Yatırım Dolandırıcıları

written by Mert SARICA | 2 December 2024

If you are looking for an English version of this article, please visit here.

İÇİNDEKİLER

Başlangıç

Hatırlayanlarınız varsa 2024 yılının Haziran ayında yayınlamış olduğum Deepfake Dolandırıcılarına Dikkat! başlıklı yazımda, Rusya merkezli olduğuna kanaat getirdiğim dolandırıcılık şebekesinin operasyonlarına dair detaylara, başka bir yazımda yer vereceğimi belirtmiştim.

O zamandan bu zamana kadar geçen sürede siber güvenlik araştırması ile elde ettiğim bilgiler öyle bir noktaya ulaştı ki hangi birini yazıya dökeceğim konusunda epey bir git gel yaşadıktan sonra farkındalık adına en çok faydası olacağına inandığım, dolandırıcılar ile aramda geçen telefon görüşmelerinin de yer aldığı kısımları yazıya dökmeye karar verdim.

Umuyorum ki benim için de önemli bir dönüm noktasına sahip olan bu 200. araştırma yazım, farkındalık yaratma anlamında arzu ettiğim noktaya ulaşır ve bu araştırma ile ortaya koyduğum en ufak bir bilgi bile dolandırıcılık dosyalarını aydınlatmada, kurbanlardan emniyet güçlerine kadar geniş bir

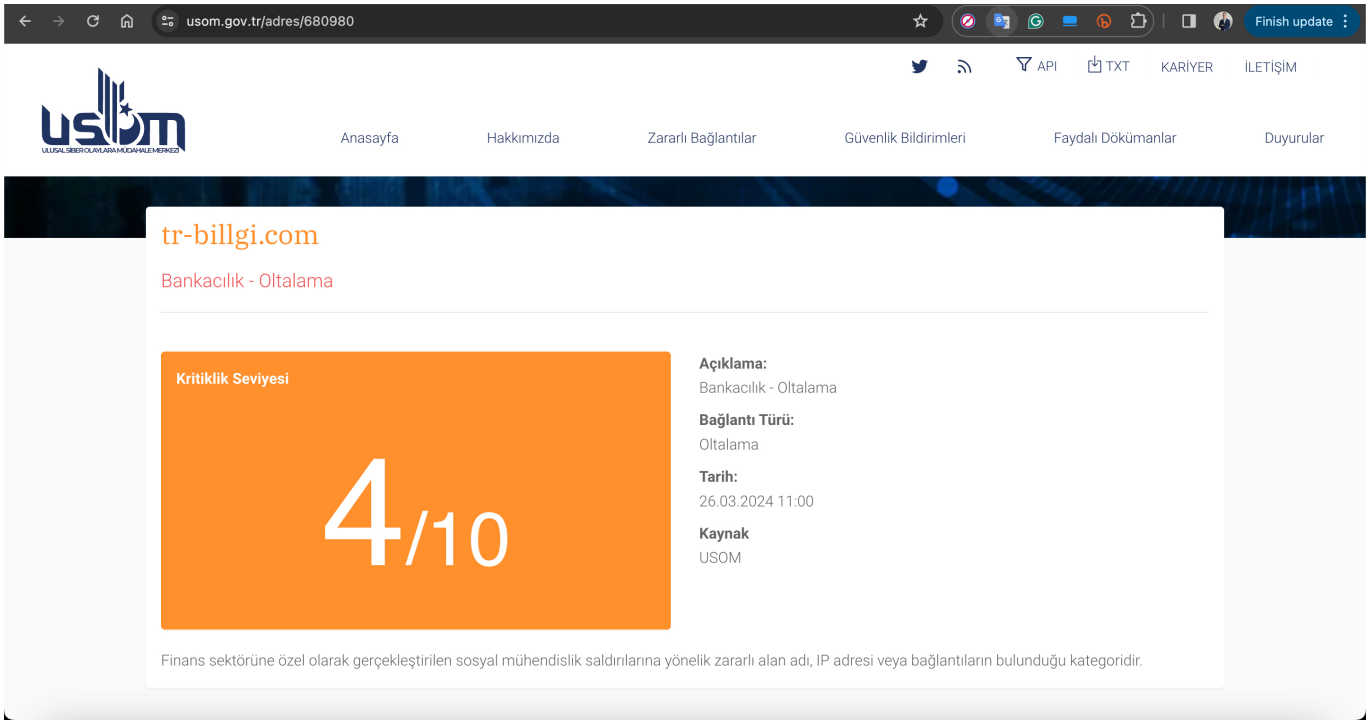
yelpazede fayda sağlar.

Lütfen sizler de daha az vatandaşın mağdur olması ve farkındalık yaratması adına bu yazıyı çevrenizdekilerle paylaşmayı ihmal etmeyin.

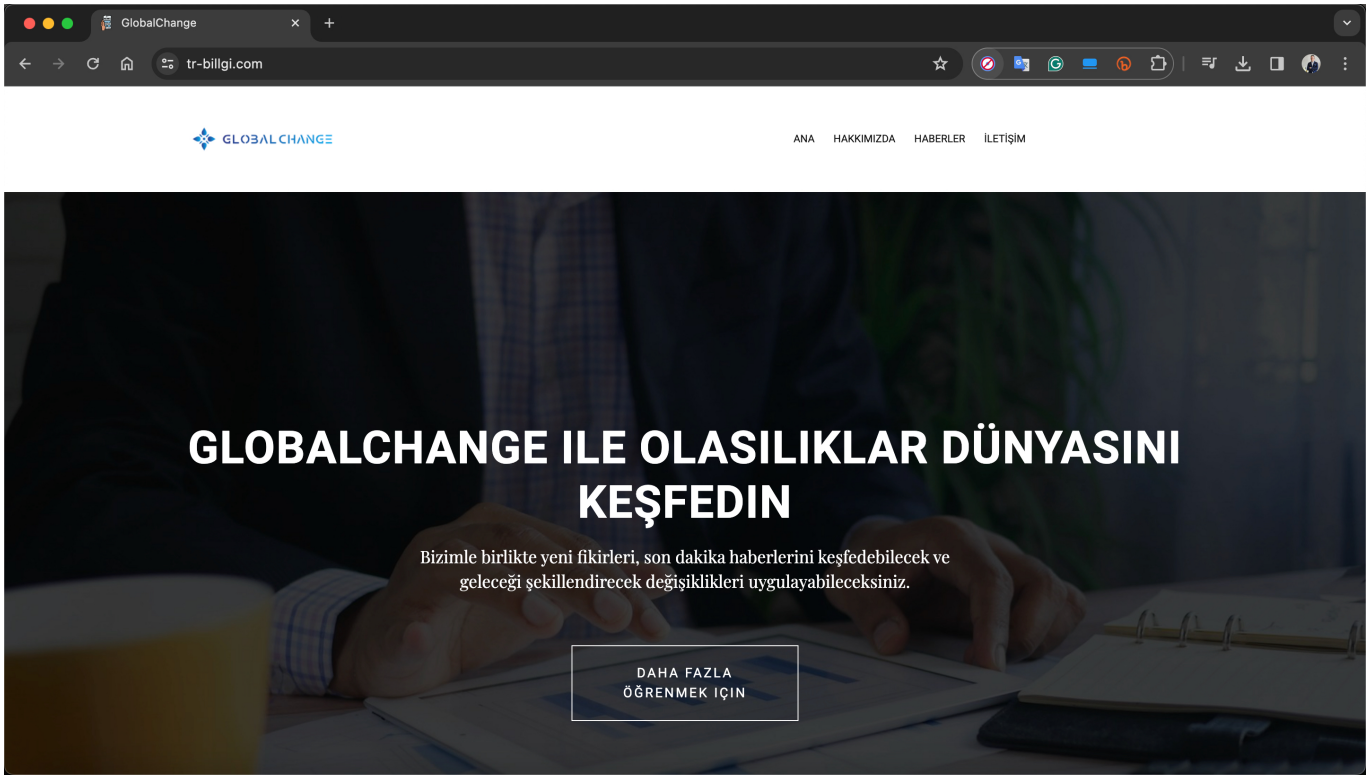
Teknik Araştırma

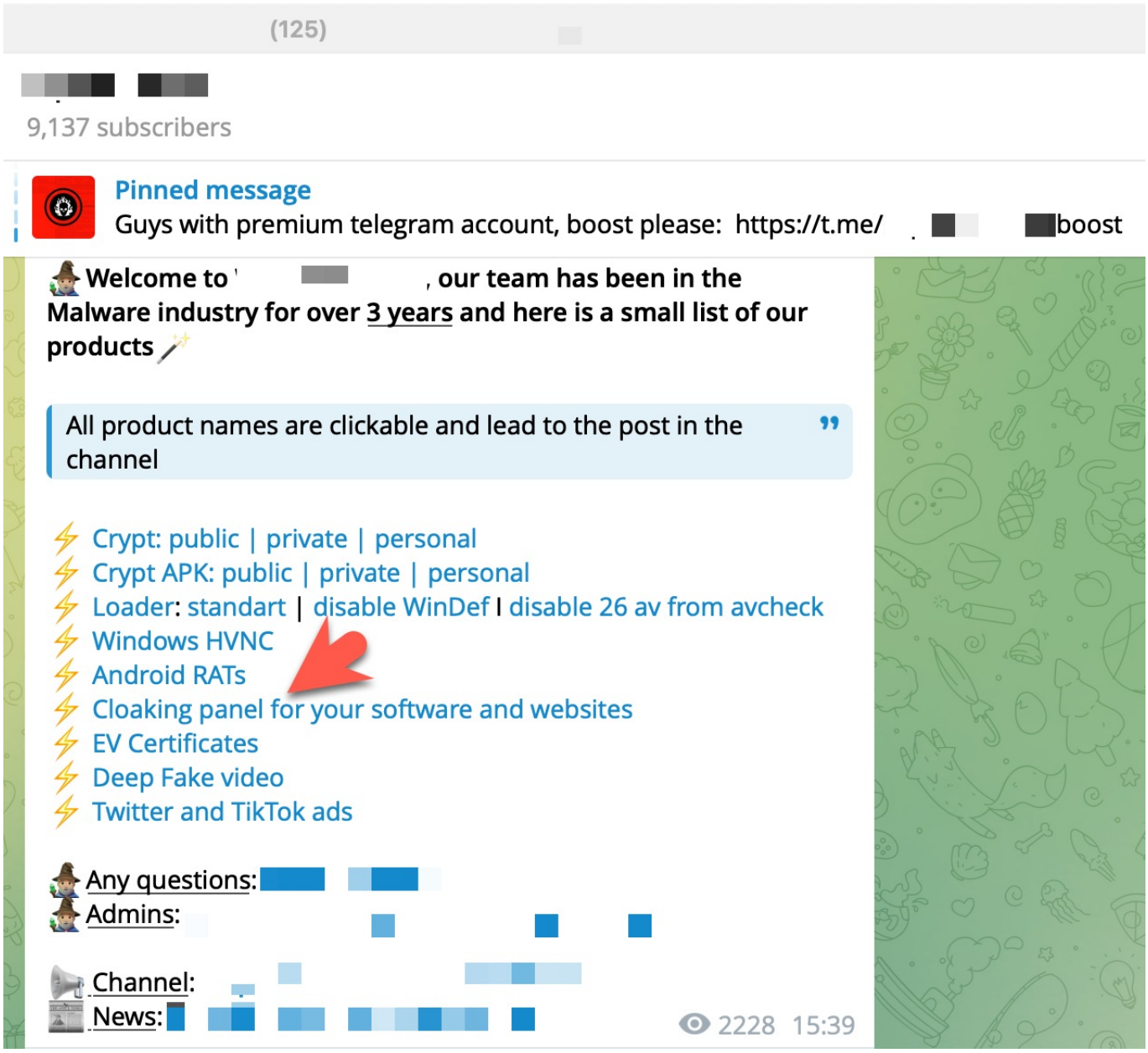
Keşif

2024 yılının Mart ayında USOM tarafından Zararlı Bağlantılar listesine Bankacılık – Oltalama açıklamasıyla eklenen tr-billgi[.]com alan adı dikkatimi çekti.



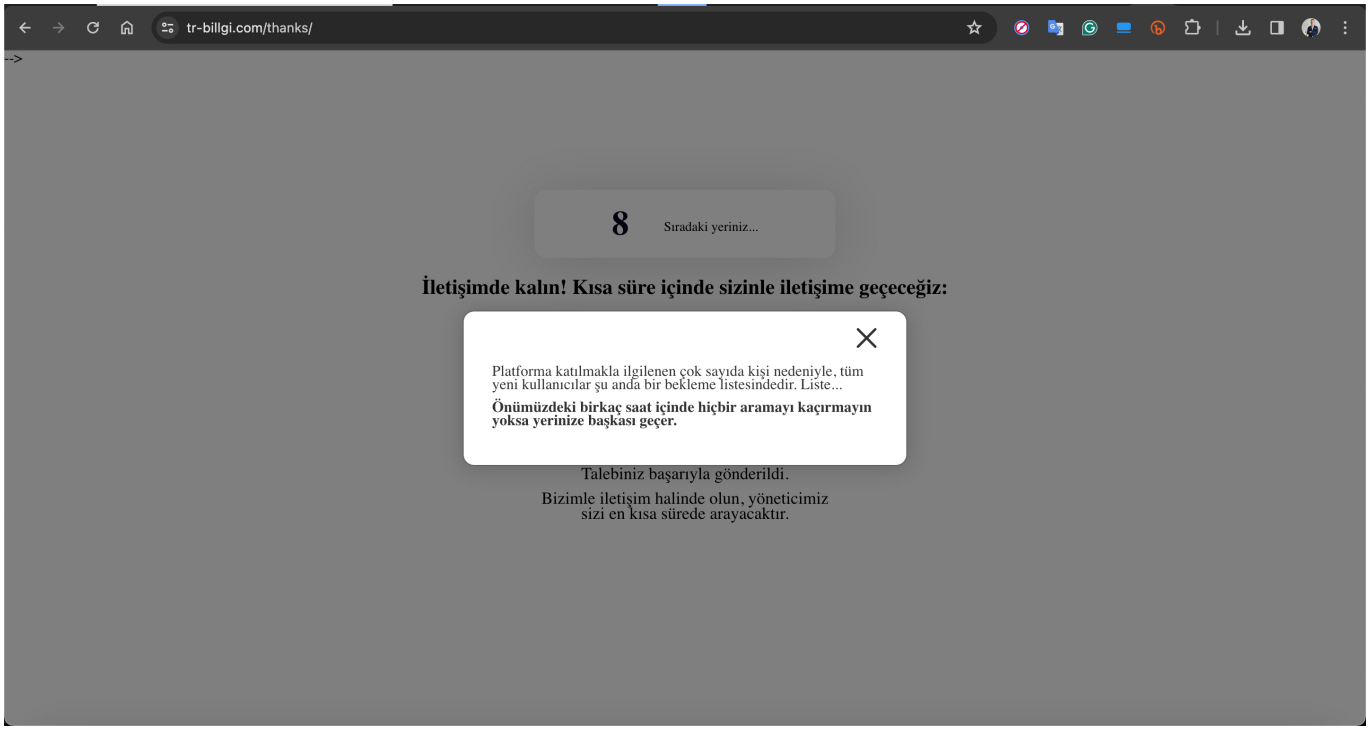
Web sitesini ziyaret ettiğimde karşılaştığım sayfa, oldukça sıradan ve zararsız görünüyordu. Olsa olsa bu sayfanın, tehdit aktörleri arasında oldukça popüler olup, asıl oltalama sayfasını gizlemek amacıyla oluşturulmuş sahte ana sayfa (cloaking) olduğunu düşünerek bu web sitesi üzerinde araştırma yapmaya karar verdim ve hikayemiz bu şekilde başlamış oldu.


GlobalChange
tr-bilgi.com
GLOBALCHANGE
ANA
HAKKIMIZDA
HABERLER
İLETİŞİM
GLOBALCHANGE ILE OLASILIKLAR DÜNYASINI KEŞFEDIN
Bizimle birlikte yeni fikirleri, son dakika haberlerini keşfedebilecek ve geleceği şekillendirecek değişiklikleri uygulayabileceksiniz.
DAHA FAZLA ÖĞRENMEK IÇIN



