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

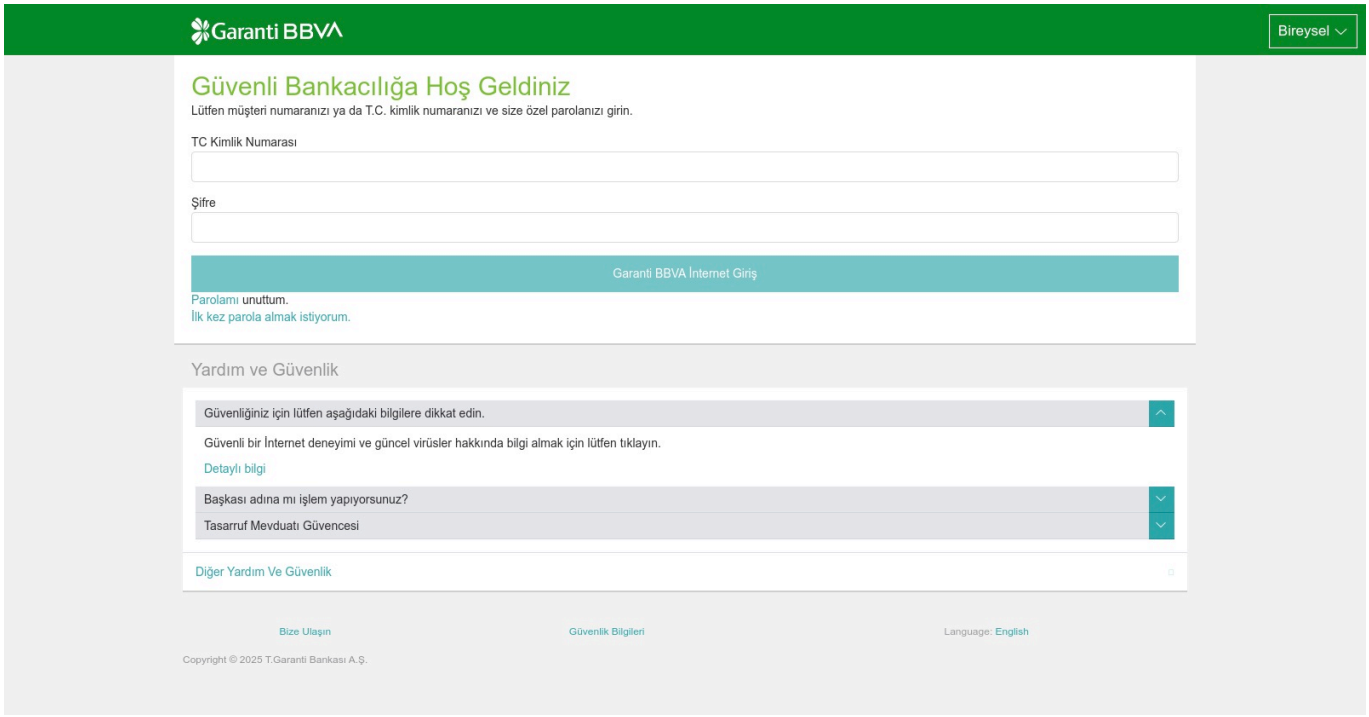
Başlangıç

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.

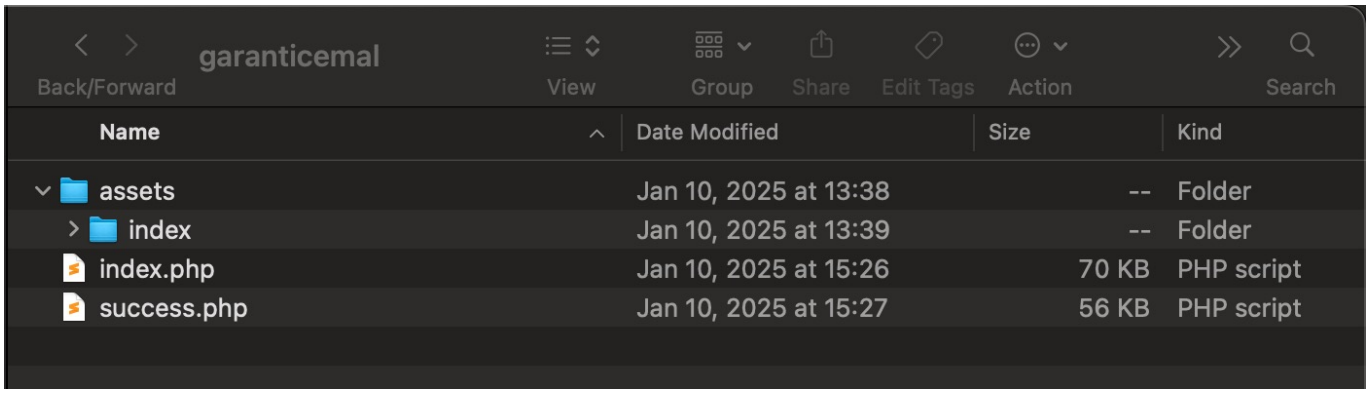
Bu yazının hikayesi, bundan neredeyse bir yıl önce, gerçekleştirdiğim bir güvenlik araştırması esnasında adını, soyadını, Garanti BBVA müşterilerini hedef almak amacıyla oluşturduğu oltalama sitelerinde ve Telegram profilinde kullanmaktan çekinmeyen, belki de bir siber güvenlik araştırmacısının bunu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

