

Phishing Cloaking Techniques

written by Mert SARICA | 1 September 2025

CONTENTS

1. Introduction
2. Geographic Cloaking
3. User-Agent Based Cloaking
4. Blacklist-Based Cloaking
5. Abra Kadabra
6. Conclusion

Introduction

Those of you who have read my blog post titled Investment Scammers have seen how scammers try to lure innocent people into their traps through fake ads on social media and networks. Just as in that article, websites play a critical role in fraud attempts and are essential for the operations of scammers.

In most cases, scammers manage to bring their victims to these websites through persuasion. From there, they steal the victims' information and then proceed to the next stage of their operation—contacting the victims via calls or messaging platforms like WhatsApp and Telegram. As one might expect, in this final stage, their aim is to trick victims into making money transfers and thus achieve their malicious goals.

Of course, the more experienced among these scammers are aware that companies fighting against cybercrime, such as SOCRadar and Netcraft, as well as national entities like USOM, scan and report these fraudulent websites and then have suspicious/malicious ones taken down. To bypass such scans, they take advantage of a technique called Cloaking, which has been used in the SEO world since 1996. In this article, I aimed to raise awareness by presenting the most common cloaking techniques and also introducing a tool I developed with artificial intelligence to easily bypass them.

Cloaking is when the content shown to search engines by a website differs from the content shown to users; this is a practice that violates search

engine optimization (SEO) rules. In this method, where different content is served to users and search engines, the goal is to gain an advantage in search results.

Purpose and Method of Cloaking

Search Engine Optimization (SEO):

Cloaking is a technique used to ensure that a website ranks higher in search engine results.

Different Content Delivery:

Search engine bots are made to believe that the website contains richer content filled with keywords relevant to search queries. However, real users are shown a different and usually less optimized version of the site.

Malicious Use:

This method is used to trick the algorithms of search engines such as Google and to display spam or misleading content to users.

To conduct a security analysis on phishing sites that use cloaking techniques, I first needed access to their source code. Since obtaining these on demand is not practically possible, I once again turned to the help of SOCRadar, as I did in my previous articles. :)

Since the SOCRadar platform not only detects phishing sites but, when necessary, can also obtain their source code to trace back to the threat actors behind them, I decided to acquire the source code of 500 phishing sites targeting Turkish citizens and perform a security analysis on them.

Geographic Cloaking

First, I examined a website belonging to the threat actor I covered in my Investment Scammers blog post. This threat actor, who has continued their fraud operations non-stop for a year, registered the domain name navoisco[.]info on August 6, 2025 and started using the website for fraudulent purposes on August 13, 2025.

When you visited this website from abroad, you were presented with content selling surf products. However, when accessed from Turkey, it appeared as a fraudulent webpage exploiting the name of the defense company Baykar, in short using the Geographic Cloaking technique. When you searched for this

address on the Google search engine, thanks to this cloaking method used by the scammers, it appeared in the records as a store selling surf products.

Note: I have been monitoring these threat actors for more than a year and concluded that they are Russian. They mainly carry out their operations through Ukrainian IP addresses (185.38.218.86, 185.237.75.100, 91.123.155.63). Since February 2025, they have launched 699 phishing websites, targeting approximately 9,000 Turkish citizens and stealing their personal information (name, surname, email address, phone number, IP address).

test@gmail.com	test	test	'380503223522	UA	159.224.64.139	volumeviin.com
test@gmail.com	test	test	'380992182888	UA	185.237.75.100	www.borusan.com
test@gmail.com	test	test	'380042124241	UA	159.224.64.139	volumeviin.com
test@gmail.com	test	test	'380991292992	UA	185.237.75.100	volumeviin.com
test@gmail.com	test	test	'380501284234	UA	31.148.245.242	breakoyclh.com
test@gmail.com	test	test	'380991292992	UA	185.237.75.100	breakoyclh.com
test@gmail.com	recr	recr	'380992929292	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380912992929	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380501929292	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380658454664	UA	159.224.64.139	noriochiai.com
test@gmail.com	Test	Mobile	'380656568864	UA	159.224.64.139	token-academ.com
test@gmail.com	test	test	'380912020020	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380991292999	UA	185.237.75.100	oliorossi.pro
test@gmail.com	test	test	'380501299299	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380991202002	UA	185.237.75.100	news.borusana.com
test@gmail.com	test	test	'380333333333	UA	91.123.155.63	www.greenexhome.com
test@gmail.com	test	test	'380919292999	UA	185.237.75.100	homogeubpz.shop
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380501299292	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380510292999	UA	185.237.75.100	gmail
test@gmail.com	test	teest	'380501229292	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380912920020	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380501239299	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380500123912	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380919239293	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380991230230	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380959120000	UA	185.237.75.100	perimasaliotel.pro
test@gmail.com	test	test	'380991230200	UA	185.237.75.100	gmail
test@gmail.com	tes	ttest	'380919239239	UA	185.237.75.100	gmail

