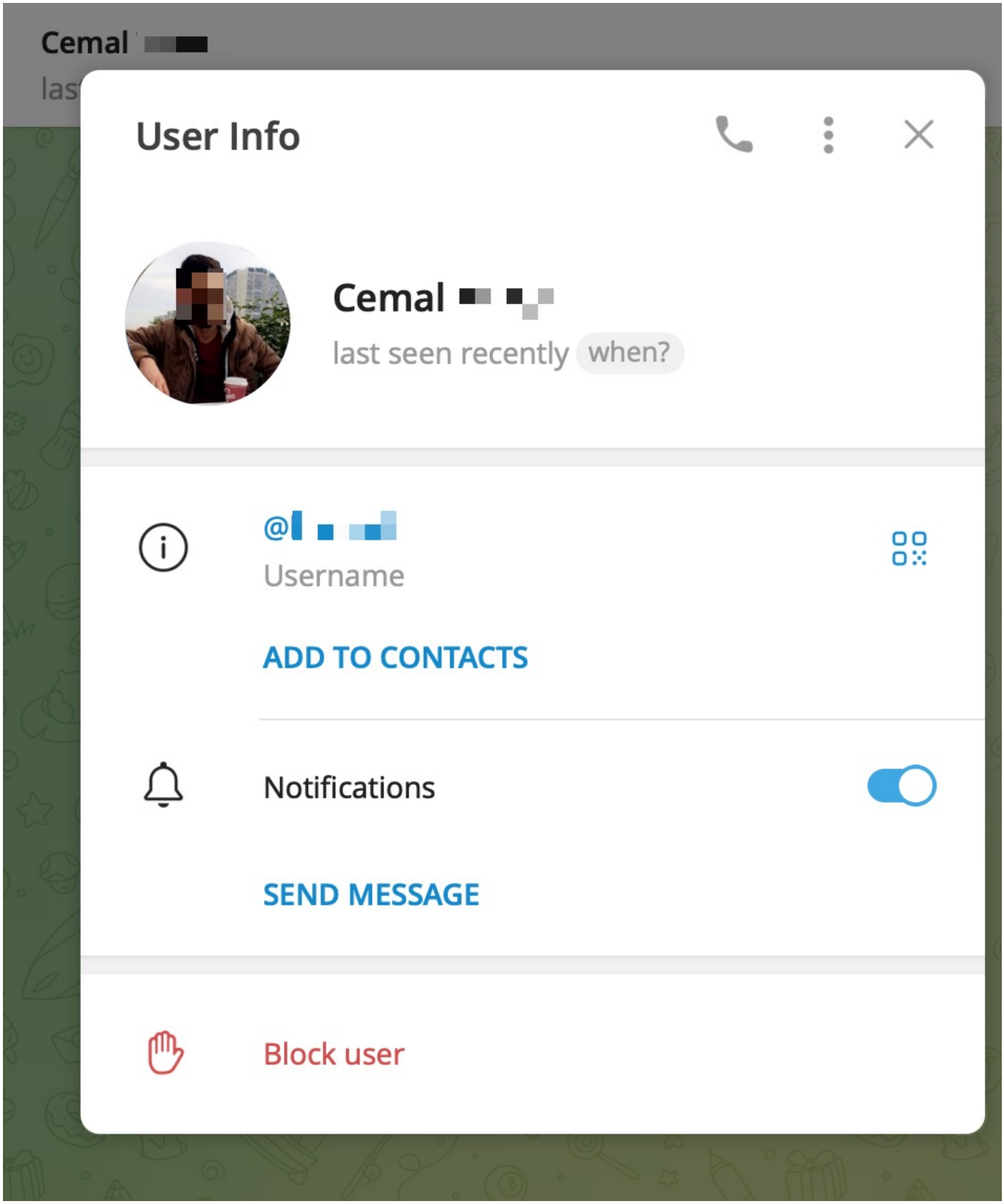


Through the token, I reached Cemal’s Telegram account and encountered his surname information and a possible profile photo. My first reaction was to think that what I was seeing must be fake. Because if I could access this

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.