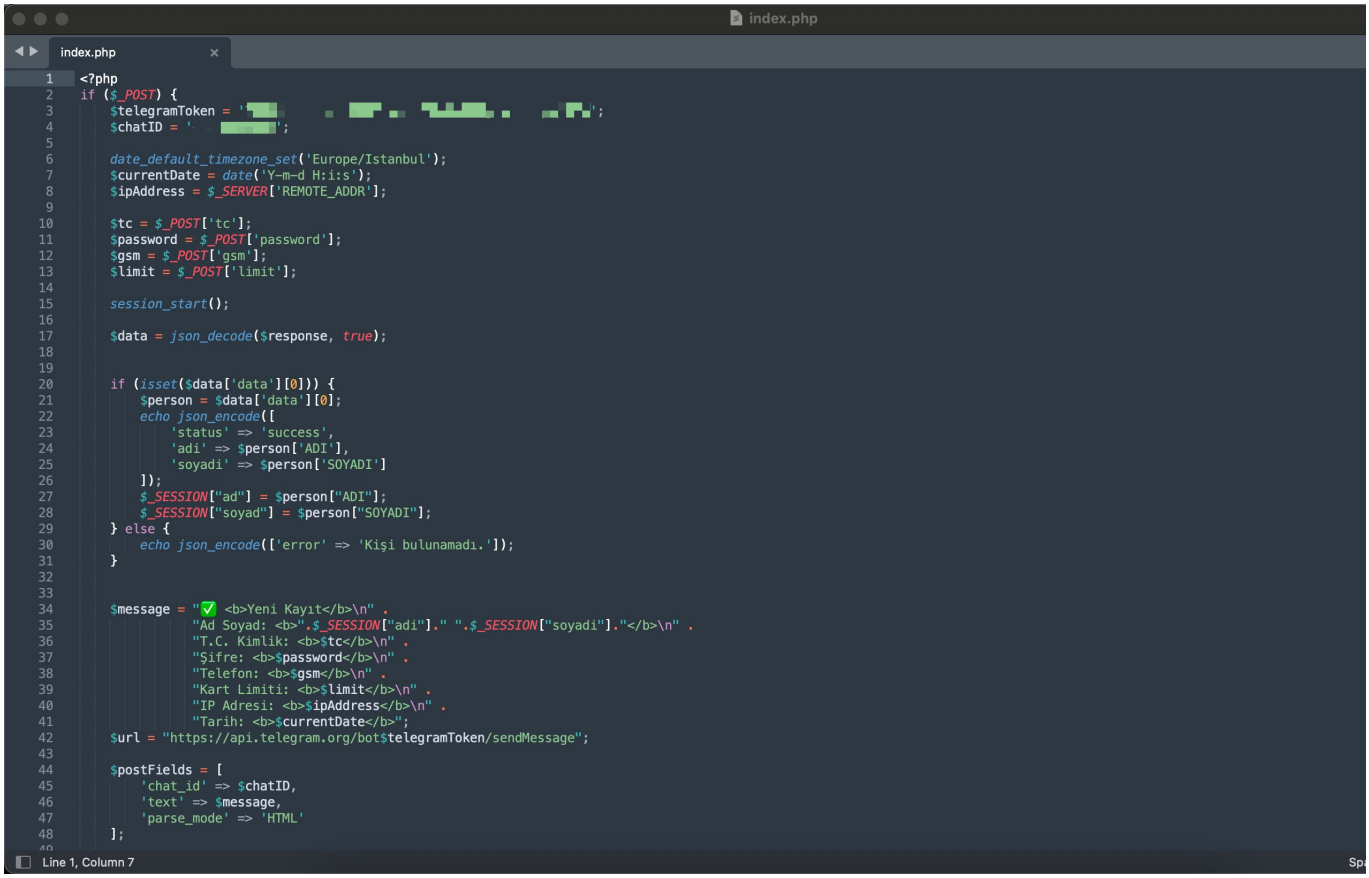
Tehdit Avı

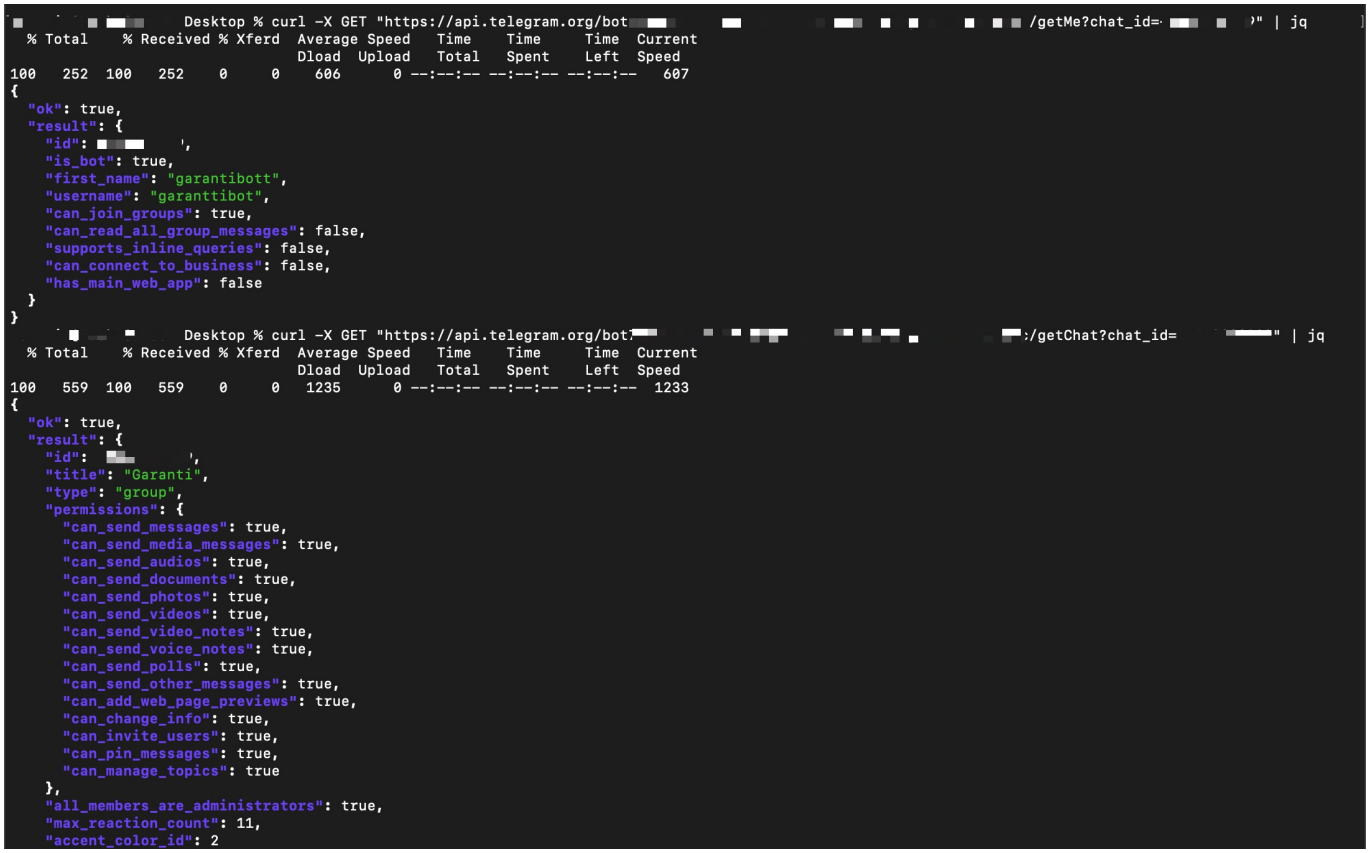
SOCRadar Siber Tehdit İstihbaratı Platformu üzerinde tespit edilen oltalama siteleri üzerinde tehdit avına çıktığım bir zamanda, grnt- ile başlayan üç alan adı, grnt-avantaj1.xyz, grnt-avantaj2.xyz ve grnt-avantaj4.xyz dikkatimi çekti.