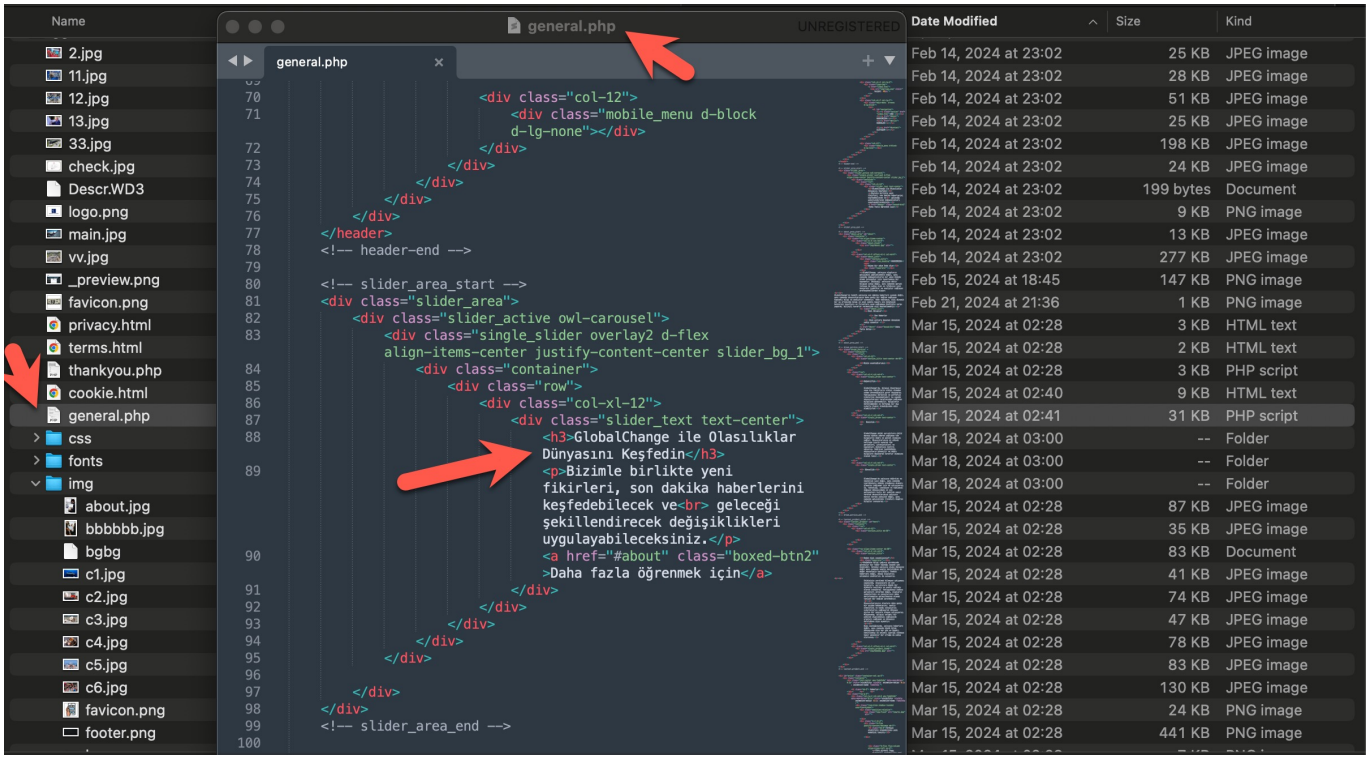
Zararlı İçerik Tespiti

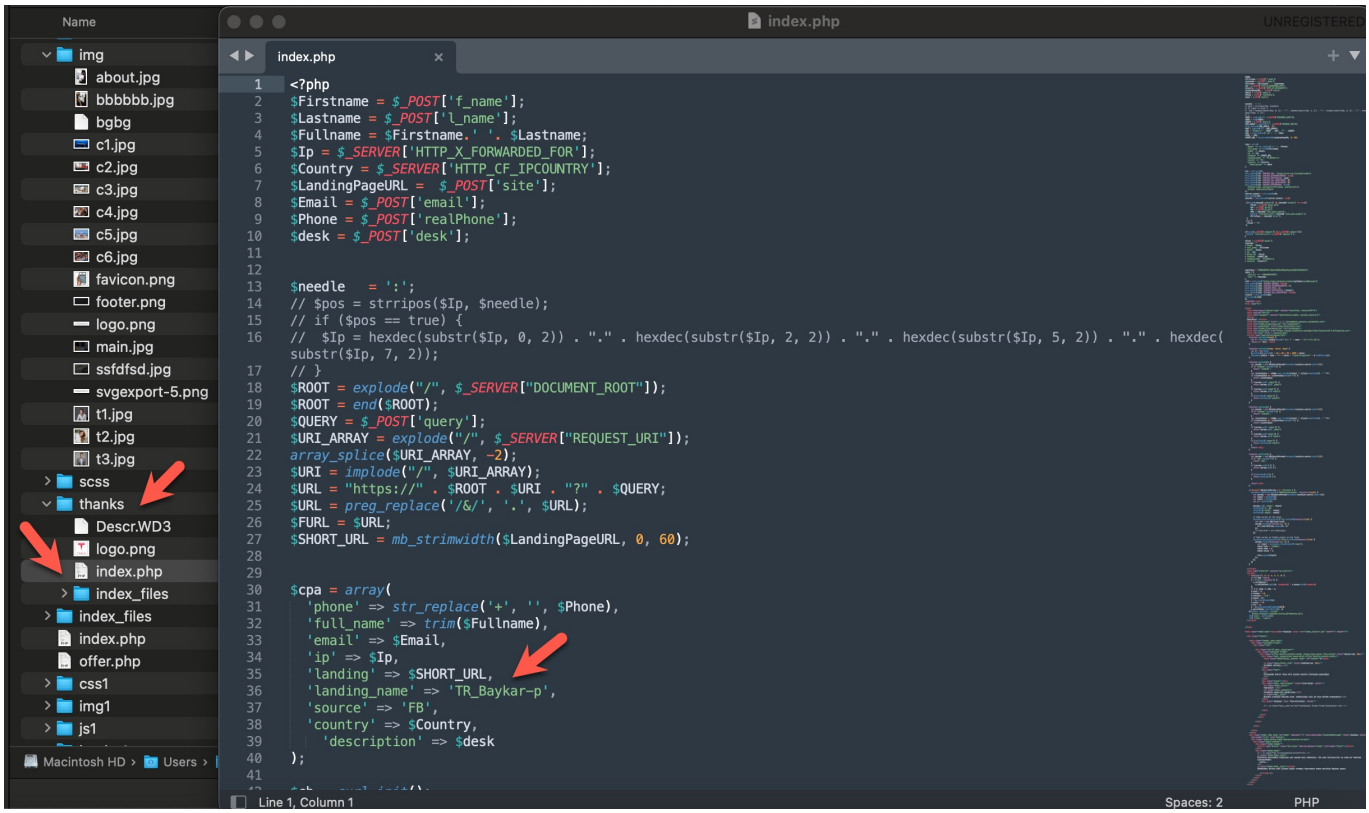
tr-billgi[.]com web sitesini biraz kurcaladığımda /thanks klasörü dikkatimi çekti. Bu sayfayı ziyaret ettiğimde, burasının web sitesinde yer alan herhangi bir formu dolduranların yönlendirildiği bir sayfa olduğunu düşünmeye başladım. Özellikle sayfada itinayla tekrarlanan “Hiçbir aramayı kaçırmayın”, “Yöneticimiz sizi en kısa sürede arayacaktır” ifadeleri bu formu dolduranların birileri tarafından arandığına işaret ediyordu.

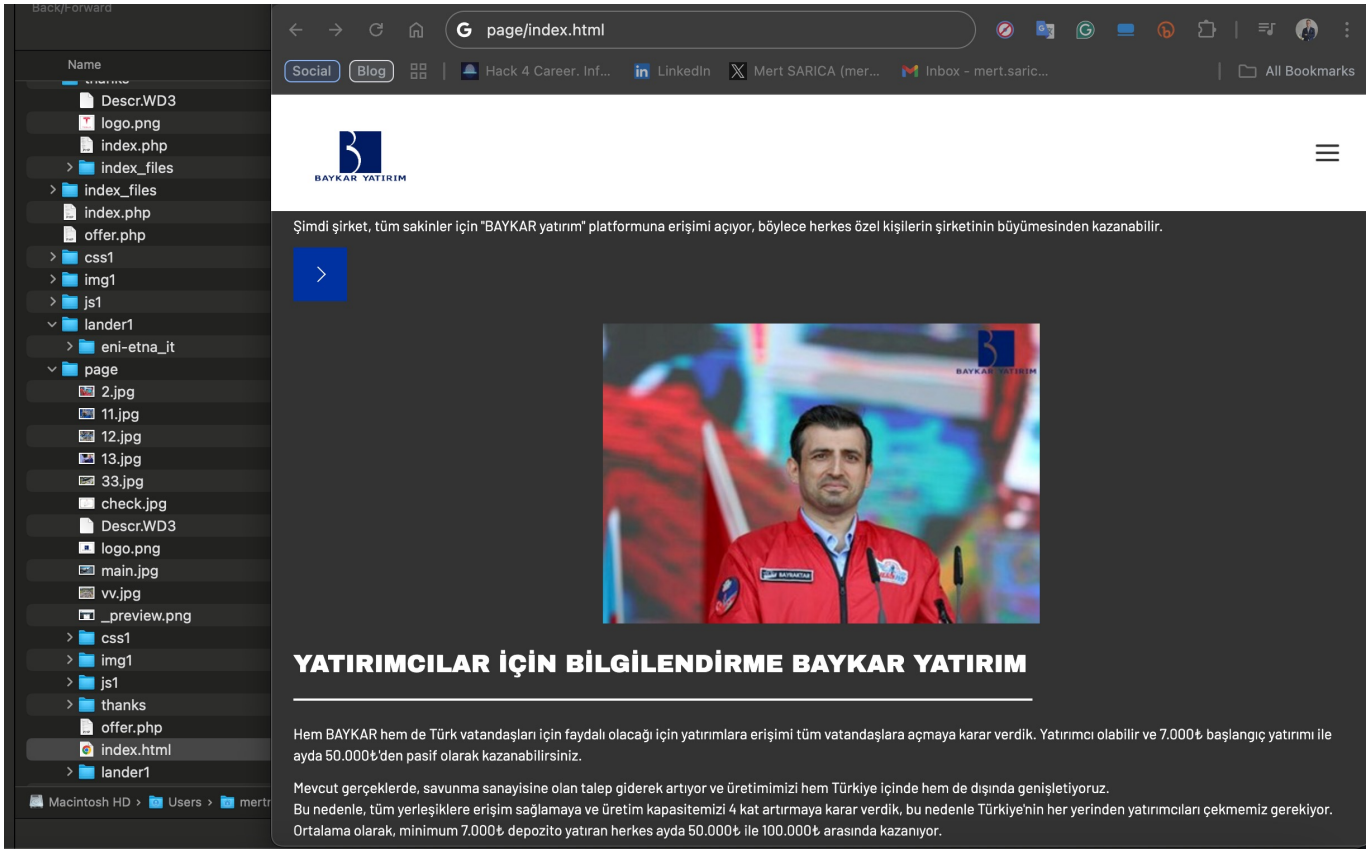


Bu web sitesini kurcalamaya devam ettiğimde bu tehdit aktörünün de, başka bir araştırma yazıma konu olanlar gibi Operasyon Güvenliği (OPSEC) noktasında hata yaptıklarını tespit ettim. Hatayı fırsata çevirip web sitesinin kaynak kodlarına eriştikten sonra kodları teker teker incelemeye başladım.

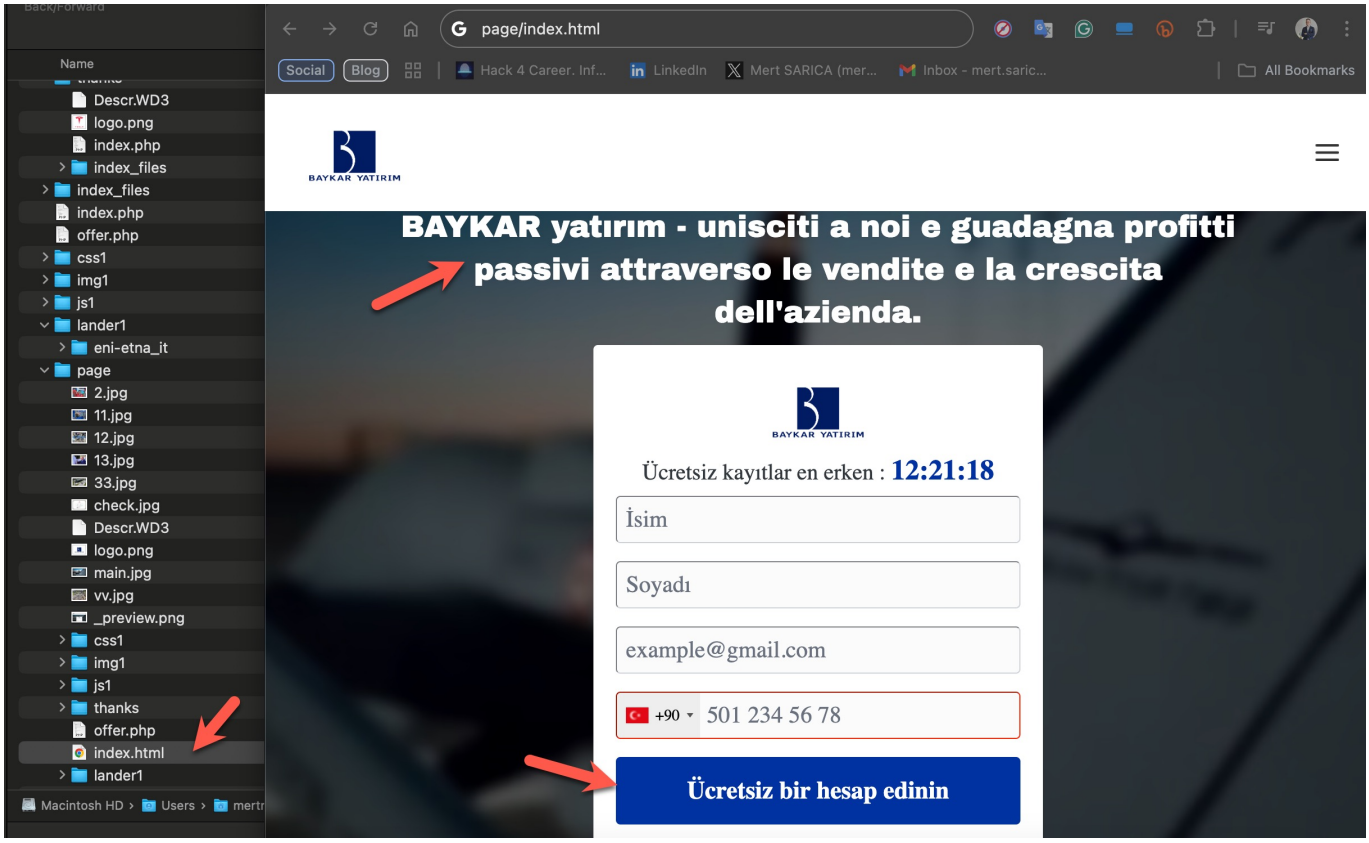
Kısa bir süre içinde general.php dosyasında sahte ana sayfaya ait kodları buldum. Thanks klasörü içinde yer alan index.php dosyasını, page klasöründe yer alan offer.php, index.html dosyalarını incelediğimde ise tehdit aktörleri tarafından bu oltalama sitesinin Baykar savunma şirketinin adını kötüye kullanarak kurbanlarını yatırım vaadiyle ağına düşürmek için tasarlandığını tespit ettim.


general.php
UNREGISTERED
Name
Date Modified
Size
Kind
2.jpg
11.jpg
12.jpg
13.jpg
33.jpg
check.jpg
Descr.WD3
logo.png
main.jpg
vv.jpg
_preview.png
favicon.png
privacy.html
terms.html
thankyou.php
cookie.html
general.php
css
fonts
img
about.jpg
bbbbbb.jpg
bgbg
c1.jpg
c2.jpg
c3.jpg
c4.jpg
c5.jpg
c6.jpg
favicon.png
footer.png
<h3>GlobalChange ile Olasılıklar Dünyasını Keşfedin</h3>
Bizimle birlikte yeni fikirleri, son dakika haberlerini keşfedebilecek ve
 geleceği şekillendirecek değişiklikleri uygulayabileceksiniz.
Daha fazla öğrenmek için


index.php
UNREGISTERED
Name
img
about.jpg
bbbbbb.jpg
bgbg
c1.jpg
c2.jpg
c3.jpg
c4.jpg
c5.jpg
c6.jpg
favicon.png
footer.png
logo.png
main.jpg
ssfdfsd.jpg
svgexport-5.png
t1.jpg
t2.jpg
t3.jpg
scss
thanks
Descr.WD3
logo.png
index.php
index_files
index_files
index.php
offer.php
css1
img1
js1
Macintosh HD › Users ›
<?php
$Firstname = $_POST['f_name'];
$Lastname = $_POST['l_name'];
$Fullname = $Firstname.' '. $Lastname;
$Ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
$Country = $_SERVER['HTTP_CF_IPCOUNTRY'];
$LandingPageURL = $_POST['site'];
$Email = $_POST['email'];
$Phone = $_POST['realPhone'];
$desk = $_POST['desk'];
$needle = ':';
// $pos = strripos($Ip, $needle);
// if ($pos == true) {
// $Ip = hexdec(substr($Ip, 0, 2)) . "." . hexdec(substr($Ip, 2, 2)) . "." . hexdec(substr($Ip, 5, 2)) . "." . hexdec(substr($Ip, 7, 2));
// }
$ROOT = explode("/", $_SERVER["DOCUMENT_ROOT"]);
$ROOT = end($ROOT);
$QUERY = $_POST['query'];
$URI_ARRAY = explode("/", $_SERVER["REQUEST_URI"]);
array_splice($URI_ARRAY, -2);
$URI = implode("/", $URI_ARRAY);
$URL = "https://" . $ROOT . $URI . "?" . $QUERY;
$URL = preg_replace('/&/', '.', $URL);
$FURL = $URL;
$SHORT_URL = mb_strimwidth($LandingPageURL, 0, 60);
$cpa = array(
'phone' => str_replace('+', '', $Phone),
'full_name' => trim($Fullname),
'email' => $Email,
'ip' => $Ip,
'landing' => $SHORT_URL,
'landing_name' => 'TR_Baykar-p',
'source' => 'FB',
'country' => $Country,
'description' => $desk
);
Line 1, Column 1
Spaces: 2
PHP

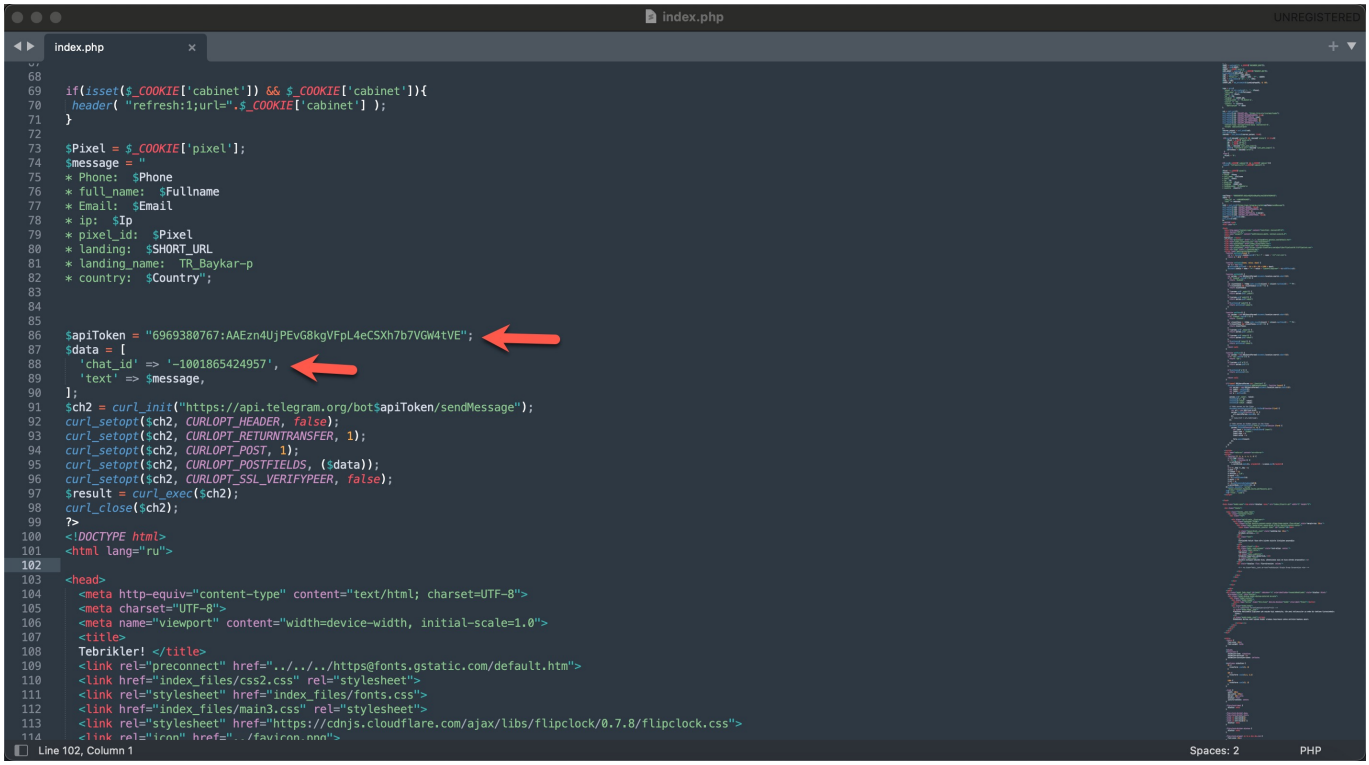


Oltalama sayfasındaki Türkçe metinlerin yanında İtalyanca metinlerin de yer alması bir yandan dikkatimi çekti. Tehdit aktörlerinin uluslararası kurumların adını (Slovnaft, INA d.d, Bosphorus Gaz, Baykar, Interpol) kullanarak dolandırıcılık girişiminde bulunduğunu Deepfake Dolandırıcılarına Dikkat! başlıklı yazımdan bildiğim için muhtemelen bu metin, İtalyan bir şirketi hedef almak için oluşturdukları İtalyanca oltalama sitesinden kalmış ve Türkçe'ye çevrilmesi unutulmuştu.