Cemal
User Info
Cemal
last seen recently
when?
Username
ADD TO CONTACTS
Notifications
SEND MESSAGE
Block user

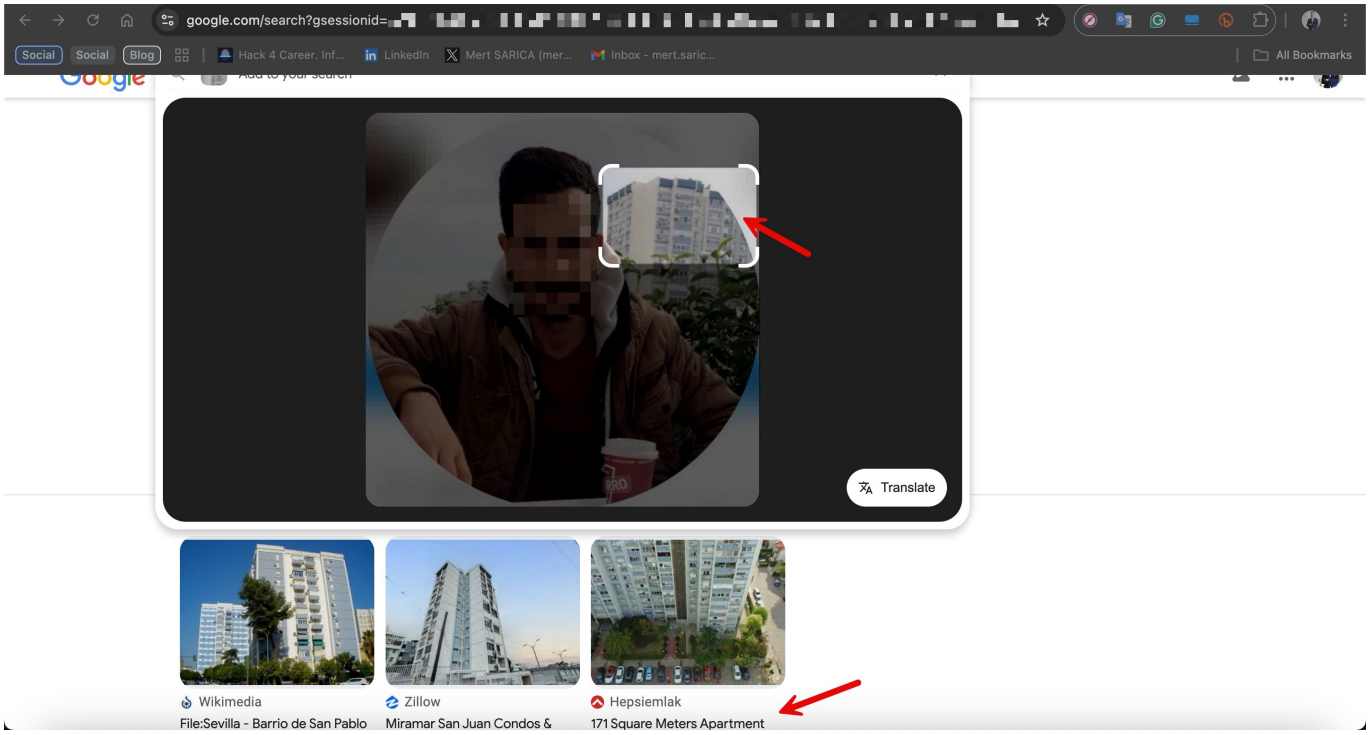


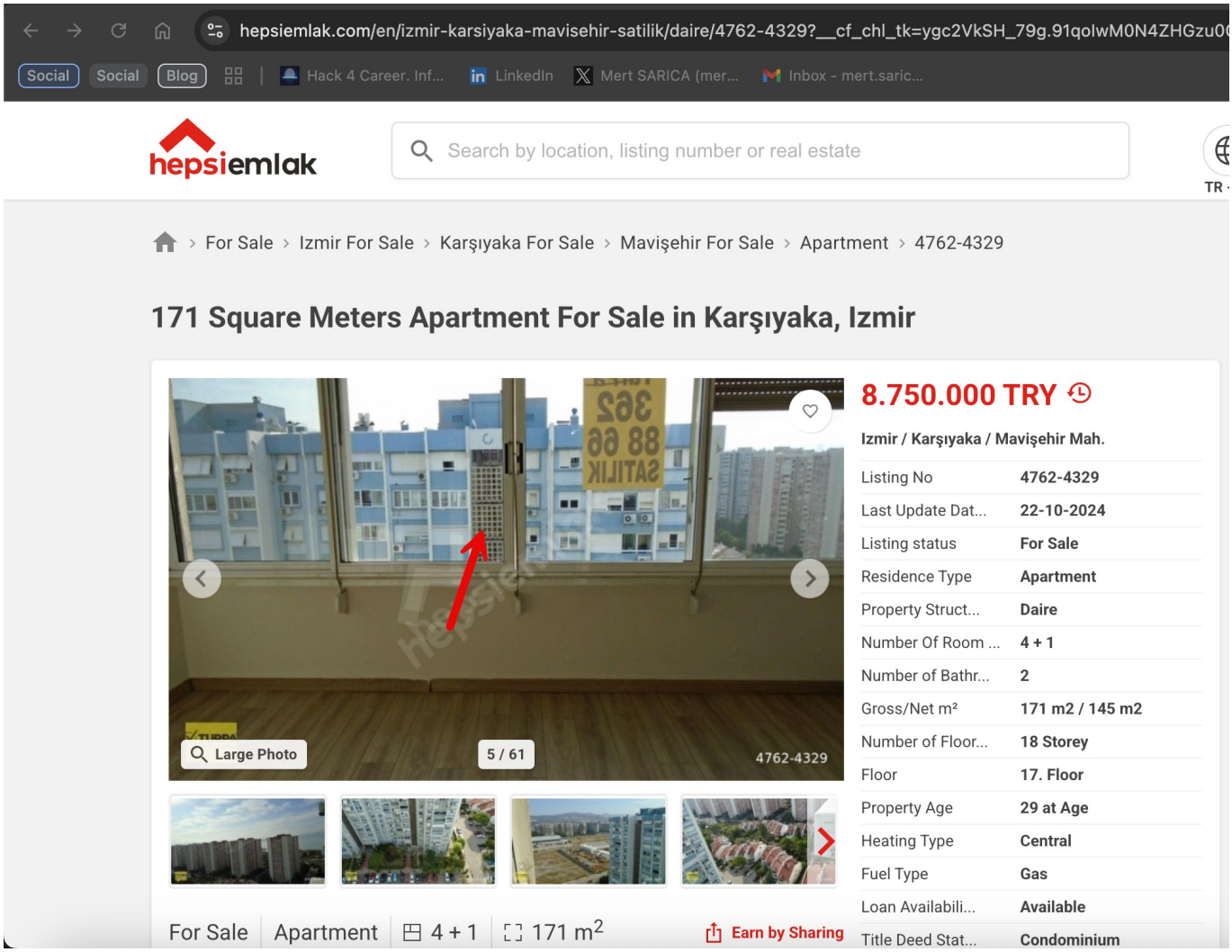
Was Cemal a threat actor unconcerned about being caught, or one who simply believed he could not be identified from the information crumbs he left behind? To understand this, I either had to contact Cemal directly and rely on his responses, or attempt to indirectly answer this question by conducting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