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.



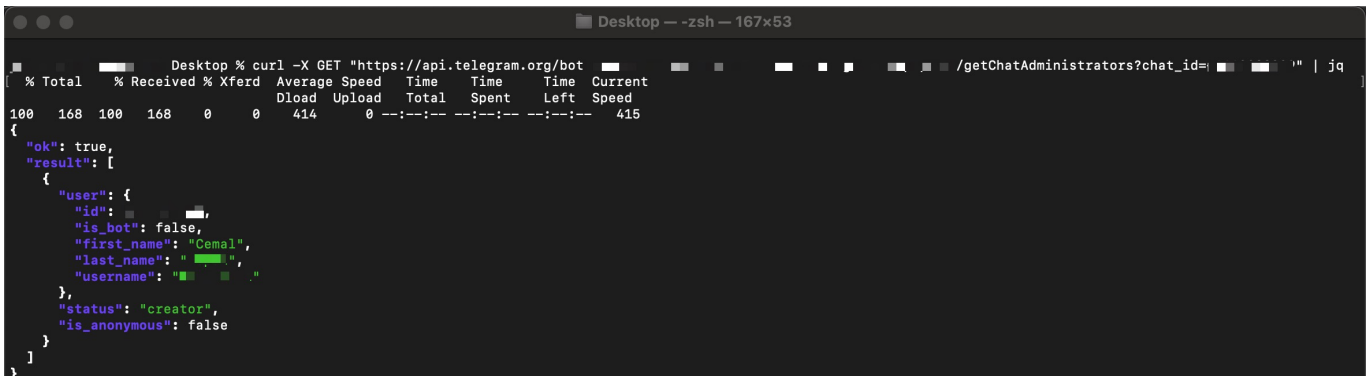


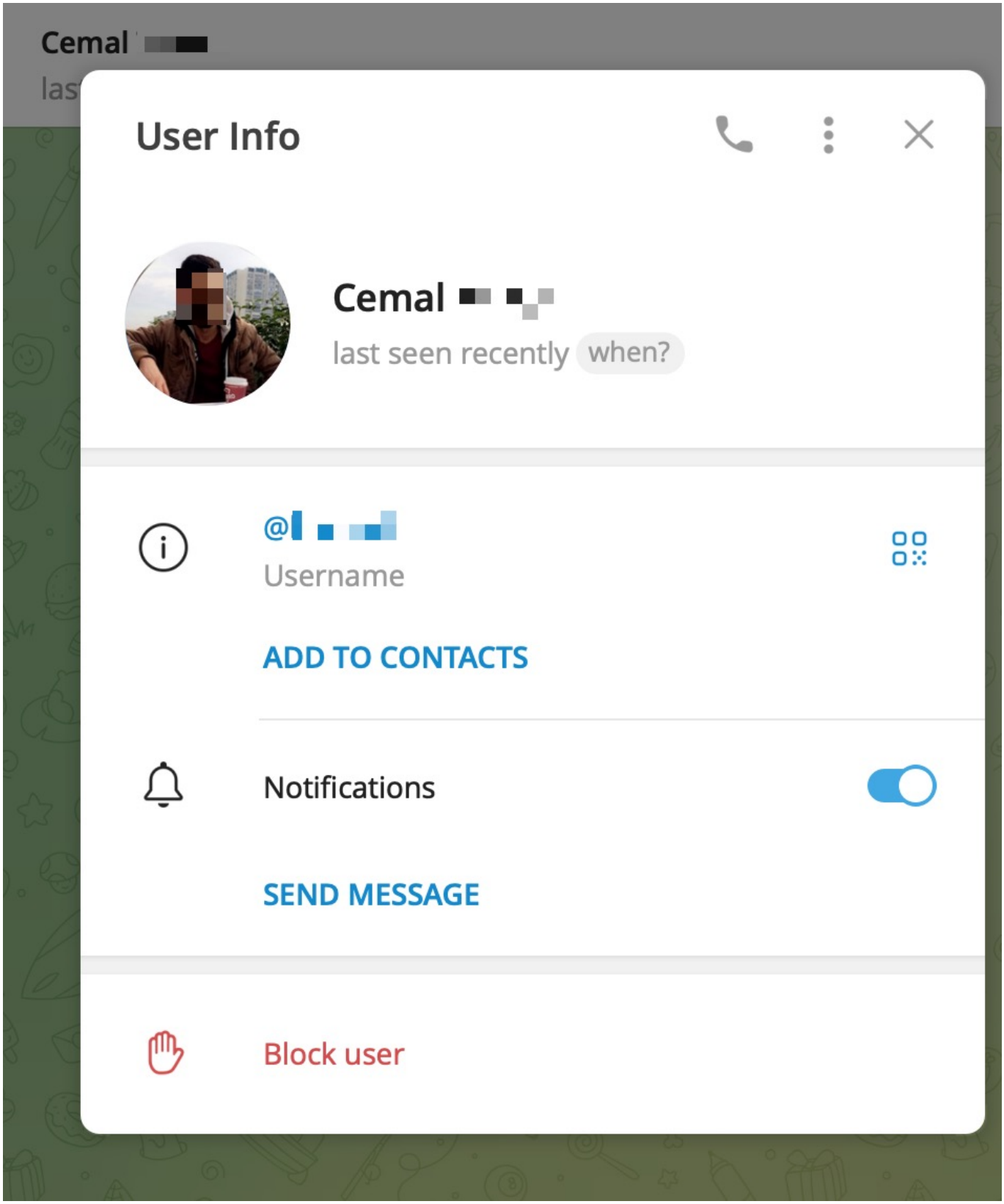


Jeton üzerinden Cemal’in Telegram hesabına ulaşıp soyadı bilgisi ve olası fotoğrafı ile karşılaştığımda ilk olarak gördüklerimin sahte olduğunu düşündüm. Çünkü ben bu bilgilere ulaşabiliyorsam kolluk kuvvetleri hayli

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.



