Istanbul Senin Data Breach

written by Mert SARICA | 6 November 2025

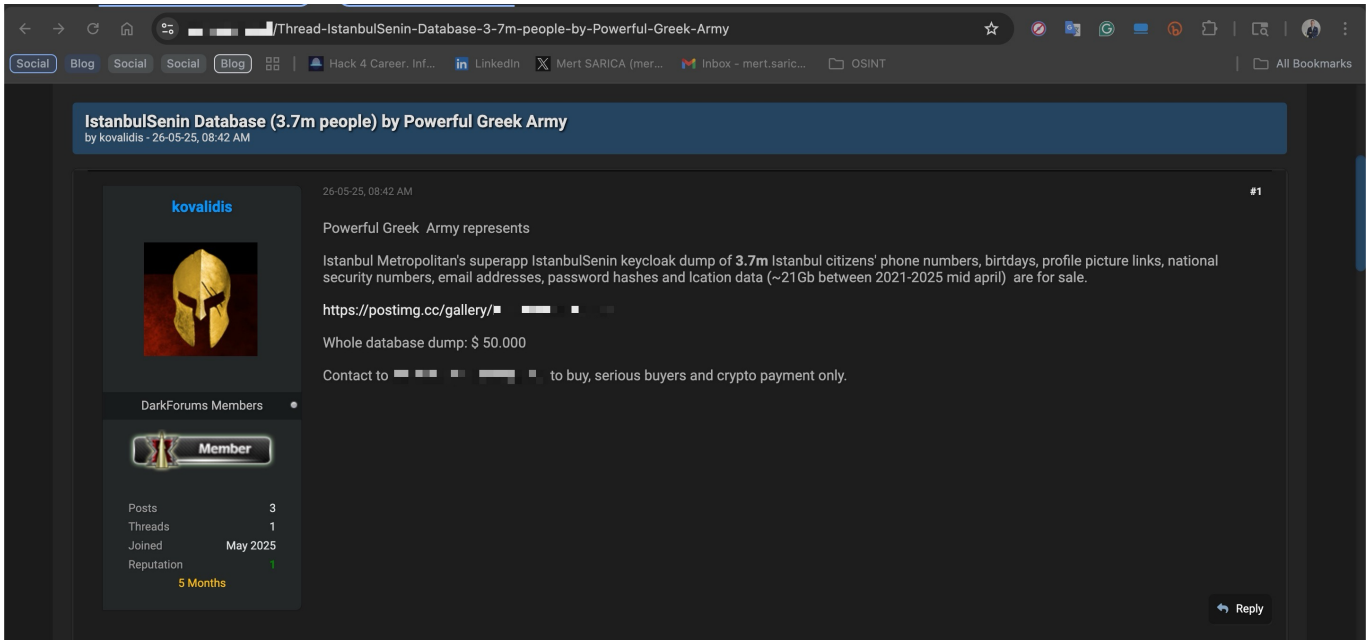
CONTENTS

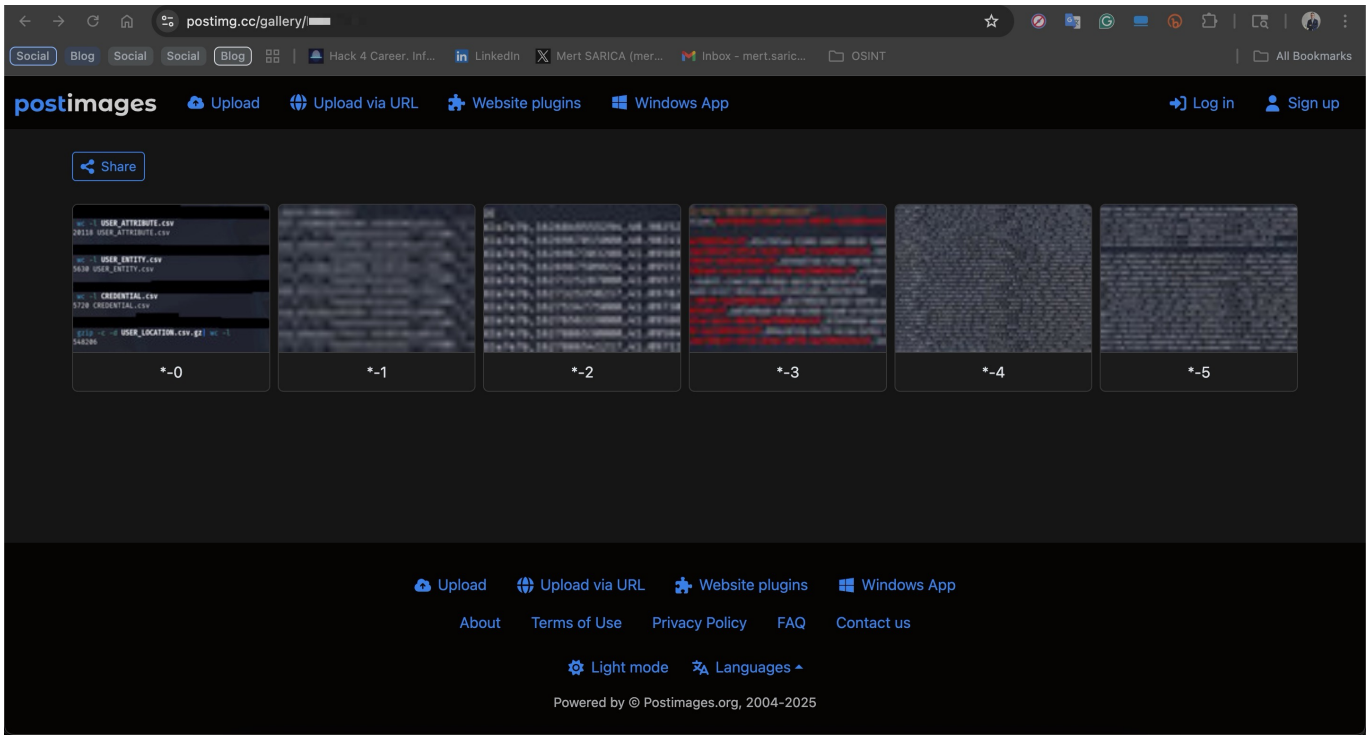
1. Introduction
2. I won’t believe it until @MertSARICA reviews it
3. Where’s My Close-Up Glasses? (Analysis)
4. Conclusion

