Hack 4 Career

THIS BOOK WAS PRODUCED WITH PRESSBOOKS

Hack 4 Career

WWW.MERTSARICA.COM

MERTSARICA

THIS BOOK WAS PRODUCED WITH PRESSBOOKS

THIS BOOK WAS PRODUCED WITH PRESSBOOKS

Contents

THIS BOOK WAS PRODUCED WITH PRESSBOOKS

Giriş

2009 yılında "Bilgi güçtür ve paylaşıldıkça artar" mottosuyla oluşturduğum blogumda, bilgi güvenliği farkındalığını arttırma 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 dileklerimle…

Mert SARICA
https://www.mertsarica.com
https://twitter.com/MertSARICA
https://www.linkedin.com/in/mertsarica
CCISO, CISSP, SSCP, OSCP, CREA, CEREA

This book was produced using

PB PRESSBOOKS

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. Troll Avı

Başlangıç

Siber tehdit istihbaratının öneminin gün be gün arttığı son yıllarda, kurumlarda bunun için kullanılan ürünlerin, hizmetlerin sayısının da katlanarak arttığını görüyoruz. Öncelikle siber tehdit istihbaratı kurumlara, bulundukları sektörü hedef alan tehdit aktörlerini tanımaları, kullandıkları taktikleri, teknikleri ve prosedürleri öğrenerek kurumlarına karşı gerçekleşebilecek olası siber saldırılara karşı hazırlıklı olmaları adına önemli bir avantaj sağlıyor. Diğer yandan siber saldırıya maruz kaldıklarında ise Siber Olay Müdahale (Incident Response) sürecinde elde edilen verilerin zenginleştirilmesinden tehdit aktörü ile olan bağlantısına kadar olayın aydınlatılmasına ışık tutabiliyor.

Kurumlar kadar teknoloji ile iç içe yaşayan son kullanıcıların, bireylerin yani bizlerin de siber tehdit istihbaratından, platformlarından kimi durumlarda (Misal Troll hesap araştırması) büyük fayda sağlayabileceğimizi unutmamamız gerekiyor.

Troll, Trolleme ve Dezenformasyon Nedir?

Tüm dünyada olduğu gibi ülkemizde de **Troll** hesaplar tarafından paylaşılan mesajların (**Trolleme**) sosyal ağlarda, medyalarda mantar gibi türediğine ve kitleleri dezenformasyon yönteminden faydalanarak manipüle etmeye çalıştığına tanıklık ediyoruz. Bazen bu yalan bilgiler kişilerin kendi hesaplarından paylaşıldığı gibi sahte, anonim hesaplar üzerinden de paylaşılabiliyor.

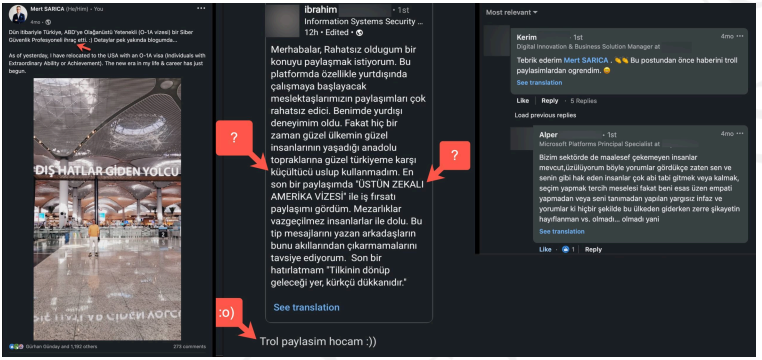
> Troll İngilizce'de olta, olta yemi, oltayla balık tutmak anlamına gelen bir kelimedir. Trolleme ise geniş bir kitleyi manipüle etmek için yalan bilgi, asılsız fikir veya yazı yaymak anlamına gelmektedir. (Kaynak: Türk Toplumunda Sosyal Medyaya Eleştirel Bakış Eksikliği: Türk Troller ve Trolleme)

> Dezenformasyon, yanlış veya doğruluğu bulunmayan ve kasıtlı olarak yayılan bilgi; bilgi çarpıtma anlamına gelir. Hasmı rencide etmeyi, aşağılayıp küçük düşürmeyi amaçlayan karşı propaganda ile benzerlik taşır. Sahte belge, el yazısı, fotomontaj ve montaj filmler ile fabrikasyon istihbarat ve dedikoduların duyurulması gibi yöntemleri bulunur. Sosyal alanda bireyleri ve toplumları yönlendirmek amacıyla, yanlış bilgi ve haber vermek için kullanılan en önemli araçlardan biridir. Yanlış bilgi üretme ve yayma yoluyla yapılabileceği gibi mevcut bir bilgiyi kötü maksatla kullanma ve çarpıtarak verme yöntemi de uygulanabilir. (Kaynak: Wikipedia)

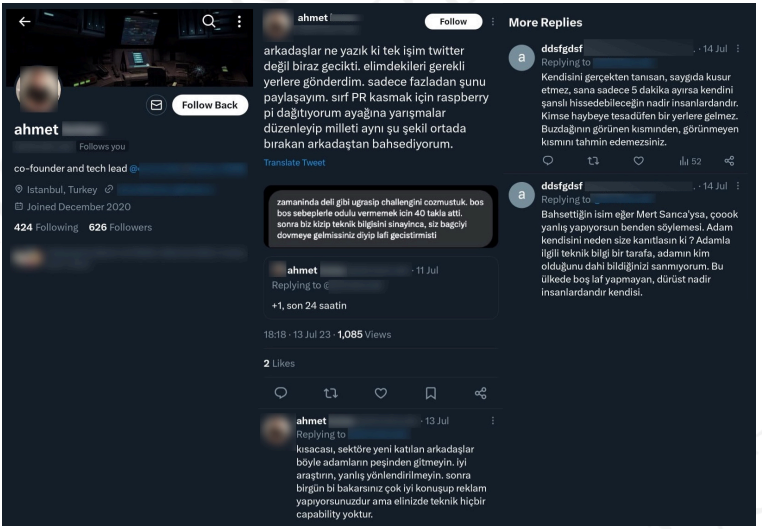
2009 yılından bu zamana dek gerçekleştirmiş olduğum **200**'den fazla siber güvenlik araştırmamı **TÜRKÇE** olarak blogumda "Bilgi güçtür ve paylaşıldıkça artar!" mottosu ile karşılıksız paylaşmış, 2015 yılından beri düzenlediğim Pi Hediyem Var oyunu ile üniversite öğrencilerine sponsorlarımın desteği ile **15**'ten fazla Raspberry Pi hediye etmiş, **30**'a yakın siber güvenlik etkinliğinde konuşmacı olmuş, Sızma Testi Uzmanlığı / Etik Hacker ve Kariyer başlıklı sunumum ile **40**'a yakın üniversitede siber güvenlik alanına meraklı binlerce öğrenciye yol göstermiş,
bir siber güvenlik profesyoneli olsam da, nadir de olsa ben de **Troll** hesapların hedefi haline gelebiliyorum.

Troll ve Trolleme Örnekleri

Çoğu zaman daha ne olduğunu anlayamadan, iyi niyetimden en ufak şüphesi olmayan sevgili takipçilerimin tepkileri, eleştirileri sayesinde Troll hesaplar çoktan ya kapanmış ya mesajlarını silmiş ya da cevaplarını almış oluyorlar. Bu gibi durumlarda siber tehdit istihbaratından, platformlarından faydalanmama pek gerek kalmıyor. Aksi durumlarda ise WhatsApp Dolandırıcıları, Kripto Para Dolandırıcıları başlıklı blog yazılarımda olduğu gibi siber tehdit istihbaratından, platformlarından bireysel olarak oldukça faydalanıyorum.



Mesaj Silinmiş



Mesaj Silinmiş

> Özellikle sosyal mecralarda bir kişiye direkt veya dolaylı yoldan hakaret ettiğinizde, küfür ettiğinizde, itibar suikastı yaptığınızda, iftira attığınızda, tehdit ettiğinizde, vatanseverliğine dil uzattığınızda, er ya da geç bunun karşınıza çıkacağını, bir nedenden pişman olup mesajınızı silseniz de, kayıtlardan ve

hafızalardan kolay kolay silinmeyeceğini unutmamanız gerekiyor.

Bazı zamanlarda e-posta, sosyal medya veya ağ üzerinden aldığınız şüpheli bir mesajın arkasındaki kişinin niyetini, kim olduğunu anlamak amacıyla da siber tehdit istihbaratı platformlarından faydalanabiliyorsunuz.

Bu örnekte bir Troll'ün web sitem üzerinden önce hakaret ettiğini, muhattap alınmadıktan 1 ay sonra ise bu defa farklı bir yaklaşımla sosyal ağ üzerinden iletişime geçmeye çalıştığını görüyorsunuz. E-posta adresini SOCRadar Siber Tehdit İstihbaratı Platformu'nda arattığınızda şahsın yıllardır hacker forumlarında gezindiğini öğrenerek niyeti ve motivasyonu hakkında kolaylıkla bilgi ve fikir sahibi olabiliyorsunuz.

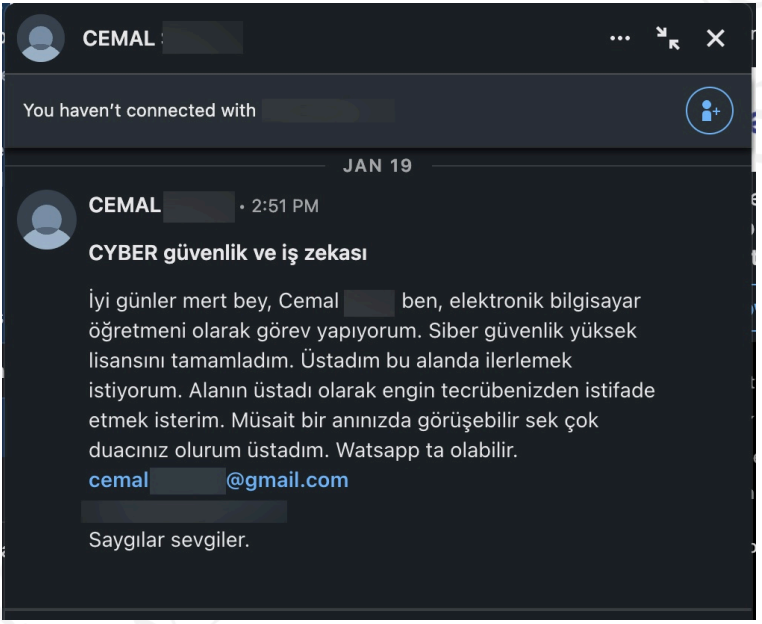

[Siber Güvenlik Günlüğü] Yorum: "ABD Olağanüstü Yetenek Vizesi (O-1A)" Inbox ×

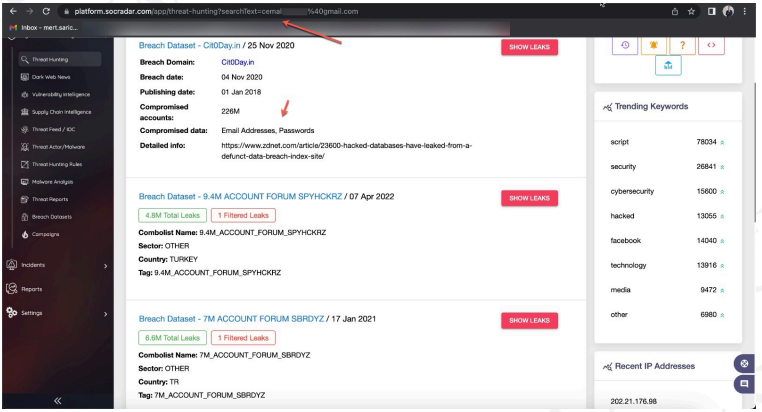
Cemal alert@mertsarica.com via
to me
Fri, Dec 30, 2022, 2:15 AM

Turkish › English Translate message
Turn off for: Turkish

"ABD Olağanüstü Yetenek Vizesi (O-1A)" yazınızda yeni yorum
Yazar: Cemal (IP adresi:)
E-posta: cemal @gmail.com
Adres: http://Yok
Yorumlar:
Şimdi tamda kına yakma zamanın gelmiş. Yani sen Sen kısaca diyorsun ki bu kadar başarını tamamı amerikanın kapısında köpek olmaya anca yetti. Sen Barış Manço dinleseydin bu hallere düşmezdin. Bu kafayla bir baltaya sap olamazsın ama gün gelir sapın ucuna olursun kazma.

Bu yazıya yapılmış tüm yorumları buradan görebilirsiniz:
https://www.mertsarica.com/abd-olaganustu-yetenek-vizesi-o-1a/#comments

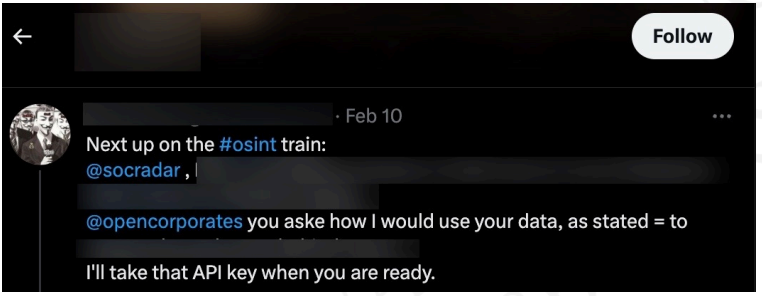




Özellikle tehdit aktörlerinin, siber suçluların, dolandıcıların izini süren, operasyonlarını ortaya çıkaran ve bununla ilgili istihbarat paylaşan bir siber tehdit istihbaratı firmasında çalışıyorsanız kimi zaman sosyal medyada anonim hesaplar üzerinden kurumunuzu hedef alan tehditvari mesajlarla da karşılaşabiliyorsunuz. Bu gibi durumlarda da kendi

platformunuzdan faydalanabildiğiniz gibi daha farklı yöntemler de izleyebiliyorsunuz.

Bu örnekte güvenlik kontrolünden geçemediği için siber tehdit istihbaratı platformuna kayıt olmasına izin verilmeyen bir şahsın önce tehditvari e-posta gönderdiğini akabinde ise Twitter'da anonim bir hesap üzerinden trolleme yapmaya başladığını görüyorsunuz.



Hesap Silinmiş

Peki gerçek kimliği ile e-posta gönderen bir kişi ile Guy Fawkes maskesi ardına gizlenen anonim bir Twitter hesabı üzerinden mesaj paylaşan bir kişinin yüksek olasılıkla aynı kişi olduğunu nasıl kanaat getirebiliriz?

Elimizde şüphelendiğimiz kişiye ait örnek e-postalar ve anonim Twitter hesabından paylaşılan mesajlar olduğu için bunlar üzerinde yazarı tespit etmeye yönelik stilometrik yöntemlerden (Noktalama, yazım yanlışları, vurgu, yabancı sözcük, argo ve jargon, bağlaç, kısaltmalar, sayılar, konu etiketleri, şekil ve işaretler) faydalanabiliyoruz.

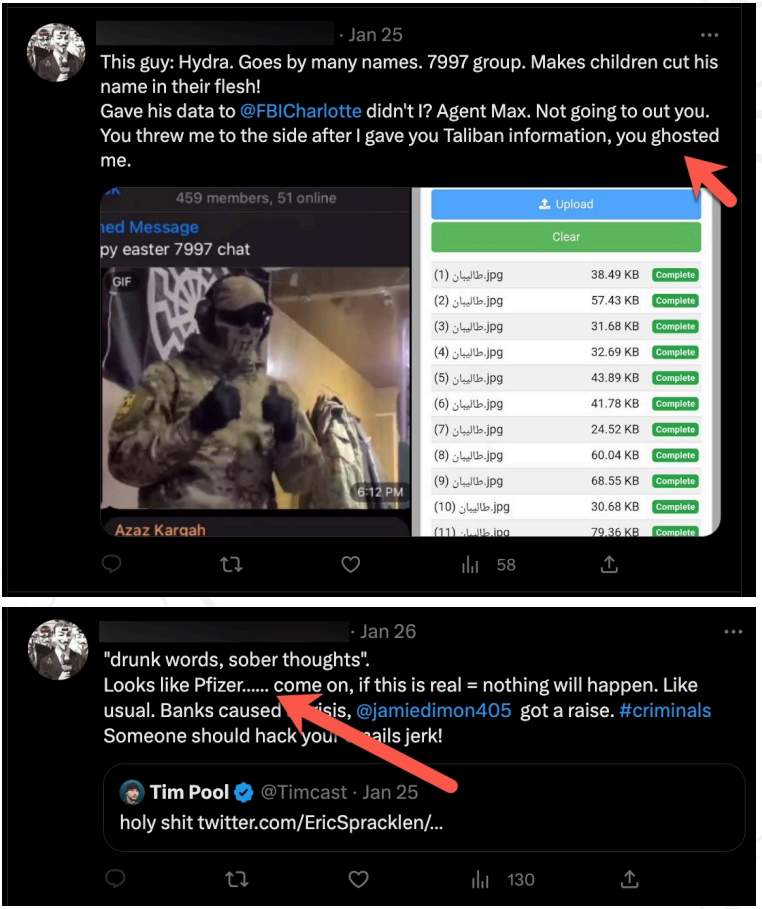
Stilometri Nedir?