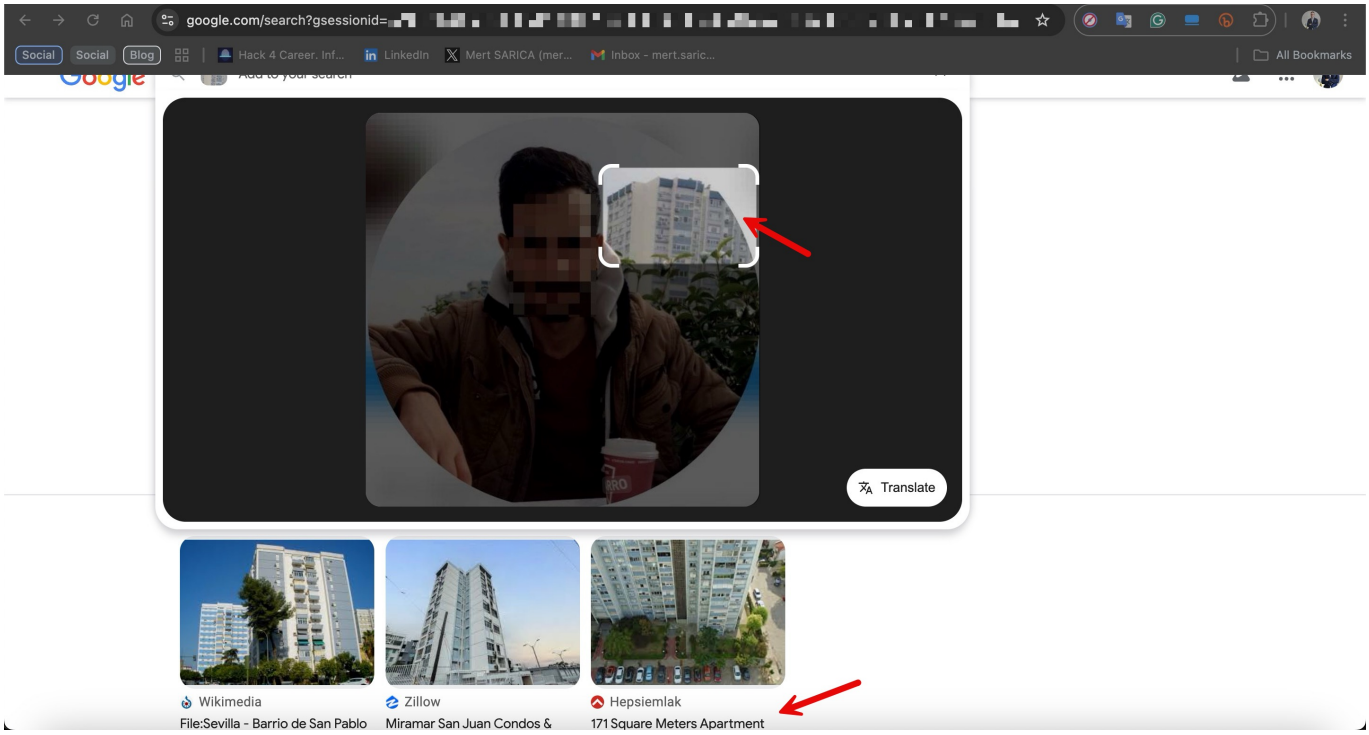

Cemal
User Info
Cemal
last seen recently
when?
Username
ADD TO CONTACTS
Notifications
SEND MESSAGE
Block user