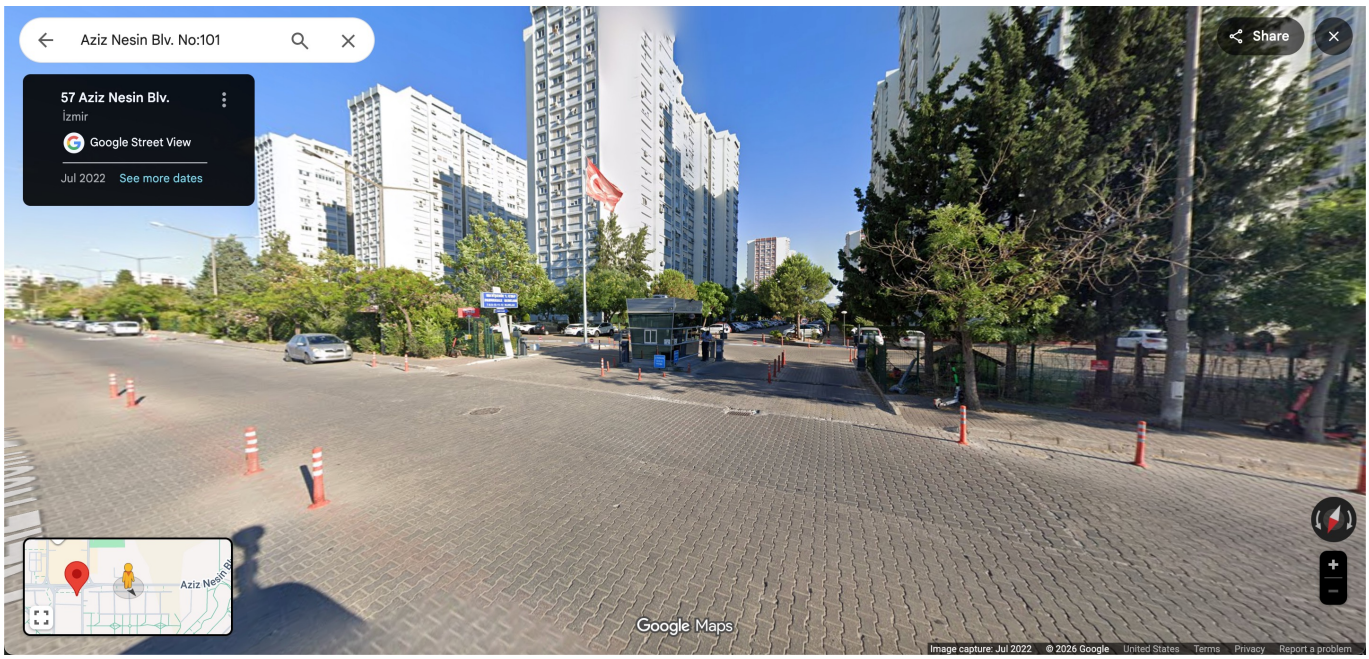
First Clue

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.





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.

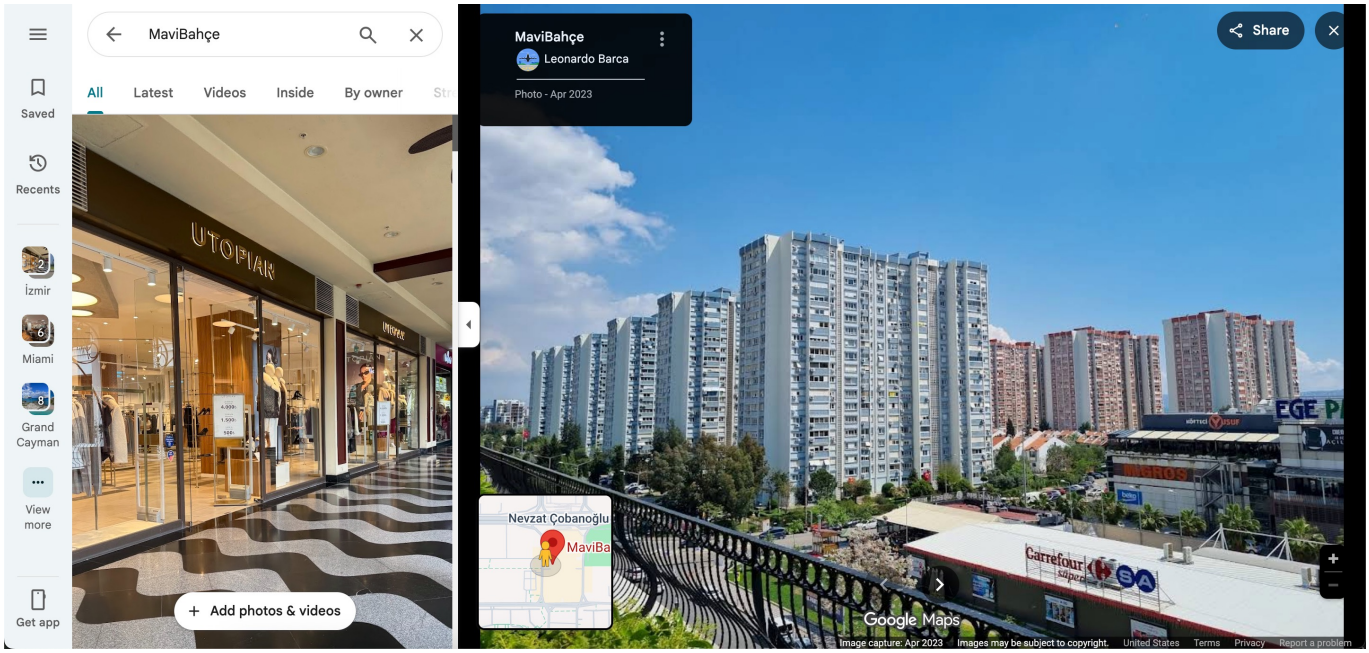
After virtually exploring the surroundings of the Mavişehir Pamukkale blocks via Google Maps and its Street View feature, I was able to locate the exact building.