> Stilometri, öncelikle yazılı edebiyat alanında olmak üzere, resim ve müzik gibi sanat dallarında, tarih, din ve hukuk alanında ve adli bilimlerde kullanılan bir üslup belirleme çalışmasıdır. Stilometri analizi ise, üslup belirteçlerinin (syle markers) değişken olarak alınıp bu değişkenlerin istatistiksel ve bilişimsel metotlar incelenmesine dayanan bir yöntemdir.
>
> Stilometri, yaklaşık iki yüz yıldır yazarların edebi

> üslubunun karşılaştırılması ve özellikle eser sahipliği (authorship attribution) problemlerinde çeşitli istatistiksel metotlar kullanılarak uygulanmıştır. Kullanılan metotlar, temel istatistiksel hesaplamalardan ve testlerden yapay sinir ağlarına kadar geniş bir aralıkta yer almaktadır. Dini metinlerden tarihi metinlere, bilimsel çalışmalardaki intihalden edebi eserlerin ve yazarların üslubunun incelenmesine kadar pek çok konuda stilometrik çalışma yapılmıştır. (Kaynak: İstatistik'ten Edebiyat'a Bir Köprü: Stilometri Analizi – Ayşe İŞİ, Fatih ÇEMREK, Zeki YILDIZ)

Troll Avı

Bu aşamada geniş kapsamlı bir Stilometri analizi yapmak yerine anonim Twitter hesabındaki **109** tane mesaja kabaca göz atıp, e-postalarla örtüşen ortak kelimelere, noktalama işaretlerine odaklanmaya karar verdim. Aldığım notlar doğrultusunda dikkatimi çeken mesajlarında bol bol **…..** noktalama işaretine yer vermesi ve İngilizce yazışmalarda pek sık rastlamadığım **ghosted** kelimesi oldu. Bunlara yönelik olarak şüphelendiğim kişiden gelen e-postalara baktığımda tespitlerim ile fazlasıyla örtüştüğünü görerek iki kişi arasındaki benzerlik olasılığını fazlasıyla arttırmış oldum.



Peki bu anonim Twitter hesabından paylaşılan mesaj sayısı 109 değil de 10009 olsaydı o zaman ne yapardım diye düşünmeye başladığımda veri bilimin yardımına başvurmaya karar verdim.

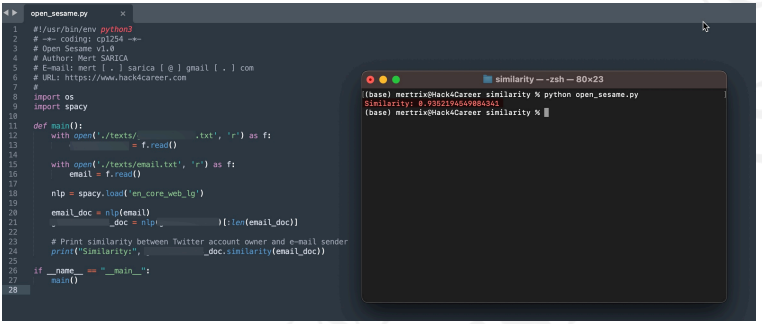
> Veri bilimi, iş için anlamlı öngörüler ayıklamak amacıyla veriler üzerinde gerçekleştirilen çalışmaların adıdır. Büyük miktardaki verileri analiz etmek için matematik, istatistik, yapay zeka ve bilgisayar mühendisliği alanlarının ilke ve uygulamalarını bir araya getiren, disiplinler arası bir

> yaklaşımdır. Bu analiz, veri bilimcilerinin ne olduğu, neden olduğu, ne olacağı ve sonuçlarla neler yapılabileceğini sormalarına ve bu soruları cevaplamalarına yardımcı olur.

Biraz araştırma yaptıktan sonra SpaCy isimli Doğal Dil İşleme (NLP) kütüphanesinde metinler arasındaki benzerliği ölçmeye yarayan ve Kosinüs Benzerliği'ni kullanan **similarity** metodundan faydalanabileceğimi öğrendim.

> Kosinüs Benzerliği, metinler arasındaki benzerliği vektörel olarak ölçmektedir. Metinlerde geçen kelimelerin metinde kaç kez geçtiği hesaplanır. Daha sonra her metin içerdiği kelimelerle 1 ve 0 şeklinde vektörel olarak ifade edilir. Her metin üç boyutlu uzayda vektörel olarak yerleştirildiğinde aralarındaki kosinüs açısı ne kadar küçük ise metinler birbirlerine o kadar yakındır. Tamamen birbiri ile ilişkisiz olan vektörler için ise kosinüs değeri 0 olurken tamamen birbirini zıddı olan dokümanlar için kosinüs değeri -1 olacaktır. (Kaynak: Netflix verileri üzerinde TF-IDF algoritması ve Kosinüs benzerliği ile bir İçerik Öneri Sistemi Uygulaması – Özlem GELEMET Hakan AYDIN Ali ÇETİNKAYA)

Python ile ufak bir kod yazıp şüphelendiğim kişiden gelen e-postalar ile Twitter mesajları arasındaki benzerliğe baktığımda SpaCy kütüphanesi sayesinde bunların çok yüksek ihtimalle aynı kişi tarafından gönderildiğine kanaat getirerek kendimi ikna etmiş ve mutlu sona ulaşmış oldum. 🙂



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Stilometrinin kullanımına yönelik daha fazla bilgi edinmek isteyenlerin Real-World Python: A Hacker's Guide to Solving Problems with Code kitabının ücretsiz olarak sunulan bölümünü okumalarını tavsiye edebilirim.

2. Deepfake Dolandırıcılarına Dikkat!

Başlangıç

2024 yılının Mayıs ayı itibariyle üretken yapay zekanın devrimine, gelişimine hem heyecanla hem de endişeyle tanıklık etmeye devam ediyoruz. OpenAI firması, duyurduğu GPT-4o ile ChatGPT'nin insana çok daha yakın şekilde diyalog kurduğunu, ses, metin ve görüntüyü anlayıp, içerik ürettiğini bir lansmanla dünyaya gösterdi. Öte yandan yapay zeka savaşlarında geride kalmak istemeyen Google ise OpenAI'nın hemen ardından kendi üretken yapay zekası Gemini'den yeni bir özellik paylaştı. Bu özellik ile Gemini, kamera uygulaması üzerinden çevrede neler olup bittiğini, konum olarak nerede olduğunu kullanıcıya anlık olarak aktarabiliyordu.

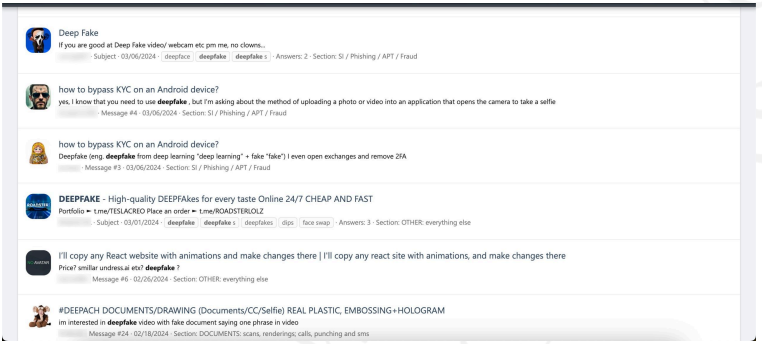
Peki büyük bir heyecanla, merakla takip ettiğimiz bu

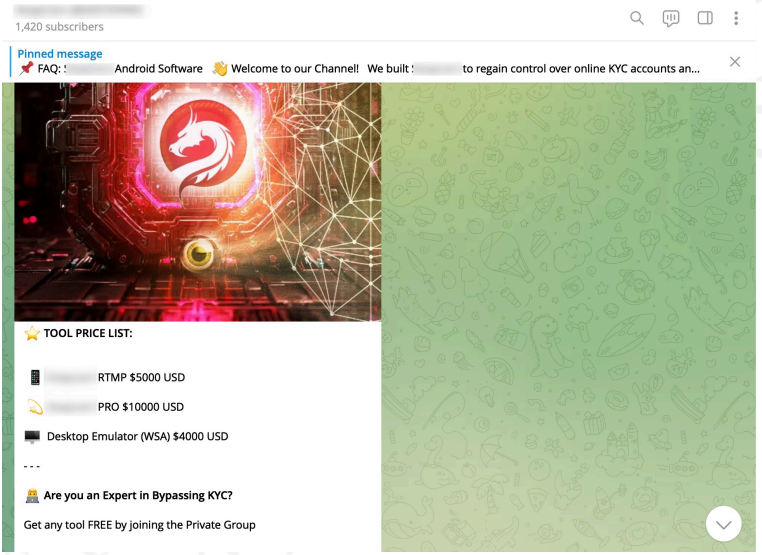
gelişmelerin yanında biz siber güvenlik profesyonellerini, araştırmacılarını en çok ne endişelendirir diye soracak olursak, kendi adıma sunulan tüm bu özelliklerin dolandırıcıların, tehdit aktörlerinin gerçekleştirecekleri dolandırıcılık girişimlerini, siber saldırıları ne kadar kolaylaştırdığı veya zorlaştırdığı olur. İnsansı robotlarda olduğu gibi üretken yapay zekada da gelişim, insan, insana yakın üretkenlikle kıyaslandığı için de genelde ortaya çıkan faydadan art niyetli kişiler de başta derin sahte, diğer orijinal adıyla deepfake ile görsel, video, ses ve metin oluşturma noktasında fazlasıyla nemalanıyorlar. OpenAI CEO'su Sam ALTMAN da benimle aynı fikirde olsa gerek ki geçtiğimiz günlerde Open AI'nın DALL-E 3 modeli ile oluşturulan deepfake görsellerinin tespit edilmesi için bir araç üzerinde çalıştıklarını duyurdu.

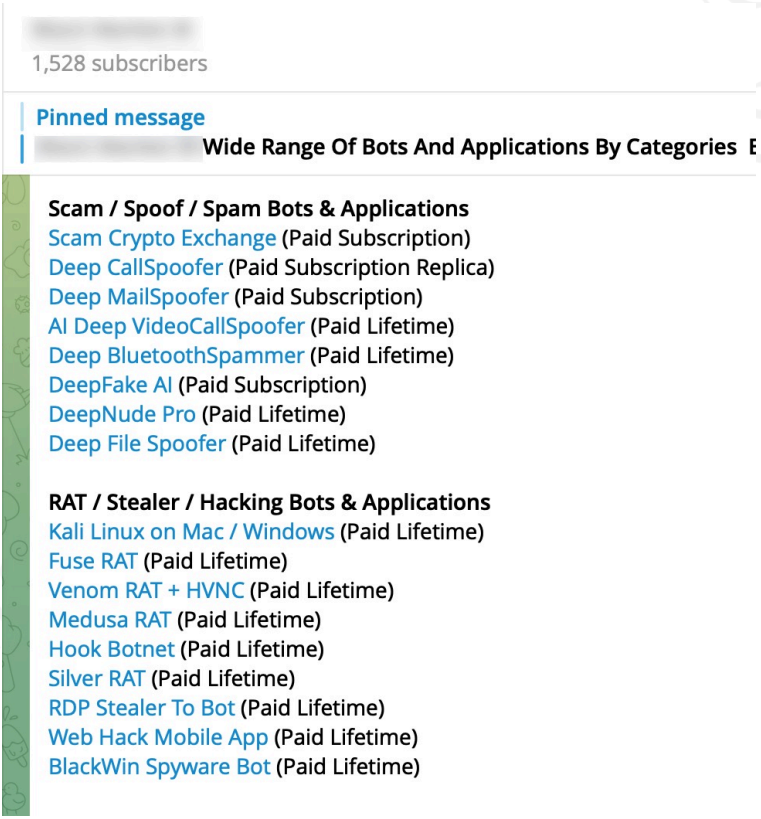
Deepfake Nedir?

> Deepfake, mevcut bir görüntü veya videoda yer alan bir kişinin, yapay sinir ağları kullanarak bir başka kişinin görüntüsü ile değiştirildiği bir medya türüdür. Sıklıkla, otomatik kodlayıcılar ve çekişmeli üretici ağlar (GAN'lar) olarak bilinen makine öğrenme tekniklerini kullanarak mevcut medyanın kaynak medya üzerinde birleştirilmesi ve üst üste konması ile üretilirler. (Kaynak: Wikipedia)

Deepfake'nin son yıllarda başta Rusya – Ukrayna savaşı olmak üzere dezenformasyon, dolandırıcılık ve parodi amacıyla sıklıkla kullanıldığını görüyoruz. Diğer yandan dolandırıcıların, tehdit aktörlerinin sıklıkla yer aldığı forumlara, Telegram kanallarına göz attığımızda da deepfake üzerine paylaşılan mesajların, dolandırıcılık servislerinin arttığı da dikkatlerden kaçmıyor. Pek tabii bu artış, sosyal ağlarda zaman geçiren kişilerin bu tür dolandırıcılık risklerine maruz kalma ihtimalini de bir o kadar arttırıyor.





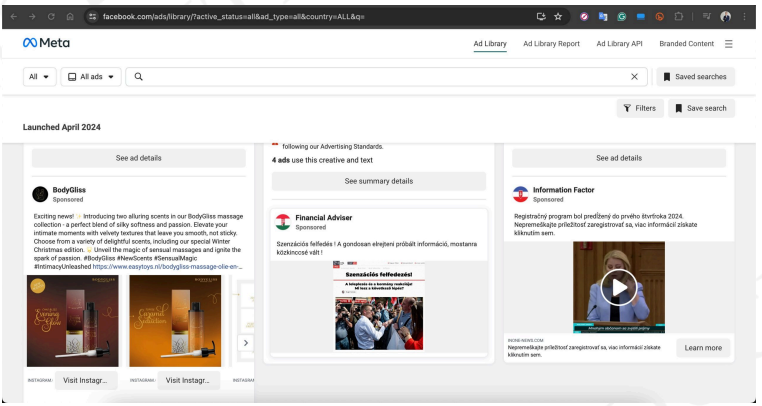


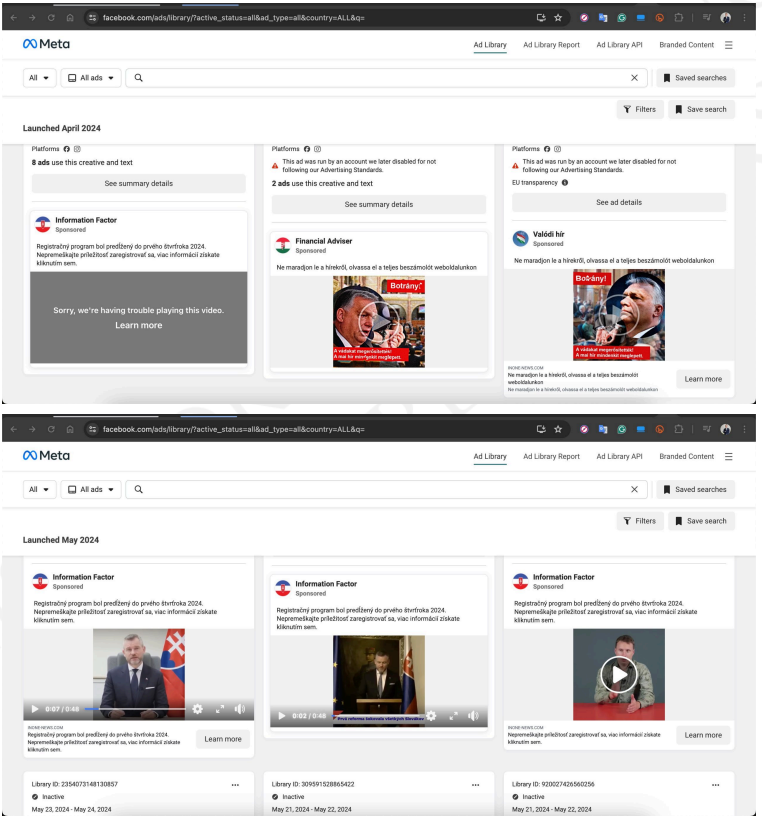
Deepfake Çetesi

SOCRadar gibi tehdit aktörlerinin, dolandırıcıların izini süren ve müşterilerine bu konuda 7/24 istihbarat sağlayan bir siber tehdit istihbaratı firmasında çalışıyor veya hizmet alıyorsanız öyle ya da böyle çok sayıda farklı mecrada art niyetli kişiler tarafından gerçekleştirilen şüpheli, zararlı aktiviteleri yakından takip etme, haberdar olma imkanınız oluyor.