Introduction

When the calendar showed May 26, 2025, a post appeared on DarkForums – a platform frequented by cybercriminals – from a threat actor using the alias kovalidis. In the message, the actor, claiming to be (or posing as) a member of the Powerful Greek Army (PGA) hacker group, announced that they were selling the İstanbul Senin database, allegedly containing personal data of 3.7 million Turkish citizens, for $50,000. To appear as a “trustworthy seller,” the post also included several screenshots showing samples of the leaked data.

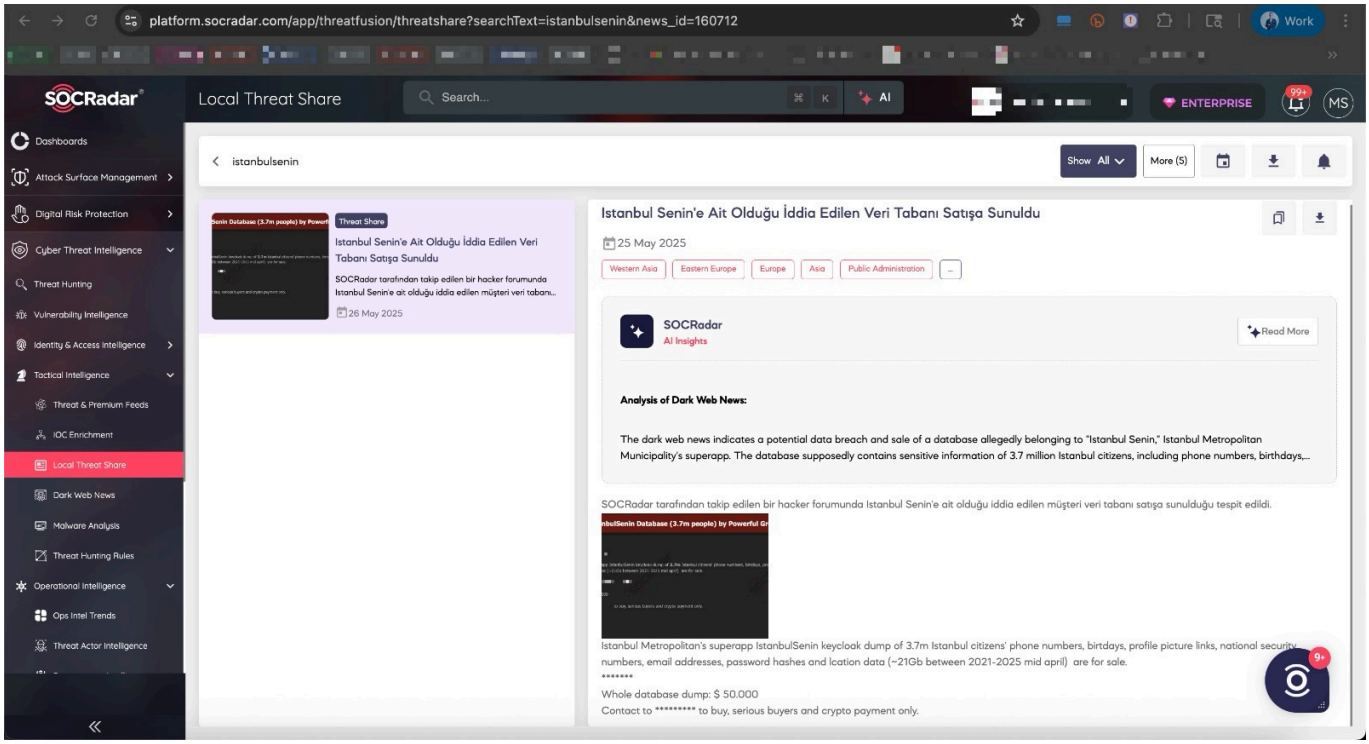
The fact that no statement about this incident was shared on PGA’s official X account, combined with the observation that the threat actor had registered on DarkForums solely to publish this post, raised suspicions that the incident could be part of a false flag operation.