Teknik Takip

Bunların yanı sıra thanks klasörü içinde yer alan index.php dosyasında araştırmamı derinleştirecek çok önemli bir bilgiye daha ulaştım. O da tehdit aktörlerine ait olan Telegram Bot API jetonuydu (token).

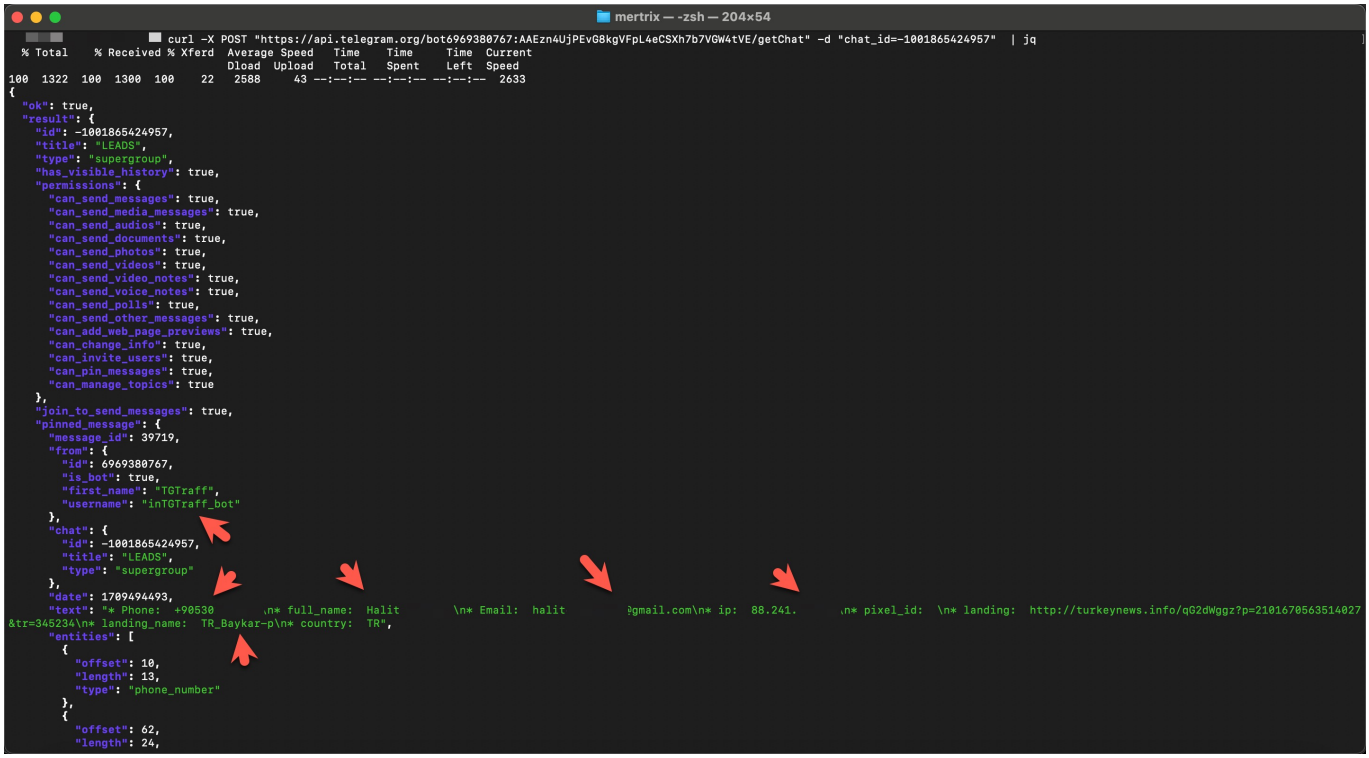


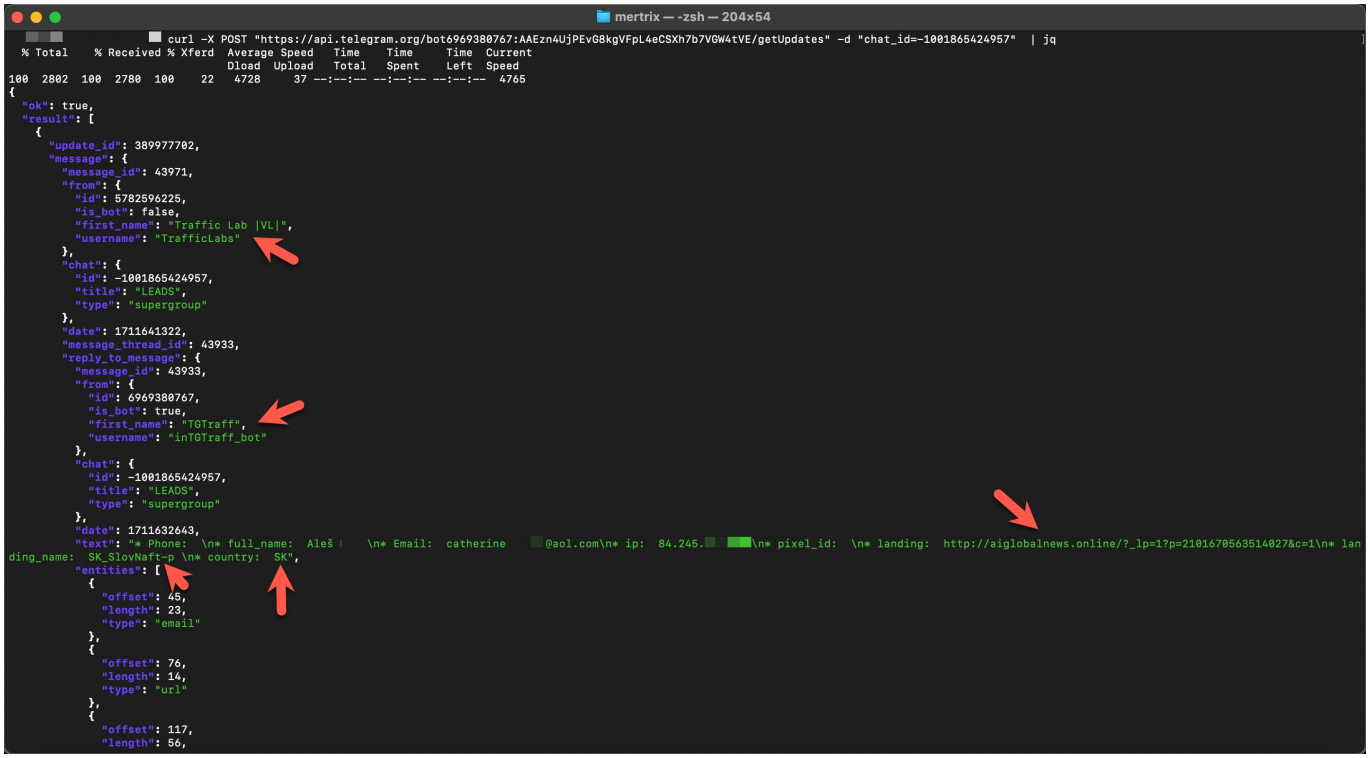
Telegram mesajlaşma uygulaması, hız, güvenlik ve dosya paylaşımı altyapısına sahip olması nedeniyle son yıllarda suç örgütlerinin, tehdit aktörlerinin, dolandırıcıların uğrak yeri olmaya devam ediyor.

Çoğu tehdit aktörü, Telegram Bot API'sinden faydalanarak oltaya düşürdükleri kişilerin çalınan bilgilerini anlık olarak oluşturdukları Telegram botları ile Telegram kanalları üzerinden takip etmektedirler. Bunun için yapmaları gereken ilk adım da botlarının jetonlarını (token) geliştirdikleri oltalama sitelerinin kaynak kodlarına yerleştirmektir.

Oltalama sitelerinin kaynak kodlarının başkalarının eline kolay kolay geçeceğini düşünmeyen tehdit aktörleri bu nedenle de bu jetonları aylarca değiştirmezler. Bu da emniyet güçlerinden, siber güvenlik araştırmacılarına kadar tehdit aktörlerinin Telegram üzerinden izlenmelerine olanak sağlar.

2024 yılının Mart ayı itibariyle bu jetonu kullanan Telegram botu üzerinden kanala gönderilen tüm mesajları mercek altına almaya başladığımda bu jetonun birden fazla oltalama sitesinde kullanıldığını gördüm. Oltalama sitesinde yer alan formu dolduran kurbanların ise adları, telefon numaraları, e-posta adresleri, IP adresleri, hangi oltalama sitesini ziyaret ettikleri ve hangi ülkeden geldikleri anlık olarak kanala iletiliyordu.

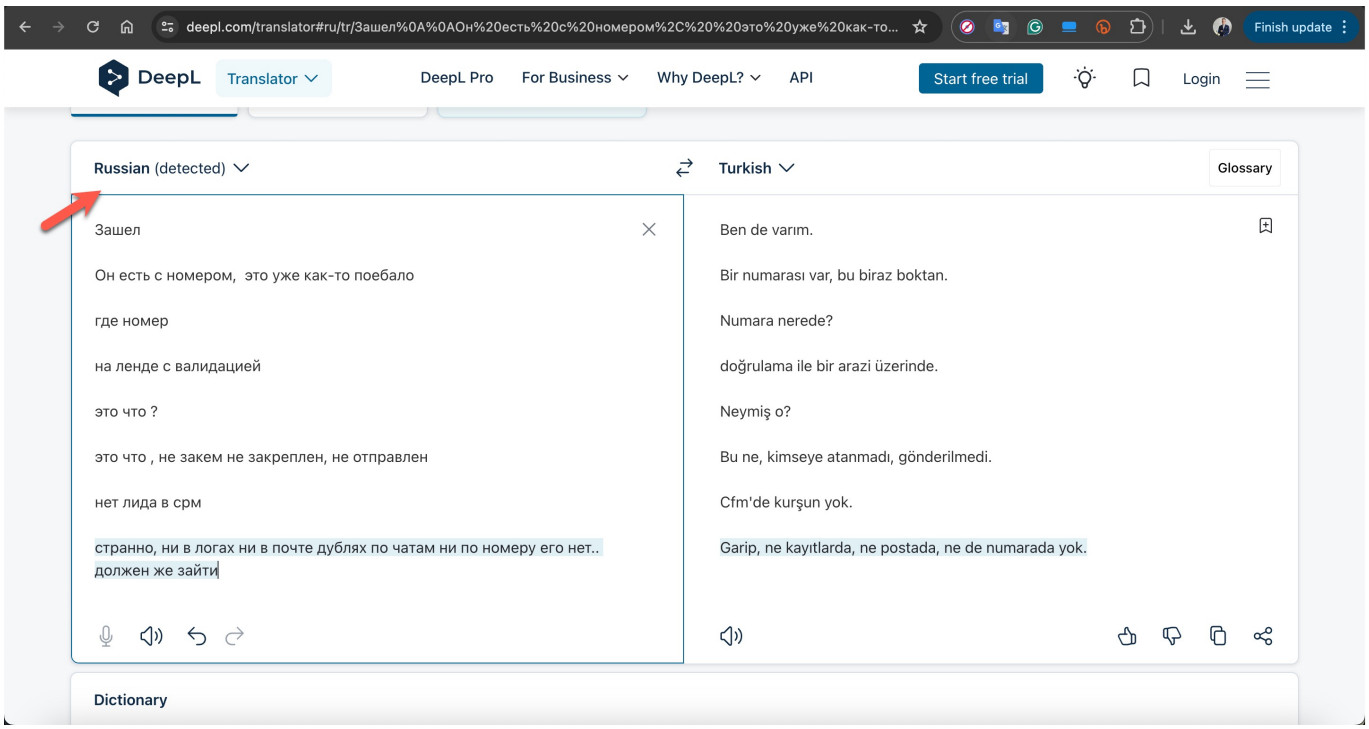


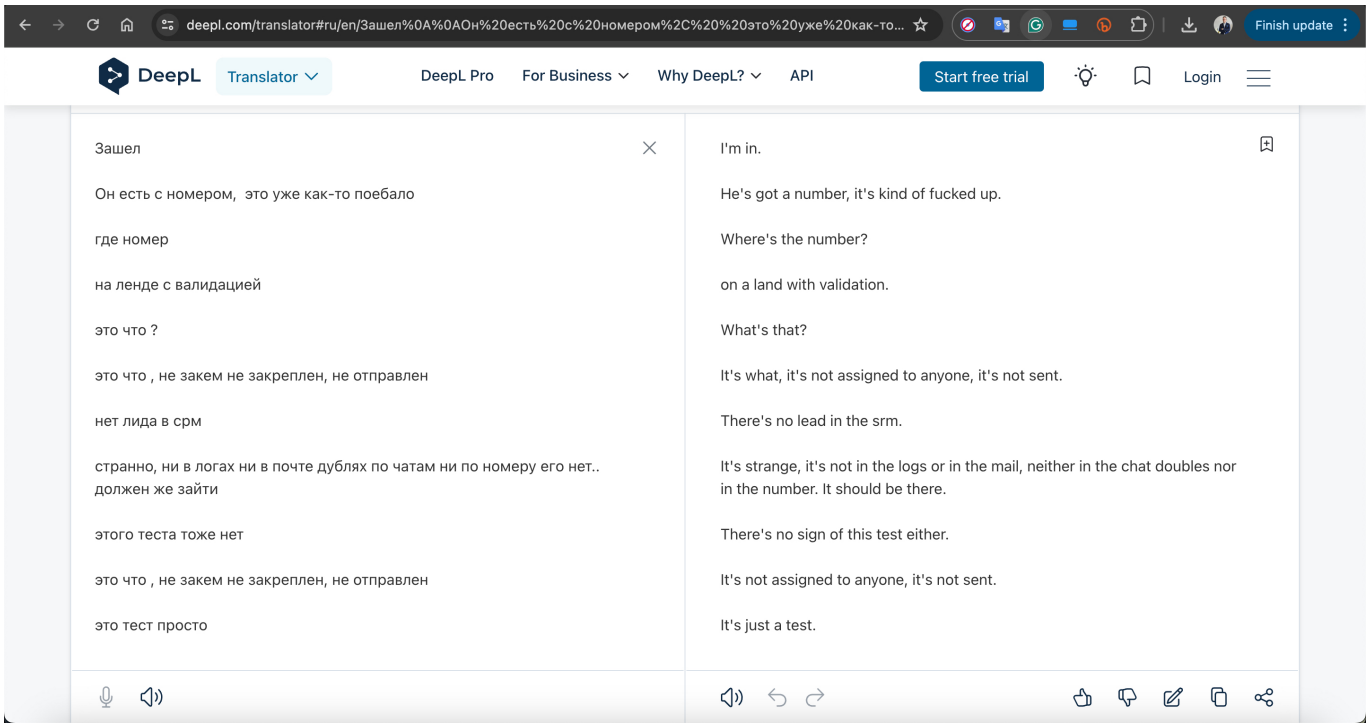


	A	B	C	D	E
1	**Phishing websites**		**Targeted Companies w/ Country Codes**		**Victim E-mails**
2	http://24main.news		CZ_Bitsoft-p		[redacted]@mailcom
3	http://allinone-news.com		EN_BitGPT-p		adriana.[redacted]@gmail.com
4	http://ca-ai-world.pro		EU_Quantum-p		alex [redacted]@centrum.sk
5	http://ca-profit-ai.com		HU_ImmediateConnect-p		alige[redacted]@hotmail.com
6	http://hurriyet-tr.today		Ru_legion-g		ana [redacted]@gmail.com
7	http://inone-news.com		SI_Petrol-l		ayem [redacted]@yahoo.com
8	http://news-online.pro		SK_SlovNaft-p		aylin[redacted]@gmail.com
9	http://news-online.wiki		TR-EU_Bosphorus-t		aysel[redacted]@hotmail.com
10	http://news-proff.pro		TR_Baykar-l		cance [redacted]@gmail.com
11	http://news-sheet.today		TR_Baykar-p		cihan [redacted]@hotmail.com
12	http://official-tr-news.today		TR_Bosphorgaz-p		cure [redacted]@gmail.com
13	http://sk-slnft.site		TR_Bosphorus-t		dogan[redacted]@gmail.com
14	http://tr-bsfr.pro		TR_Kalyon-t		efehan [redacted]@hotmail.com
15	http://tr-haberler.today				ejder[redacted]@gmail.com
16	http://tr-inf.com				ekremc[redacted].@gmail.com
17	http://tr-inform.com				fatma[redacted]@gmail.com
18	http://tr-pro.info				fena[redacted]@hotmail.com
19	http://turkeynews.info				fidan_[redacted]@gmail.com
20	https://ch-back-ltd.com				fm [redacted]@gmail.com
21	https://tr-bkr.com				[redacted]@ss.ss
22	https://tr-byr.com				gabriel[redacted]@gmail.com
23	https://news-inform.site				gyula[redacted]@gmail.com
24	https://baslangicnoktasi.online/				halil [redacted]@gmail.com
25	https://proinfo-trader.site				havasi[redacted]@gmail.com
26	https://bilgihazinesi.online/				hilul [redacted]@gmail.com
27	https://xn--hayalmezar-6ub.online				hj[redacted]@dsd.dd
28	https://moniwise.info				h[redacted]@gmai.com
29					jancobalog17@gmail.com

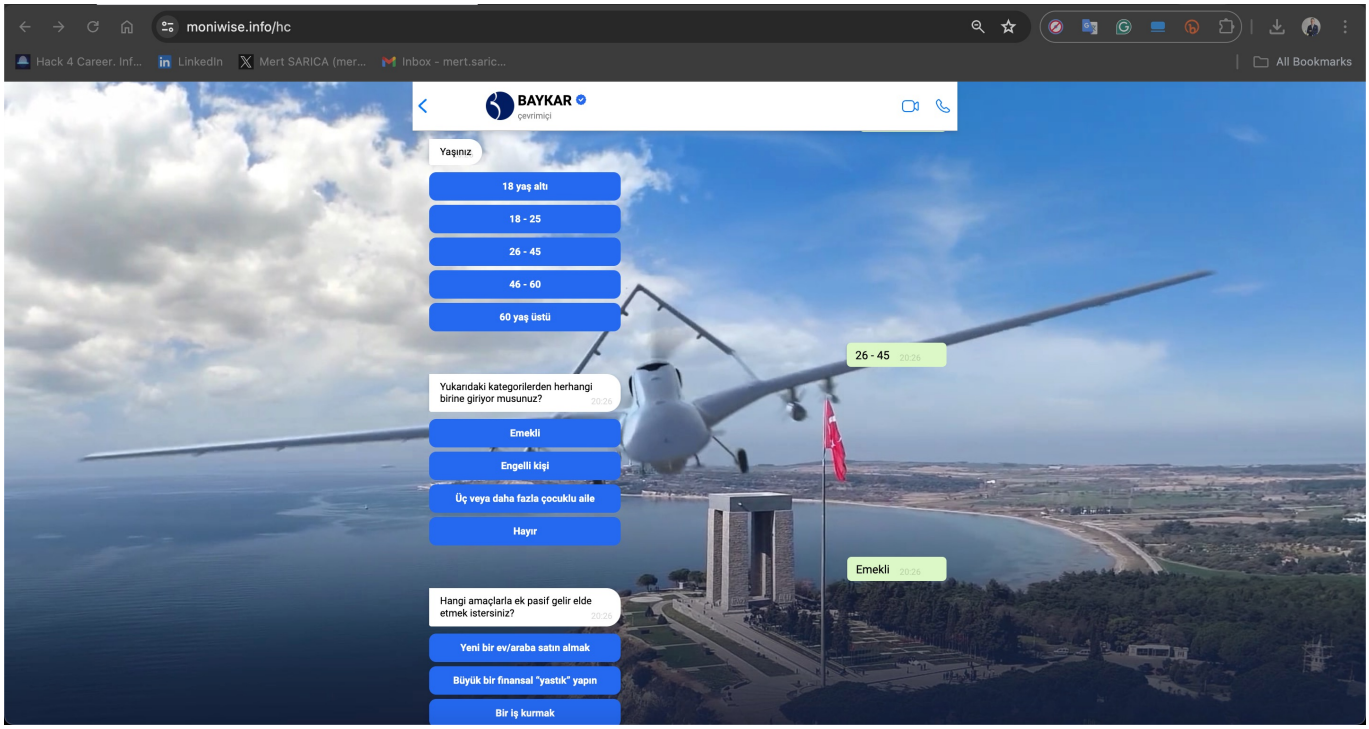
Kanalda yer alan kullanıcıların profillerine ve aralarında geçen yazışmalara baktığımda Rus mu yoksa Ukraynalı mı olduklarına kanaat getirmekte zorlandığım için son kararı Deepl çeviri uygulamasına bırakmaya karar verdim. Deepl, tüm bu metinlerin Rusça olduğunu belirtti. Bu kullanıcılar gerçekten bu oltalama sitelerini kuran, operasyonunu yürüten kişiler miydi yoksa sadece