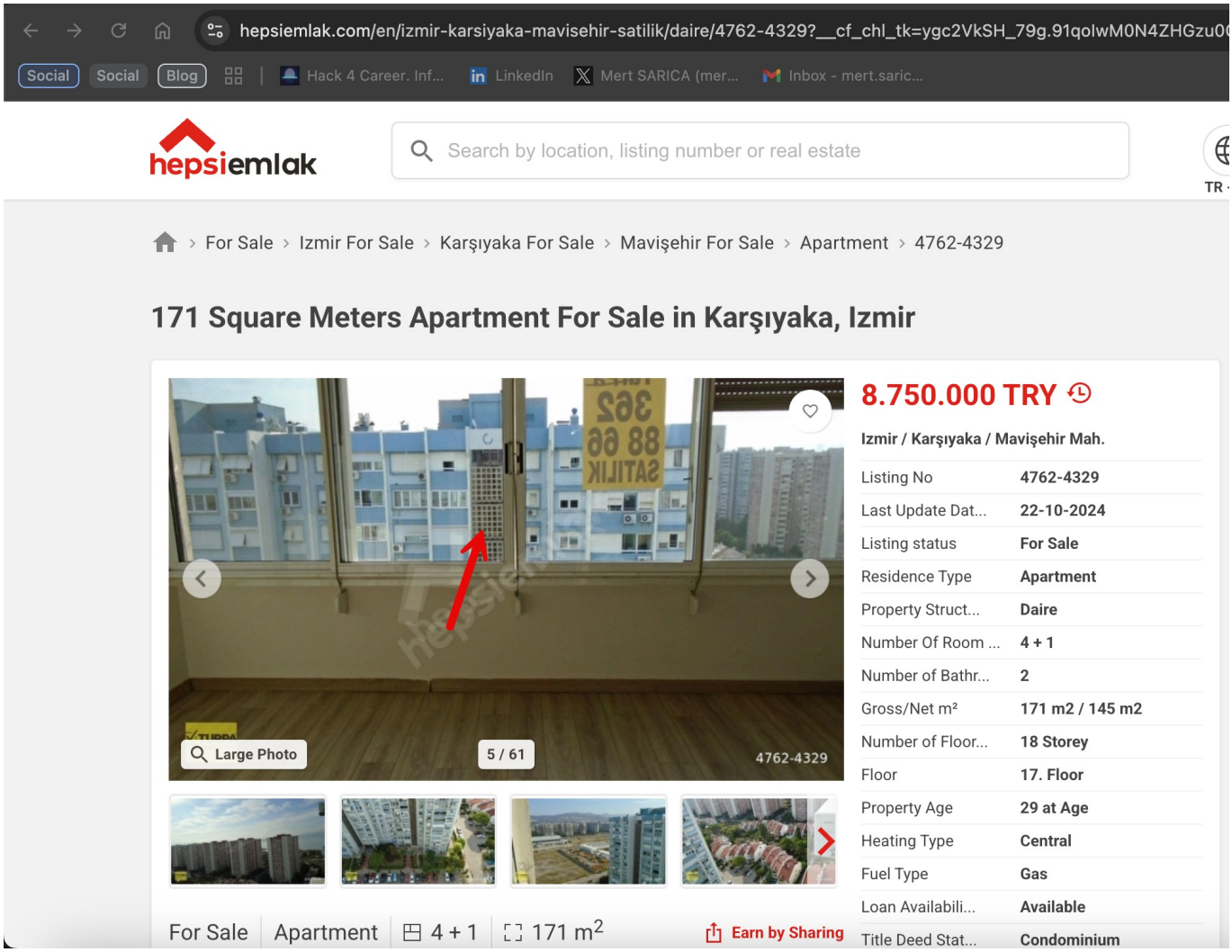
Cemal gerçekte yakalanmaktan endişe etmeyen bir tehdit aktörü müydü yoksa geride bıraktığı bilgi kırıntıları üzerinden yakalanabileceğine ihtimal vermeyen bir tehdit aktörü müydü? Bunu anlamak için ya Cemal ile direkt iletişime geçip verdiği yanıtlarla yetinecektim ya da Açık Kaynak İstihbaratı (OSINT)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

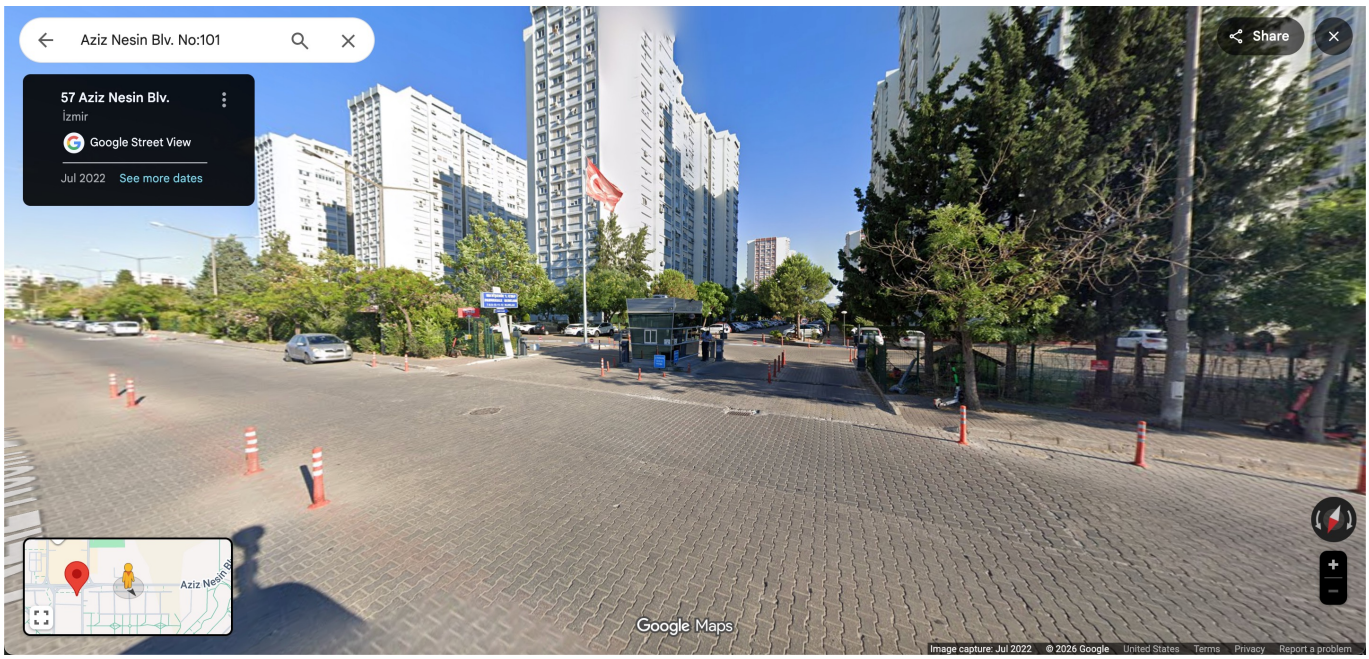
Birinci Çinko

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.