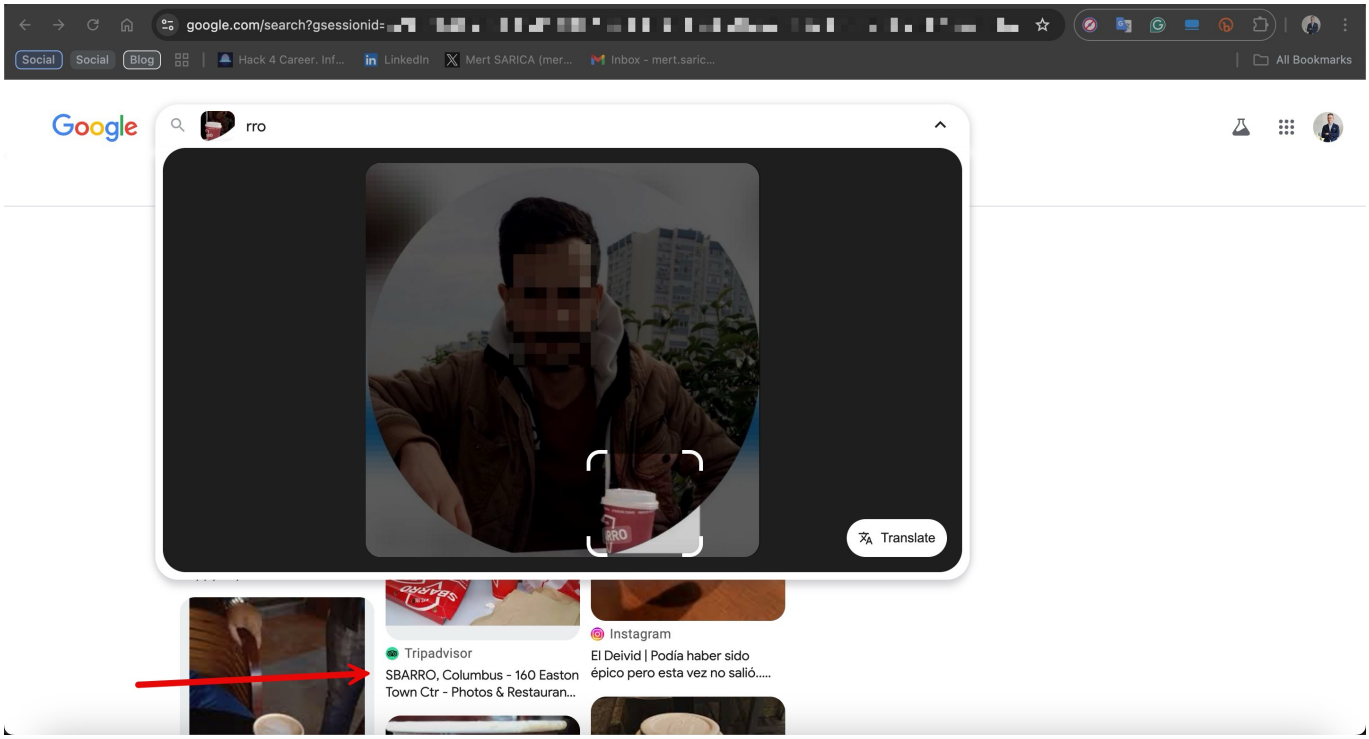
Second Clue

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.