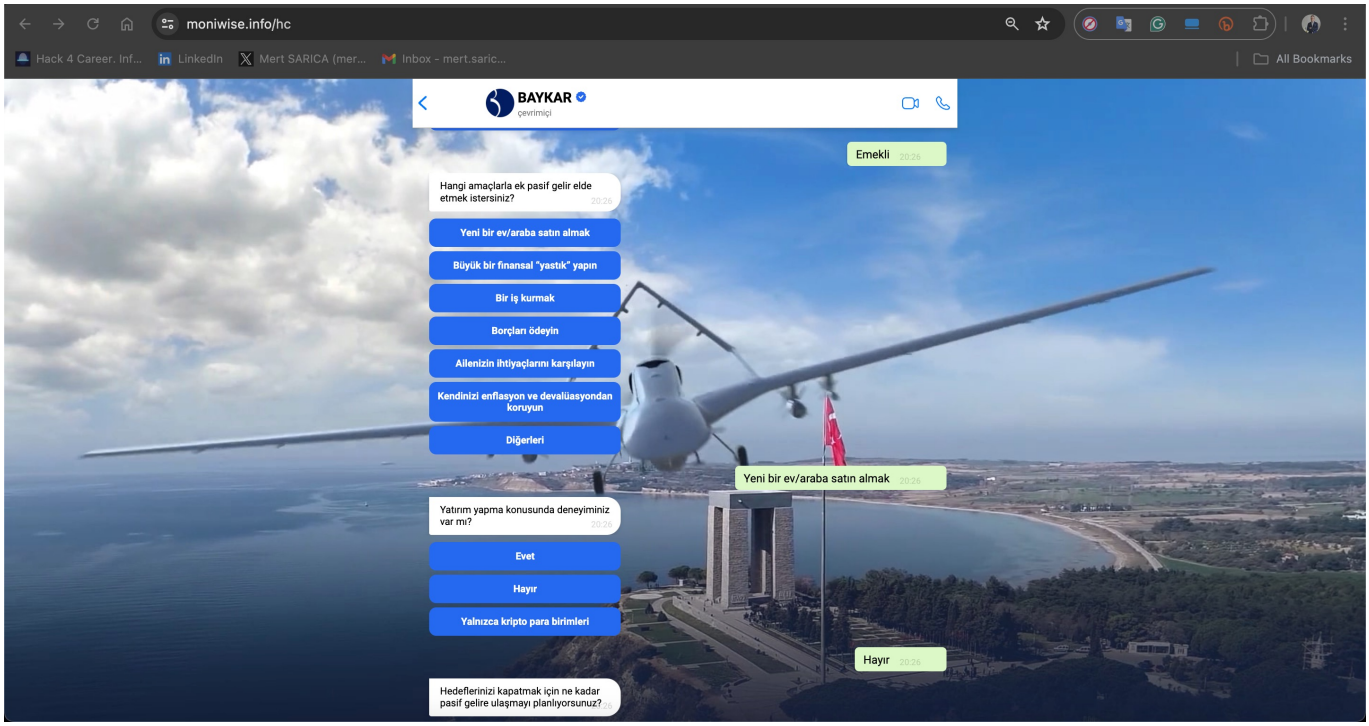
tehdit aktörlerine Telegram Botu hizmeti sağlayan aracı hizmet sağlayıcısının yöneticileri miydi bu kısımdan çok emin olamadım.

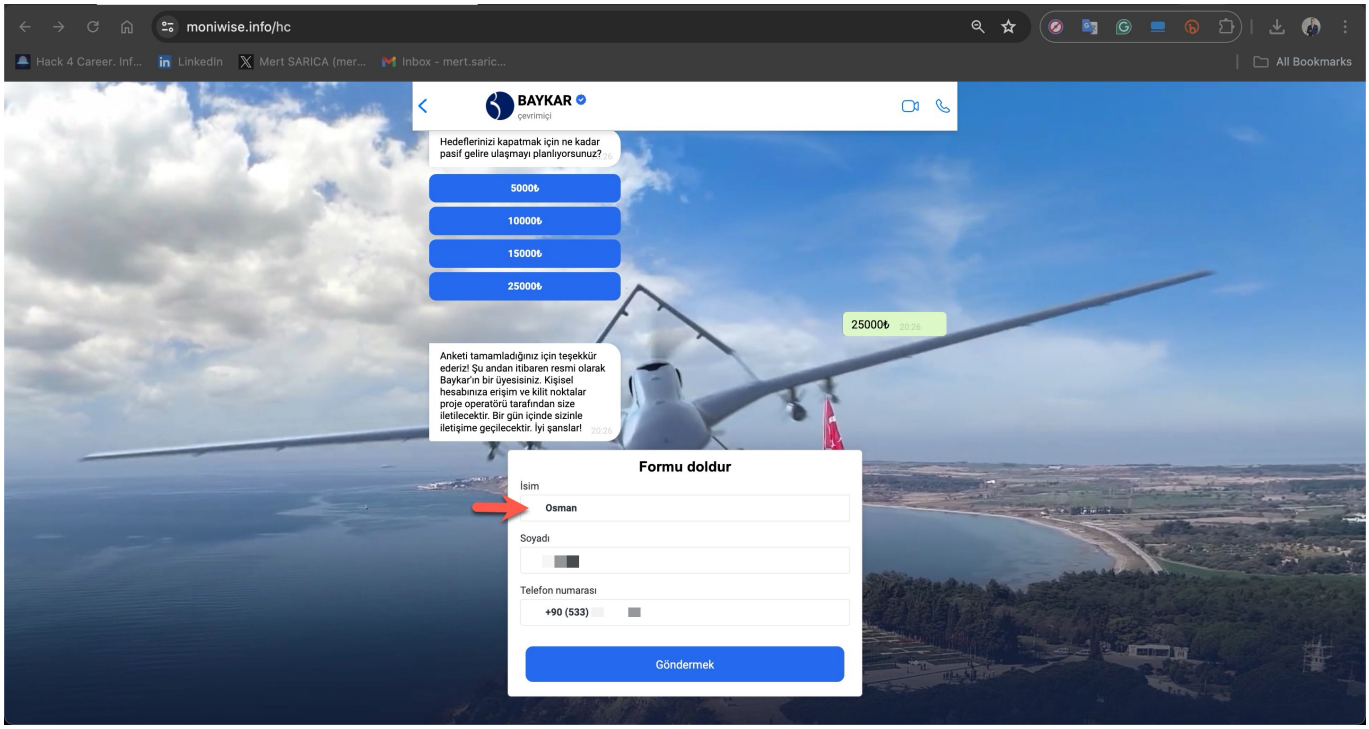


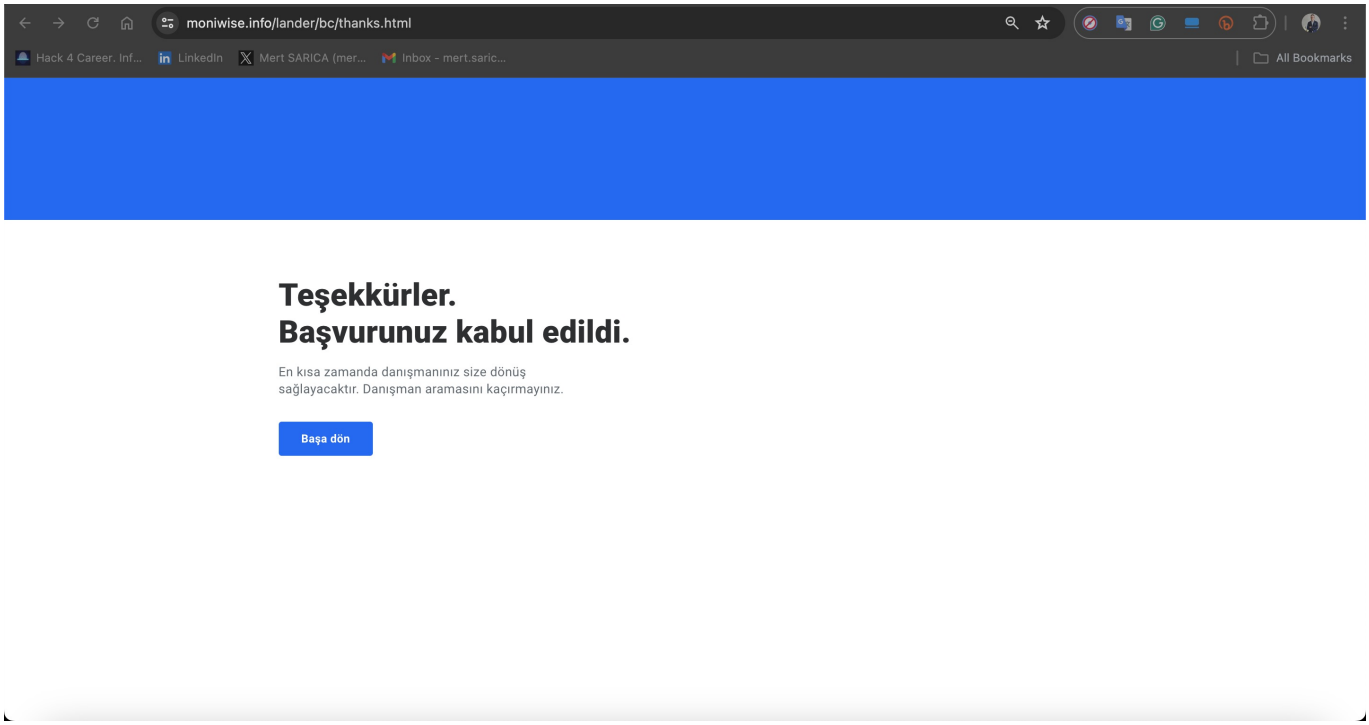


2024 yılının Temmuz ayına kadar dolandırıcıların oltalama amacıyla kullandığı web sitelerini yakın takibe aldıktan sonra bu web sitelerindeki formlara dolandırıcılarla iletişim kurabilmek için telefon numaramı girmeye başladım.


moniwise.info/hc
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
All Bookmarks
BAYKAR
çevrimiçi
Yaşınız
18 yaş altı
18 - 25
26 - 45
46 - 60
60 yaş üstü
26 - 45
Yukarıdaki kategorilerden herhangi birine giriyor musunuz?
Emekli
Engelli kişi
Üç veya daha fazla çocuklu aile
Hayır
Emekli
Hangi amaçlarla ek pasif gelir elde etmek istersiniz?
Yeni bir ev/araba satın almak
Büyük bir finansal "yastık" yapın
Bir iş kurmak

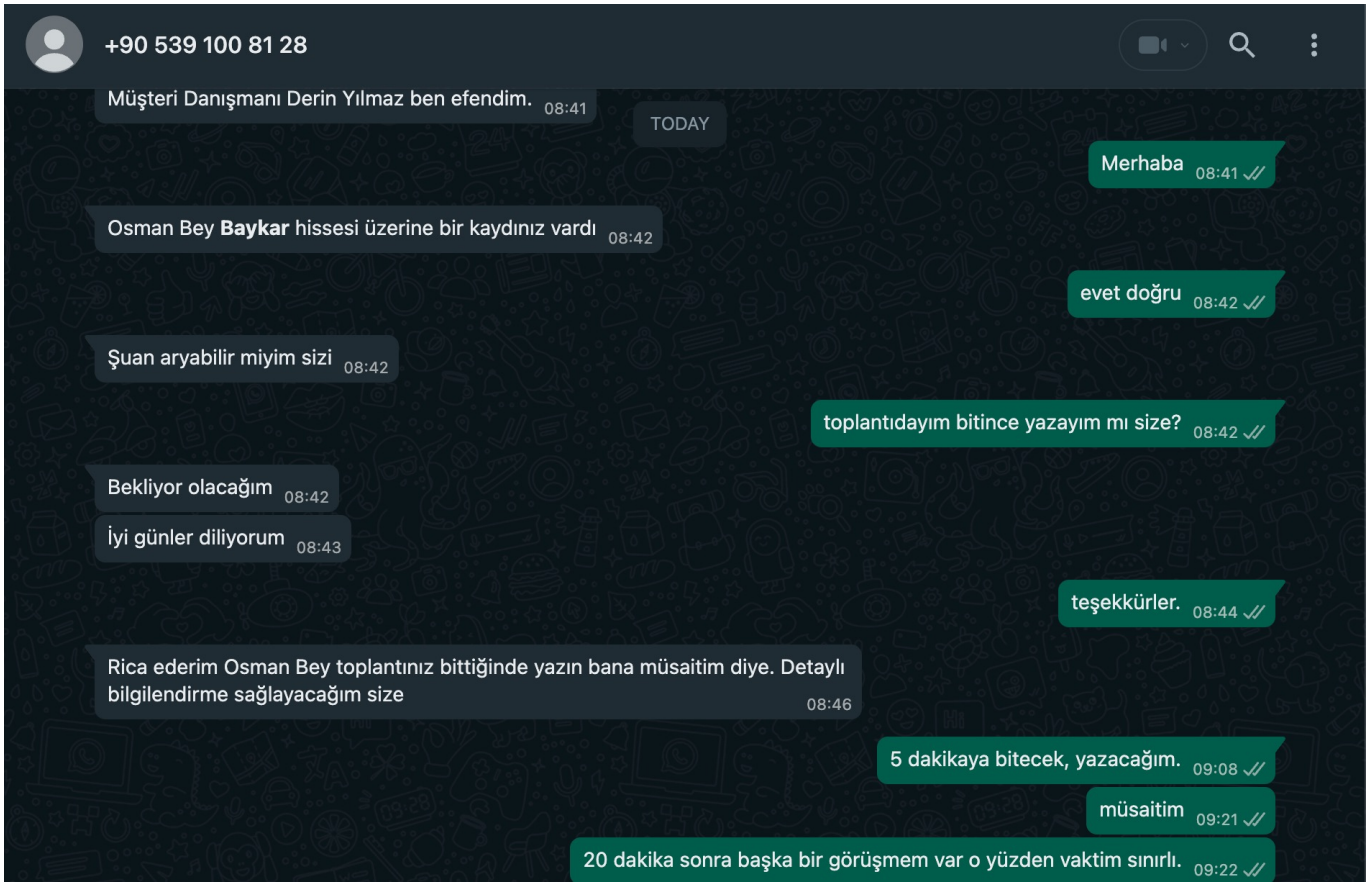

moniwise.info/hc
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
All Bookmarks
BAYKAR
çevrimiçi
Emekli
Hangi amaçlarla ek pasif gelir elde etmek istersiniz?
Yeni bir ev/araba satın almak
Büyük bir finansal "yastık" yapın
Bir iş kurmak
Borçları ödeyin
Ailenizin ihtiyaçlarını karşılayın
Kendinizi enflasyon ve devalüasyondan koruyun
Diğerleri
Yeni bir ev/araba satın almak
Yatırım yapma konusunda deneyiminiz var mı?
Evet
Hayır
Yalnızca kripto para birimleri
Hayır
Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz?