İstanbul Senin is an innovative mobile application developed by the Istanbul Metropolitan Municipality to digitize urban life and provide faster services to citizens. The app consolidates numerous features under one platform, including public transportation data, traffic updates, parking information, cultural and art events, sports facility reservations, access to municipal services, payment options, and neighborhood-specific announcements. With features such as Istanbulkart integration, online applications, appointment systems, and city-wide discount programs, users can easily manage their daily needs. İstanbul Senin is a comprehensive city app designed to serve as the city’s digital assistant, making life easier for everyone living in Istanbul.

Thanks to the SOCRadar Extended Threat Intelligence Platform, which continuously monitors regional cyber threats, and its instant alerting capabilities, many organizations were promptly informed about this potential data breach at the time.



I won’t believe it until @MertSARICA reviews it

Time passed, and about five months after that initial post, on November 4, 2025, I received a notification on X (formerly Twitter) that I had been mentioned by a user under the alias red.eth. The mention included the phrase “I won’t believe it until @MertSARICA reviews it”, which immediately caught my attention. When I checked the main post, I saw that a journalist named Ece SEVİM had shared a message about this same incident from five months earlier.

Here is the English translation of his message;

“Ece Sevim (@ecesevimtr) — Nov 4
 DETAIL — USOM REPORT / İBB “İstanbul Senin” App Data Sold on the Dark Web for $50,000
On May 26, 2025, personal data (such as name, surname, Turkish ID number, GSM number, and location coordinates) belonging to 3.7 million citizens registered to the İstanbul Senin app were allegedly put up for sale on the

dark web by the Powerful Greek Army group.

red.eth (@tcctus) – Nov 4
I won’t believe it until @MertSARICA reviews it”

Because terms like Clear Web, Deep Web, and Dark Web are often confused not only by end users but also by members of the media, I wanted to clarify them here. Based on these definitions, we can confidently say that DarkForums is not part of the Dark Web.

Clear Web (Surface Web): Websites indexed by search engines and publicly accessible. Corporate pages, news sites, social media platforms, and forums belong to this layer.

Deep Web: Content that is not indexed by search engines but still includes legal and legitimate areas. Paid databases, academic archives, and portals requiring authentication (such as hospital systems, government services, and private forums) fall into this category.

Dark Web: A small subset of the Deep Web that requires special software like Tor or I2P to access. It hosts illegal marketplaces, data leak forums, and ransomware operation hubs, which are highly relevant from a threat intelligence perspective.

As a citizen who has long been away from Türkiye and its ever-changing agenda, I couldn’t quite understand why the message shared by this threat actor on DarkForums resurfaced after five months.
Leaving that question aside, I decided to respond to red.eth’s call for help – just as I have done in my previous blog posts such as Smart Kids’ Watches, Instagram Scammers, Backdoor Hunt, and Hunting Hackers with a Honeypot System – as a cybersecurity researcher who always listens to his readers and followers.