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



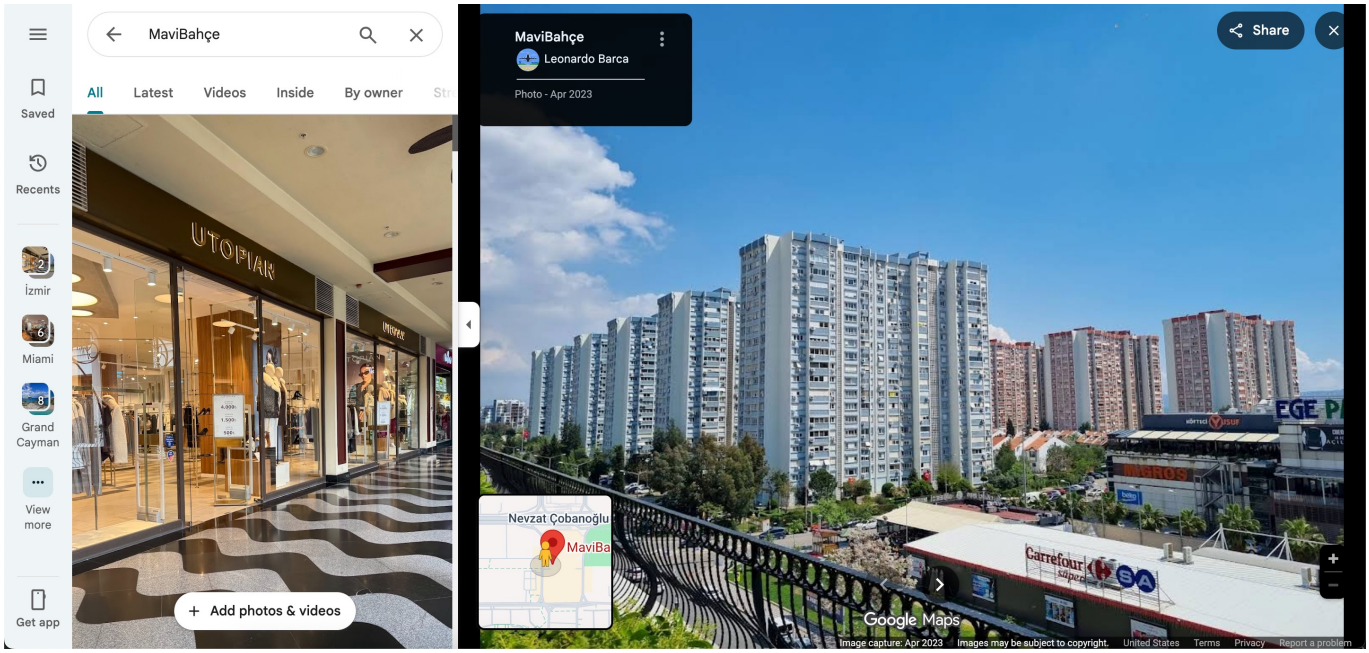
Daha sonra Cemal’in bu fotoğrafı aşağı yukarı nerede ve ne zaman çektirdiği

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

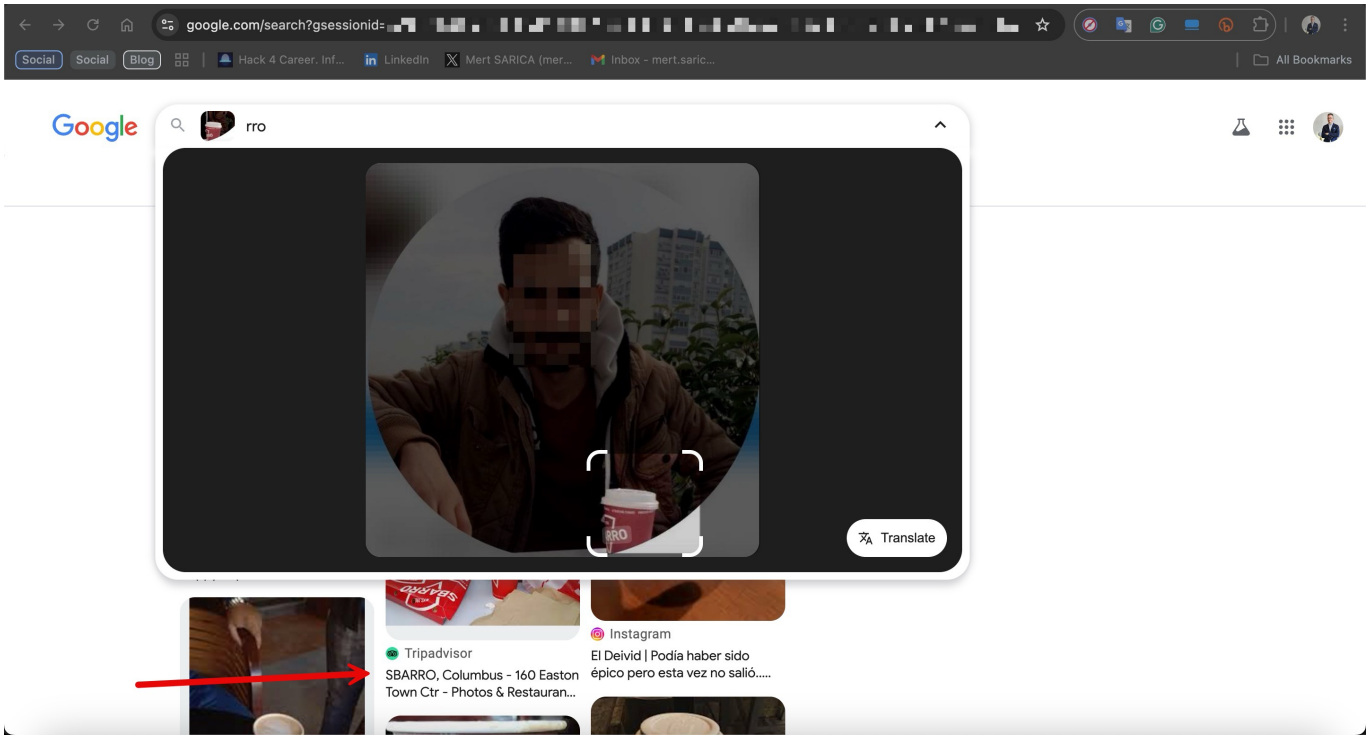
Mavişehir Pamukkale bloklarının etrafında Google Haritalar'ın Sokak Görünümü ile biraz gezindikten sonra profil fotoğrafındaki apartmanı bulabildim.

İkinci Çinko

Sıra fotoğrafın nereden çekildiğini bulmaya geldiğinde çekim açısından ilerdiğimde 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.