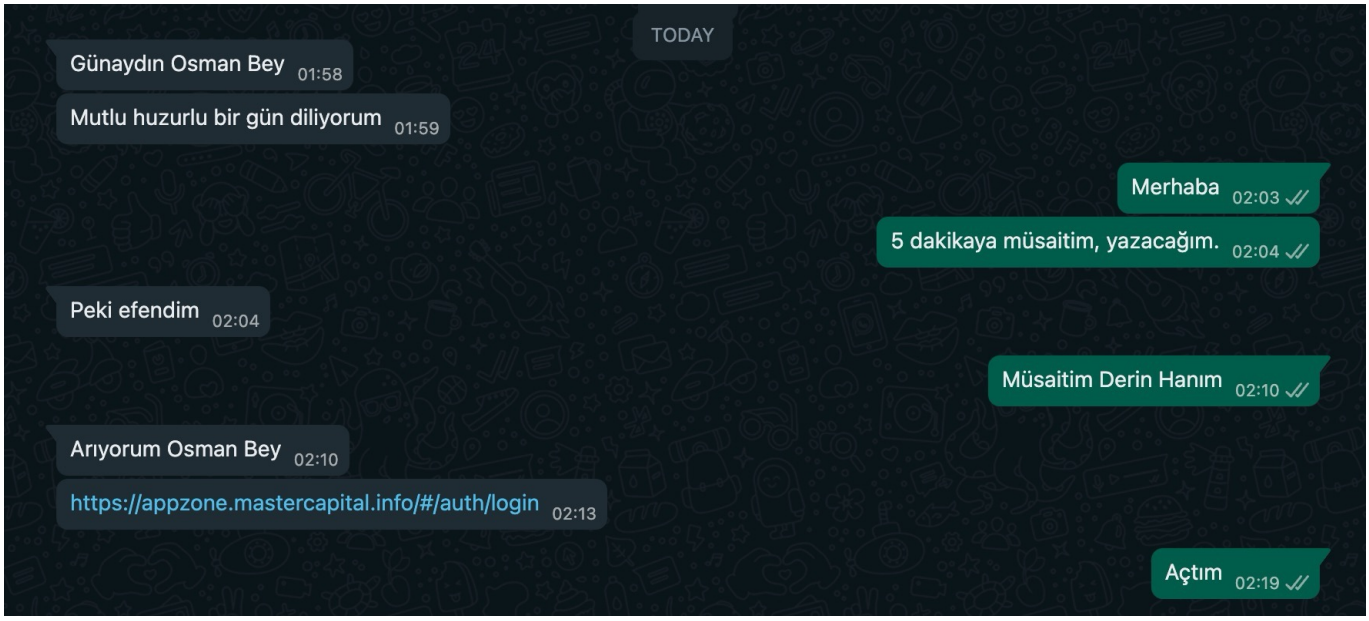
1. Dolandırıcılık Girişimi

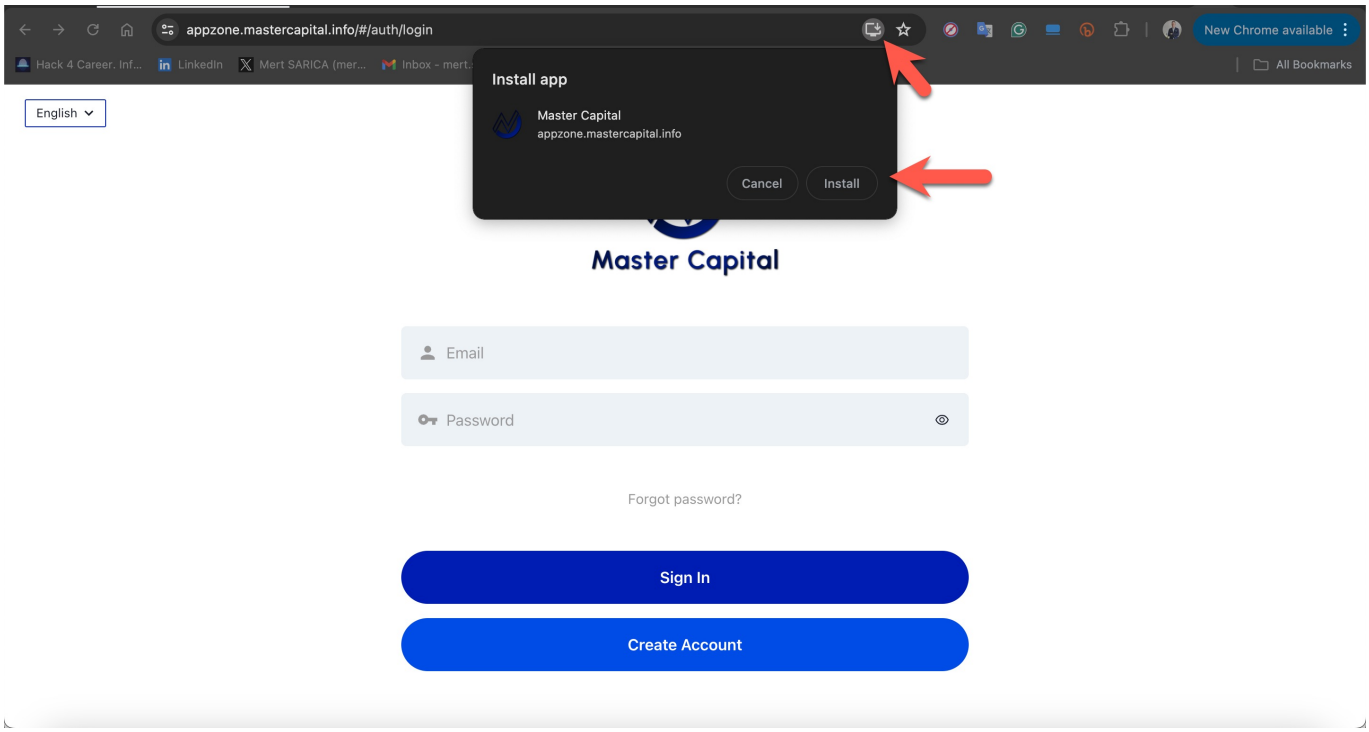
Takvimler 22 Temmuz 2024'ü gösterdiğinde +90 539 100 81 28 numaralı cep telefonundan kendisini müşteri danışmanı olarak tanıtan Derin isimli bir kişiden doldurduğum forma istinaden WhatsApp mesajı aldım.



Amerika'da yaşadığım ve Türkiye ile saat farkı 7 saat olduğu için dolandırıcı ile iletişim kurmak zaman zaman zor oldu. Özellikle dolandırıcı Türkiye saati ile 9/6 çalıştığı (fazla mesai yapmayan bir meslek dalı :)) ve benimle iletişim kurmayı sabah saatlerinde yapmayı tercih ettiği için benim saatime göre çoğu görüşmemiz gece saat 02:00'dan sonra gerçekleşti. Amacım bu dolandırıcılık çarkını ortaya çıkarmak olduğu için gecenin körü de olsa tüm çağrılarını büyük bir motivasyonla yanıtlamayı başardım.

Dolandırıcı ile 23 Temmuz 2024 tarihinde yaptığım WhatsApp görüşmesinde, hisse alım satımı gerçekleştirebilmek için öncelikle mobil cihazıma bir uygulama yüklemem gerektiğini ve bunun için de https://appzone[.]mastercapital[.]info/#/auth/login web adresini ziyaret etmem gerektiğini belirtti. Her ne kadar dolandırıcı bunu mobil uygulama olarak adlandırsa da işin aslında bunun bir Progressive Web Apps (PWA) web uygulaması olduğunu gördüm.


TODAY
Günaydın Osman Bey 01:58
Mutlu huzurlu bir gün diliyorum 01:59
Merhaba 02:03
5 dakikaya müsaitim, yazacağım. 02:04
Peki efendim 02:04
Müsaitim Derin Hanım 02:10
Arıyorum Osman Bey 02:10
https://appzone.mastercapital.info/#/auth/login 02:13
Açtım 02:19


appzone.mastercapital.info/#/auth/login
New Chrome available
All Bookmarks
Install app
Master Capital
appzone.mastercapital.info
Cancel
Install
English
Master Capital
Email
Password
Forgot password?
Sign In
Create Account

pzone.mastercapital.info

Master Capital

Email

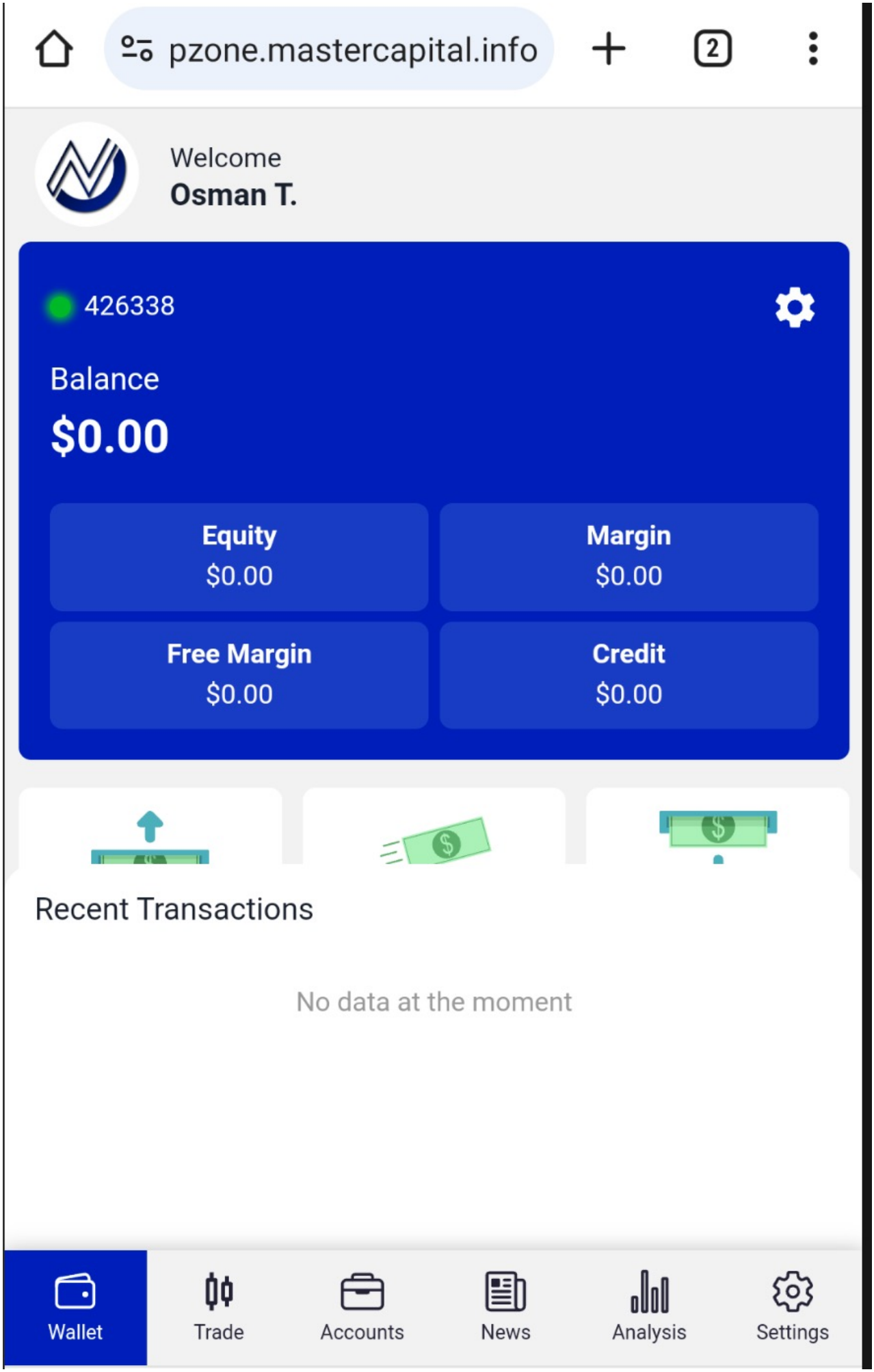
Password

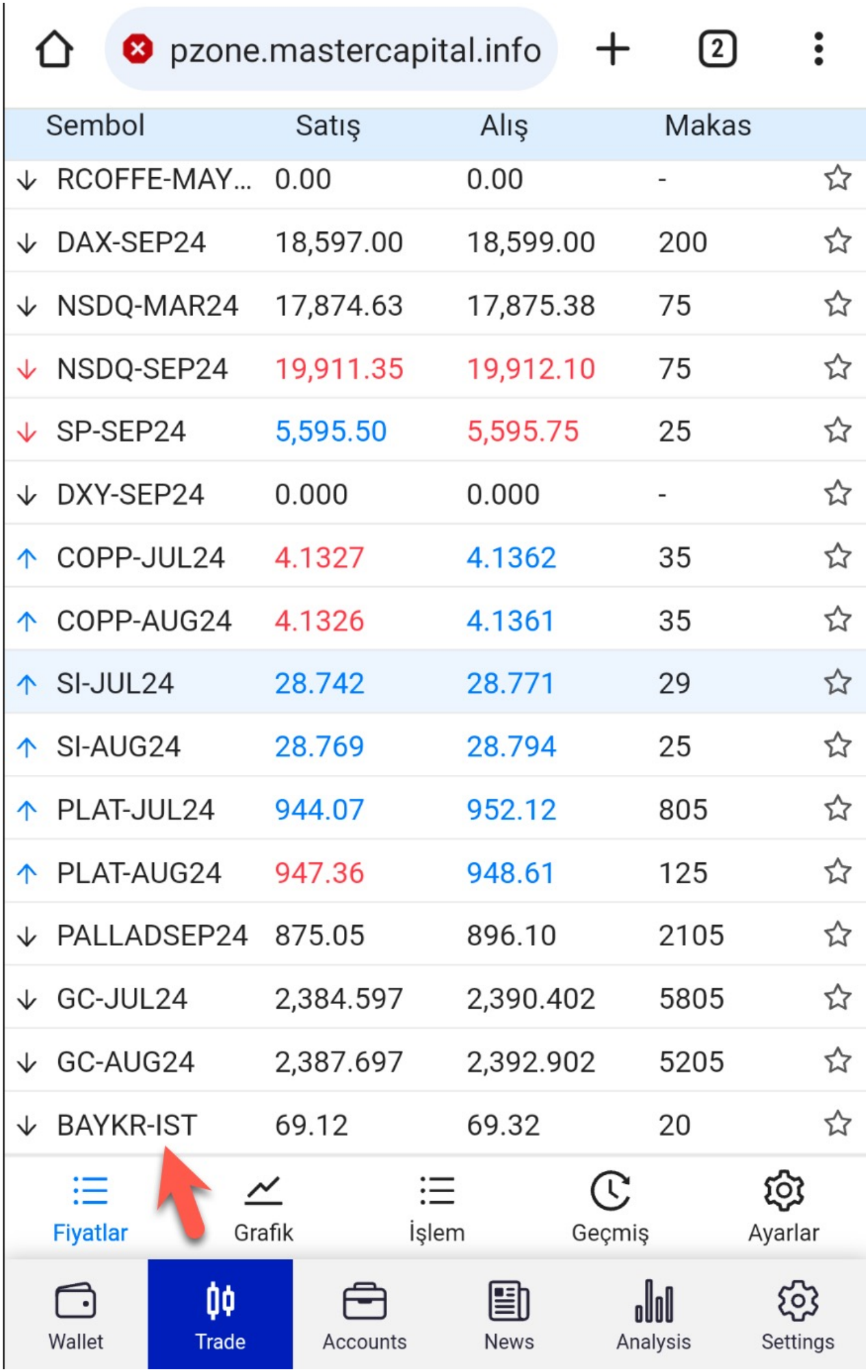
Forgot password?

Sign In

Create Account

Web uygulamasına giriş yaptığımda karşılaştığım ekranlar Kripto Para Dolandırıcıları başlıklı yazıma konu olan sahte borsaya oldukça benziyordu. Farklı olan kısım, dolandırıcılar tarafından uygulamada yer alan sembol listesine sahte Baykar hisse senedi sembolünü (BAYKR-IST) eklemiş olmalarıydı.

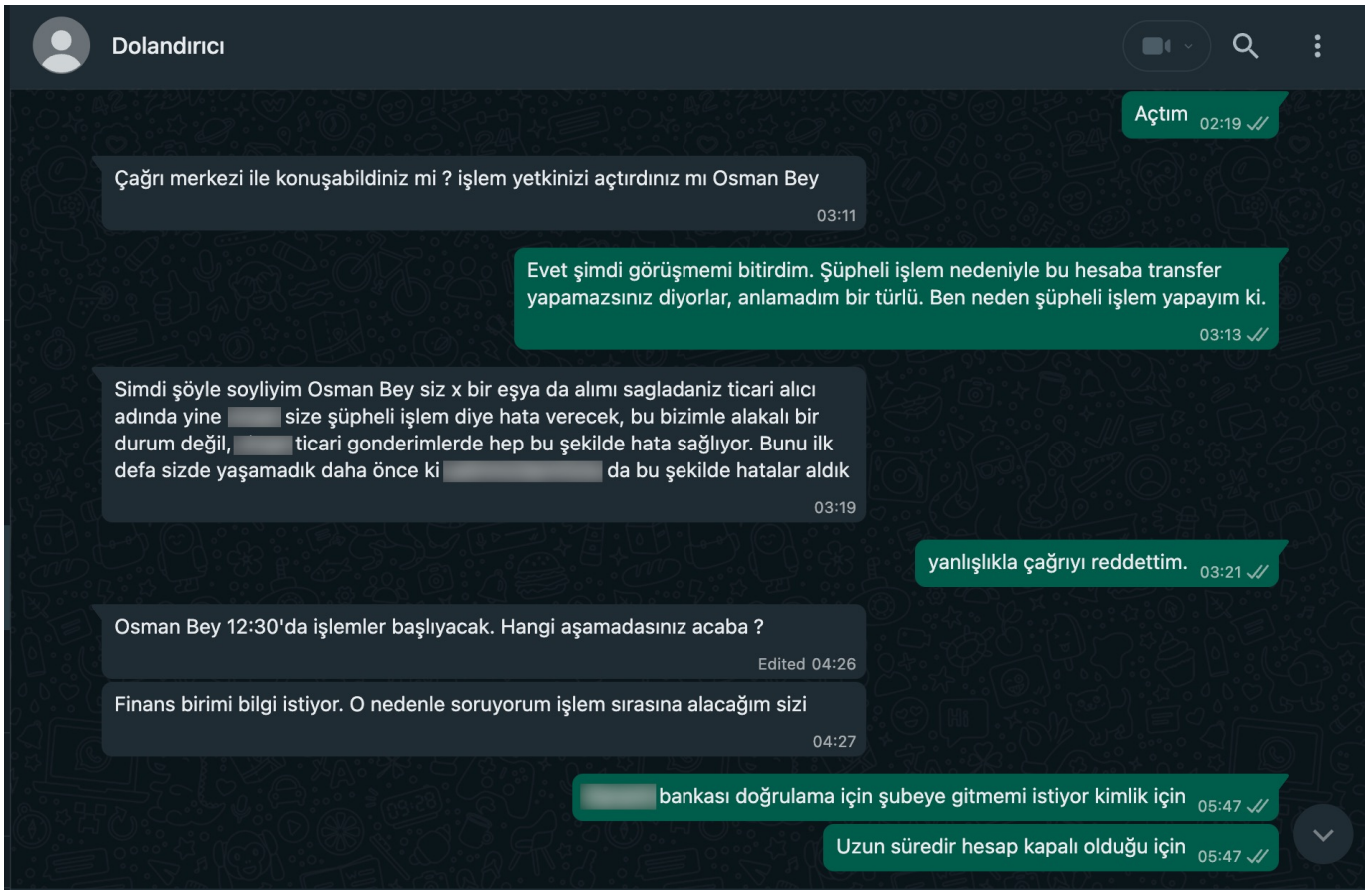

pzone.mastercapital.info
2
Welcome
Osman T.
426338
Balance
$0.00
Equity
$0.00
Margin
$0.00
Free Margin
$0.00
Credit
$0.00
Recent Transactions
No data at the moment
Wallet
Trade
Accounts
News
Analysis
Settings