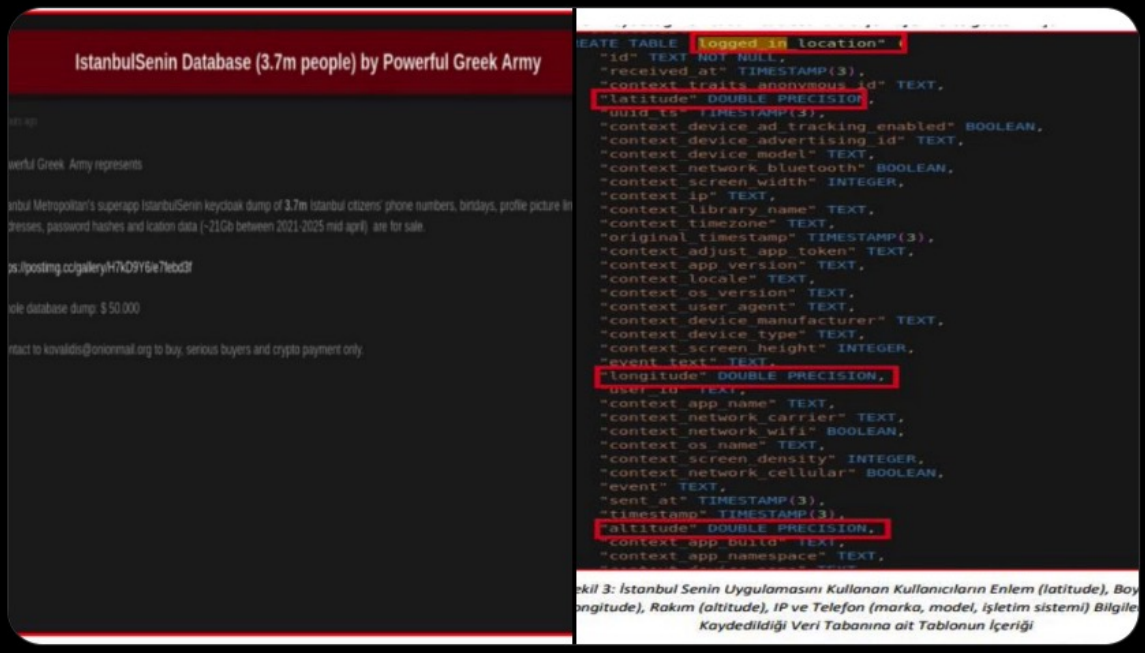
← **Post** Reply

Ece Sevim @ecesevimtr · Nov 4

DETAY - USOM RAPORU / İBB İSTANBUL SENİN UYGULAMASI VERİLERİNİN DARKWEB'DE 50 BİN DOLAR'A SATIŞI

26 Mayıs 2025 tarihinde, USAM'a İstanbul Senin uygulamasına kaydolan 3.7 milyon vatandaşa ait kimlik (ad, soyad, TCKN), GSM, konum (enlem, boylam) gibi kişisel verilerin

Show more



Kaydedildiği Veri Tabanına ait Tablonun İçeriği

33 168 368 15K

red.eth @tcctus · Nov 4

@MertSARICA incelemeden inanmam

2 430

red.eth
@tcctus

Show translation

@MertSARICA abi inceleyip bi döküman olsa sitede tadından yenmez valla

1:44 AM · Nov 5, 2025 · **61** Views

Here is the English translation of his message;

“Ece Sevim (@ecesevimtr) — Nov 4
 DETAIL — USOM REPORT / İBB “İstanbul Senin” App Data Sold on the Dark Web for $50,000
On May 26, 2025, personal data (such as name, surname, Turkish ID number, GSM number, and location coordinates) belonging to 3.7 million citizens registered to the İstanbul Senin app were allegedly put up for sale on the dark web by the Powerful Greek Army group.

red.eth (@tcctus) — Nov 4
I won’t believe it until @MertSARICA reviews it

red.eth (@tcctus) — Nov 5, 1:44 AM
@MertSARICA Bro, if you review it and publish a write-up on your site, it would be absolutely perfect.”

red.eth was essentially like an ordinary citizen who either didn’t have $50,000 or didn’t want to spend it — they simply wanted to know whether their data had been stolen. Rightfully so, it’s often hard to get accurate information from media reports about hacks or data leaks. So, from the perspective of an average person, I decided to write a guide on how a data leak can be verified under realistic conditions.

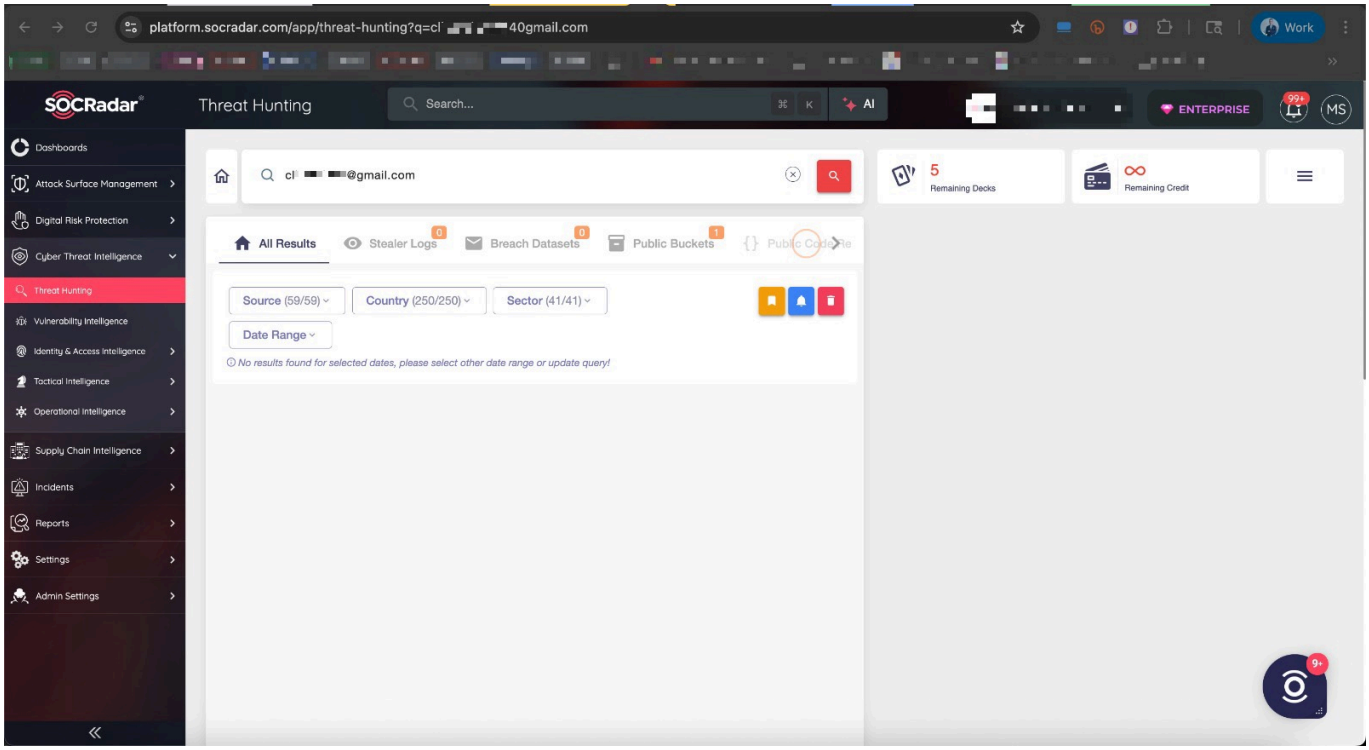
Where’s My Close-Up Glasses? (Analysis)