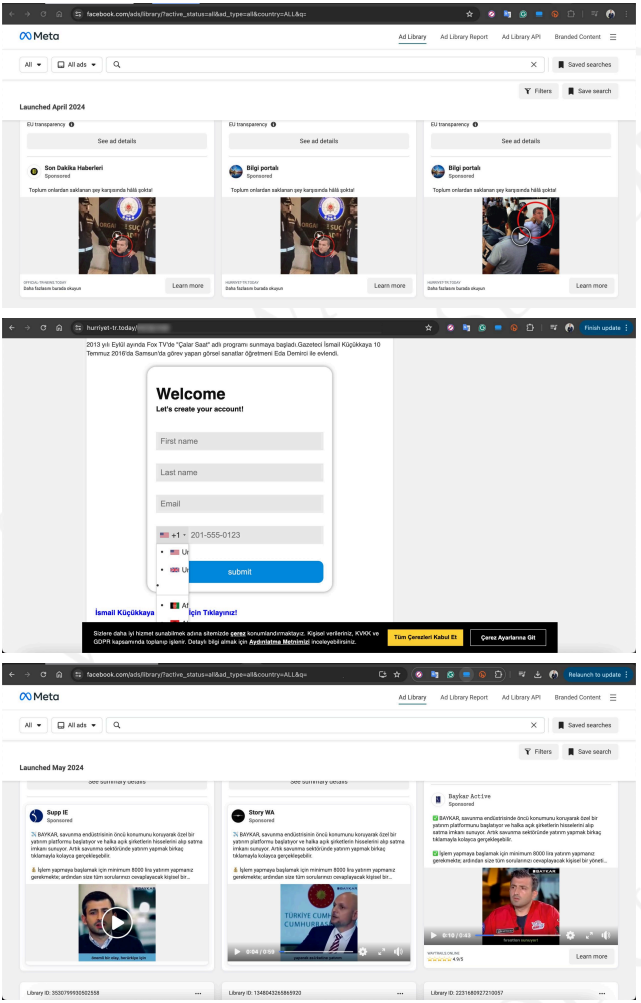
Yakın bir süre önce elde ettiğim bilgiler doğrultusunda Rusya merkezli olduğuna kanaat getirdiğim, operasyonlarının teknik

detaylarına başka bir yazımda yer vermeyi planladığım bir dolandırıcılık çetesini yakından takip etmeye başladım. 2023 yılının Ekim ayından bu yana Slovnaft, INA d.d, Bosphorus Gaz gibi petrol rafineri, gaz dağıtım şirketlerinden, Baykar gibi savunma şirketlerine hatta Interpol'e kadar uluslararası kurumların adını kullanarak dolandırıcılık girişiminde bulunan bu çete, Meta çatı şirketine ait Facebook, Instagram, Messenger üzerinden sahte reklamlarla kurbanlarını avlamaya çalışıyordu. Zaman zaman Google arama sayfasına da sahte reklam veren bu çete özellikle hedef aldıkları ülkelerin vatandaşlarını ağlarına düşürmek için siyasetçilere, iş insanlarına, haber sunucularına ait deepfake ile oluşturulmuş görseller, videolar kullanmaktan da geri kalmıyorlardı.



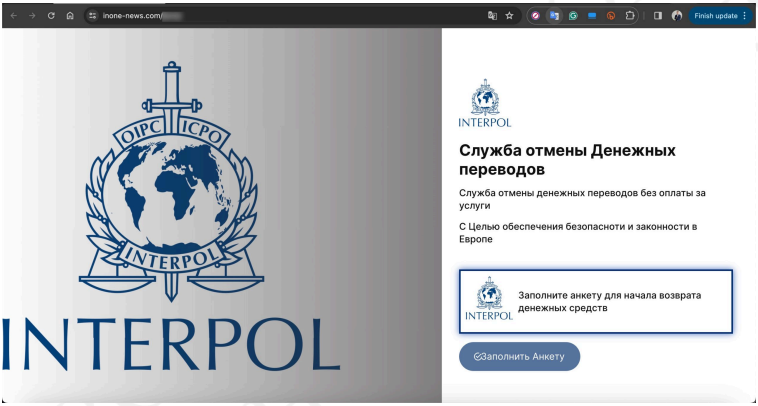


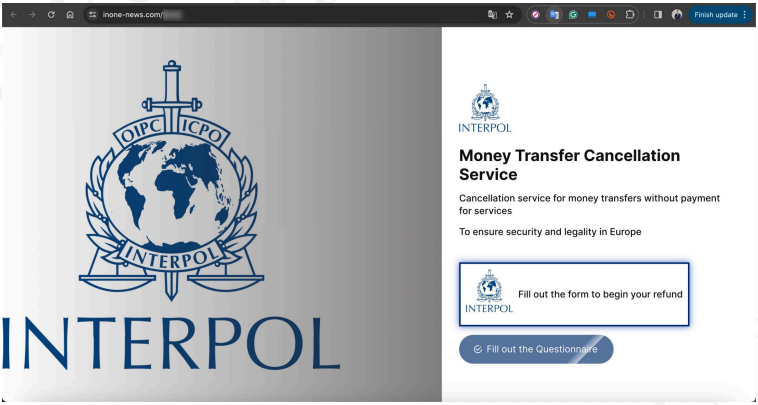
Örneğin Türk vatandaşlarını hedef aldıkları reklamlarında Selçuk BAYRAKTAR, Acun ILICALI, İsmail KÜÇÜKKAYA gibi isimlerin deepfake görsellerini ve videolarını kullanıyorlardı.

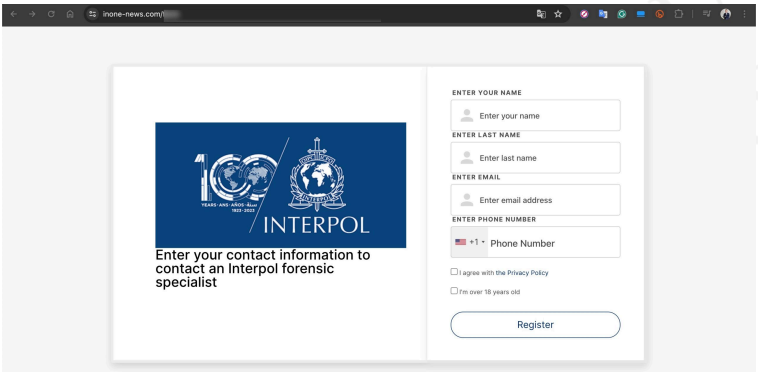


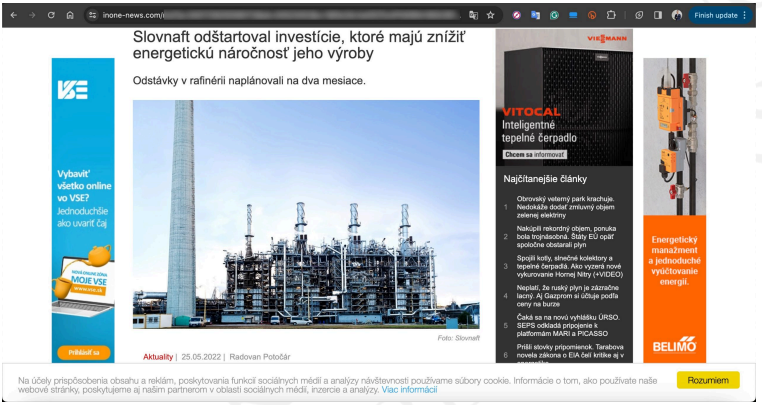
Minimum **8000 TL** yatırım ile ayda **100.000 TL** kazanç elde edilebileceğinin vaad edildiği sahte, deepfake videolarına konu olan bağlantı adresleri ziyaret edildiğinde karşınıza kimi zaman sadece isim, soyad, e-posta adresi ve cep telefonu numarasını isteyen oldukça basit kimi zaman ise görsel açıdan zengin, çoktan seçmeli seçeneklerle daha fazla bilgi toplayan ve

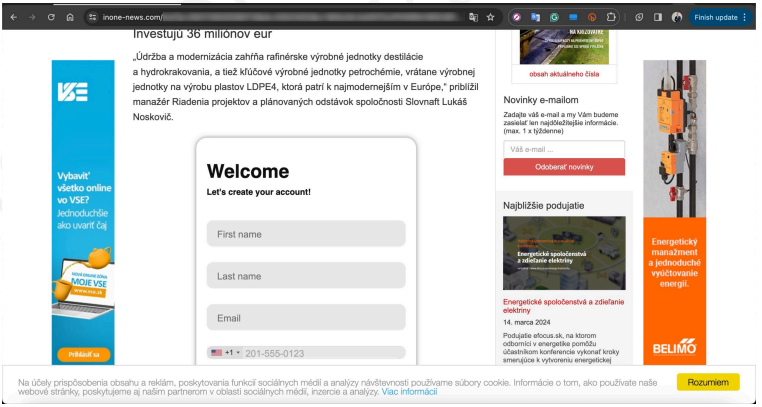
ardından bir operatörün sizinle iletişime geçeceğini söyleyen bir başvuru formu çıkıyordu.

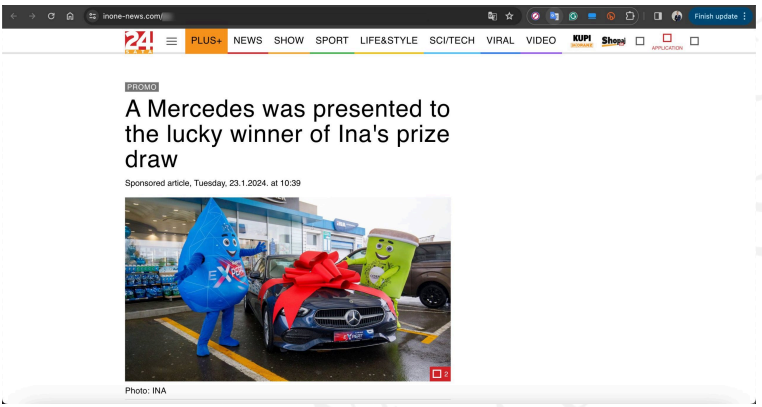


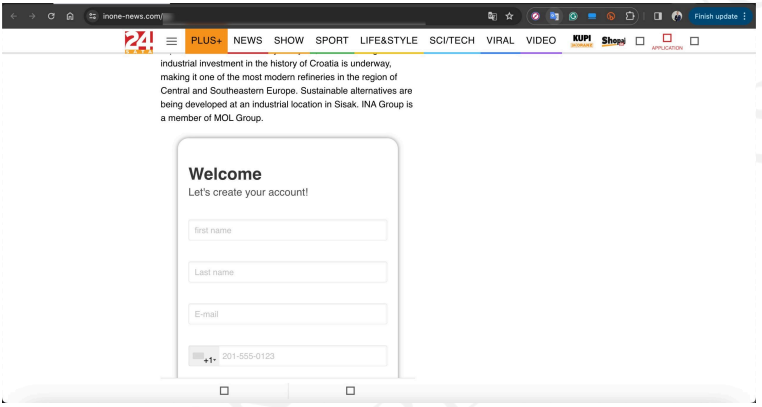


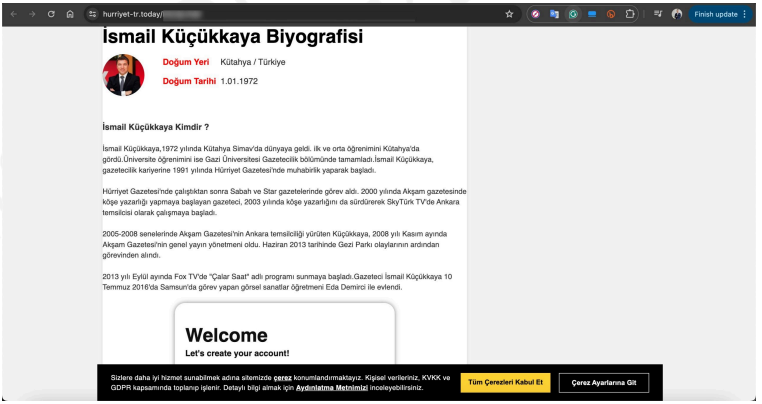


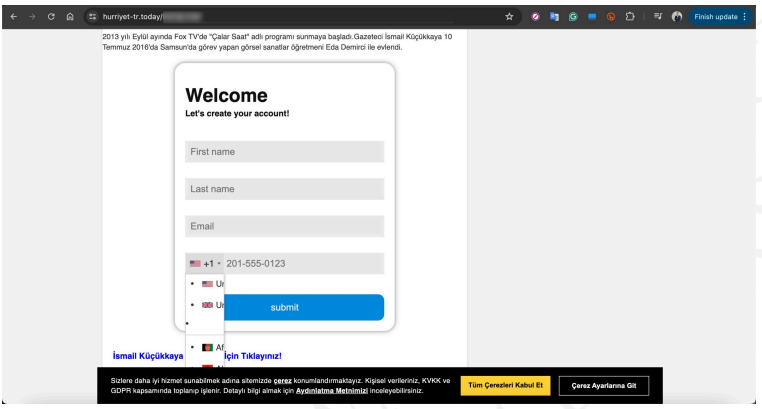

Slovnaft odštartoval investície, ktoré majú znížiť energetickú náročnosť jeho výroby
Odstávky v rafinérii naplánovali na dva mesiace.
Foto: Slovnaft
Aktuality | 25.05.2022 | Radovan Potočár
Najčítanejšie články
Vybavíť všetko online vo VSE?
Jednoduchšie ako uvariť čaj
Energetický manažment a jednoduché vyúčtovanie energií.
BELIMO
Na účely prispôsobenia obsahu a reklám, poskytovania funkcií sociálnych médií a analýzy návštevnosti používame súbory cookie. Informácie o tom, ako používate naše webové stránky, posky tujeme aj naším partnerom v oblasti sociálnych médií, inzercie a analýzy. Viac informácií
Rozumiem

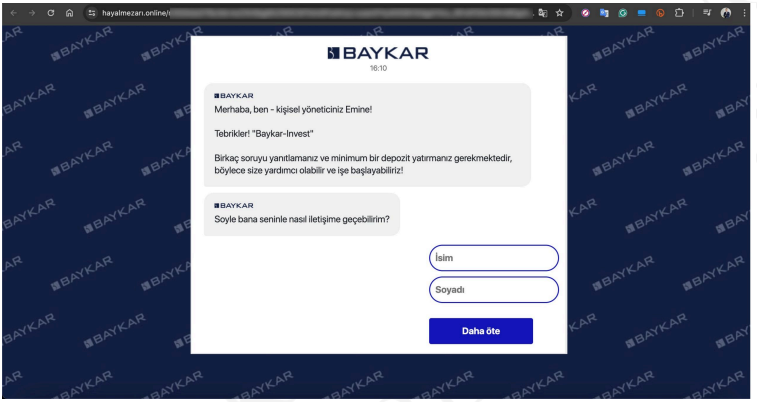

Investujú 36 miliónov eur
„Údržba a modernizácia zahŕňa rafinérske výrobné jednotky destilácie a hydrokrakovania, a tiež kľúčové výrobné jednotky petrochémie, vrátane výrobnej jednotky na výrobu plastov LDPE4, ktorá patrí k najmodernejším v Európe," priblížil manažér Riadenia projektov a plánovaných odstávok spoločnosti Slovnaft Lukáš Noskovič.
Welcome
Let's create your account!
First name
Last name
Email
201-555-0123
obsah aktuálneho čísla
Novinky e-mailom
Zadajte váš e-mail a my Vám budeme zasielať len najdôležitejšie informácie. (max. 1 x týždenne)
Váš e-mail ...
Odoberať novinky
Najbližšie podujatie
Energetické spoločenstvá a zdieľanie elektriny
14. marca 2024
Podujatie efocus.sk, na ktorom odborníci v energetike pomôžu účastníkom konferencie vykonať kroky smerujúce k vytvoreniu energetickej
Vybavíť všetko online vo VSE?
Jednoduchšie ako uvariť čaj
Energetický manažment a jednoduché vyúčtovanie energií.
BELIMO
Na účely prispôsobenia obsahu a reklám, poskytovania funkcií sociálnych médií a analýzy návštevnosti používame súbory cookie. Informácie o tom, ako používate naše webové stránky, posky tujeme aj naším partnerom v oblasti sociálnych médií, inzercie a analýzy. Viac informácií
Rozumiem