Index	Time	Source	Destination	Protocol	Port	Country	ASN	Organization
2169	02.07.2025 17:35:09 UTC+05:00	gmail.com	Abdullah	TCP	90536	TR	78.11	materialchikitz.com
2170	02.07.2025 17:35:11 UTC+05:00	mail.com	Ökkeş	TCP	90509	TR	31.1	nakiyatpro.info
2171	02.07.2025 17:35:12 UTC+05:00	9@gmail.com	Mustafa	TCP	90538	TR	88.2	nakiyatpro.info
2172	02.07.2025 17:35:14 UTC+05:00	mail.cim	Cemal	TCP	90507	TR	78.1	nakiyatpro.info
2173	02.07.2025 17:35:15 UTC+05:00	il.com	Aysun	TCP	90537	TR	159.	nakiyatpro.info
2174	02.07.2025 17:35:17 UTC+05:00	rhaba.com	Okuz	TCP	90532	TR	176.8	nakiyatpro.info
2175	02.07.2025 17:35:18 UTC+05:00	mail.com	Saim	TCP	90552	TR	151.	materialchikitz.com
2176	02.07.2025 17:35:20 UTC+05:00	td3011@gmail.com	Muhammed	TCP	90552	TR	149.	incigulus.info
2177	02.07.2025 17:40:39 UTC+05:00	td3011@gmail.com	Muhammed	TCP	90552	TR	149.	incigulus.info
2178	02.07.2025 17:40:40 UTC+05:00	@gmail.com	Firat	TCP	90534	TR	78.11	incigulus.info
2179	02.07.2025 17:40:41 UTC+05:00	48@gmail.com	Adnan	TCP	90541	TR	88.2	incigulus.info
2180	02.07.2025 17:40:43 UTC+05:00	48@gmail.com	Adnan	TCP	90541	TR	88.2	incigulus.info
2181	02.07.2025 17:40:45 UTC+05:00	tdtmail.com	Berkay	TCP	90530	TR	31.2	materialchikitz.com
2182	02.07.2025 17:40:46 UTC+05:00	@gmail.com	Sinan	TCP	90546	TR	176.8	incigulus.info
2183	02.07.2025 17:40:48 UTC+05:00	mail.com	Şükrü	TCP	90546	TR	85.1	incigulus.info
2184	02.07.2025 17:40:49 UTC+05:00	@gmail.com	Wisam	TCP	90552	TR		incigulus.info
2185	02.07.2025 17:40:51 UTC+05:00	td134@gmail.com	Yusuf	TCP	90565	TR	31.1	materialchikitz.com
2186	02.07.2025 17:40:52 UTC+05:00	td134@gmail.com	Yusuf	TCP	90565	TR	31.1	materialchikitz.com
2187	02.07.2025 17:40:54 UTC+05:00	mail.com	Tahir	TCP	90541	TR	176.	materialchikitz.com
2188	02.07.2025 17:40:55 UTC+05:00	isoymayin@gmail.com	Birakin	TCP	90555	TR	217.	materialchikitz.com
2189	02.07.2025 17:40:56 UTC+05:00	gmail.com	Resul	TCP	90531	TR	178.	incigulus.info
2190	02.07.2025 17:40:58 UTC+05:00	gmail.com	Furkan	TCP	90541	TR		incigulus.info
2191	02.07.2025 17:40:59 UTC+05:00	@gmail.com	Yasemin	TCP	90546	TR		incigulus.info
2192	02.07.2025 17:41:01 UTC+05:00	td1@gmail.com	Alpaslan	TCP	90539	TR	31.1	gmail
2193	02.07.2025 17:41:02 UTC+05:00	td52@hotmail.com	Hasan	TCP	90507	TR	85.1	incigulus.info
2194	02.07.2025 17:41:04 UTC+05:00	mail.com	Azad	TCP	90534	TR	5.46.	wrylyqbqn.shop
2195	02.07.2025 17:41:05 UTC+05:00	mail.com	Husamettin	TCP	90542	TR	31.14	incigulus.info
2196	02.07.2025 17:41:07 UTC+05:00	mail.com	HASAN	TCP	90532	TR	194.	incigulus.info
2197	02.07.2025 17:41:08 UTC+05:00	@gmail.com	Nurguen	TCP	90538	TR	188.	incigulus.info
2198	02.07.2025 17:41:10 UTC+05:00	gmail.com	Uğur	TCP	90505	TR	5.17	incigulus.info
2199	02.07.2025 17:41:11 UTC+05:00	td34@gmail.com	Recep	TCP	90545	TR	37.1	incigulus.info
2200	02.07.2025 17:41:13 UTC+05:00	mail.com	Muhammed	TCP	90543	TR	188.	incigulus.info

User-Agent Based Cloaking

Secondly, on April 17, 2025, I began examining the source code of the phishing site mybbau[.]sa[.]com, which targeted Ziraat Bankası customers, and among the files, the one named netcraft_check.php caught my attention.

Netcraft is a UK-based cybersecurity and internet measurement company that has been operating since 1995. It is best known for its phishing and abuse reporting services and also provides hosting analysis and internet infrastructure statistics.

In this file, which was called from the index.php file located in the ziraatbank subfolder of the phishing site, there was a User-Agent string believed to be used by Netcraft to detect phishing sites. When a connection was made to the website with this string, the user's browser was redirected via google.ca to the web address <https://appleid.apple.com>, thereby carrying out the cloaking process.