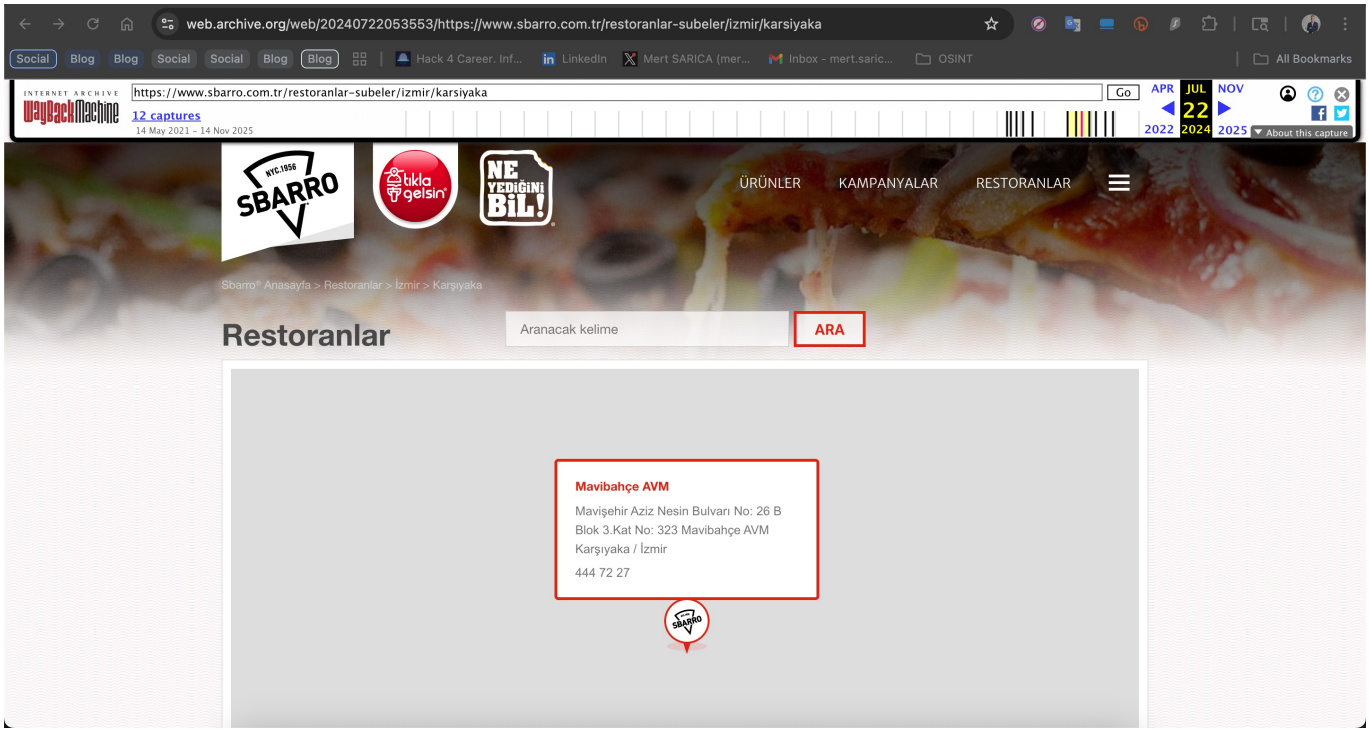
Finally, to determine approximately when the photo was taken, I once again relied on the profile photo. When I searched the letters RRO visible on the cardboard cup Cemal was holding using Google Images, I discovered that it belonged to the fast-service Italian restaurant chain Sbarro.