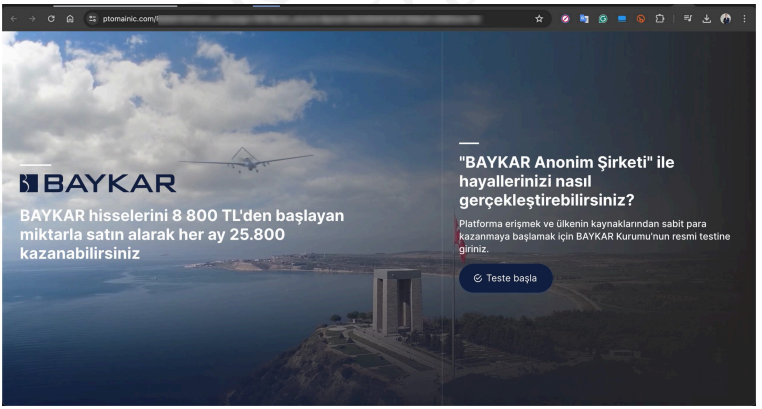

PLUS+ NEWS SHOW SPORT LIFE&STYLE SCI/TECH VIRAL VIDEO
PROMO
A Mercedes was presented to the lucky winner of Ina's prize draw
Sponsored article, Tuesday, 23.1.2024. at 10:39
Photo: INA

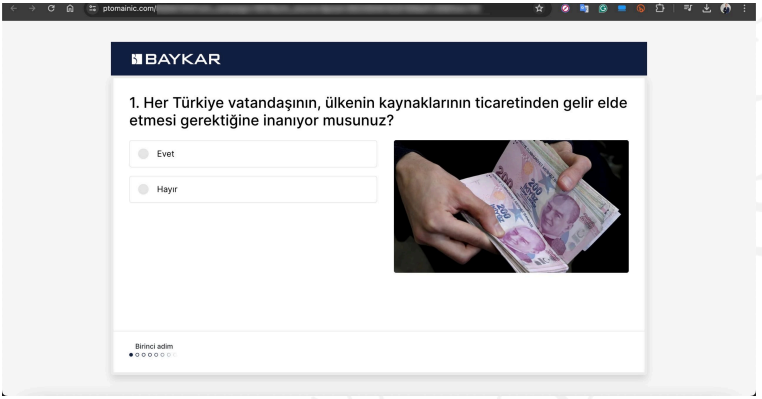

inone-news.com/
Finish update
PLUS+ NEWS SHOW SPORT LIFE&STYLE SCI/TECH VIRAL VIDEO
industrial investment in the history of Croatia is underway, making it one of the most modern refineries in the region of Central and Southeastern Europe. Sustainable alternatives are being developed at an industrial location in Sisak. INA Group is a member of MOL Group.
Welcome
Let's create your account!
first name
Last name
E-mail
+1 201-555-0123

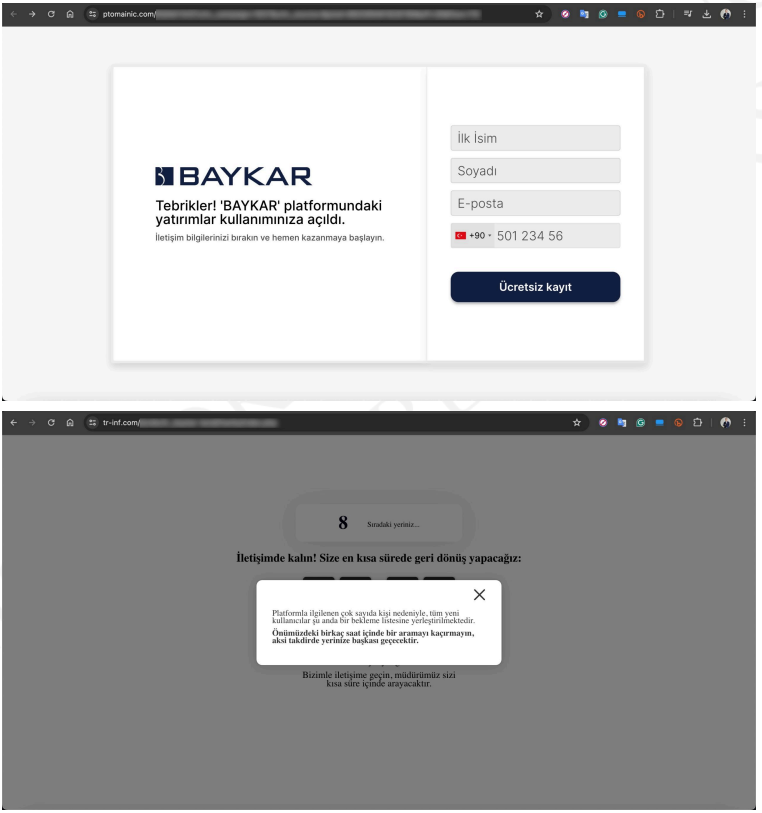

hurriyet-tr.today/
Finish update
İsmail Küçükkaya Biyografisi
Doğum Yeri Kütahya / Türkiye
Doğum Tarihi 1.01.1972
İsmail Küçükkaya Kimdir ?
İsmail Küçükkaya,1972 yılında Kütahya Simav'da dünyaya geldi. İlk ve orta öğrenimini Kütahya'da gördü.Üniversite öğrenimini ise Gazi Üniversitesi Gazetecilik bölümünde tamamladı.İsmail Küçükkaya, gazetecilik kariyerine 1991 yılında Hürriyet Gazetesi'nde muhabirlik yaparak başladı.
Hürriyet Gazetesi'nde çalıştıktan sonra Sabah ve Star gazetelerinde görev aldı. 2000 yılında Akşam gazetesinde köşe yazarığı yapmaya başlayan gazeteci, 2003 yılında köşe yazarlığını da sürdürerek SkyTürk TV'de Ankara temsilcisi olarak çalışmaya başladı.
2005-2008 senelerinde Akşam Gazetesi'nin Ankara temsilciliği yürüten Küçükkaya, 2008 yılı Kasım ayında Akşam Gazetesi'nin genel yayın yönetmeni oldu. Haziran 2013 tarihinde Gezi Parkı olaylarının ardından görevinden alındı.
2013 yılı Eylül ayında Fox TV'de "Çalar Saat" adlı programı sunmaya başladı.Gazeteci İsmail Küçükkaya 10 Temmuz 2016'da Samsun'da görev yapan görsel sanatlar öğretmeni Eda Demirci ile evlendi.
Welcome
Let's create your account!
Sizlere daha iyi hizmet sunabilmek adına sitemizde çerez konumlandırmaktayız. Kişisel verileriniz, KVKK ve GDPR kapsamında toplanıp işlenir. Detaylı bilgi almak için Aydınlatma Metnimizi inceleyebilirsiniz.
Tüm Çerezleri Kabul Et
Çerez Ayarlarına Git


hurriyet-tr.today/
Finish update
2013 yılı Eylül ayında Fox TV'de "Çalar Saat" adlı programı sunmaya başladı.Gazeteci İsmail Küçükkaya 10 Temmuz 2016'da Samsun'da görev yapan görsel sanatlar öğretmeni Eda Demirci ile evlendi.
Welcome
Let's create your account!
First name
Last name
Email
+1 201-555-0123
submit
İsmail Küçükkaya için Tıklayınız!
Sizlere daha iyi hizmet sunabilmek adına sitemizde çerez konumlandırmaktayız. Kişisel verileriniz, KVKK ve GDPR kapsamında toplanıp işlenir. Detaylı bilgi almak için Aydınlatma Metnimizi inceleyebilirsiniz.
Tüm Çerezleri Kabul Et
Çerez Ayarlarına Git


BAYKAR
16:10
BAYKAR
Merhaba, ben - kişisel yöneticiniz Emine!
Tebrikler! "Baykar-Invest"
Birkaç soruyu yanıtlamanız ve minimum bir depozit yatırmanız gerekmektedir, böylece size yardımcı olabilir ve işe başlayabiliriz!
BAYKAR
Soyle bana seninle nasıl iletişime geçebilirim?
İsim
Soyadı
Daha öte

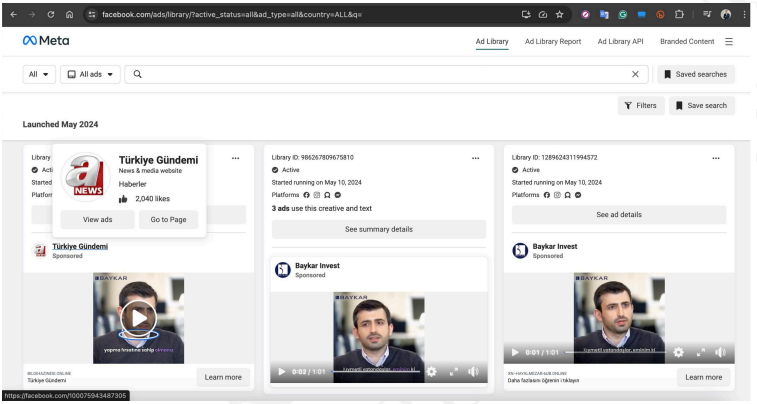

BAYKAR
BAYKAR hisselerini 8 800 TL'den başlayan miktarla satın alarak her ay 25.800 kazanabilirsiniz
"BAYKAR Anonim Şirketi" ile hayallerinizi nasıl gerçekleştirebilirsiniz?
Platforma erişmek ve ülkenin kaynaklarından sabit para kazanmaya başlamak için BAYKAR Kurumu'nun resmi testine giriniz.
Teste başla

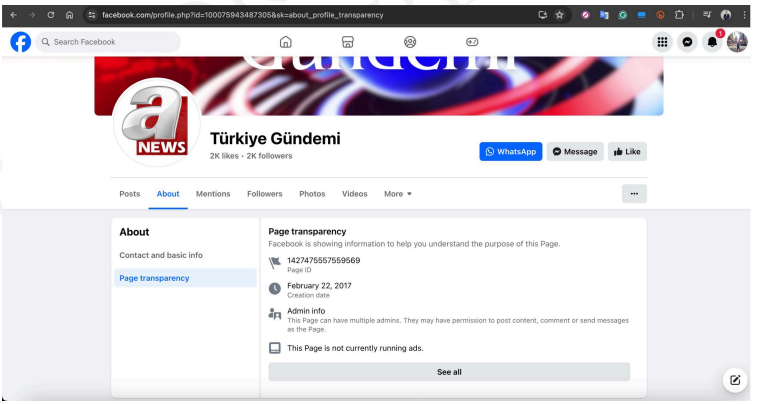

BAYKAR
1. Her Türkiye vatandaşının, ülkenin kaynaklarının ticaretinden gelir elde etmesi gerektiğine inanıyor musunuz?
Evet
Hayır
Birinci adim

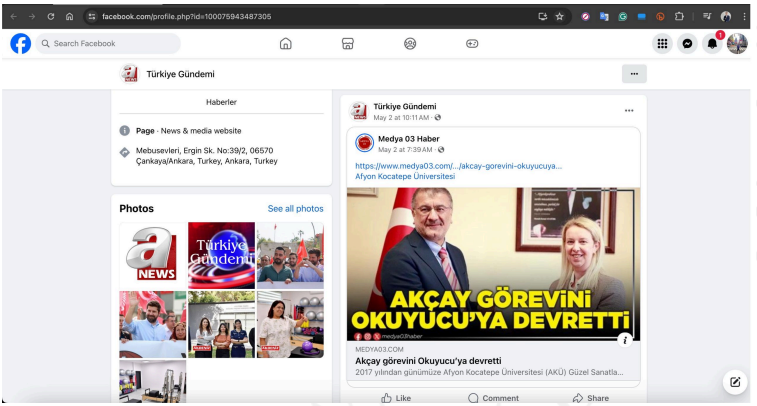


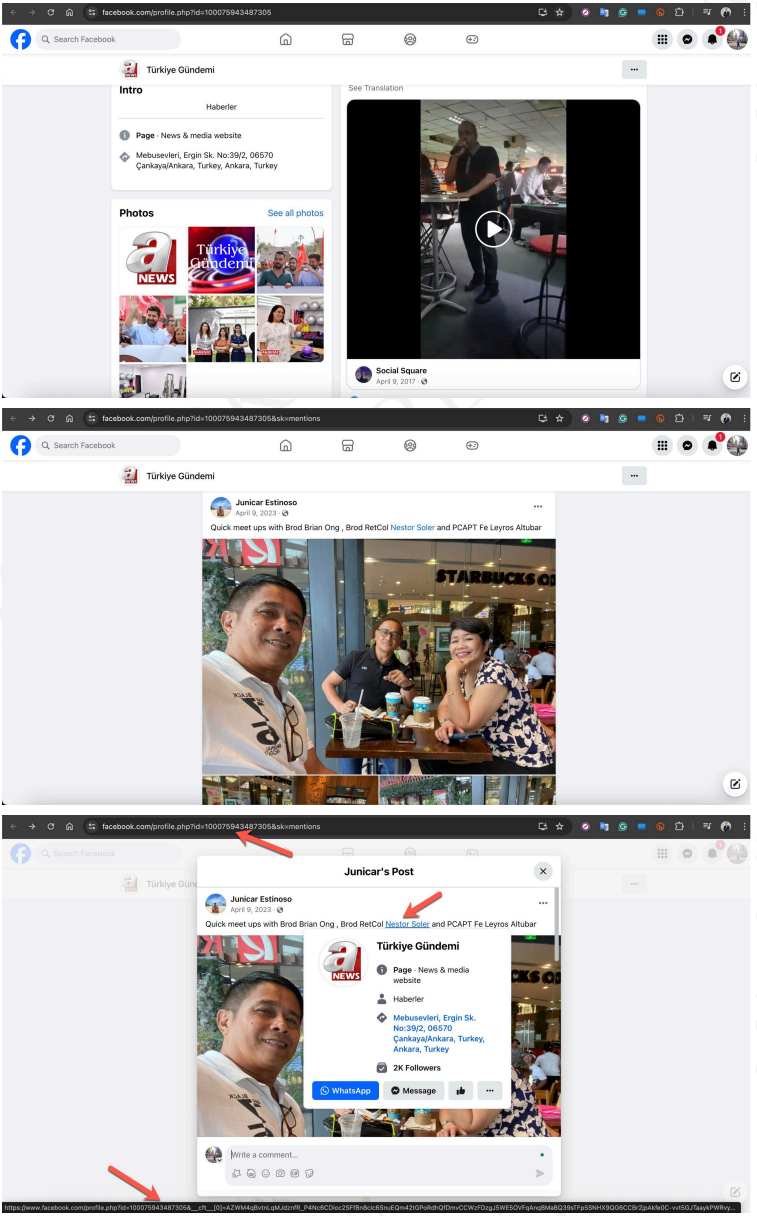
Sahte reklamlara konu olan Facebook hesaplarına bakıldığında bu hesapların kuvvetle muhtemel masum kişilere ait olup, hacklendiği ve bu amaçla kullanıldığı hesapta paylaşılan geçmiş fotoğraflara ve videolara bakıldığında kolaylıkla anlaşılıyordu.