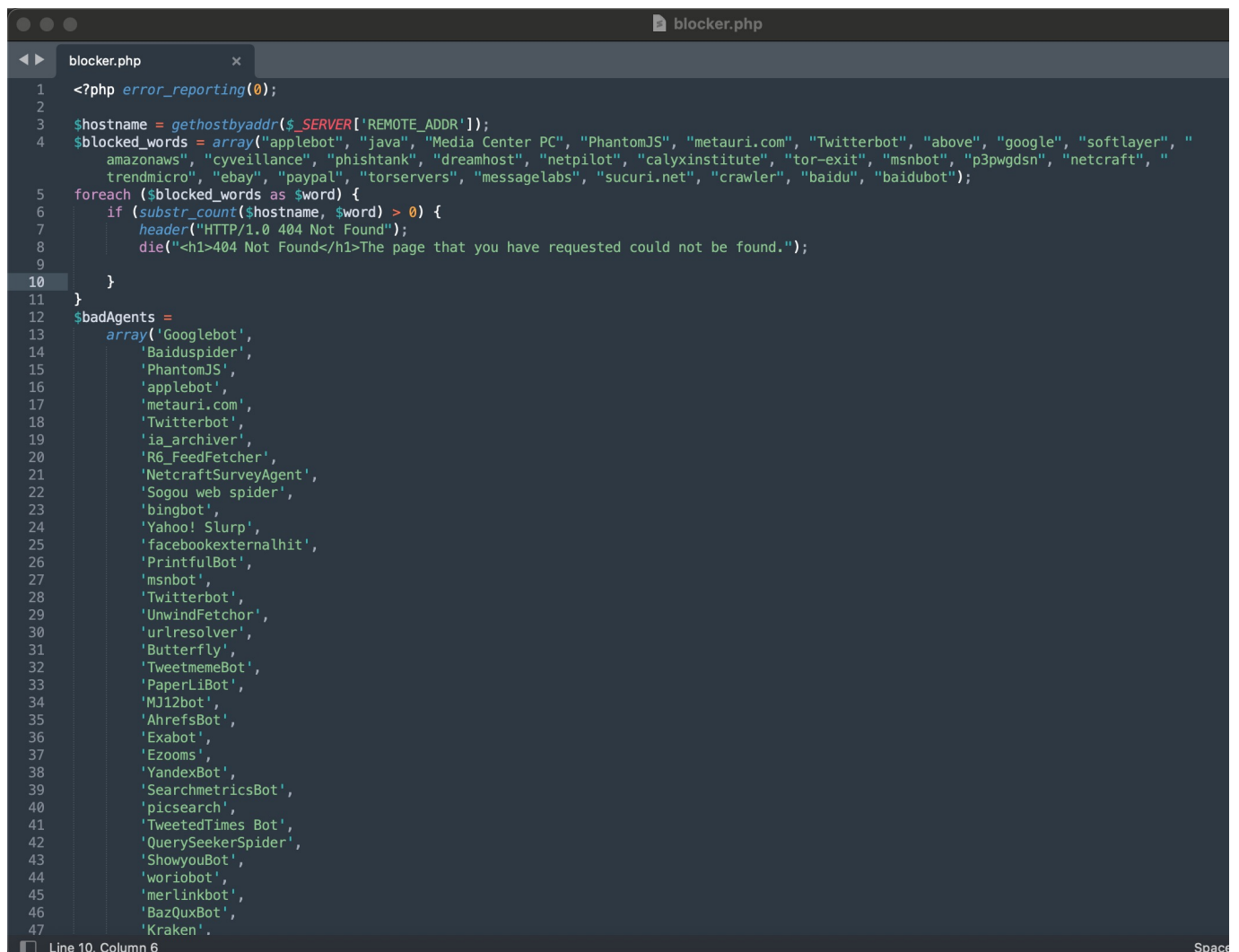
mybbau.sa.com				Search			
Back/Forward				View	Group	Share	Action
				New File Menu			
				Keka			
				Search			
Name		Date Modified	Size	Kind			
ziraat		Today at 16:53	--	Folder			
admin_ziirtata.sql		Apr 17, 2025 at 02:15	40 KB	SQL file			
assets		Apr 17, 2025 at 02:15	--	Folder			
Content		Apr 17, 2025 at 02:15	--	Folder			
core91f5.js		Apr 17, 2025 at 02:15	1.2 MB	JavaScript			
index.php		Apr 17, 2025 at 02:15	4 KB	PHP script			
jquery361c.js		Apr 17, 2025 at 02:15	321 KB	JavaScript			
plugins.min7a39.css		Apr 17, 2025 at 02:15	345 KB	Text Document			
sub.min179c.css		Apr 17, 2025 at 02:15	340 KB	Text Document			
ui.min4f26.js		Apr 17, 2025 at 02:15	143 KB	JavaScript			
ziraat.zip		Apr 16, 2025 at 12:27	6.3 MB	ZIP archive			
ziraatbank		Today at 16:53	--	Folder			
_block		Apr 17, 2025 at 02:15	--	Folder			
blacklist_lookup.php		Apr 17, 2025 at 02:15	7 KB	PHP script			
blacklist.dat		Apr 17, 2025 at 02:15	32 KB	DAT file			
blocker.php		Apr 17, 2025 at 02:15	4 KB	PHP script			
netcraft_check.php		Apr 17, 2025 at 02:15	362 bytes	PHP script			
visitor_log.php		Apr 17, 2025 at 02:15	299 bytes	PHP script			
_kontrol		Apr 17, 2025 at 02:15	--	Folder			
_net		Apr 17, 2025 at 02:15	--	Folder			
_ZAE23AFeAd		Apr 17, 2025 at 02:15	--	Folder			
baglanz.php		Today at 17:56	5 KB	PHP script			
Firstsms.php		Apr 17, 2025 at 02:15	19 KB	PHP script			
index.php		Apr 17, 2025 at 02:15	27 KB	PHP script			
loading.gif		Apr 17, 2025 at 02:15	119 KB	GIF Image			
loading.php		Apr 17, 2025 at 02:15	24 KB	PHP script			
Login		Apr 17, 2025 at 02:15	--	Folder			
pola.php		Apr 17, 2025 at 02:15	4 KB	PHP script			
ProcDone.php		Apr 17, 2025 at 02:15	7 KB	PHP script			
robots.txt		Apr 17, 2025 at 02:15	61 KB	Plain Text			
SecureSms.php		Apr 17, 2025 at 02:15	15 KB	PHP script			
security_phone.php		Apr 17, 2025 at 02:15	18 KB	PHP script			
WebResource.axd		Apr 17, 2025 at 02:15	23 KB	Document			
ziraatOnav.php		Apr 17, 2025 at 02:15	20 KB	PHP script			

Index.php

```
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
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
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2
```

Blacklist-Based Cloaking

While looking through the files, the blocker.php file referenced in the index.php file caught my attention. When I examined this file, I saw that it performed blacklist checks against the IP address connecting to the website and its reverse DNS record. If one of these was detected, instead of displaying the site's content, the server returned a 404 Not Found error, thereby carrying out the cloaking process.



```
blocker.php
1 <?php error_reporting(0);
2
3 $hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
4 $blocked_words = array("applebot", "java", "Media Center PC", "PhantomJS", "metauri.com", "Twitterbot", "above", "google", "softlayer", "
amazonaws", "cyveillance", "phishtank", "dreamhost", "netpilot", "calyxinstitute", "tor-exit", "msnbot", "p3pwgdsn", "netcraft", "
trendmicro", "ebay", "paypal", "torservers", "messagelabs", "sucuri.net", "crawler", "baidu", "baidubot");
5 foreach ($blocked_words as $word) {
6     if (substr_count($hostname, $word) > 0) {
7         header("HTTP/1.0 404 Not Found");
8         die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
9     }
10 }
11
12 $badAgents =
13     array('Googlebot',
14         'Baiduspider',
15         'PhantomJS',
16         'applebot',
17         'metauri.com',
18         'Twitterbot',
19         'ia_archiver',
20         'R6_FeedFetcher',
21         'NetcraftSurveyAgent',
22         'Sogou web spider',
23         'bingbot',
24         'Yahoo! Slurp',
25         'facebookexternalhit',
26         'PrintfulBot',
27         'msnbot',
28         'Twitterbot',
29         'UnwindFetchor',
30         'urlresolver',
31         'Butterfly',
32         'TweetmemeBot',
33         'PaperLiBot',
34         'MJ12bot',
35         'AhrefsBot',
36         'Exabot',
37         'Ezooks',
38         'YandexBot',
39         'SearchmetricsBot',
40         'picsearch',
41         'TweetedTimes Bot',
42         'QuerySeekerSpider',
43         'ShowyouBot',
44         'woriobot',
45         'merlinkbot',
46         'BazQuxBot',
47         'Kraken'.
```