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.)



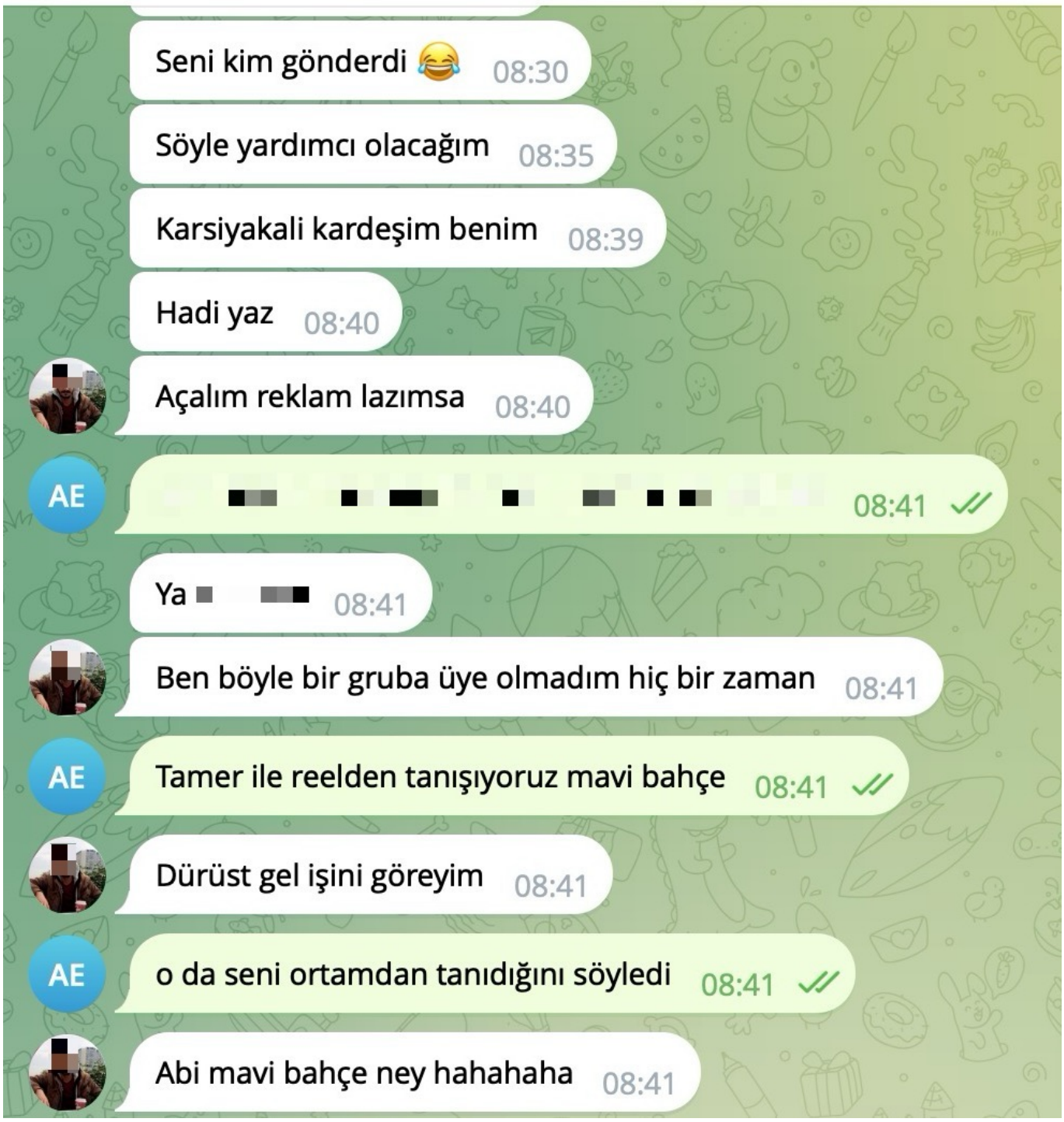
Conclusion

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.



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.



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? □



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 Hediyem Var Cybersecurity Game #20 game.