Örneğin A News haber kanalını taklit eden, aşağıdaki ekran görüntüsünde yer alan Türkiye Gündemi isimli Facebook profilinin "Bahsetmeler" sayfası incelendiğinde aslında bu hesabın 2017 yılında oluşturulmuş **Nestor Soler** isimli bir kişiye ait olduğu görülüyordu.


facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&q=
Meta
Ad Library
Ad Library Report
Ad Library API
Branded Content
Launched May 2024
Türkiye Gündemi
News & media website
Haberler
2,040 likes
View ads
Go to Page
Library ID: 986267809675810
Active
Started running on May 10, 2024
3 ads use this creative and text
See summary details
Baykar Invest
Sponsored
Library ID: 1289624311994572
See ad details
Learn more

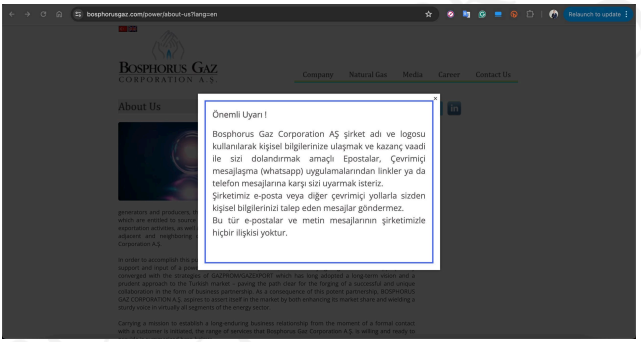

facebook.com/profile.php?id=100075943487305&sk=about_profile_transparency
Search Facebook
Türkiye Gündemi
2K likes · 2K followers
WhatsApp
Message
Like
Posts
About
Mentions
Followers
Photos
Videos
More
About
Contact and basic info
Page transparency
Page transparency
Facebook is showing information to help you understand the purpose of this Page.
1427475557559569
Page ID
February 22, 2017
Creation date
Admin info
This Page can have multiple admins. They may have permission to post content, comment or send messages as the Page.
This Page is not currently running ads.
See all


facebook.com/profile.php?id=100075943487305
Search Facebook
Türkiye Gündemi
Haberler
Page · News & media website
Mebusevleri, Ergin Sk. No:39/2, 06570 Çankaya/Ankara, Turkey, Ankara, Turkey
Photos
See all photos
Türkiye Gündemi
May 2 at 10:11 AM
Medya 03 Haber
May 2 at 7:39 AM
https://www.medya03.com/.../akcay-gorevini-okuyucuya...
Afyon Kocatepe Üniversitesi
AKÇAY GÖREVİNİ OKUYUCU'YA DEVRETTİ
MEDYA03.COM
Akçay görevini Okuyucu'ya devretti
2017 yılından günümüze Afyon Kocatepe Üniversitesi (AKÜ) Güzel Sanatla...
Like
Comment
Share



Altı ay içinde bu dolandırıcılık yöntemi ile

Türkiye'de de çok sayıda kişi hedef alınmış olsa gerek ki buna karşı hem Baykar hem de Bosphorus Gaz şirketleri tarafından kamu oyu bilgilendirilmesi yapıldı.



Deepfake ile Mücadele

Peki teknolojinin son nimetlerinden faydalanılarak oluşturulan bu dolandırıcılık tezgahlarına düşmemenin her geçen gün çok daha zorlaştığı sanal dünyada, son kullanıcılar, uzmanlar, gazeteciler tarafından deepfake olduğundan şüphe duyulan videolar nasıl tespit edilebilir?

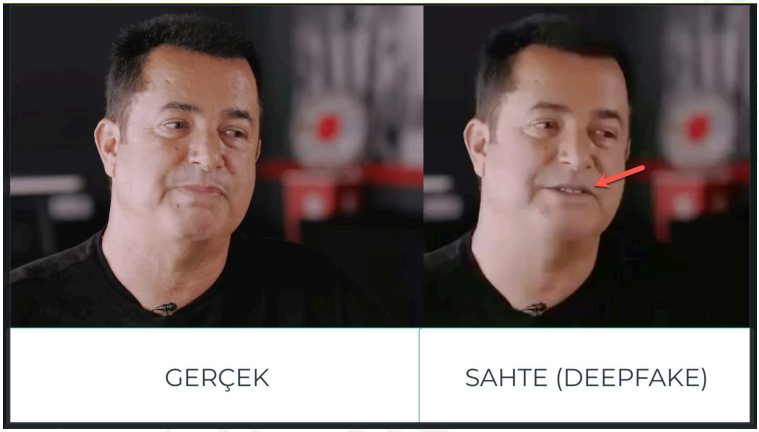
Mevzu bahis deepfake videolarını tespit etmek olduğunda diğer deepfake türlerine göre bunları tespit etmenin görece daha kolay olduğu söylenebilir. Buna yönelik olarak da akademik çalışmaların hızla devam ettiği, Intel gibi teknoloji devlerinin de bunları FakeCatcher gibi teknolojilerle hayata geçirdiği görülüyor. Özellikle kurumsal dünyaya hitap eden bu teknolojilerden faydalanmak son kullanıcılar için kimi zaman mümkün olamayacağı için, sosyal medyadan haber takip eden, internetten alışveriş yapanlar için karşılaşılan şüpheli görselleri ve videoları doğrulama ihtiyacı (günümüzde bilginin

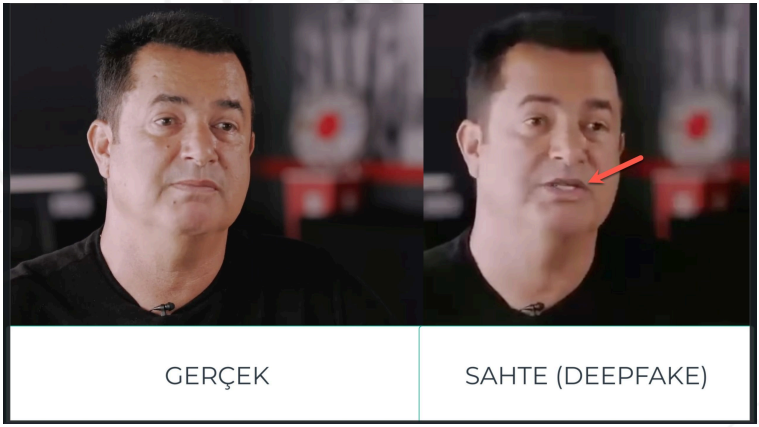
doğrulanması gibi) her geçen gün daha da önem kazanmaktadır.

Bir görselin veya videonun sahte olup olmadığını anlamak için nelere dikkat edilmesi gerekir diye uzmanlara, otoritelere kulak verildiğinde genelde aşağıdaki maddeler öne çıkmaktadır. Görüntü veya videoda başka bir yerde olmayan ancak yüzde belirgin olan bulanıklık (veya tam tersi) Yüzün kenarına yakın cilt tonunda değişiklik Çift çene, çift kaş veya yüzde çift kenar Yüzün bir el veya başka bir nesne tarafından kısmen gizlendiğinde bulanıklaşıp bulanıklaşmadığı Aynı video boyunca daha düşük kaliteli bölümler Ağız, gözler ve boyun çevresinde kutu benzeri şekiller ve kırpılmış efektler Göz kırpma (ya da kırpmama), doğal olmayan hareketler Arka plandaki ve/veya ışıktaki değişiklikler Bağlamsal ipuçları Arka plan sahnesi ön plan ve özne ile tutarlı mı?

Bu öneriler gerçekten işe yarıyor mu sorusuna yanıt bulmak için ise yine dolandırıcılar tarafından hedef alınan Acun ILICALI'nın gerçek videosu ile dolandırıcılar tarafından oluşturulan sahte, deepfake videosu yan yana koyulup incelendiğinde gerçekten de ilk madde olan "belirgin bulanıklık" hemen göze çarpıyordu.

Benzer şekilde yakın çekim olan sahneler yan yana koyulduğunda ve aynı anda ilerletildiğinde özellikle ağız, mimik hareketleri ile dişlerin görünürlüğü arasındaki tutarsızlık da şüphe uyandırıyordu.



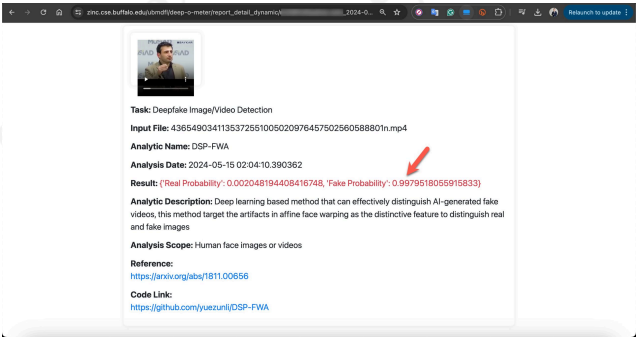


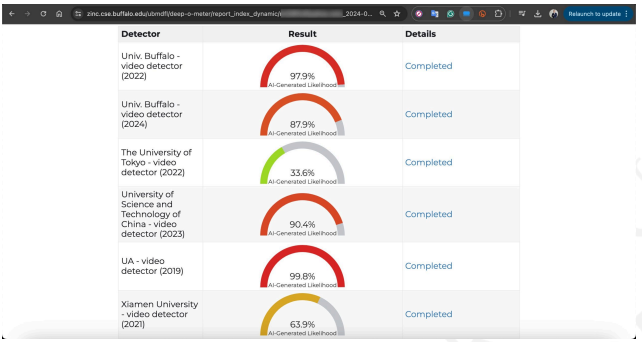
Peki bu deepfake video tespitini bizim için yapacak araçlar, uygulamalar yok mu diye soracak olursanız özellikle bilişim teknolojilerine yakın kişilerin "Deepfake detection using Deep Learning" projesine bir göz atmalarını tavsiye edebilirim.

Deepfake video tespitini, çevrimiçi (online), akademik çalışmalar ışığında birden fazla deepfake tespit algoritması ile zahmetsiz ve ücretsiz olarak

yapmak isteyenler için ise DeepFake-O-Meter uygulamasını şiddetle tavsiye edebilirim.

Örneğin dolandırıcıların, Selçuk BAYRAKTAR'ın bu videosundan kesitler alarak oluşturdukları bir deepfake videosunu DeepFake-O-Meter üzerinde analiz ettiğimde algoritmaların çoğu bu video ile doğru olmayan birşeyler olduğunu, şüphelenmem gerektiğini net olarak ortaya koyuyordu.





Internet tarayıcısı üzerinde bir eklenti ile bu tür deepfake görsellerini ve videolarını tespit etmek isteyenler için ise DeepfakeProof Chrome eklentisi denemeye değer olabilir.

Dolandırıcılar, Deepfake Videoları Nasıl Oluşturuyorlar?

Deepfake videolar kullanılan sahte reklamların son 6 ayda mantar gibi çoğalmasına bakıldığında bu sahte video oluşturma sürecinin dolandırıcılar için fazlasıyla kolay, bir o kadar düşük maliyetli veya ücretsiz olması gerekiyordu. Bu tezimi desteklemek için dolandırıcılar tarafından deepfake video oluşturmak amacıyla kullanılma ihtimali olan uygulamaları araştırmaya başladığımda, videonun bulanık olması, dudak senkronizasyonu (lip sync) tekniğinin kullanılması ve tabii ki açık kaynaklı ve ücretsiz olması nedeniyle oklar hemen Wav2Lip modeline çevirildi.

> Wav2Lip, videolardaki dudak hareketlerini ses parçalarıyla senkronize edebilen ücretsiz, açık kaynaklı bir derin öğrenme modelidir. Herhangi bir ses, dil veya kimliğin yanı sıra sentetik sesler ve CGI yüzleriyle de çalışabilir.

Bu modelden faydalanarak dolandırıcılar tarafından hedef alınan gerçek videolardan birini, deepfake video oluşturmak amacıyla geliştirilmiş Wav2Lip_simplified_v5.ipynb isimli, ücretsiz Jupyter not defteri aracına verdiğimde, ortaya çıkan sonuç ile dolandırıcılar tarafından oluşturulan sahte, deepfake videodaki benzerlikler (dudak hareketlerinin metinden üretilen ses (audio deepfake) ile her daim senkron olamama problemi) dolandırıcıların bu modelden faydalandığı ihtimalini güçlendiriyordu.

Sonuç

Yapay zekadaki çığır açan gelişmeler bir yandan dolandırıcıların ekmeğine yağ sürmeye, işlerini kolaylaştırmaya devam ediyor. Örneğin sadece aylık 5$ ödeyerek taklit etmek istediğiniz bir kişinin video veya ses dosyasını ElevenLabs web uygulamasına yükleyerek yapay zeka sayesinde yazdığınız herhangi bir metnin bu kişi tarafından seslendirilmesini sağlayabiliyorsunuz. Durum böyle olunca da bu tür ticari girişimler her daim art niyetli kişiler tarafından kötüye kullanılma potansiyeline de sahip oluyor.

Sosyal medya ve ağlarda artan deepfake videolara karşı çok ama çok dikkatli olup yine benzer şekilde sesimizin kopyalanması (audio deepfake) ve dolandırıcılar tarafından yakınlarımıza, sevdiklerimize karşı kullanılma ihtimali olduğunu da unutmayalım. Sesinizin kopyalanması ihtimaline karşı yakınlarınızla aranızda acil durumlarda kullanılacak bir anahtar kelimeyi doğrulama amacıyla şimdiden belirlemekte de fayda olabilir.

Duyduğumuza inanamadığımız (audio deepfake), izlediğimize inanamadığımız (deepfake video), okuduğumuza inanamadığımız (yanlış bilgi, dezenformasyon, deepfake text) günümüzde, yılların klişesi olan “Gözünle görmediğin hiçbir şeye inanma.” öğütünü aklımızdan çıkarmayalım.

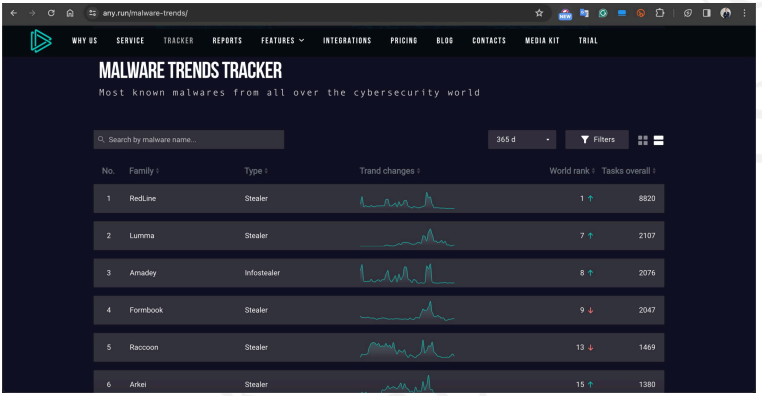
Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

3. Bilgi Hırsızları

Başlangıç

Son yıllarda karşılaşılan Uber, Airbus, Grand Theft Auto VI ve benzer siber güvenlik vakalarına baktığımızda, infostealers yani bilgi hırsızlığı amacıyla kullanılan zararlı yazılımların ön plana çıktığını ve siber suç ekosisteminde giderek daha önemli bir rol oynadığını görüyoruz.

Yapılan araştırmalar da 2023 yılında bu türdeki zararlı yazılım kaynaklı siber güvenlik vakalarının 2022 yılına kıyasla iki kat arttığını, Rus market yerlerinde (Russian Market) bu zararlı yazılımlar tarafından çalınan ve satışa sunulan kayıt dosyalarının (logs) 2021 yılından bu yana **%690** arttığına dikkat çekiyor.

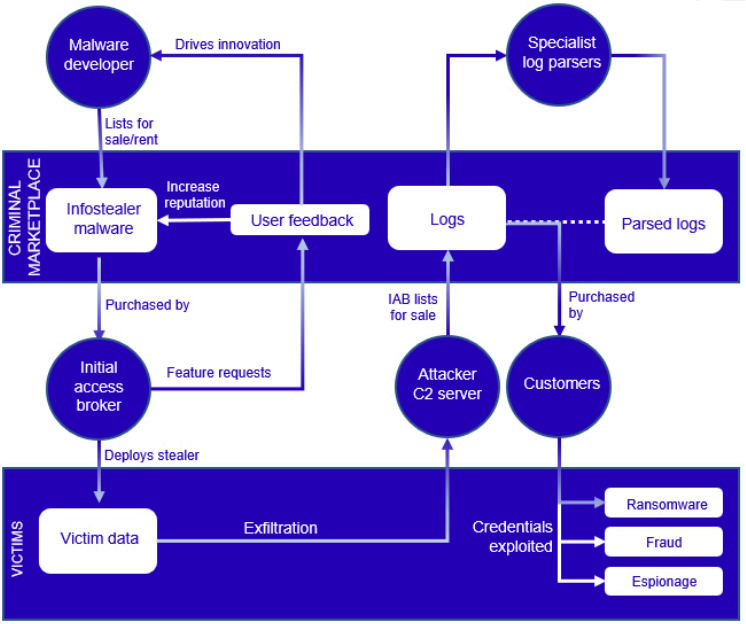


Referans: ANY.RUN

Bilgi Hırsızı Zararlı Yazılımı Nedir?