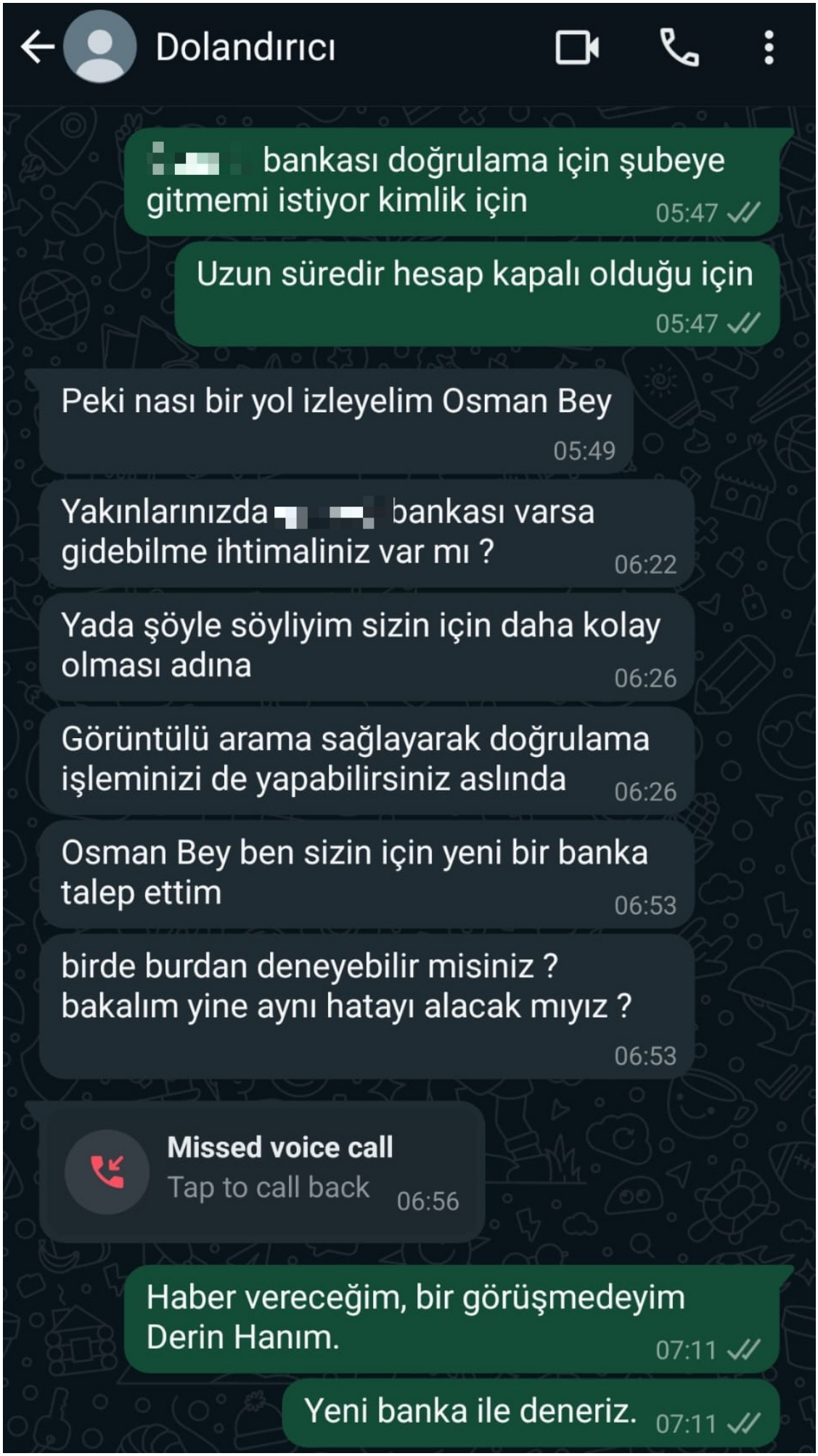

pzone.mastercapital.info
2
Sembol Satış Alış Makas
RCOFFE-MAY... 0.00 0.00 -
DAX-SEP24 18,597.00 18,599.00 200
NSDQ-MAR24 17,874.63 17,875.38 75
NSDQ-SEP24 19,911.35 19,912.10 75
SP-SEP24 5,595.50 5,595.75 25
DXY-SEP24 0.000 0.000 -
COPP-JUL24 4.1327 4.1362 35
COPP-AUG24 4.1326 4.1361 35
SI-JUL24 28.742 28.771 29
SI-AUG24 28.769 28.794 25
PLAT-JUL24 944.07 952.12 805
PLAT-AUG24 947.36 948.61 125
PALLADSEP24 875.05 896.10 2105
GC-JUL24 2,384.597 2,390.402 5805
GC-AUG24 2,387.697 2,392.902 5205
BAYKR-IST 69.12 69.32 20
Fiyatlar
Grafik
İşlem
Geçmiş
Ayarlar
Wallet
Trade
Accounts
News
Analysis
Settings

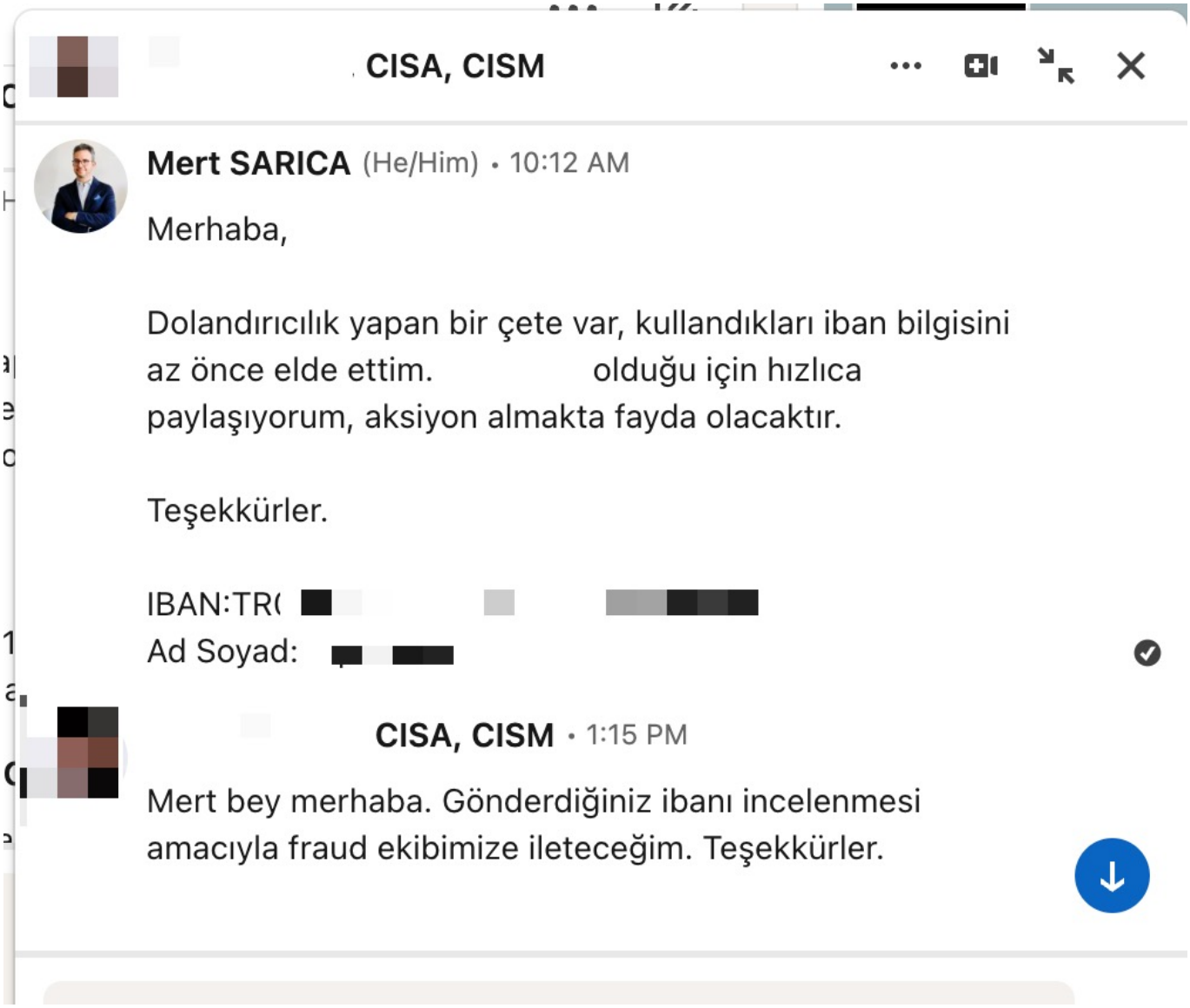
Görüşmenin devamında dolandırıcı, bu borsaya para gönderebilmem ve sözde Baykar hissesini satın alabilmem için benden paylaşmış olduğu banka hesaplarına para transferi yapmam gerektiğini söyledi. Ana amacım hem dolandırıcıların yöntemini öğrenmek hem de WhatsApp Dolandırıcıları başlıklı yazımda yaptığım gibi kötüye kullanılan banka hesap bilgilerini öğrenip banka yetkilileri ile paylaşmak olduğu için bir mizansen kurgulamaya karar verdim.

Benimle harcadıkları her bir dakikanın, masum vatandaşları dolandırmak için ayıracakları zamandanın eksildiğini bildiğim için mizansenin uzun ve gerçekçi olmasına gayret ettim.

Büyük bir hevesle para transferi yapmaya çalışan ama sürekli hata alan bir kurban rolüne büründükten sonra dolandırıcıya hata aldığımı belirttim. Dolandırıcı da bir zaman sonra yeni bir banka hesap bilgisini benimle paylaştı. Ben de vakit kaybetmeden elde ettiğim bilgileri banka yetkilileri ile paylaştım.




Dolandırıcı
[redacted] bankası doğrulama için şubeye gitmemi istiyor kimlik için
05:47
Uzun süredir hesap kapalı olduğu için
05:47
Peki nası bir yol izleyelim Osman Bey
05:49
Yakınlarınızda [redacted] bankası varsa gidebilme ihtimaliniz var mı ?
06:22
Yada şöyle söyliyim sizin için daha kolay olması adına
06:26
Görüntülü arama sağlayarak doğrulama işleminizi de yapabilirsiniz aslında
06:26
Osman Bey ben sizin için yeni bir banka talep ettim
06:53
birde burdan deneyebilir misiniz ?
bakalım yine aynı hatayı alacak mıyız ?
06:53
Missed voice call
Tap to call back
06:56
Haber vereceğim, bir görüşmedeyim Derin Hanım.
07:11
Yeni banka ile deneriz.
07:11



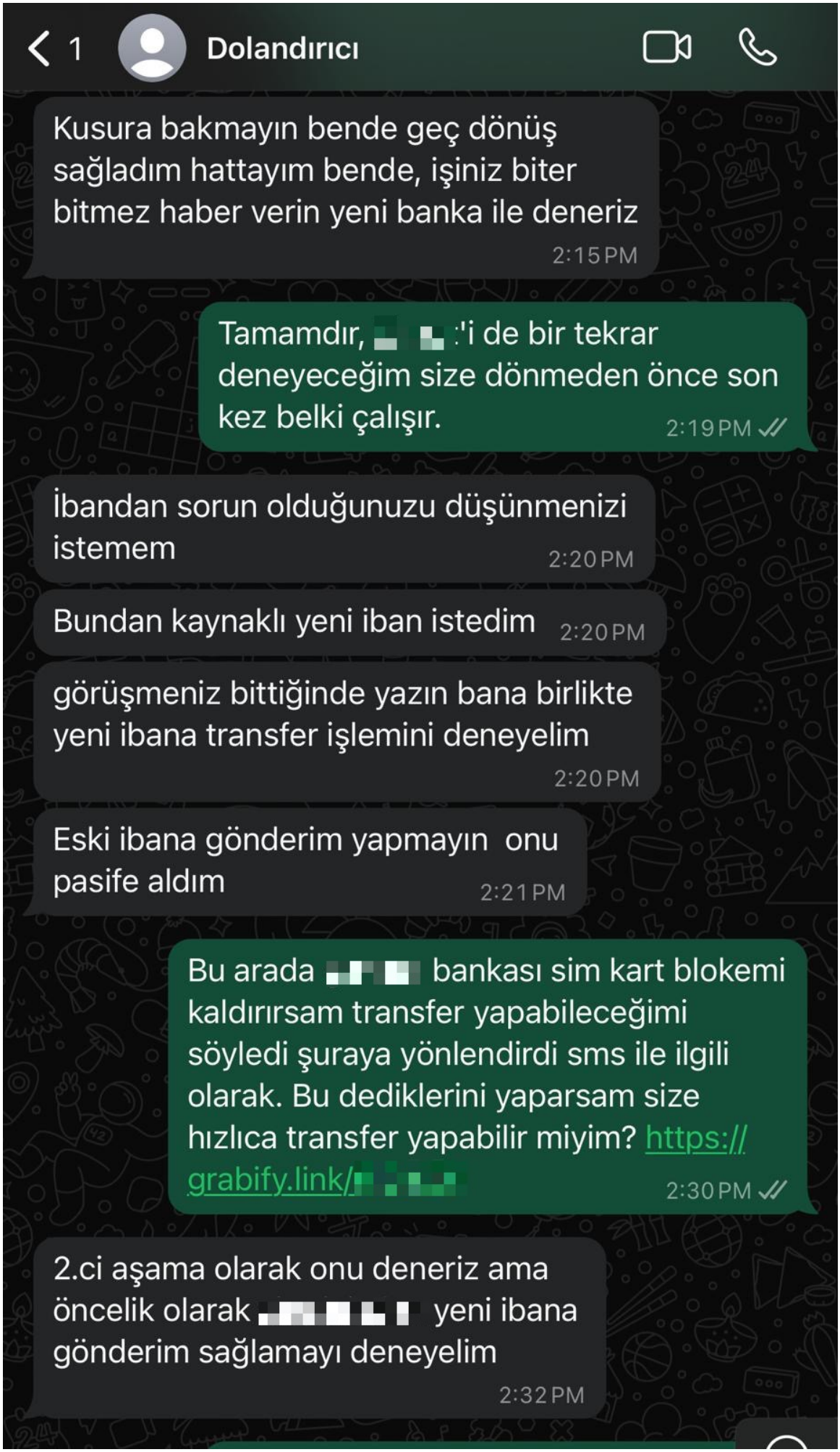
Aldığım hatalardan yaka silken Derin isimli dolandırıcı beni vakit kaybetmeden bankaların internet/mobil şube ekranları konusunda çok daha bilgili ve tecrübeli olduğunu düşündüğüm Demir isim dolandırıcıya (+90 539 105 14 31) yönlendirse de şans pek yüzüne gülmedi.

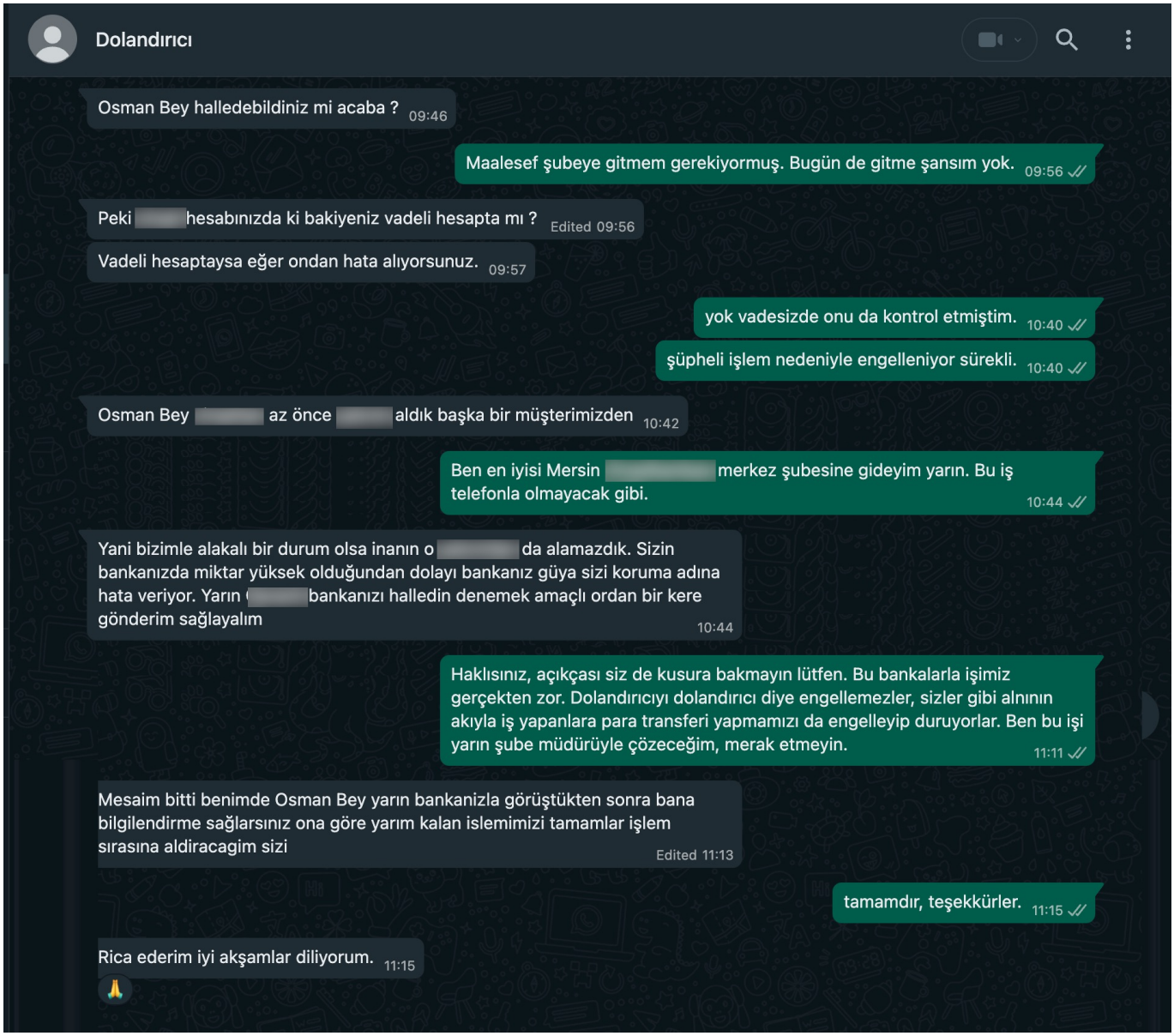
IP Tespiti

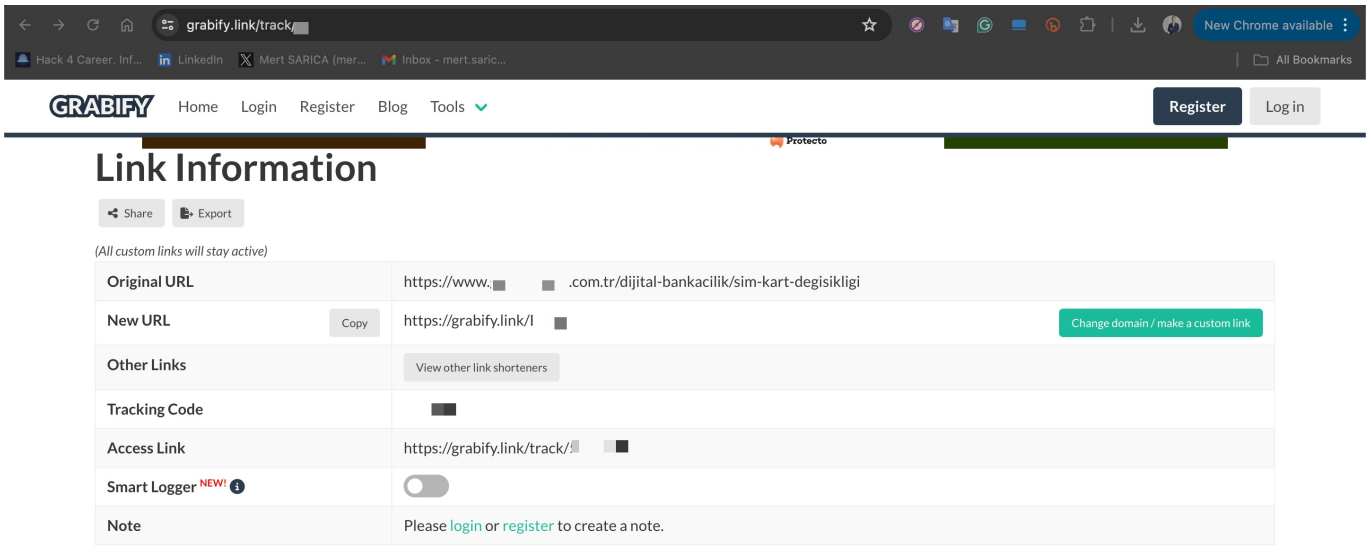
Görüşmenin ilerleyen dakikalarında benimle WhatsApp üzerinden iletişim halinde olan dolandırıcının IP adresini öğrenmek için Grabify IP Logger uygulamasından faydalanmaya karar verdim.