Line 10, Column 6


```
blocker.php
56     'grokkit-crawler',
57     'SMXCrawler',
58     'PulseCrawler',
59     'YIJ-BRW',
60     '80legs.com/webcrawler',
61     'Mediapartners-Google',
62     'Spinn3r',
63     'InAGist',
64     'Python-urllib',
65     'NING',
66     'TencentTraveler',
67     'Feedfetcher-Google',
68     'mon.itor.us',
69     'spbot',
70     'Feedly',
71     'bot',
72     'java',
73     'curl',
74     'spider',
75     'crawler');
76 foreach ($badAgents as $agent) {
77     if (strpos($_SERVER['HTTP_USER_AGENT'], $agent) !== false) {
78         die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
79     }
80 }
81 $bannedIP = array("81.161.59.*", "66.135.200.*", "66.102.*.*", "38.100.*.*", "107.170.*.*", "149.20.*.*", "38.105.*.*", "74.125.*.*", "
66.150.14.*", "54.176.*.*", "38.100.*.*", "184.173.*.*", "66.249.*.*", "128.242.*.*", "72.14.192.*", "209.19.*.*", "64.71.*.*", "
207.70.*.*", "208.65.144.*", "74.125.*.*", "209.85.128.*", "216.239.32.*", "74.125.*.*", "207.126.144.*", "173.194.*.*", "
64.233.160.*", "72.14.192.*", "66.102.*.*", "64.18.*.*", "194.52.68.*", "194.72.238.*", "62.116.207.*", "212.50.193.*", "69.65.*.*",
", "50.7.*.*", "131.212.*.*", "46.116.*.*", "62.90.*.*", "89.138.*.*", "82.166.*.*", "85.64.*.*", "85.250.*.*", "89.138.*.*", "
93.172.*.*", "109.186.*.*", "194.90.*.*", "212.29.192.*", "212.29.224.*", "212.143.*.*", "212.150.*.*", "212.235.*.*", "
217.132.*.*", "50.97.*.*", "217.132.*.*", "209.85.*.*", "66.205.64.*", "204.14.48.*", "64.27.2.*", "67.15.*.*", "202.108.252.*", "
193.47.80.*", "64.62.136.*", "66.221.*.*", "64.62.175.*", "198.54.*.*", "192.115.134.*", "216.252.167.*", "193.253.199.*", "
69.61.12.*", "64.37.103.*", "38.144.36.*", "64.124.14.*", "206.28.72.*", "209.73.228.*", "158.108.*.*", "168.188.*.*", "
66.207.120.*", "167.24.*.*", "192.118.48.*", "67.209.128.*", "12.148.209.*", "12.148.196.*", "193.220.178.*", "68.65.53.71", "
198.25.*.*", "64.106.213.*", "91.103.66.*", "208.91.115.*", "199.30.228.*");
82 if (in_array($_SERVER['REMOTE_ADDR'], $bannedIP)) {
83     header('HTTP/1.0 404 Not Found');
84     exit();
85 } else {
86     foreach ($bannedIP as $ip) {
87         if (preg_match('/' . $ip . '/', $_SERVER['REMOTE_ADDR'])) {
88             header('HTTP/1.0 404 Not Found');
89             die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
90         }
91     }
92 }
93
94 7>
```

On August 16, 2025, when I looked at the source code of another phishing site created to target the CarrefourSA brand with the domain name yazgeldihosgeldi[.]online, this time I noticed the name USOM in one of the files. When I examined the botMother.php file located in the same folder, I saw that it contained various checks related to USOM. In one of the checks, people accessing the site from their computers who suspected the site were deceived and redirected to a fake USOM blocking page—in short, an attempt was made to prevent the site from being reported.

yazgeldihosgeldi.online							
Back/Forward				View			
				Group			
				Share			
				Edit Tags			
				Action			
				New File Menu			
				Keka			
				Search			
Name				Date Modified	Size	Kind	
admin				Today at 17:13	--	Folder	
admin				Aug 16, 2025 at 02:02	--	Folder	
admin.zip				Aug 14, 2025 at 11:32	20.7 MB	ZIP archive	
botMother				Aug 16, 2025 at 12:03	--	Folder	
botMother.php				Aug 16, 2025 at 02:02	21 KB	PHP script	
Credits.txt				Aug 16, 2025 at 02:02	183 bytes	Plain Text	
data				Aug 16, 2025 at 11:42	--	Folder	
debug.log				Aug 16, 2025 at 02:02	27 KB	Log File	
desktop_debug.log				Aug 16, 2025 at 02:02	618 bytes	Log File	
exmaple.php				Aug 16, 2025 at 02:02	952 bytes	PHP script	
ipapi_debug.log				Aug 16, 2025 at 02:02	75 bytes	Log File	
lanet_olasi_federaller.txt				Aug 16, 2025 at 02:02	841 bytes	Plain Text	
usom_debug.log				Aug 16, 2025 at 02:02	207 bytes	Log File	
botMother.zip				Aug 16, 2025 at 02:02	10 KB	ZIP archive	
bots_log.txt				Aug 16, 2025 at 02:02	618 KB	Plain Text	
carrefour.sql				Aug 16, 2025 at 02:02	103 KB	SQL file	
error_log				Aug 16, 2025 at 02:02	19 KB	Document	
inc				Aug 16, 2025 at 02:02	--	Folder	
index.php				Aug 16, 2025 at 02:02	56 bytes	PHP script	
log.txt				Aug 16, 2025 at 02:02	424 KB	Plain Text	
nakliye				Aug 16, 2025 at 11:43	--	Folder	
phpinfo.php				Aug 16, 2025 at 02:02	21 bytes	PHP script	
sadece-online-ozel				Aug 16, 2025 at 15:22	--	Folder	