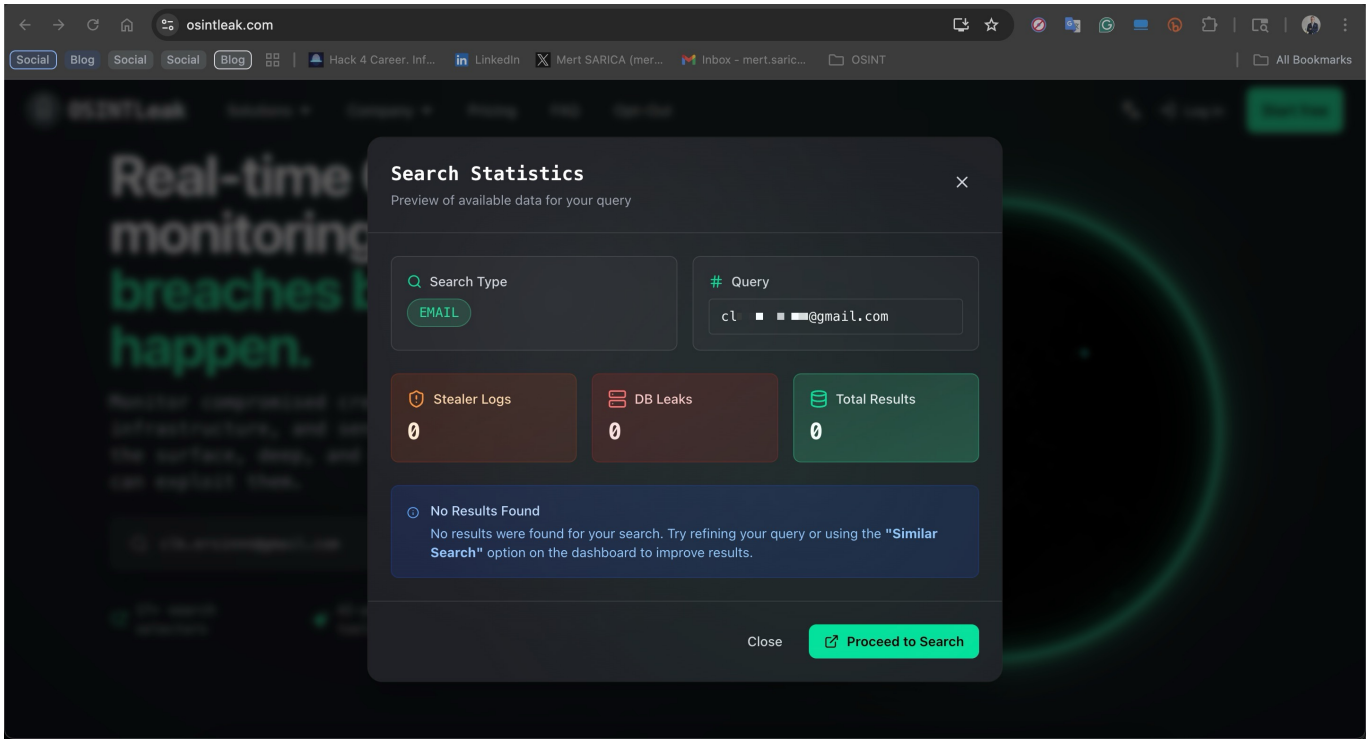
From an average-citizen viewpoint, in one of the screenshots posted by the threat actor kovalidis, I first noticed a value marked in red that looked like a UUID / GUID (unique identifier), and then two verification-useful fields: date of birth (05.04.****) and mobile phone number (055184*****).