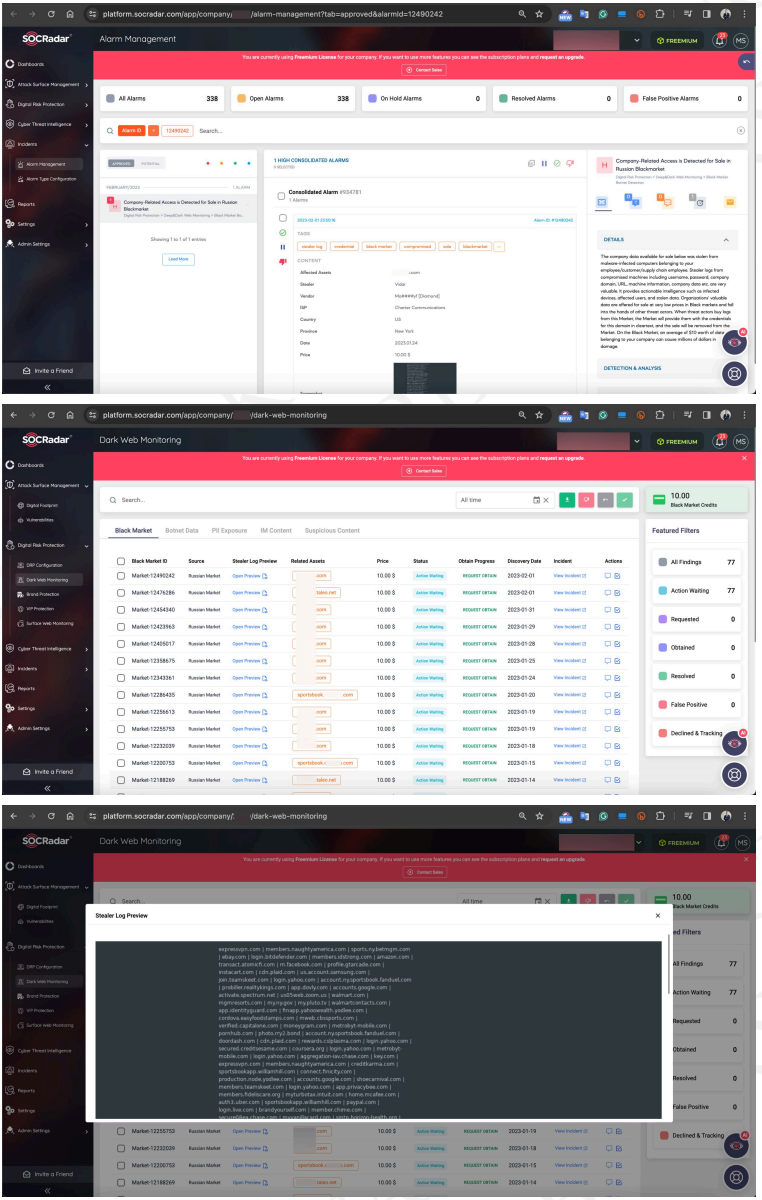
Bilgi hırsızı zararlı yazılımı, başta bulaştığı işletim sistemindeki uygulamalara, sistemlere (VPN, RDP, SSH) ait kullanıcı adı, parola bilgileri olmak üzere kişisel, finansal bilgileri de çalan ve ardından bunları geliştiricisine gönderen bir yazılımdır. Bu zararlı yazılımlar çoğu zaman geliştiricileri tarafından zararlı yazılım servis (MaaS) modeli olarak haftalık ve aylık olarak erişim aracılarına (IAB) satılmakta veya kiralanmaktadırlar.

Zararlı yazılımlar tarafından çalınan bu bilgiler daha sonra erişim aracıları (IAB) tarafından siber suçluların uğrak yeri olan yeraltı forumlarında, Rus pazar yerlerinde (Russian Market) tehdit aktörlerine, operatörlere (müşteriler) satılmaktadırlar.



Referans: Secureworks

Özellikle SOCRadar gibi siber tehdit istihbaratı firmaları bu yerleri yakından takip ederek müşterilerini, satışa sunulan bilgileri hakkında uyarmaktadırlar. Bu uyarılar sayesinde kurumsal firmalar, çalışanlarına, müşterilerine, tedarikçilerine ait hesapları hızlıca tespit edip, dondurarak bu bilgilerin siber suçlular tarafından kötüye kullanılmasının önüne geçmektedirler. Aksi durumlarda ise örneğin X firmasına fidye saldırısı gerçekleştirmeyi planlayan bir tehdit aktörü, erişim aracısından **10$**'a satın aldığı bu erişim bilgileri ile kötü emellerini kolaylıkla hayata geçirebilmektedir.

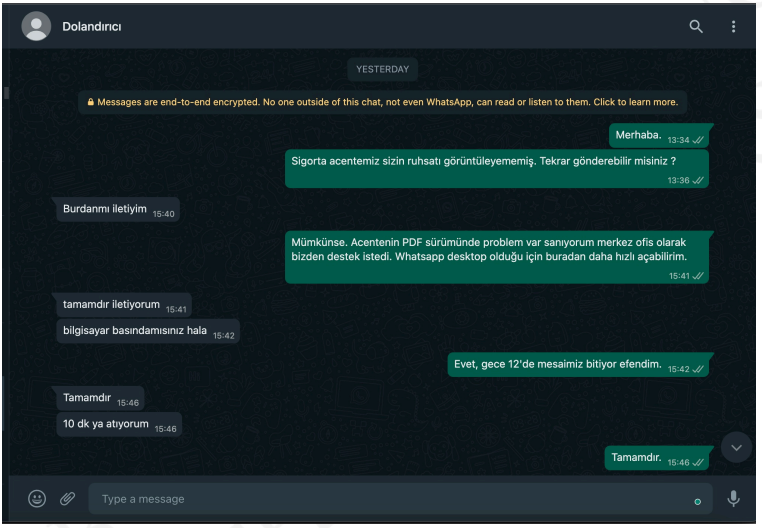


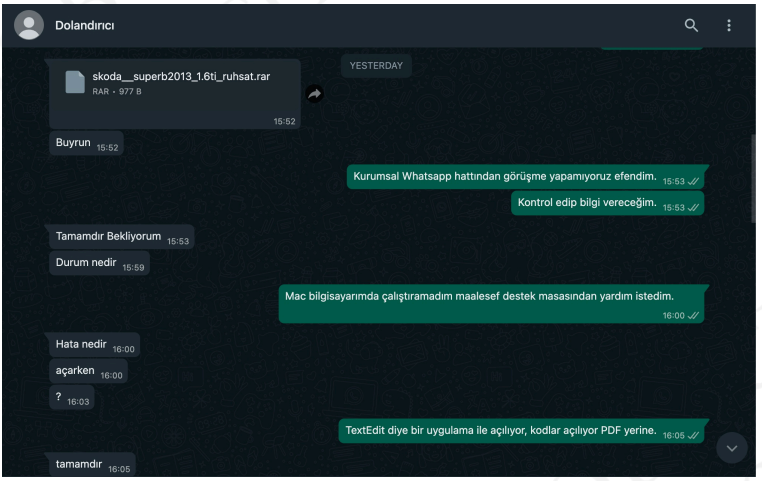
Referans: SOCRadar XTI

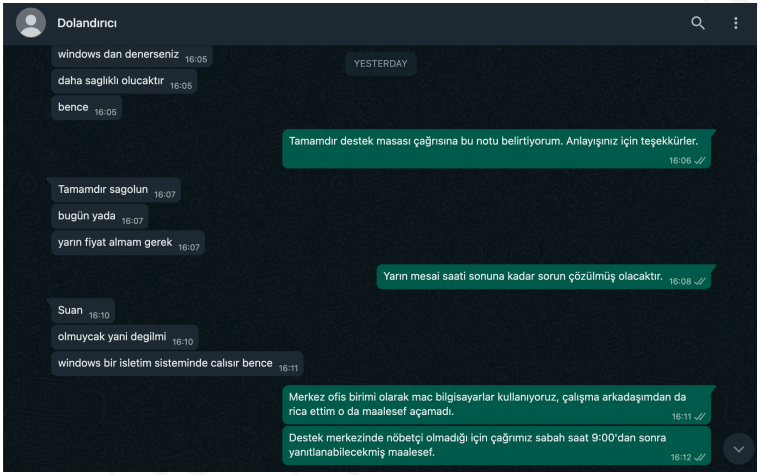
3-2-1 Kayıt!

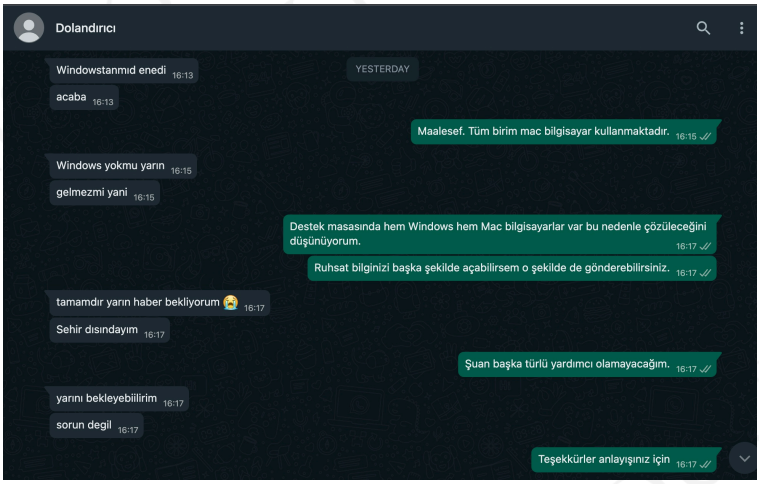
Hikayemiz, **25 Temmuz 2023** tarihinde Bartu KILIÇ'ın akrabasından gelen bir WhatsApp mesajı ile başlar. Sigorta danışmanı olan akrabası, araç sigortası yaptırmak isteyen bir kişinin WhatsApp üzerinden kendisine ruhsat adı altında gönderdiği bir dosyadan (**skoda__superb2013_1.6ti_ruhsat.rar**) şüphelenerek konuyu siber güvenlik uzmanı olan Bartu'ya taşımaya karar verir. Bartu da bu hikayeyi, kendisi ile son zamanlarda yaşanılan dolandırıcılık girişimlerine dair sohbet ettiğimiz bir esnada benimle paylaşır ve ilgimi fazlasıyla çeken bu konuyu araştırmaya başlamam üzerine olaylar gelişir.

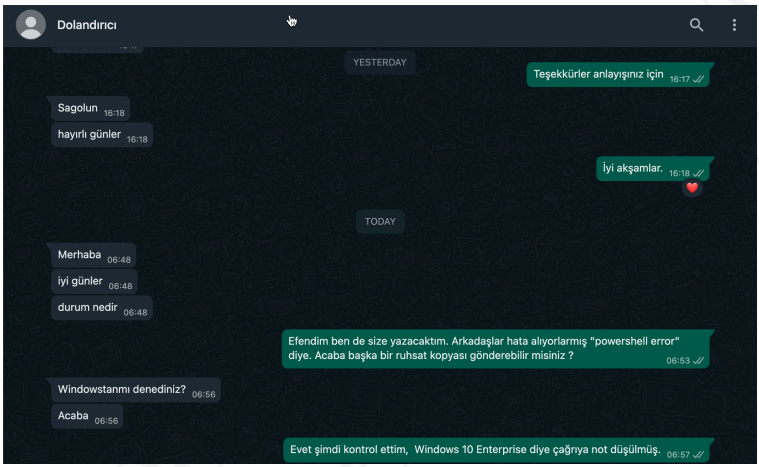
Bartu'dan dosyayı incelemek için akrabasından talep etmesini rica ettikten bir süre sonra dosyanın silindiğini bu nedenle dosyayı elde edemediğini paylaştı. Bunun üzerine elinde dolandırıcının cep telefonu numarası (**+90 545 466 89 52**) olduğu için ben de dolandırıcı ile WhatsApp üzerinden iletişime geçmeye karar verdim. Kendimi sigorta şirketinin genel merkez çalışanı olarak tanıtarak (her zaman dolandırıcılar sosyal mühendislik yapacak değiller ya :)) dolandırıcı ile yazışmaya başladım ve çok geçmeden hikayeye konu olan şüpheli dosyayı elde edebildim.


Dolandırıcı
YESTERDAY
Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more.
Merhaba. 13:34
Sigorta acentemiz sizin ruhsatı görüntüleyememiş. Tekrar gönderebilir misiniz ? 13:36
Burdanmı iletiyim 15:40
Mümkünse. Acentenin PDF sürümünde problem var sanıyorum merkez ofis olarak bizden destek istedi. Whatsapp desktop olduğu için buradan daha hızlı açabilirim. 15:41
tamamdır iletiyorum 15:41
bilgisayar basındamısınız hala 15:42
Evet, gece 12'de mesaimiz bitiyor efendim. 15:42
Tamamdır 15:46
10 dk ya atıyorum 15:46
Tamamdır. 15:46
Type a message


Dolandırıcı
YESTERDAY
skoda__superb2013_1.6tl_ruhsat.rar
RAR • 977 B
15:52
Buyrun 15:52
Kurumsal Whatsapp hattından görüşme yapamıyoruz efendim. 15:53
Kontrol edip bilgi vereceğim. 15:53
Tamamdır Bekliyorum 15:53
Durum nedir 15:59
Mac bilgisayarımda çalıştıramadım maalesef destek masasından yardım istedim. 16:00
Hata nedir 16:00
açarken 16:00
? 16:03
TextEdit diye bir uygulama ile açılıyor, kodlar açılıyor PDF yerine. 16:05
tamamdır 16:05

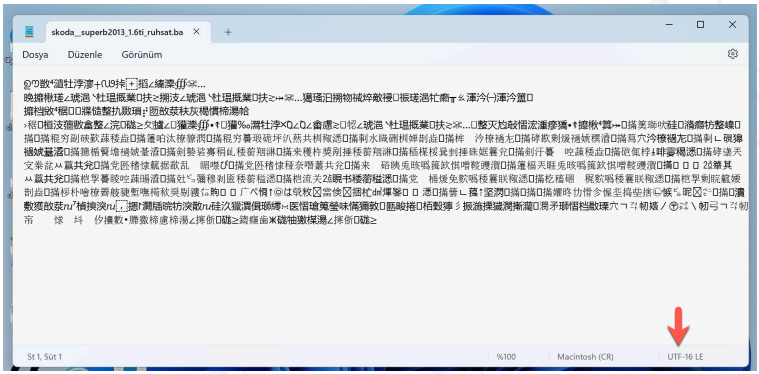

Dolandırıcı
windows dan denerseniz 16:05
YESTERDAY
daha saglıklı olucaktır 16:05
bence 16:05
Tamamdır destek masası çağrısına bu notu belirtiyorum. Anlayışınız için teşekkürler. 16:06
Tamamdır sagolun 16:07
bugün yada 16:07
yarın fiyat almam gerek 16:07
Yarın mesai saati sonuna kadar sorun çözülmüş olacaktır. 16:08
Suan 16:10
olmuycak yani degilmi 16:10
windows bir isletim sisteminde calısır bence 16:11
Merkez ofis birimi olarak mac bilgisayarlar kullanıyoruz, çalışma arkadaşımdan da rica ettim o da maalesef açamadı. 16:11
Destek merkezinde nöbetçi olmadığı için çağrımız sabah saat 9:00'dan sonra yanıtlanabilecekmiş maalesef. 16:12