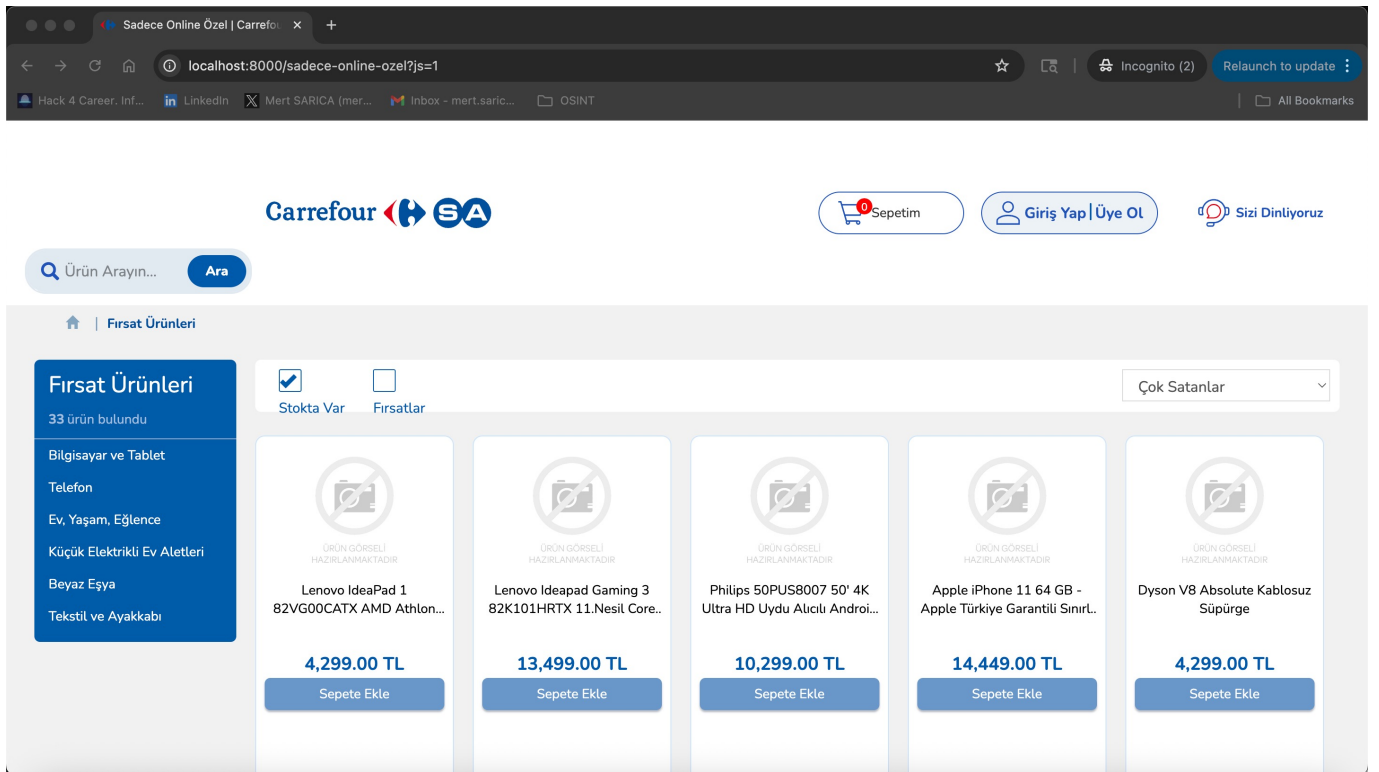
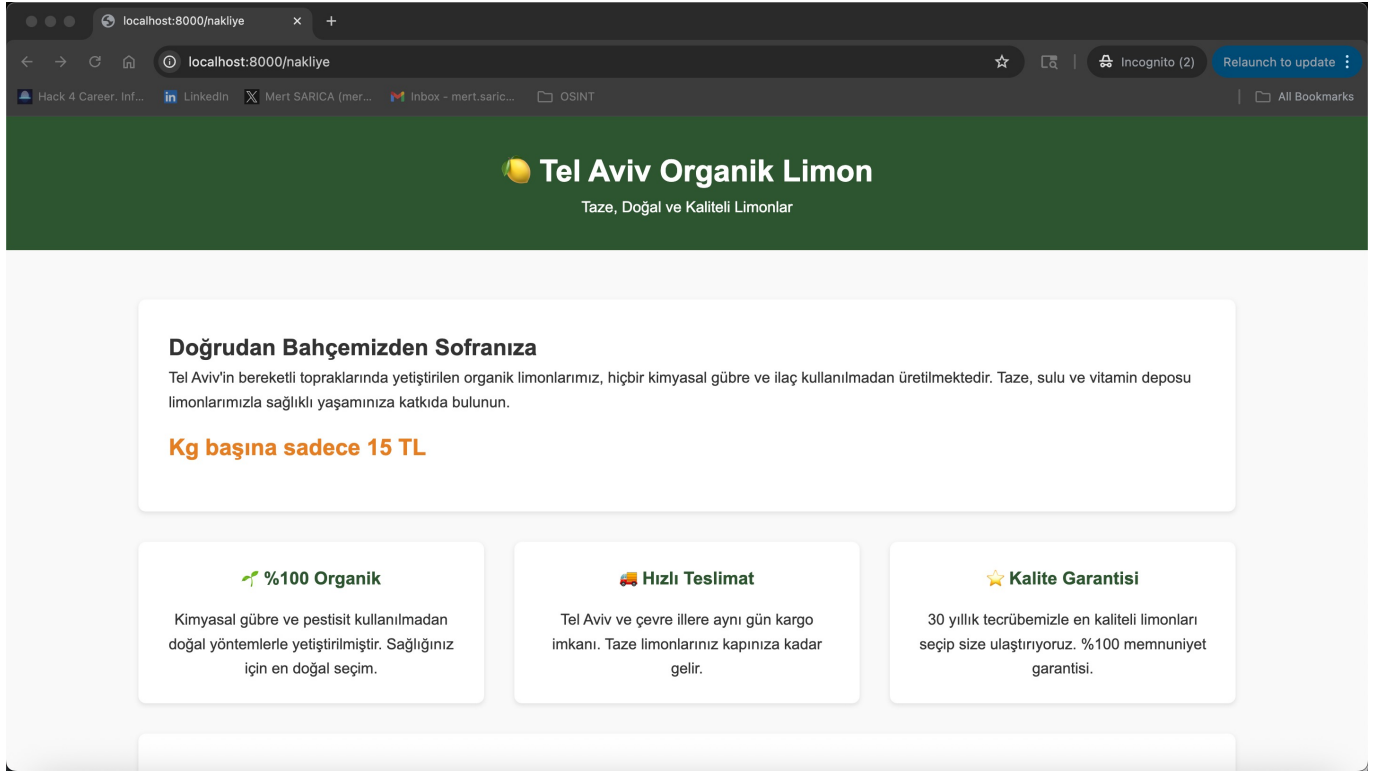
```
botMother.php
374
375 // Eğer cookie zaten varsa (önceki ziyaretten), direkt fake page dön (refresh'te kalıcı olsun)
376 if (isset($_COOKIE['usom_blocked']) && $_COOKIE['usom_blocked'] === 'true') {
377     $debugLog = "[ " . date("Y-m-d H:i:s") . " ] Cookie Block Triggered | IP: {$this->USER_IP} | UA: {$this->USER_AGENT}\n";
378     file_put_contents(__DIR__.'/usom_debug.log', $debugLog, FILE_APPEND);
379     $this->showFakeUsomPage();
380     exit;
381 }
382
383 $countryCode = $this->getIpInfo("countryCode");
384 $city = strtolower($this->getIpInfo("city")); // Şehir al (log için)
385
386 // Debug: TR check öncesi log
387 $isDesktopResult = $this->isDesktop() ? 'true' : 'false';
388 $debugLog = "[ " . date("Y-m-d H:i:s") . " ] TR Check: Country: $countryCode | isDesktop: $isDesktopResult | IP: {$this->USER_IP} | UA: {$this->USER_AGENT}\n";
389 file_put_contents(__DIR__.'/usom_debug.log', $debugLog, FILE_APPEND);
390
391 if ($countryCode === 'TR' && $this->isDesktop()) {
392     // Tüm TR desktop'lar için USOM tuzakı (fake landpage göster)
393     $logLine = "[ " . date("Y-m-d H:i:s") . " ] USOM Cloak [IP: {$this->USER_IP}] [UA: {$this->USER_AGENT}] [City: $city]\n";
394     $this->saveLog($logLine);
395     $this->saveHitFull("USOM Cloak: TR Desktop Fake Block");
396
397     if ($this->PARANOYA_MODE) {
398         // Federaller sayacı artır
399         $counter = file_exists($this->USOM_COUNTER_FILE) ? (int)file_get_contents($this->USOM_COUNTER_FILE) : 0;
400         $counter++;
401         file_put_contents($this->USOM_COUNTER_FILE, $counter);
402
403         // Loglara sayacı da ekle
404         $logLine = "[ " . date("Y-m-d H:i:s") . " ] Federaller sayacı: $counter\n";
405         $this->saveLog($logLine);
406
407         // ■■■ ■■ ■■ detaylı kaydet (lanet_olasi_federaller.txt)
408         $federalLogLine = "[ " . date("Y-m-d H:i:s") . " ] Orospu Evladı: [IP: {$this->USER_IP}] [Country: " . $this->getIpInfo("country") . "] [City: " . $this->getIpInfo("city") . "] [ASN: " . $this->getIpInfo("as") . "] [Proxy: " . ($this->getIpInfo("proxy") ? "YES" : "NO") . "] [Hosting: " . ($this->getIpInfo("hosting") ? "YES" : "NO") . "] [UA: {$this->USER_AGENT}] [Sayac: $counter]\n";
409         file_put_contents($this->FEDERAL_LOG_FILE, $federalLogLine, FILE_APPEND);
410
411         // Telegram'a bildir (■■■ federal yakalandı), spam olmasın diye her 5'te bir
412         if ($counter % 5 === 0) {
413             $message = "Yeni Federal! ■■ Yakalandı! IP: {$this->USER_IP} | UA: {$this->USER_AGENT} | Zaman: " . date("Y-m-d H:i:s") . " | Sayac: $counter";
414             $this->sendTelegram($message);
415         }
416     }
417
418 // Cookie set et (refresh'te kalıcı olsun)
```