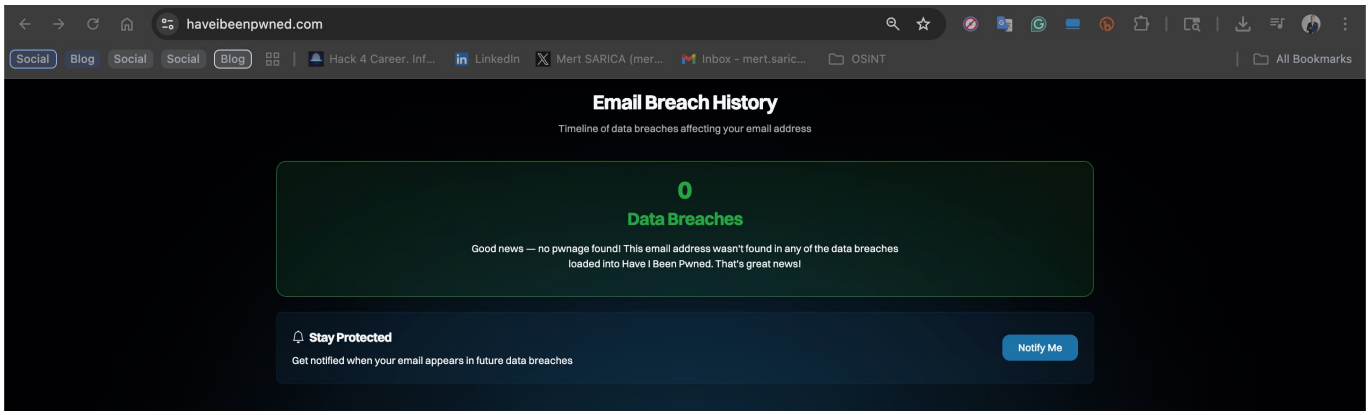
In another screenshot, when I searched for the user record tied to that UUID / GUID, I quickly found the user’s first name, last name, email address, their TCKN (Turkish national ID number) (245********), and the date they

registered in the İstanbul Senin app.

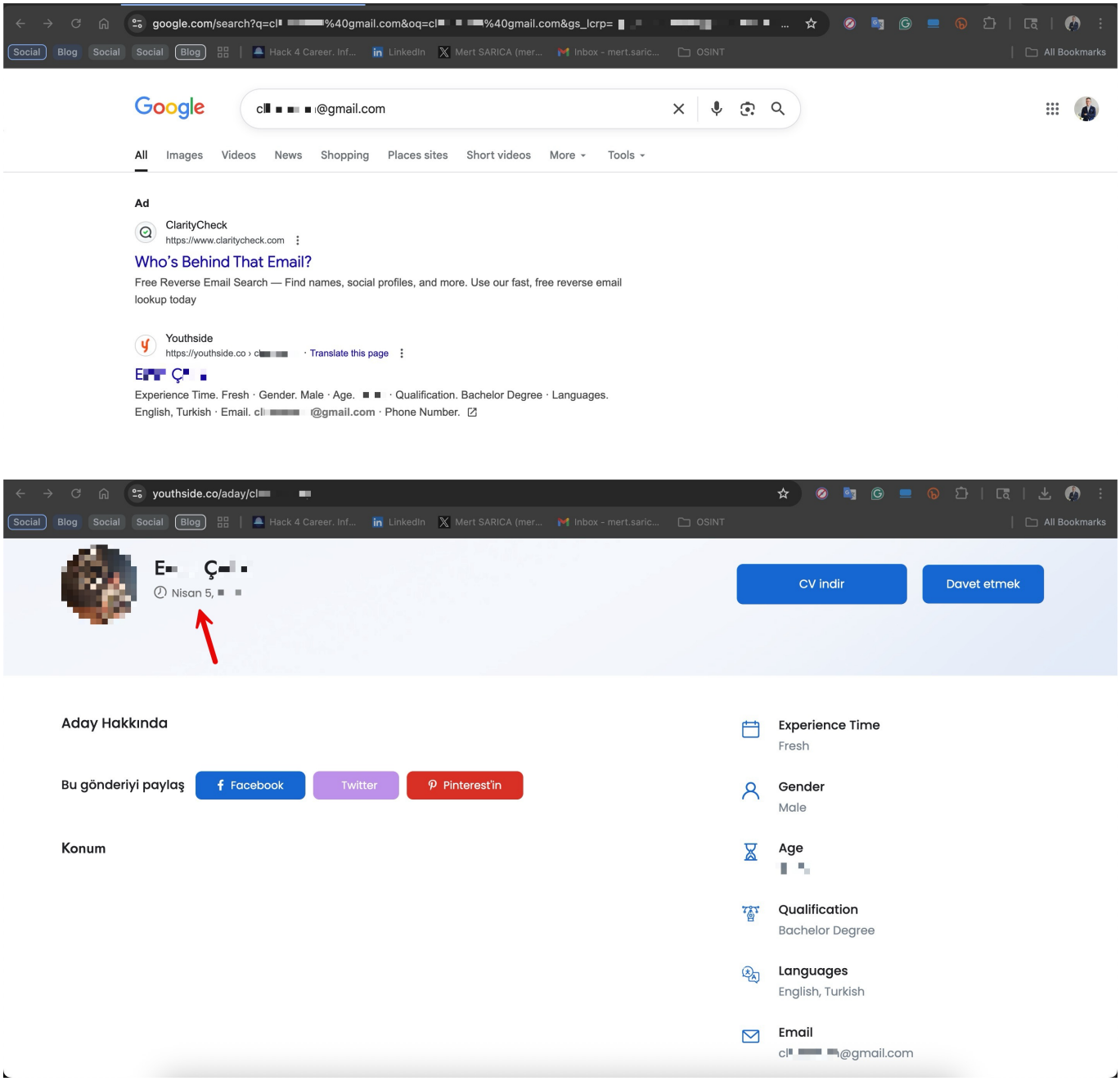
First, to make sure these records didn’t come from previously leaked databases or were not compiled from info-stealer malware logs disguised as a fake data breach, I began by searching the sample email address on the paid SOCRadar platform. Since no results appeared related to any known data leaks, I expanded my search to free resources such as OSINTLeak and Have I Been Pwned. When these also returned no matches, I became confident that the data sample wasn’t a compilation from existing breaches.