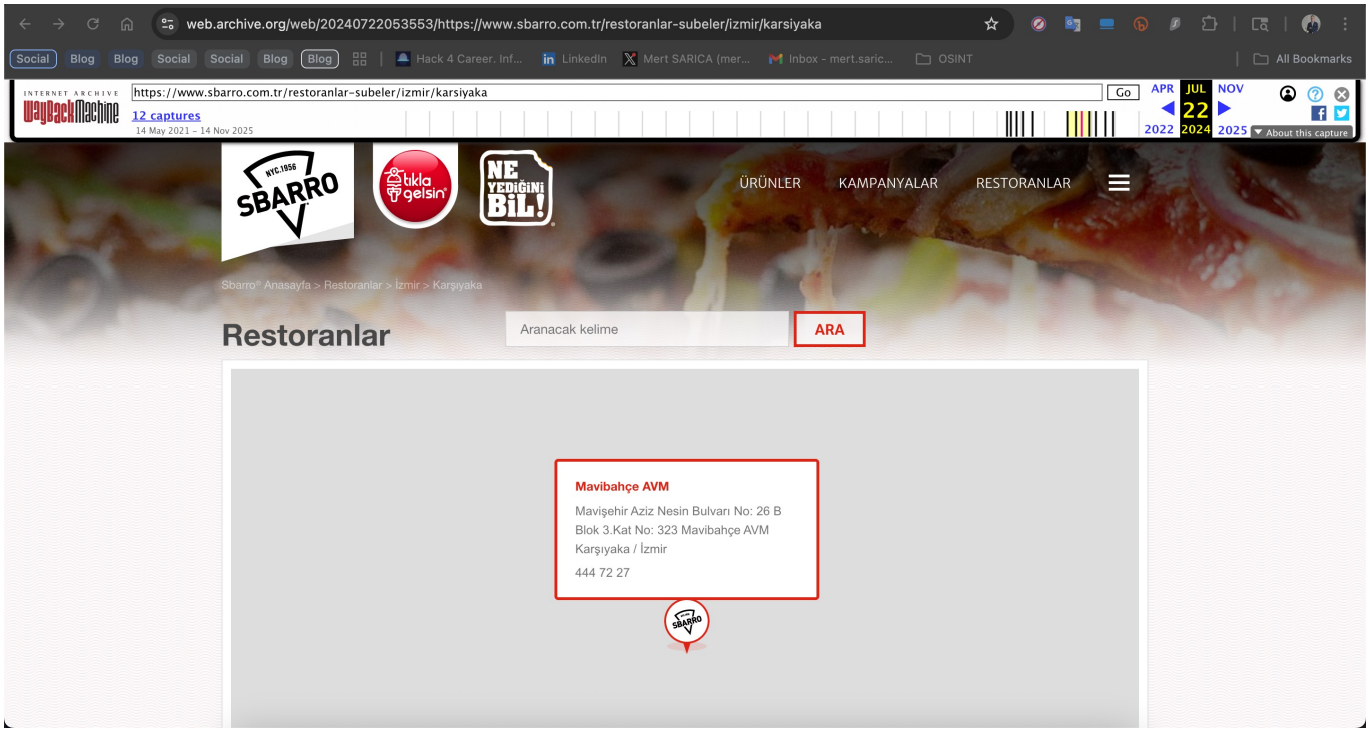


Son olarak fotoğrafın aşağı yukarı ne zaman çekildiğini bulmaya geldiğinde yine profil fotoğrafından faydalanmaya karar verdim. Cemal'in tuttuğu karton bardaktaki RRO harflerini Google Images üzerinde arattığımda hızlı servis İtalyan restoranlarından Sbarro olduğunu öğrendim.



Tombala

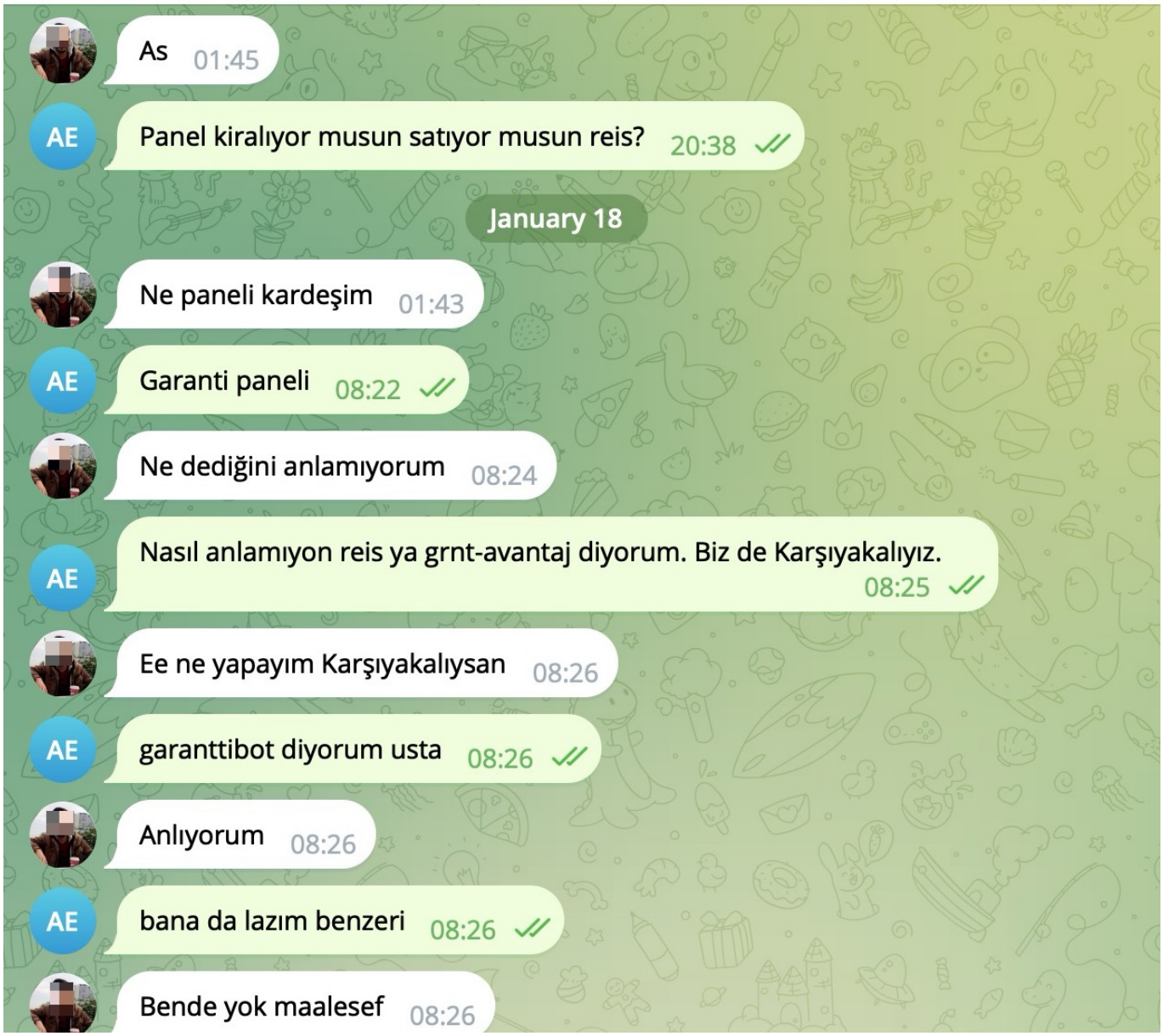
Daha sonra bu zincirin MaviBahçe alışveriş merkezinde bir şubesi olup olmadığını kontrol ettiğimde, olmadığını öğrendim. Bu şubenin aşağı yukarı ne zaman kapandığını öğrenmek için ise internet sitelerinin eski sürümlerini, tasarımlarını ve içeriklerini arşivleyen Web Archive isimli kütüphanesinden faydalanmaya 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