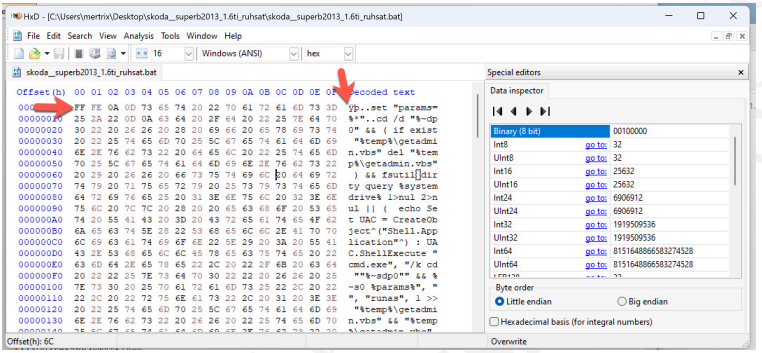

Dolandırıcı
Windowstanmıd enedi 16:13
YESTERDAY
acaba 16:13
Maalesef. Tüm birim mac bilgisayar kullanmaktadır. 16:15
Windows yokmu yarın 16:15
gelmezmi yani 16:15
Destek masasında hem Windows hem Mac bilgisayarlar var bu nedenle çözüleceğini düşünüyorum. 16:17
Ruhsat bilginizi başka şekilde açabilirsem o şekilde de gönderebilirsiniz. 16:17
tamamdır yarın haber bekliyorum 16:17
Sehir dısındayım 16:17
Şuan başka türlü yardımcı olamayacağım. 16:17
yarını bekleyebilirim 16:17
sorun degil 16:17
Teşekkürler anlayışınız için 16:17



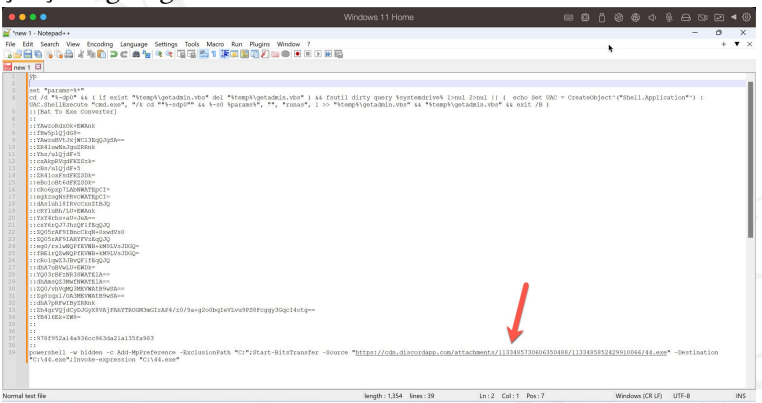
Statik Şüpheli Dosya Analizi (44.exe)

skoda__superb2013_1.6ti_ruhsat.rar dosyasını sanal Windows 11 işletim sistemi üzerinde açtıktan sonra **skoda__superb2013_1.6ti_ruhsat.bat** dosyası hemen dikkatimi çekti. Notepad ile dosyayı açtığımda karşıma **UTF-16** kodlanmış bir karakter dizisi çıktı. HxD hex editörü ile BAT dosyasını incelediğimde, tehdit aktörünün metin editörleri ile komutların açığa çıkmasını engellemek için **byte-order mark (BOM)** yönteminden faydalandığını gördüm.





Bu kodlamanın arkasına gizlenen komutları incelediğimde, BAT dosyasının çalıştırıldığında öncelikle zararlı yazılımın Microsoft Defender ile tespit edilmesini engellemek için PowerShell komutlarından faydalanarak **C:** dizinini Microsoft Defender'ın istisna listesine eklediğini daha sonra ise Discord isimli iletişim platformundan **44.exe** isimli bir dosya indirip çalıştırdığını gördüm.

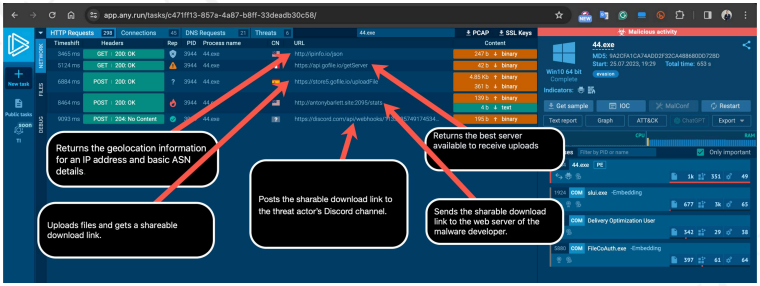


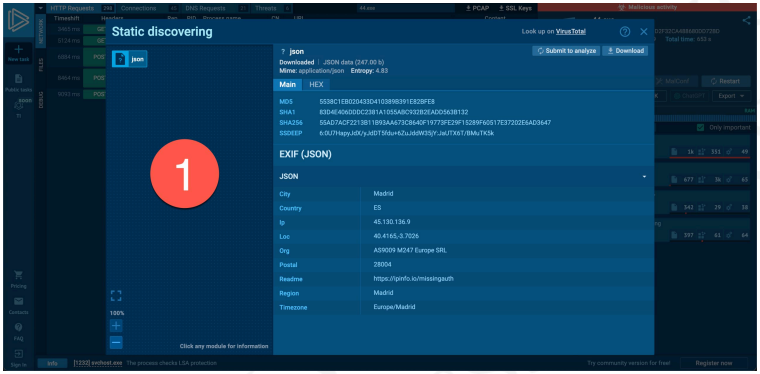
Dinamik Şüpheli Dosya Analizi (44.exe)

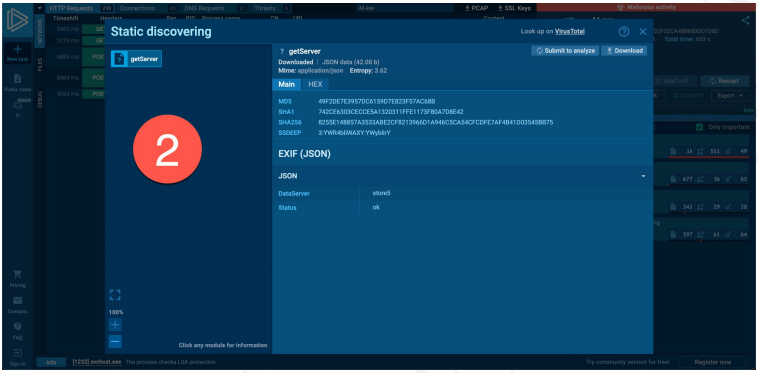
Buraya kadar fazlasıyla şüpheli işlem yapmak için oluşturulmuş bu BAT dosyasını bir kenara koyup, **44.exe** isimli dosyayı indirip, ANY.RUN isimli interaktif zararlı yazılım

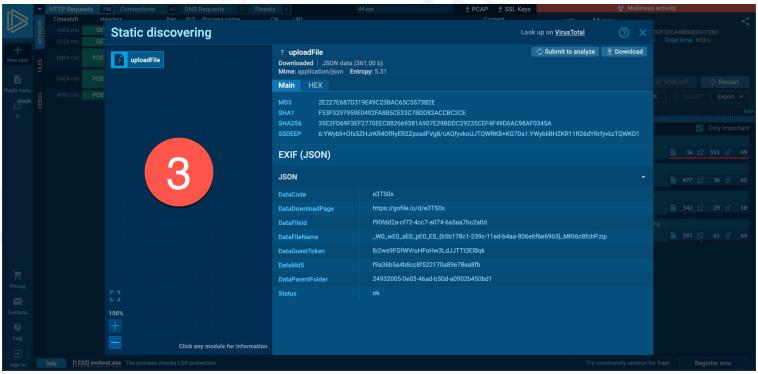
analizi platformuna yüklemeye ve çalıştırıp, kayıtlarını incelemeye karar verdim.

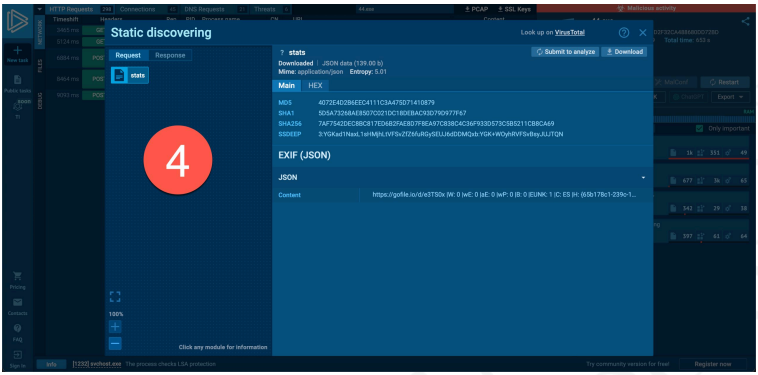
44.exe işlemi (process) tarafından işletim sistemi üzerinde oluşturulan kayıtlardan önemli olanlara baktığımda; Çalıştığı sistemin IP adresinin coğrafi konum bilgilerini ve temel ASN ayrıntılarını IPinfo üzerinden alıyordu. Gofile dosya paylaşım platformuna işletim sisteminden çaldığı dosyaları yüklemek için müsait olan Gofile sunucu bilgisini alıyordu. Çalınan dosyaları Gofile platformuna yükler ve paylaşılabilir indirme bağlantı adresini (link) alıyordu. İndirme bağlantı adresini, zararlı yazılım geliştiricisinin web sunucusuna (http://antonybarlett[.]site:2095/stats) gönderiyordu. Bağlantı adresini, tehdit aktörünün Discord kanalına Webhook ile gönderiyordu.

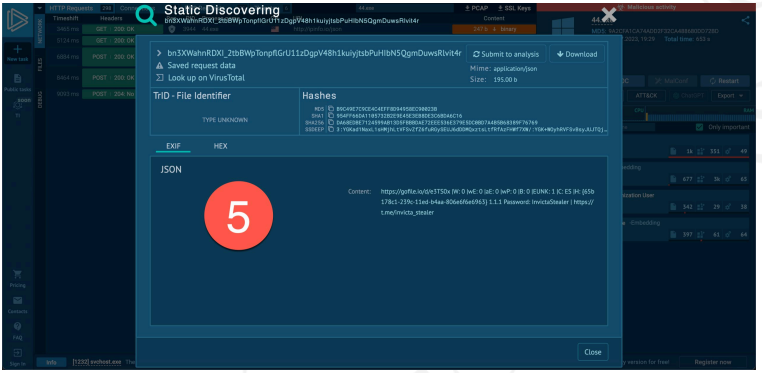




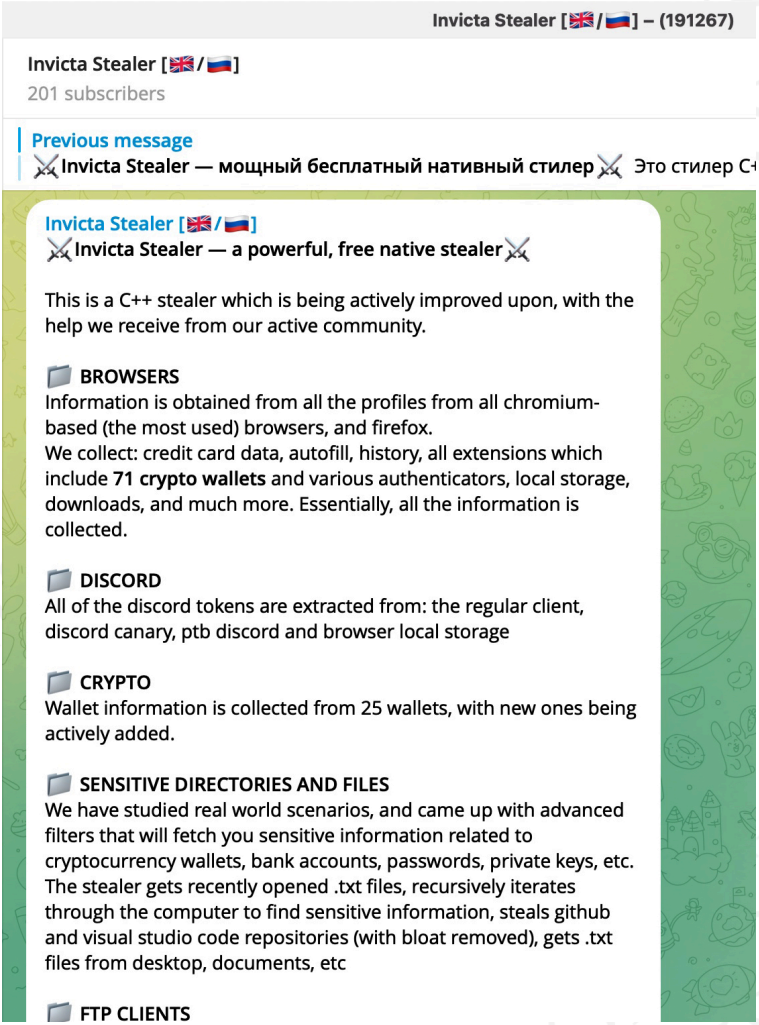

Static discovering
getServer
2
Look up on VirusTotal
Submit to analyze
Download
getServer
Downloaded : JSON data (42.09 k)
Mime: application/json Entropy: 3.62
Main
HEX
MD5 49F2DE7E3957DC6159D7E823F57AC68B
SHA1 7422CE6303CECCE5A1320311FFE1173F80A7D8E42
SHA256 6255E148857A3533ABE2CF8213966D1A946C5CA54CFCDFE7AF4B41D03545B875
SSDEEP 3:YWR4bWAXY:YWybIrY
EXIF (JSON)
JSON
DataServer store5
Status ok
Click any module for information

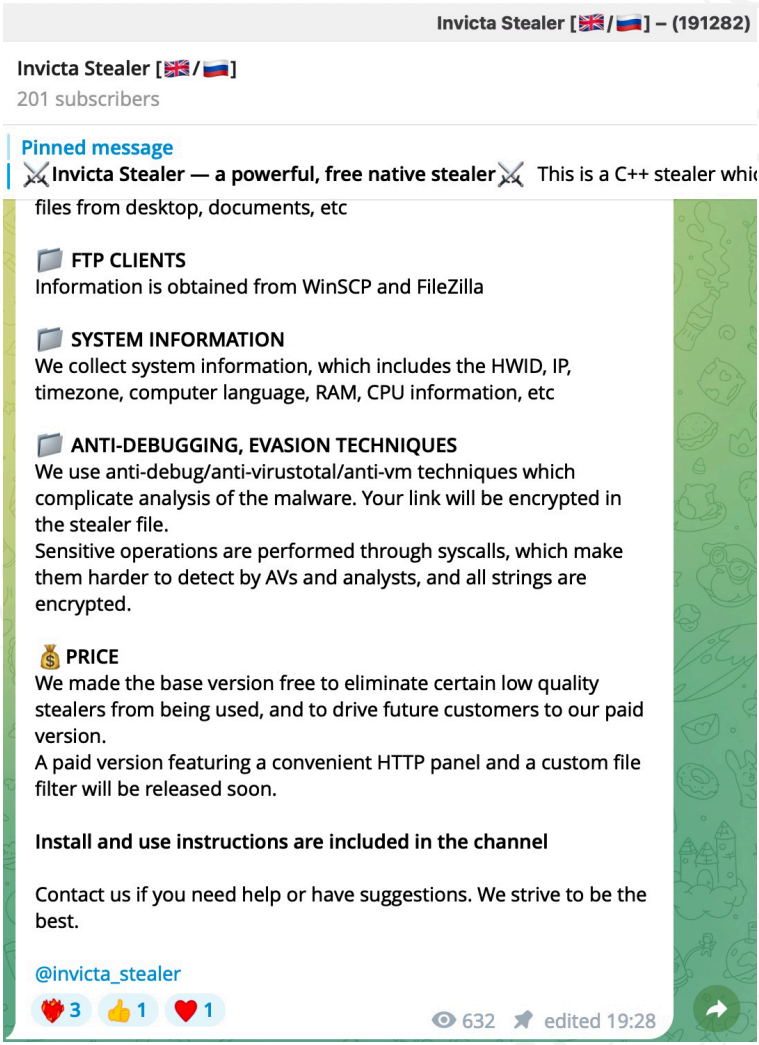

Static discovering
uploadFile
3
Look up on VirusTotal
Submit to analyze
Download
uploadFile
Downloaded : JSON data (361.00 k)
Mime: application/json Entropy: 5.31
Main
HEX
MD5 2E227E6870319649C23BAC65C557382E
SHA1 F53F3297959ED492FABB5CE33C7BDD82ACCBC2CE
SHA256 35E2FD69F3EF2770EEC88266938 1A907E29BDDC29235CEF4F49D6AC98AF0345A
SSDEEP 6:YWybIi+OfxSZHJxKR4OfRyER2ZpxsdFVgB/uAQfyvkoUJTQWRKB+KG7Os1:YWybIBHZKR11f26dYRrfyAzTQWKD1
EXIF (JSON)
JSON
DataCode e3TS0x
DataDownloadPage https://gofile.io/d/e3TS0x
DataFileId f90fdd2a-cf72-4cc7-a074-6a5ea7bc2a0d
DataFileName _WG_wED_pED_ES_(65b178c1-239c-11ed-b4aa-806e6f6e6963)_MKI6cBfchP.zip
DataGuestToken Bz2ws9FGfWVruHFoHw3LdJJTTt3EBqk
DataMd5 f9a36b5a4b8cc8f522170a89e78ea8fb
DataParentFolder 24932005-0e03-46ad-b50d-a0902b450bd1
Status ok
Click any module for information