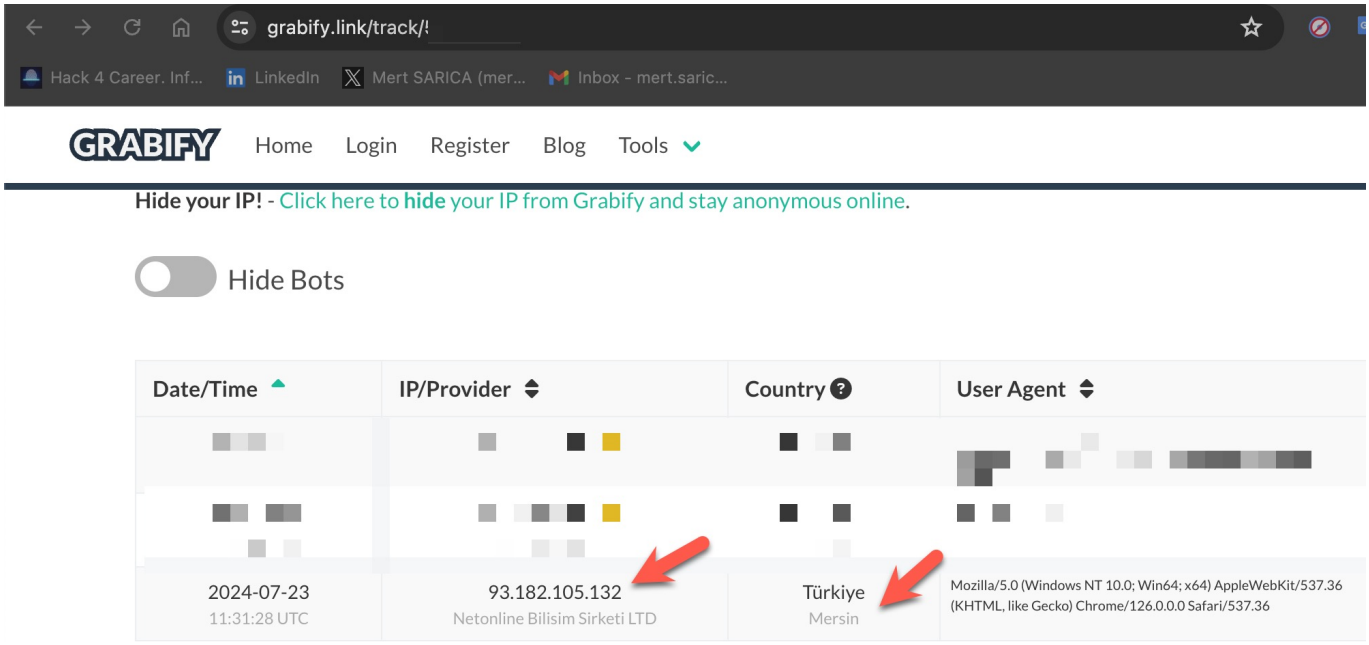
Grabify üzerinde, ziyaret edildiğinde X bir bankanın SIM kartı bloke kaldırma sayfasına yönlendiren bir bağlantı adresi (link) oluşturduktan sonra bunu dolandırıcı ile paylaştım. Sohbetin gidişatına göre doğru zamanda bağlantı adresini dolandırıcıya gönderdiğim için çok geçmeden dolandırıcının IP adresini ve bağlandığı şehri Grabify üzerinden tespit edebildim.

(93.182.105.132 – Mersin)

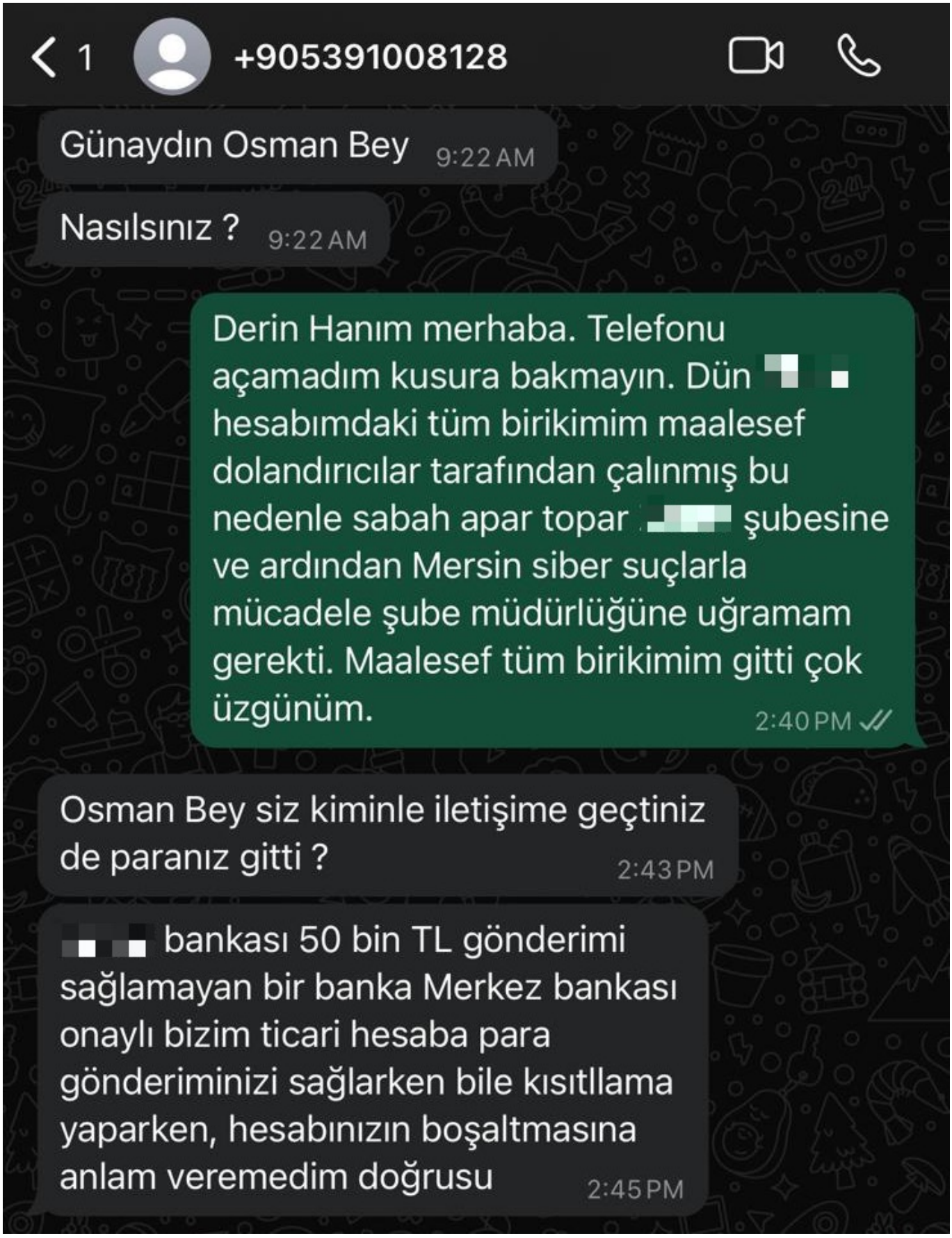

1
Dolandırıcı
Kusura bakmayın bende geç dönüş sağladım hattayım bende, işiniz biter bitmez haber verin yeni banka ile deneriz
2:15 PM
Tamamdır, [redacted]'i de bir tekrar deneyeceğim size dönmeden önce son kez belki çalışır.
2:19 PM
İbandan sorun olduğunuzu düşünmenizi istemem
2:20 PM
Bundan kaynaklı yeni iban istedim
2:20 PM
görüşmeniz bittiğinde yazın bana birlikte yeni ibana transfer işlemini deneyelim
2:20 PM
Eski ibana gönderim yapmayın onu pasife aldım
2:21 PM
Bu arada [redacted] bankası sim kart blokemi kaldırırsam transfer yapabileceğimi söyledi şuraya yönlendirdi sms ile ilgili olarak. Bu dediklerini yaparsam size hızlıca transfer yapabilir miyim? https://grabify.link/[redacted]
2:30 PM
2.ci aşama olarak onu deneriz ama öncelik olarak [redacted] yeni ibana gönderim sağlamayı deneyelim
2:32 PM

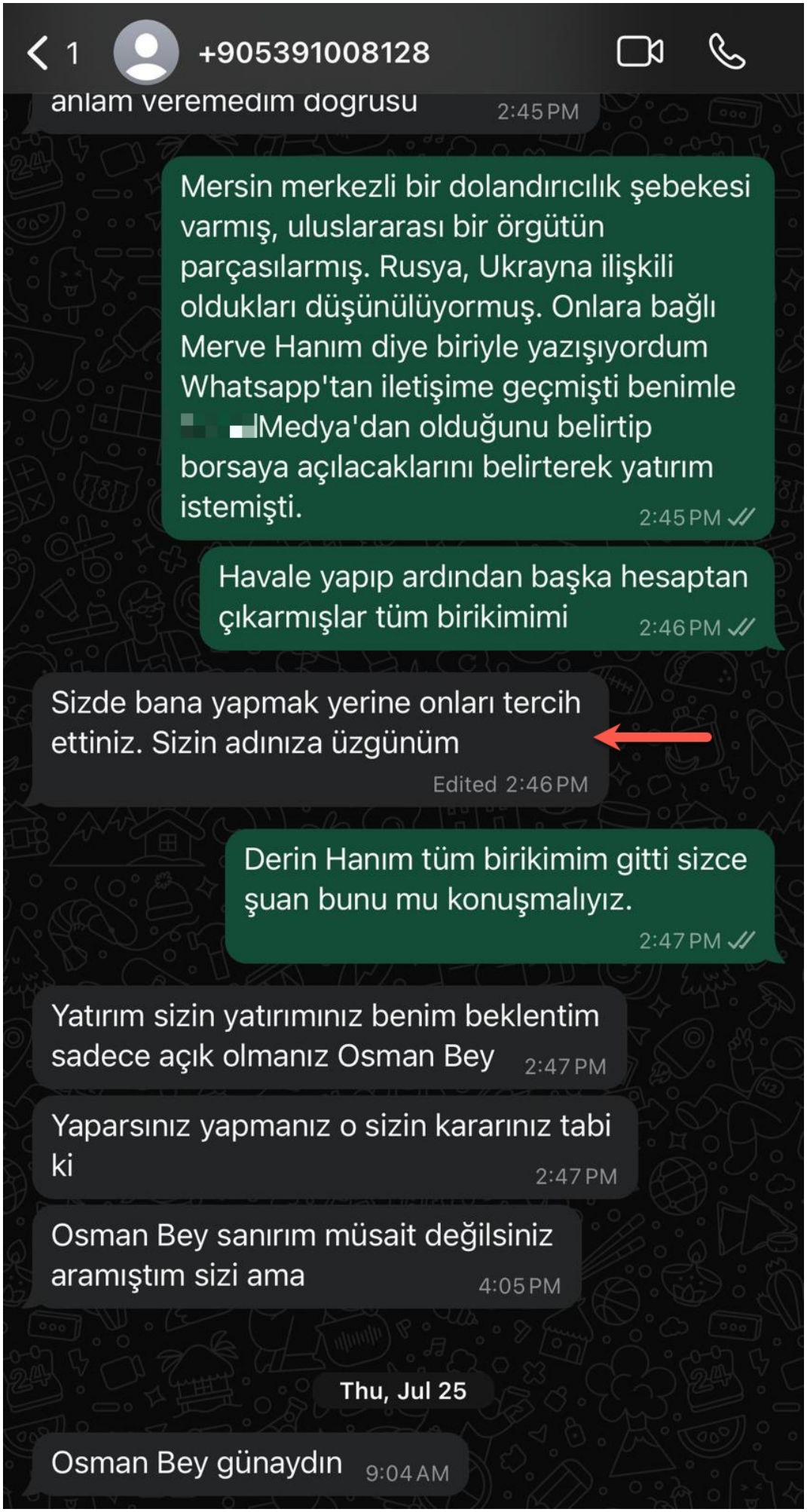

Dolandırıcı
Osman Bey halledebildiniz mi acaba ? 09:46
Maalesef şubeye gitmem gerekiyormuş. Bugün de gitme şansım yok. 09:56
Peki [redacted] hesabınızda ki bakiyeniz vadeli hesapta mı ? Edited 09:56
Vadeli hesaptaysa eğer ondan hata alıyorsunuz. 09:57
yok vadesizde onu da kontrol etmiştim. 10:40
şüpheli işlem nedeniyle engelleniyor sürekli. 10:40
Osman Bey [redacted] az önce [redacted] aldık başka bir müşterimizden 10:42
Ben en iyisi Mersin [redacted] merkez şubesine gideyim yarın. Bu iş telefonla olmayacak gibi. 10:44
Yani bizimle alakalı bir durum olsa inanın o [redacted] da alamazdık. Sizin bankanızda miktar yüksek olduğundan dolayı bankanız güya sizi koruma adına hata veriyor. Yarın [redacted] bankanızı halledin denemek amaçlı ordan bir kere gönderim sağlayalım 10:44
Haklısınız, açıkçası siz de kusura bakmayın lütfen. Bu bankalarla işimiz gerçekten zor. Dolandırıcıyı dolandırıcı diye engellemezler, sizler gibi alnının akıyla iş yapanlara para transferi yapmamızı da engelleyip duruyorlar. Ben bu işi yarın şube müdürüyle çözeceğim, merak etmeyin. 11:11
Mesaim bitti benimde Osman Bey yarın bankanizla görüştükten sonra bana bilgilendirme sağlarsınız ona göre yarım kalan islemimizi tamamlar işlem sırasına aldiracagim sizi Edited 11:13
tamamdır, teşekkürler. 11:15
Rica ederim iyi akşamlar diliyorum. 11:15
🙏

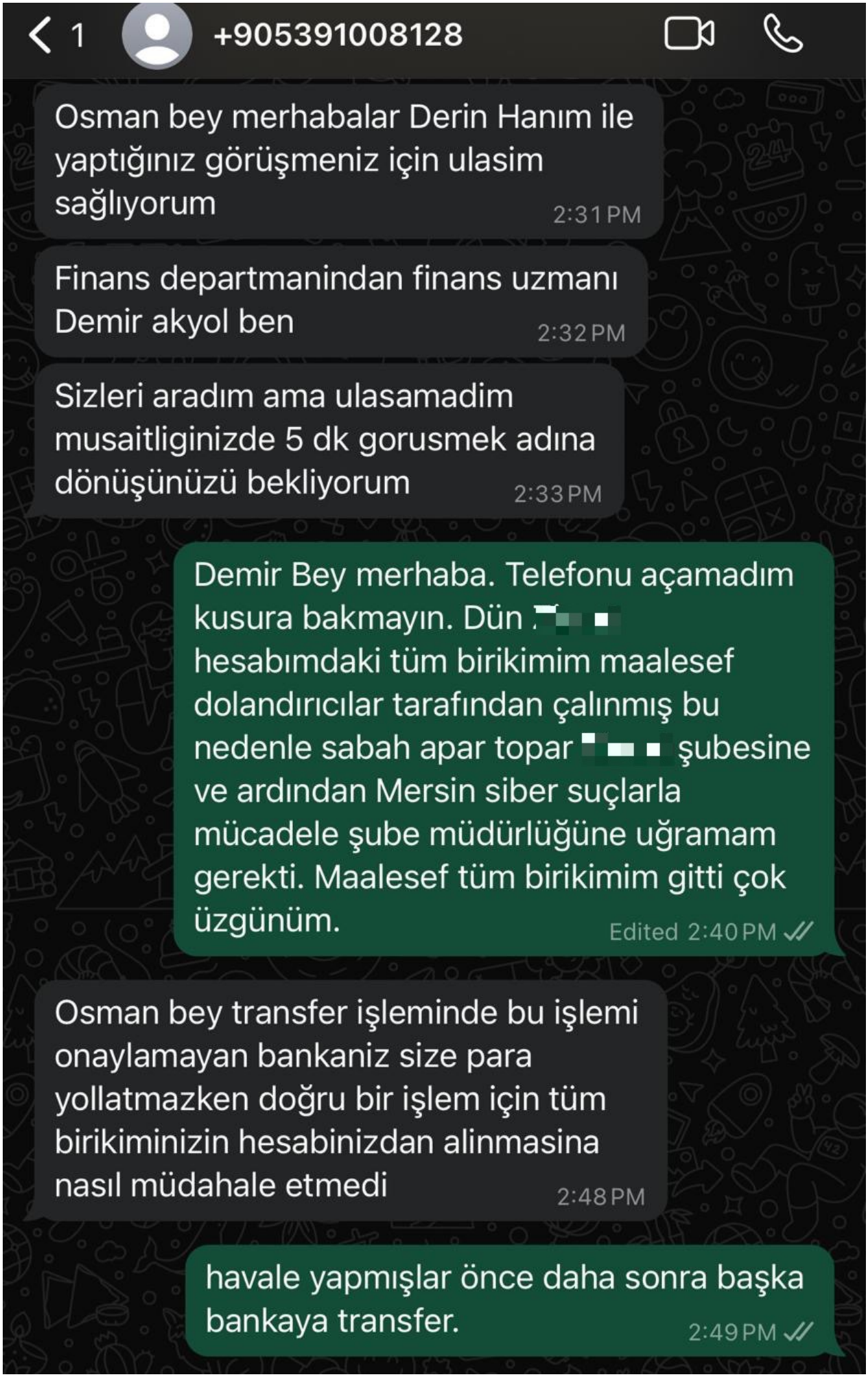

grabify.link/track/
New Chrome available
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
All Bookmarks
GRABIFY
Home
Login
Register
Blog
Tools
Register
Log in
Protecto
Link Information
Share
Export
(All custom links will stay active)
Original URL
https://www. .com.tr/dijital-bankacilik/sim-kart-degisikligi
New URL
Copy
https://grabify.link/I
Change domain / make a custom link
Other Links
View other link shorteners
Tracking Code
Access Link
https://grabify.link/track/
Smart Logger NEW!
Note
Please login or register to create a note.