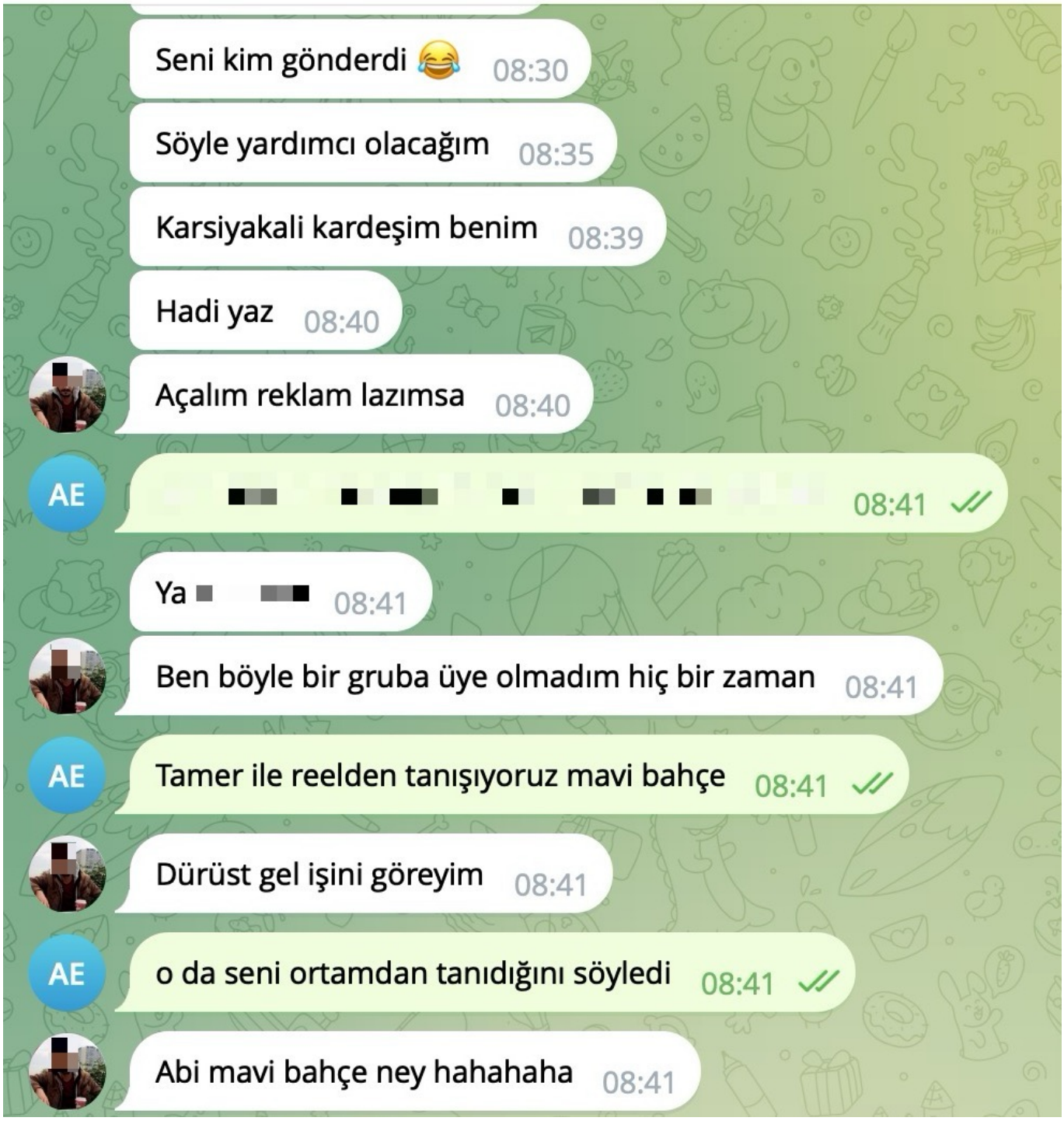
Elde ettiğim tüm bu bilgiler ışığında Cemal ile yazışmaya başladım. Başlarda söylediklerimi inkar etse de yazışmaların sonuna doğru onu tanıdığı birinin işletmediğini aksine işlerin git gide ciddiye bindiğini anlayan Cemal bir anda sırra kadem bastı.

Cemal [redacted]
online



Cemal [redacted]

online



Cemal [redacted]

last seen recently

Ben de bu yaklaşımından yola çıkarak elde ettiğim bilgilerin kuvvetle muhtemel doğru olduğuna kanaat getirmiş ve bir bilgi kırıntısından 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 Güvenliği (OPSEC) ihmali çoğu zaman küçük bir detay ile başlar. Tehdit aktörleri için önemsiz görünen her ayrıntı, bir siber güvenlik araştırmacısı için başlangıç noktası olabilir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

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