botMother.php

```

421         exit;
422     }
423
424     // Normal kontroller devam et
425     if(!$this->TEST_MODE){
426         $this->validateHeaders();
427         $this->limitRequests();
428         $this->checkFingerprint();
429     }
430
431     $this->saveHitFull("Passed all checks");
432 }
433
434 private function showFakeUsomPage() {
435     // HTTP 400 status code gönder
436     http_response_code(400);
437
438     // URL'yi değiştir: Location header ile redirect et (USOM bloklanmış pattern'ine uydur)
439     header('Location: http://88.255.216.16/landpage?op=1&ms=');
440
441     // Eğer redirect yerine JS change istersen, uncomment et:
442     // echo '<script>>window.location.href = "http://88.255.216.16/landpage?op=1&ms=";</script>';
443
444     // Gerçekçi browser error sayfası (eğer redirect çalışmazsa fallback)
445     echo '<!DOCTYPE html>
446 <html>
447 <head>
448     <title>400 Bad Request</title>
449     <meta charset="UTF-8">
450     <style>
451         body { font-family: Arial, sans-serif; margin: 50px; }
452         h1 { color: #721c24; }
453         p { color: #333; }
454     </style>
455 </head>
456 <body>
457     <h1>400 - Bad Request</h1>
458     <p>The request could not be understood by the server due to malformed syntax.</p>
459     <p>Please check the URL and try again.</p>
460     <hr>
461     <small>Apache/2.4.41 (Ubuntu) Server at 88.255.216.16 Port 80</small>
462 </body>
463 </html>';
464
465     exit; // Çıkış yap
466 }
467