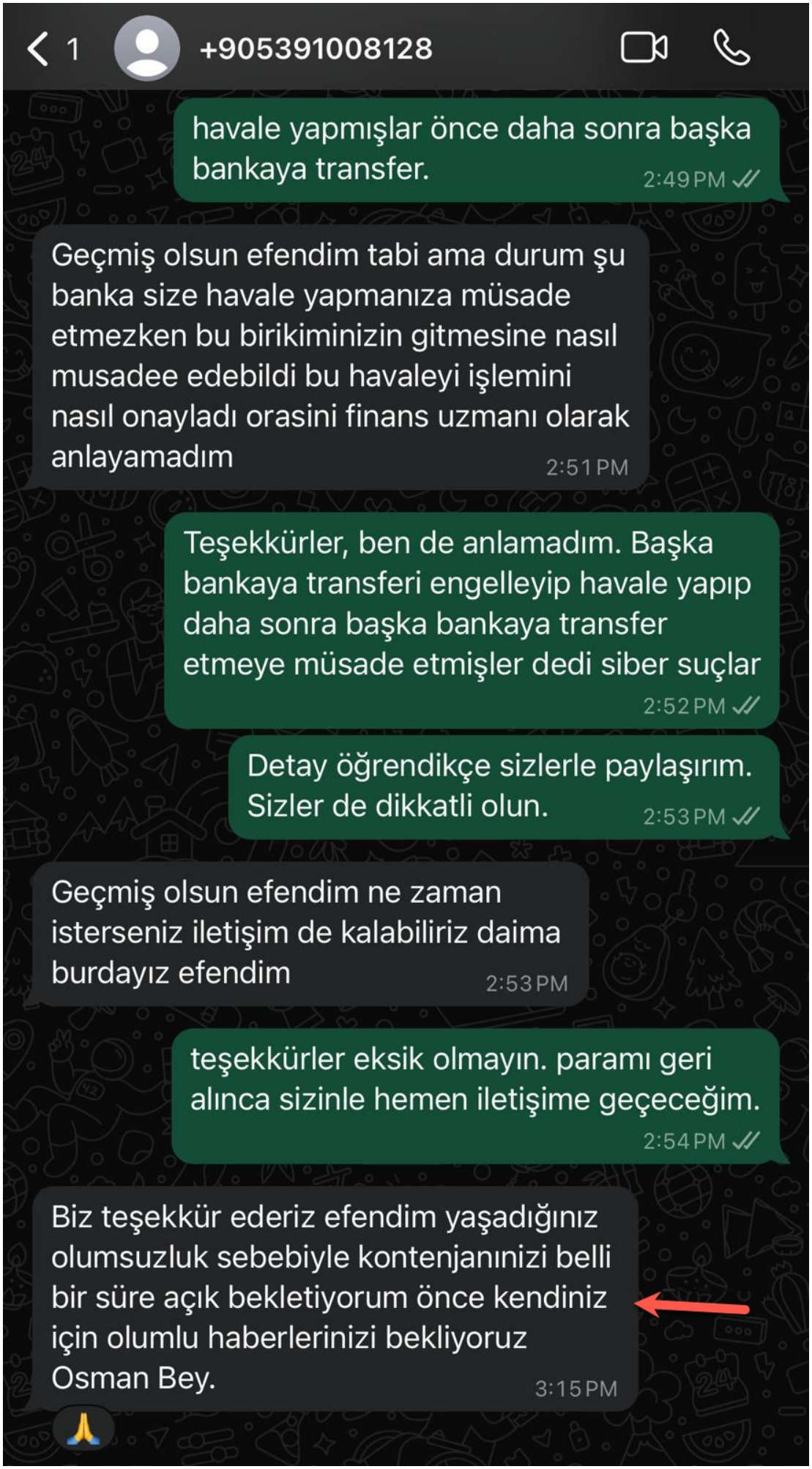
İstediğim bilgileri elde ettikten sonra dolandırıcılara soğuk duş etkisi yaratmak için başka dolandırıcı tarafından dolandırılan kurban senaryosu ile ilerlemeye karar verdim. Yazdığım mesajlar sonucunda, dolandırıcılar arasındaki rekabete yenik düştüklerini düşünen dolandırıcılar, sırasıyla sitem dolu mesajlar göndermeye başladılar.


1
+905391008128
Günaydın Osman Bey 9:22 AM
Nasılsınız ? 9:22 AM
Derin Hanım merhaba. Telefonu açamadım kusura bakmayın. Dün [redacted] hesabımdaki tüm birikimim maalesef dolandırıcılar tarafından çalınmış bu nedenle sabah apar topar [redacted] şubesine ve ardından Mersin siber suçlarla mücadele şube müdürlüğüne uğramam gerekti. Maalesef tüm birikimim gitti çok üzgünüm. 2:40 PM
Osman Bey siz kiminle iletişime geçtiniz de paranız gitti ? 2:43 PM
[redacted] bankası 50 bin TL gönderimi sağlamayan bir banka Merkez bankası onaylı bizim ticari hesaba para gönderiminizi sağlarken bile kısıtllama yaparken, hesabınızın boşaltmasına anlam veremedim doğrusu 2:45 PM


1
+905391008128
anlam veremedim dogrusu
2:45 PM
Mersin merkezli bir dolandırıcılık şebekesi varmış, uluslararası bir örgütün parçasılarmış. Rusya, Ukrayna ilişkili oldukları düşünülüyormuş. Onlara bağlı Merve Hanım diye biriyle yazışıyordum Whatsapp'tan iletişime geçmişti benimle [redacted]Medya'dan olduğunu belirtip borsaya açılacaklarını belirterek yatırım istemişti.
2:45 PM
Havale yapıp ardından başka hesaptan çıkarmışlar tüm birikimimi
2:46 PM
Sizde bana yapmak yerine onları tercih ettiniz. Sizin adınıza üzgünüm
Edited 2:46 PM
Derin Hanım tüm birikimim gitti sizce şuan bunu mu konuşmalıyız.
2:47 PM
Yatırım sizin yatırımınız benim beklentim sadece açık olmanız Osman Bey
2:47 PM
Yaparsınız yapmanız o sizin kararınız tabi ki
2:47 PM
Osman Bey sanırım müsait değilsiniz aramıştım sizi ama
4:05 PM
Thu, Jul 25
Osman Bey günaydın
9:04 AM


1
+905391008128
Osman bey merhabalar Derin Hanım ile yaptığınız görüşmeniz için ulasim sağlıyorum
2:31 PM
Finans departmanindan finans uzmanı Demir akyol ben
2:32 PM
Sizleri aradım ama ulasamadim musaitliginizde 5 dk gorusmek adına dönüşünüzü bekliyorum
2:33 PM
Demir Bey merhaba. Telefonu açamadım kusura bakmayın. Dün [redacted] hesabımdaki tüm birikimim maalesef dolandırıcılar tarafından çalınmış bu nedenle sabah apar topar [redacted] şubesine ve ardından Mersin siber suçlarla mücadele şube müdürlüğüne uğramam gerekti. Maalesef tüm birikimim gitti çok üzgünüm.
Edited 2:40 PM
Osman bey transfer işleminde bu işlemi onaylamayan bankaniz size para yollatmazken doğru bir işlem için tüm birikiminizin hesabinizdan alinmasina nasıl müdahale etmedi
2:48 PM
havale yapmışlar önce daha sonra başka bankaya transfer.
2:49 PM

Yazdıklarıma rağmen beni ikinci defa dolandırma umutlarını sonuna kadar koruyan ve iletişimi devam ettirmeye motive olmuş vicdansız, serin kanlı dolandırılarıcıların mesajları ben yanıt vermeyi bıraktıktan bir süre sonra kesildi.


1
+905391008128
havale yapmışlar önce daha sonra başka bankaya transfer.
2:49 PM
Geçmiş olsun efendim tabi ama durum şu banka size havale yapmanıza müsade etmezken bu birikiminizin gitmesine nasıl musadee edebildi bu havaleyi işlemini nasıl onayladı orasini finans uzmanı olarak anlayamadım
2:51 PM
Teşekkürler, ben de anlamadım. Başka bankaya transferi engelleyip havale yapıp daha sonra başka bankaya transfer etmeye müsade etmişler dedi siber suçlar
2:52 PM
Detay öğrendikçe sizlerle paylaşırım. Sizler de dikkatli olun.
2:53 PM
Geçmiş olsun efendim ne zaman isterseniz iletişim de kalabiliriz daima burdayız efendim
2:53 PM
teşekkürler eksik olmayın. paramı geri alınca sizinle hemen iletişime geçeceğim.
2:54 PM
Biz teşekkür ederiz efendim yaşadığınız olumsuzluk sebebiyle kontenjanınızi belli bir süre açık bekletiyorum önce kendiniz için olumlu haberlerinizi bekliyoruz Osman Bey.
3:15 PM
🙏

Tüm bu olup bitenler devam ederken Baykar şirketi de 2024 yılının başından bu yana vatandaşları uyarmak için yazılı, görsel ve sosyal medya hesaplarından bu konuda uyarılar (#1, #2, #3) yayınlamaya hız kesmeden devam etti.

Ses Kayıtları

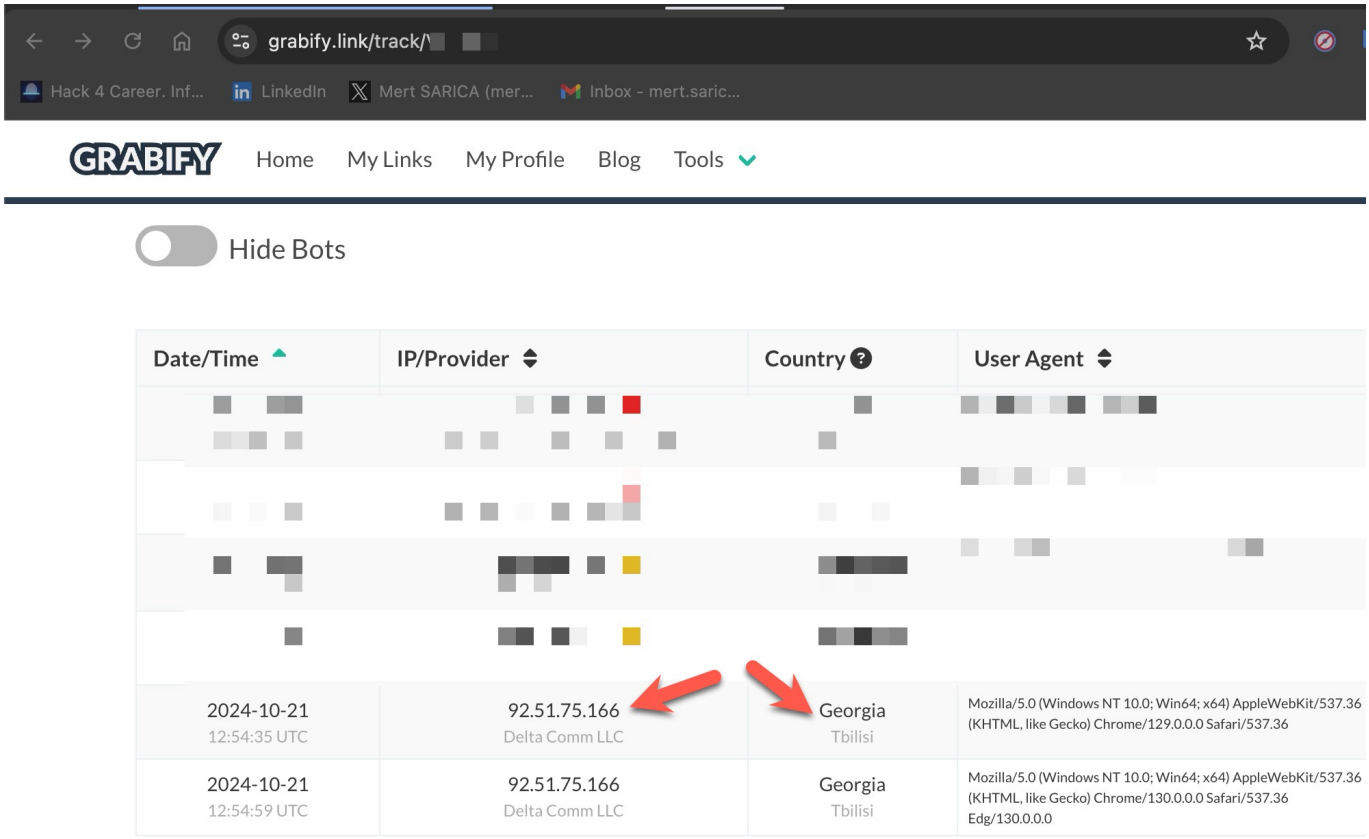
Merak edenleriniz dolandırıcılarla gerçekleştirmiş olduğum akıllara durgunluk veren görüşmelerin ses kayıtlarını aşağıda, YouTube kanalım üzerinden dinleyebilirler.

2. Dolandırıcılık Girişimi

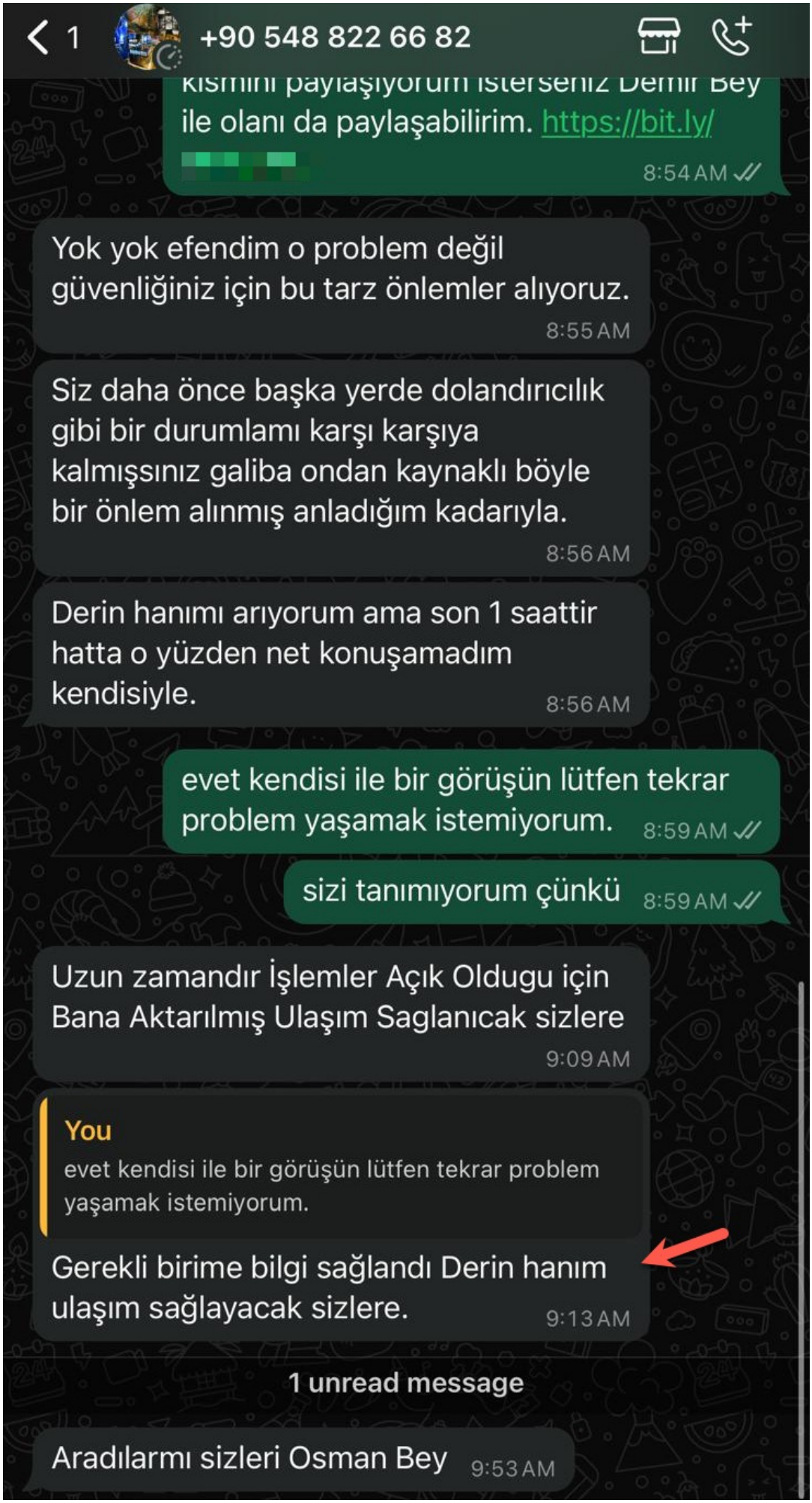
IP Tespiti

Takvimler 2024 yılının Ekim ayını yani bir önceki dolandırıcılık girişiminden neredeyse 3 ay sonrasını gösterdiğinde bu defa +90 548 822 66 82 numaralı cep telefonundan İpek isimli başka bir dolandırıcı yine aynı senaryo ile benimle iletişime geçti. Ben de fırsat bu fırsat daha önceki yöntemle bu dolandırıcının da IP adresini elde etmeye karar verdim. Yine benzer bir şekilde dolandırıcıyı yemledikten sonra bu dolandırıcının öncekinin aksine Mersin yerine Gürcistan'ın başkenti Tiflis'ten bağlantı kurduğunu tespit ettim. (Dolandırıcının vekil sunucu (proxy) kullanmadığını varsaydım.)


3
+90 548 822 66 82
Today
Günaydınlar hayırlı haftalar Osman bey.
1:32 AM
Demir bey yıllık izinde. Sistem uzman olarak beni atamış sizlere müsait olduğunuzda aramak isterim.
1:33 AM
Açıkçası onlar tembih etmişler başkası ile konuşmamam için o nedenle onları beklemek isterim.
8:02 AM
Efendim yanlışlık olmasın benim danışmanım onlar aynı kuruma hizmet vermekteyiz. Aradığımda görebilirsiniz aynı numara ile arama gerçekleştiriyorum zaten. 100 adet danışmanız mevcut.
8:08 AM
Missed voice call
Tap to call back
8:24 AM
bit.ly
https://bit.ly/40c3kxC
bit.ly
Açıkası o zaman ufak bir problem yaşamıştım ve kesinlikle Derin Hanım kaynaklı değildi fakat yine de başkası ile görüşmemem gerektiğini paylaşmıştı güvenliğim için. Yazışmamımızın bir kısmını paylaşıyorum isterseniz Demir Bey ile olanı da paylaşabilirim. https://bit.ly/
8:54 AM



Bir önceki dolandırıcılık girişiminin baş aktörlerinden Derin veya Demir'in hala görevlerinin başında olup olmadıklarını da bir yandan merak ettiğim için bu dolandırıcıya Derin veya Demir'den başka kimseyle görüşmeyeceğimi ısrarla dile getirdikten sonra dolandırıcı ısrarlarıma yenik düşüp Derin'e ulaşmaya ve bana yönlendirmeye karar verdi. Bu sayede dolandırıcıların son 3 aydır operasyonlarına aynı kadro ile hız kesmeden devam ettiğini öğrenmiş oldum.


1
+90 548 822 66 82
kısmını paylaşıyorum isterseniz Demir Bey ile olanı da paylaşabilirim. https://bit.ly/
8:54 AM
Yok yok efendim o problem değil güvenliğiniz için bu tarz önlemler alıyoruz.
8:55 AM
Siz daha önce başka yerde dolandırıcılık gibi bir durumlamı karşı karşıya kalmışsınız galiba ondan kaynaklı böyle bir önlem alınmış anladığım kadarıyla.
8:56 AM
Derin hanımı arıyorum ama son 1 saattir hatta o yüzden net konuşamadım kendisiyle.
8:56 AM
evet kendisi ile bir görüşün lütfen tekrar problem yaşamak istemiyorum.
8:59 AM
sizi tanımıyorum çünkü
8:59 AM
Uzun zamandır İşlemler Açık Oldugu için Bana Aktarılmış Ulaşım Saglanıcak sizlere
9:09 AM
You
evet kendisi ile bir görüşün lütfen tekrar problem yaşamak istemiyorum.
Gerekli birime bilgi sağlandı Derin hanım ulaşım sağlayacak sizlere.
9:13 AM
1 unread message
Aradılarmı sizleri Osman Bey
9:53 AM

Sonuç

Sonuç itibariyle bu güvenlik araştırması ile Slovnaft, INA d.d, Bosphorus Gaz gibi petrol rafineri, gaz dağıtım şirketlerinden, Baykar gibi savunma şirketlerine hatta Interpol‘e kadar önde gelen kurumların adını kullanarak dolandırıcılık girişiminde bulunan uluslararası dolandırıcılık çetesinin arka planda kurbanlarını nasıl ağlarına düşürdüklerini öğrenmiş oldum. Umuyorum ki masum vatandaşların paralarına göz diken bu dolandırıcılar en kısa sürede yakalanır ve hak ettikleri cezayı alırlar.

Yazının başında da belirttiğim üzere çok iyi kurgulanmış bu organize dolandırıcılık çarkına daha fazla masum insanın düşmemesi, kurban olmaması adına bu yazıyı çevrenizdekilerle ve tüm sevdiklerinizle paylaşmanızı gönülden rica ederim.

Bu yazı vesilesiyle de yeni yılınızı kutlar, 2025 yılının hem sizlere hem de tüm sevdiklerinize önce sağlık sonra mutluluk ve başarı getirmesini dilerim.