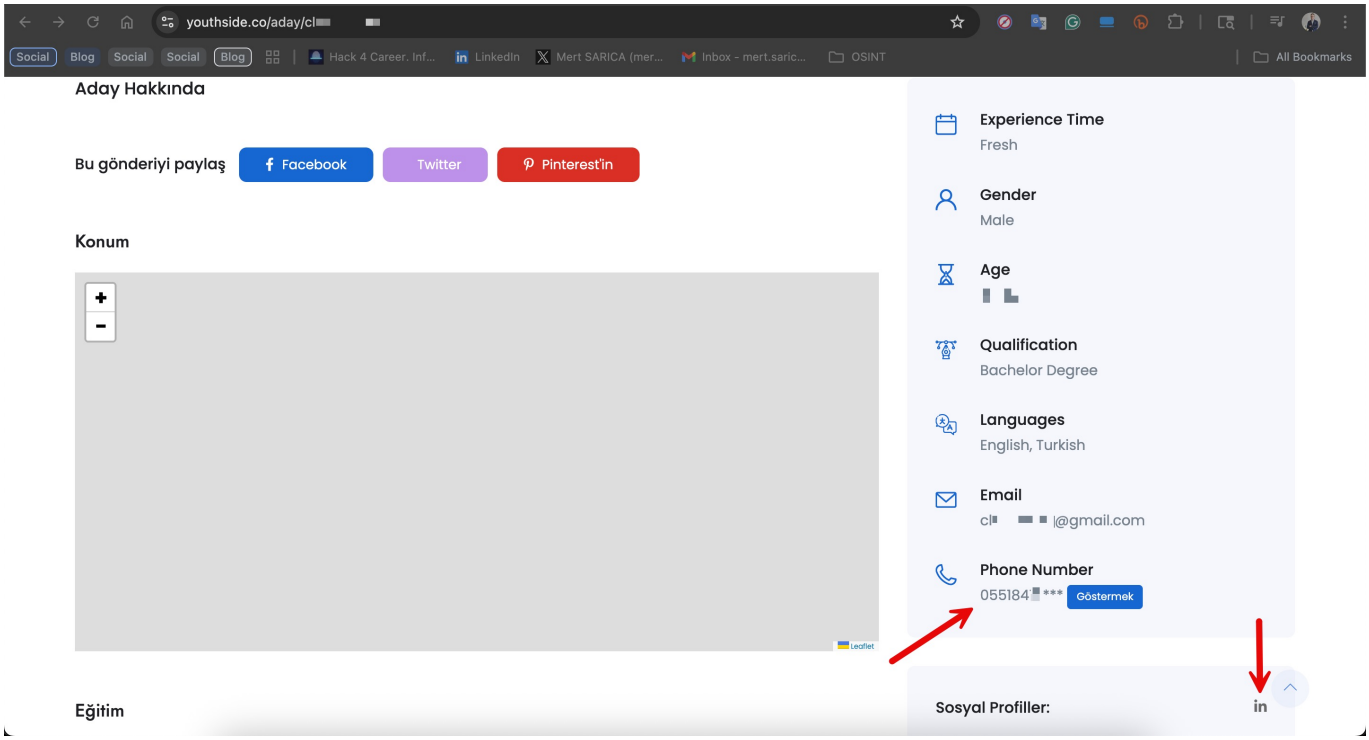




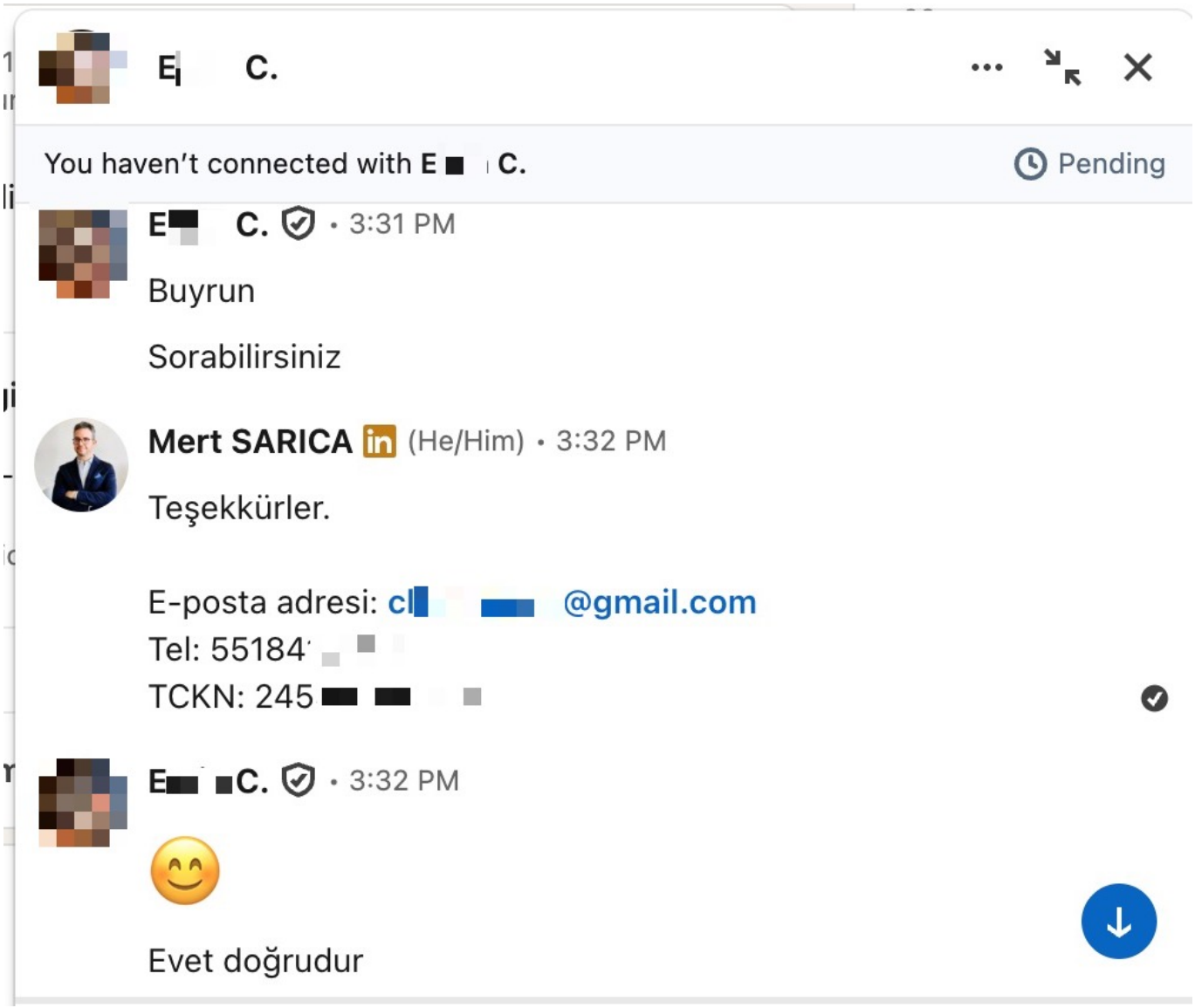


When it was time to verify the stolen information using Open Source Intelligence (OSINT) and publicly available tools, a Google search turned up the affected citizen’s publicly visible profile on Youthside, a next-generation career platform. From that page I was able to confirm the name, surname, email address and date of birth shown in the screenshots.


google.com/search?q=cl%40gmail.com&oq=cl%40gmail.com&gs_lcrp=
Social Blog Social Social Blog Hack 4 Career. Inf... LinkedIn Mert SARICA (mer... Inbox - mert.saric... OSINT All Bookmarks
Google
cl@gmail.com
All Images Videos News Shopping Places sites Short videos More Tools
Ad
ClarityCheck
https://www.claritycheck.com
Who's Behind That Email?
Free Reverse Email Search — Find names, social profiles, and more. Use our fast, free reverse email lookup today
Youthside
https://youthside.co › cl · Translate this page
E Ç
Experience Time. Fresh · Gender. Male · Age. · Qualification. Bachelor Degree · Languages. English, Turkish · Email. cl @gmail.com · Phone Number.
youthside.co/aday/cl
Social Blog Social Social Blog Hack 4 Career. Inf... LinkedIn Mert SARICA (mer... Inbox - mert.saric... OSINT All Bookmarks
E Ç
Nisan 5,
CV indir
Davet etmek
Aday Hakkında
Bu gönderiyi paylaş
Facebook
Twitter
Pinterest'in
Konum
Experience Time
Fresh
Gender
Male
Age
Qualification
Bachelor Degree
Languages
English, Turkish
Email
cl@gmail.com



Finally, I decided to contact this individual via the LinkedIn link available on their profile to verify the information and complete my investigation. Thankfully, they kindly and transparently answered all my questions, confirming the accuracy of the data. As a result, it became clear that the information belonging to the İstanbul Senin application had, in all likelihood, fallen into the hands of malicious actors.



Here is the English translation of his message;

“E. C.:
Sure, go ahead. You can ask.

Mert SARICA:
Thank you.
Email address: cl•••@gmail.com
Phone: 55184••••
National ID (TCKN): 245•••

E. C.:
□
That’s correct.”

Conclusion

From the perspective of an ordinary citizen – without diving too deep into the technical side – I managed to determine whether the data involved in the investigation concerning the Istanbul Metropolitan Municipality's "İstanbul Senin" app had actually been stolen – all without paying $50,000. Just like red.eth, I wanted to understand how such verification could be done, and by sharing this process, I hope I've shown others how it's possible.

Since this is my last post of the year, I'd like to take the opportunity to wish you all a happy new year! May 2026 bring you and your loved ones health, happiness, and success.

See you next year. :)