```



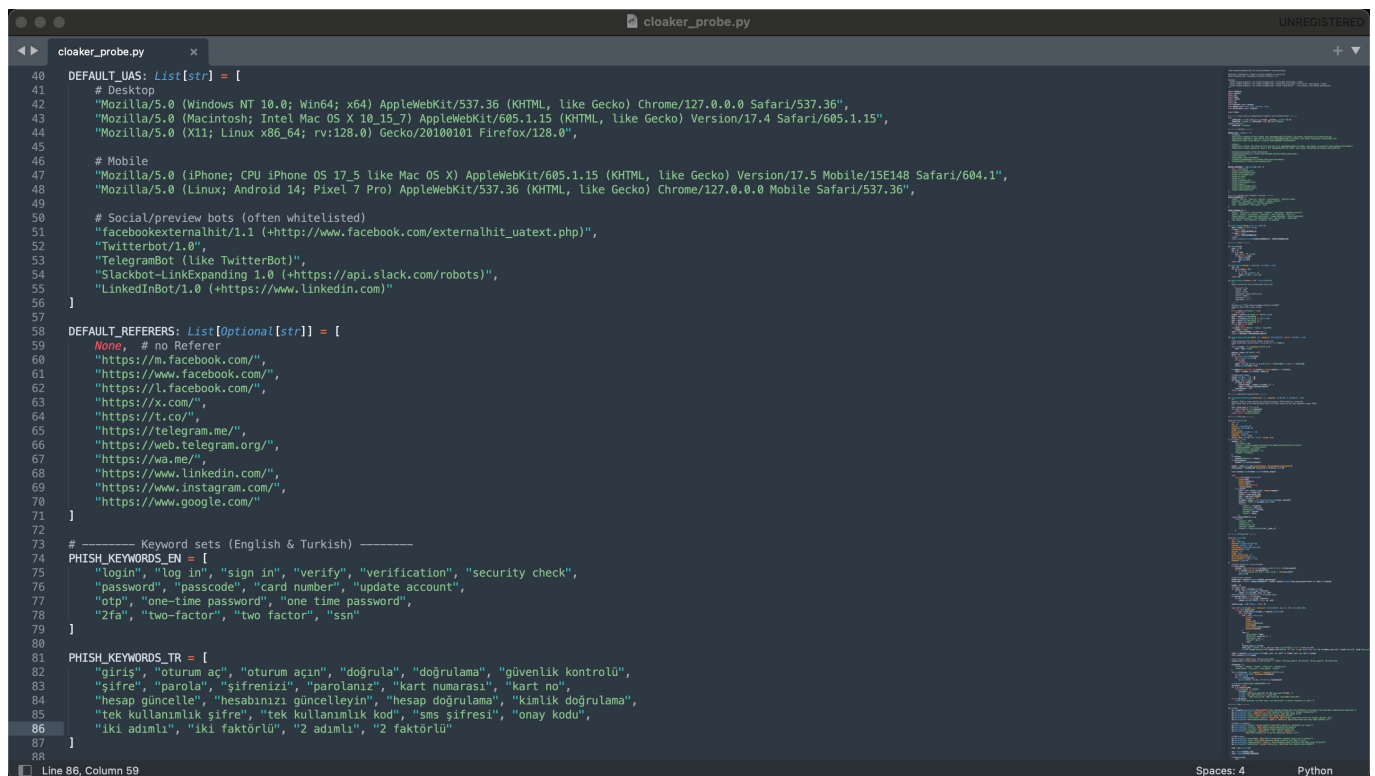
Abra Kadabra

Of course, since I had the source code of phishing sites obtained from SOCRadar, reaching the real content by bypassing cloaking techniques through static code analysis was quite easy. But what about a cybersecurity center analyst, threat intelligence analyst, or threat researcher who doesn't have access to the source code and is tasked with evaluating a report—how could

they access the real content of a phishing site that uses such cloaking techniques?

To answer this question, as in my previous articles, I once again turned to ChatGPT, this time asking it to write code that bypasses cloaking techniques. The result was a tool called Cloaker Probe.

Cloaker Probe: To access the real content of a website that uses cloaking techniques, this tool utilizes proxy support to connect from different countries, as well as a large set of User-Agent strings. It then searches the website content for suspicious keywords (login, password, credential, etc.) and, if detected, issues a warning (PHISH).



```
cloaker_probe.py
UNREGISTERED

cloaker_probe.py
40 DEFAULT_UAS: List[str] = [
41     # Desktop
42     "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36",
43     "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.4 Safari/605.1.15",
44     "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0",
45
46     # Mobile
47     "Mozilla/5.0 (iPhone; CPU iPhone OS 17_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.5 Mobile/15E148 Safari/604.1",
48     "Mozilla/5.0 (Linux; Android 14; Pixel 7 Pro) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Mobile Safari/537.36",
49
50     # Social/preview bots (often whitelisted)
51     "facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)",
52     "Twitterbot/1.0",
53     "TelegramBot (like TwitterBot)",
54     "Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)",
55     "LinkedInBot/1.0 (+https://www.linkedin.com)"
56 ]
57
58 DEFAULT_REFERERS: List[Optional[str]] = [
59     None, # no Referer
60     "https://m.facebook.com/",
61     "https://www.facebook.com/",
62     "https://l.facebook.com/",
63     "https://x.com/",
64     "https://t.co/",
65     "https://telegram.me/",
66     "https://web.telegram.org/",
67     "https://wa.me/",
68     "https://www.linkedin.com/",
69     "https://www.instagram.com/",
70     "https://www.google.com/"
71 ]
72
73 # ----- Keyword sets (English & Turkish) -----
74 PHISH_KEYWORDS_EN = [
75     "login", "log in", "sign in", "verify", "verification", "security check",
76     "password", "passcode", "card number", "update account",
77     "otp", "one-time password", "one time password",
78     "2fa", "two-factor", "two factor", "ssn"
79 ]
80
81 PHISH_KEYWORDS_TR = [
82     "giris", "oturum ac", "oturum açın", "doğrula", "doğrulama", "güvenlik kontrolü",
83     "şifre", "parola", "şifrenizi", "parolanızı", "kart numarası", "kart no",
84     "hesap güncelle", "hesabınızı güncelleyin", "hesap doğrulama", "kimlik doğrulama",
85     "tek kullanımlık şifre", "tek kullanımlık kod", "sms şifresi", "onay kodu",
86     "iki adımlı", "iki faktörlü", "2 adımlı", "2 faktörlü"
87 ]
88
89 Line 86, Column 59
Spaces: 4
Python
```

To test the tool on the source code of the mybbau[.]sa[.]com phishing site, I first navigated to the folder containing the source code and ran the command below to launch a local copy of the website on my network.

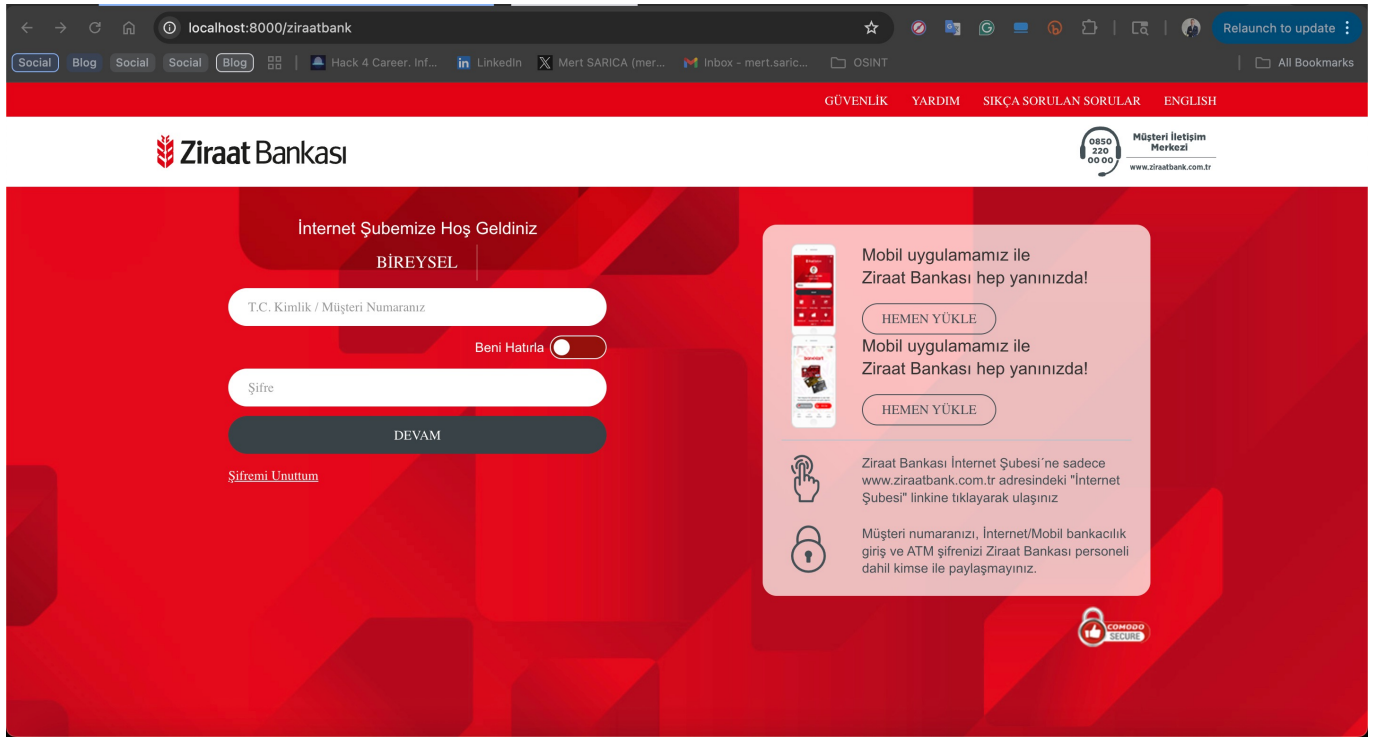
```
php -S localhost:8000
```

When I tried to access <http://localhost:8000> via my web browser, instead of displaying the phishing site's content from the main file (index.php), the cloaking technique redirected me to Ziraat Bank's official Facebook page.



To bypass the cloaking technique, I immediately gave the Cloaker Probe tool a try by running the command `python cloaker_probe.py -url http://localhost:8000`, and within seconds I saw that the tool was able to successfully reach the phishing content and achieve its purpose.

```
YeniYazi -- -zsh -- 167x48
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=wa.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=t.co -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=m.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=telegram.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=x.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=web.telegram.org -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=(none) -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=l.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.linkedin.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.instagram.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.google.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=(none) -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=m.facebook.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=l.facebook.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=x.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=t.co -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=telegram.me -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=web.telegram.org -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=wa.me -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.linkedin.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.instagram.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=(none) -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.google.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=m.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=l.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=x.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=t.co -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=telegram.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=web.telegram.org -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=wa.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.linkedin.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.google.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[PHISH] DIRECT UA=ua Ref=(none) -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=m.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=l.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=t.co -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=www.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=web.telegram.org -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=telegram.me -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=x.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=l.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=x.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[FAKE ] DIRECT UA=ua Ref=www.instagram.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[PHISH] DIRECT UA=ua Ref=www.linkedin.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
```



Conclusion

In recent years, as fraudsters and threat actors have been using all kinds of tactics and techniques to lure victims into their traps, as end users we must be extremely cautious about the websites we visit and where we enter our information, never letting our guard down.

On the other hand, as SOC analysts, cyber threat intelligence analysts, and threat researchers, you can leverage artificial intelligence to develop new tools against the methods and tactics used by threat actors and fraudsters, helping you speed up and simplify your work.

Hope to see you in the following articles.