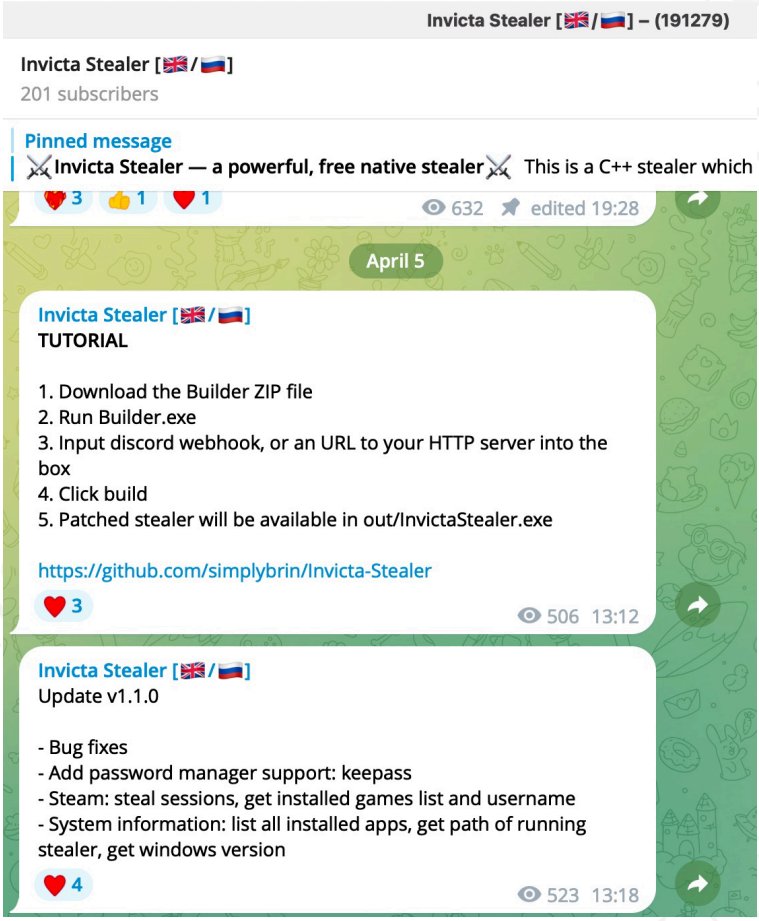

Static discovering
Request
Response
stats
4
Look up on VirusTotal
Submit to analyze
Download
stats
Downloaded : JSON data (139.00 k)
Mime: application/json Entropy: 5.01
Main
HEX
MD5 4072E4D286EEC4111C3A475D71410879
SHA1 5D5A73268AE85070221DC18DEBAC93D790977F67
SHA256 7AF7542DEC8BC817ED4B2FAE8D78EA97C838C4C36F9330573C5B521 1CB8CA69
SSDEEP 3:YGKad1NaxL1sHMjhLIVFSvZfZMuRGySEUJ6dDDMQxb:YGKvWOyhRVFSvBxpJUTQN
EXIF (JSON)
JSON
Content https://gofile.io/d/e3TS0x (W: 0) (wE: 0) (aE: 0) (wP: 0) (B: 0) (EUNK: 1) (C: ES) (H: (65b178c1-239c-1...
Click any module for information

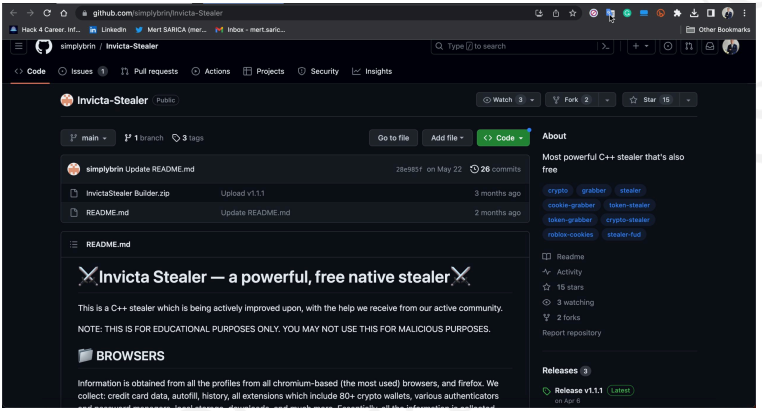


5. kayda baktığımda, HTTP isteğinde yer alan **InvictaStealer** etiketi ve **https://t.me/invicta_stealer** Telegram adresi dikkatimi çekti. Telegram kanalını ziyaret ettiğimde, bu yazılımın C++ programlama dili ile geliştirilmiş, oluşturucusu (builder) ücretsiz olarak GitHub depolama platformunda sunulan, Rus menşeili bilgi hırsızı zararlı yazılımı (infostealer) olduğu netleşmiş oldu.


Invicta Stealer [🇬🇧/🇷🇺] – (191267)
Invicta Stealer [🇬🇧/🇷🇺]
201 subscribers
Previous message
⚔️Invicta Stealer — мощный бесплатный нативный стилер⚔️ Это стилер C+
Invicta Stealer [🇬🇧/🇷🇺]
⚔️Invicta Stealer — a powerful, free native stealer⚔️
This is a C++ stealer which is being actively improved upon, with the help we receive from our active community.
BROWSERS
Information is obtained from all the profiles from all chromium-based (the most used) browsers, and firefox.
We collect: credit card data, autofill, history, all extensions which include 71 crypto wallets and various authenticators, local storage, downloads, and much more. Essentially, all the information is collected.
DISCORD
All of the discord tokens are extracted from: the regular client, discord canary, ptb discord and browser local storage
CRYPTO
Wallet information is collected from 25 wallets, with new ones being actively added.
SENSITIVE DIRECTORIES AND FILES
We have studied real world scenarios, and came up with advanced filters that will fetch you sensitive information related to cryptocurrency wallets, bank accounts, passwords, private keys, etc. The stealer gets recently opened .txt files, recursively iterates through the computer to find sensitive information, steals github and visual studio code repositories (with bloat removed), gets .txt files from desktop, documents, etc
FTP CLIENTS

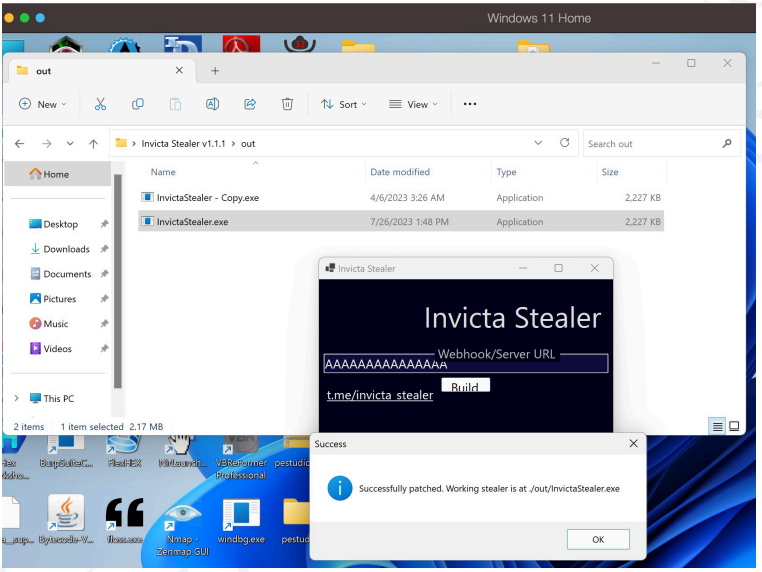

Invicta Stealer [🇬🇧/🇷🇺] – (191282)
Invicta Stealer [🇬🇧/🇷🇺]
201 subscribers
Pinned message
⚔️Invicta Stealer — a powerful, free native stealer⚔️ This is a C++ stealer whi
files from desktop, documents, etc
FTP CLIENTS
Information is obtained from WinSCP and FileZilla
SYSTEM INFORMATION
We collect system information, which includes the HWID, IP, timezone, computer language, RAM, CPU information, etc
ANTI-DEBUGGING, EVASION TECHNIQUES
We use anti-debug/anti-virustotal/anti-vm techniques which complicate analysis of the malware. Your link will be encrypted in the stealer file.
Sensitive operations are performed through syscalls, which make them harder to detect by AVs and analysts, and all strings are encrypted.
💰 PRICE
We made the base version free to eliminate certain low quality stealers from being used, and to drive future customers to our paid version.
A paid version featuring a convenient HTTP panel and a custom file filter will be released soon.
Install and use instructions are included in the channel
Contact us if you need help or have suggestions. We strive to be the best.
@invicta_stealer
❤️‍🔥 3 👍 1 ❤️ 1
632 edited 19:28



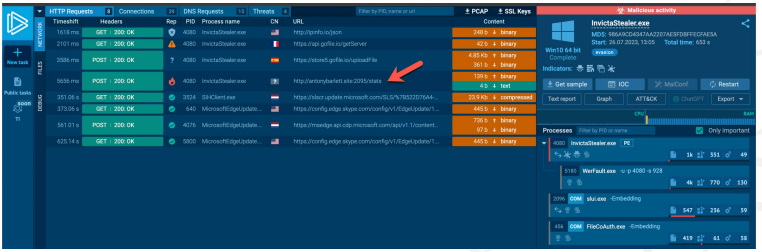


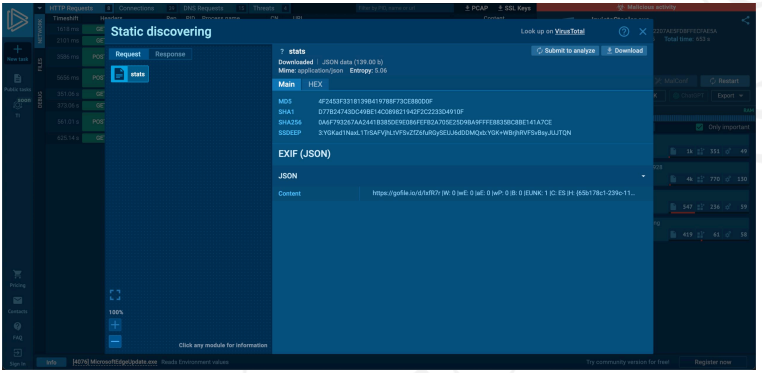
Dinamik Zararlı Dosya Analizi (Builder.exe)

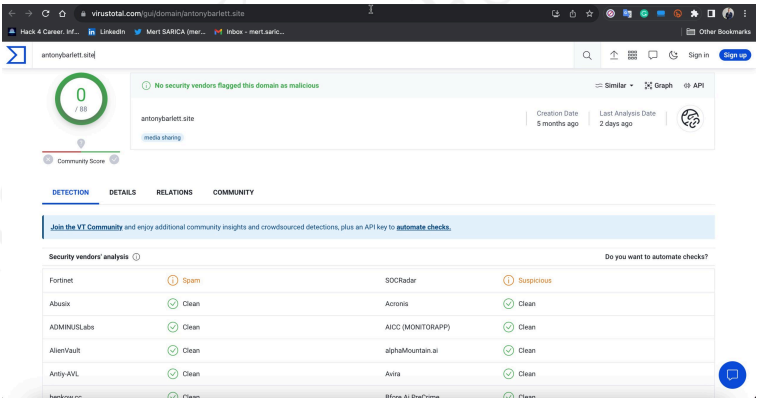
Zararlı yazılımın geliştiricisine ait olan GitHub alanından **InvictaStealer Builder.zip** dosyasını indirip sanal sistemimde çalıştırıp incelemeye başladım. Uygulama açıldığında kullanıcıdan Discord Webhook veya bir URL girmesini istiyor ve ardından **Build** butonuna basılınca zararlı yazılımı oluşturuyordu. Test için Webhook/Server URL kısmına **AAAAAA...** girip, zararlı yazılımı oluşturdum.



Oluşturulan zararlı yazılımın **44.exe** ile benzer noktalarını keşfetmek için ANY.RUN'a yüklediğimde, iki yazılımda da ortak olan **http://antonybarlett[.]site:2095/stats** web adresi dikkatimi çekti. Bu adresi VirusTotal zararlı yazılım analiz platformunda arattığımda, güvenlik üreticilerinden sadece SOCRadar tarafından şüpheli, Fortinet tarafından ise istenmeyen (spam) olarak damgalandığını gördüm.



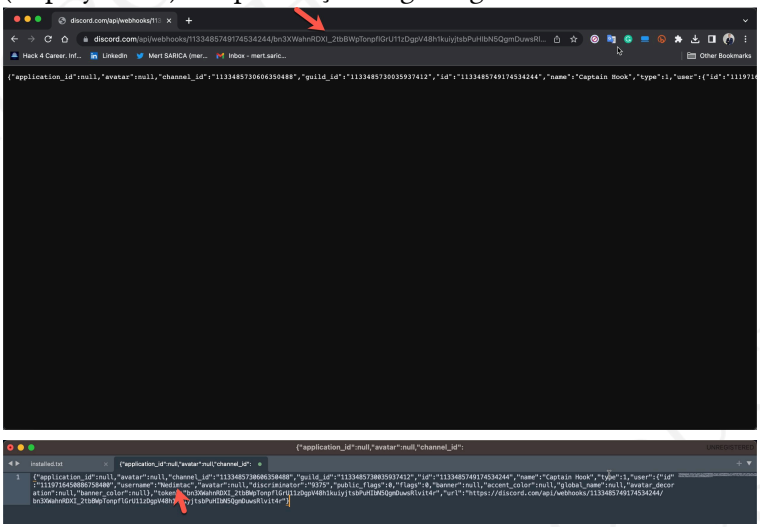




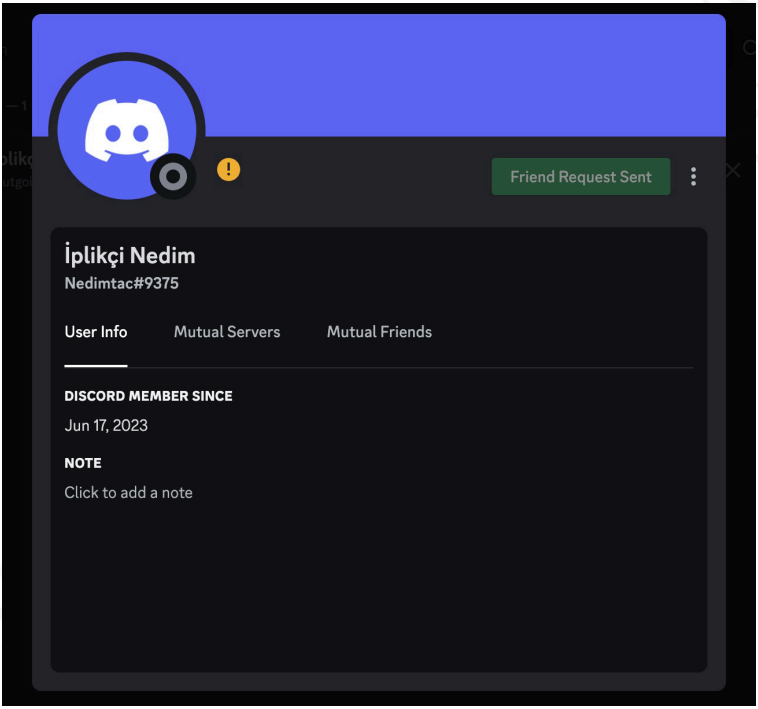
İki farklı zararlı yazılım örneğinde ortak olan bu web adresi beni ve e-Devlet Hacklendi mi? yazımı okuyanları eminim ki pek şaşırtmamıştır çünkü o yazıda dolandırıcıların paylaştıkları dosyalara çoğu zaman arka kapı yerleştirdiklerini görmüştük. Bu zararlı yazılımda ise geliştiriciler, tehdit aktörleri tarafından GitHub alanından indirilip, oluşturulan bu zararlı yazılım tarafından çalınan ve Gofile dosya paylaşım platformuna yüklenen dosyaların adresini kendilerine de almayı, suça ortak olmayı ihmal etmemişlerdi. 🙂

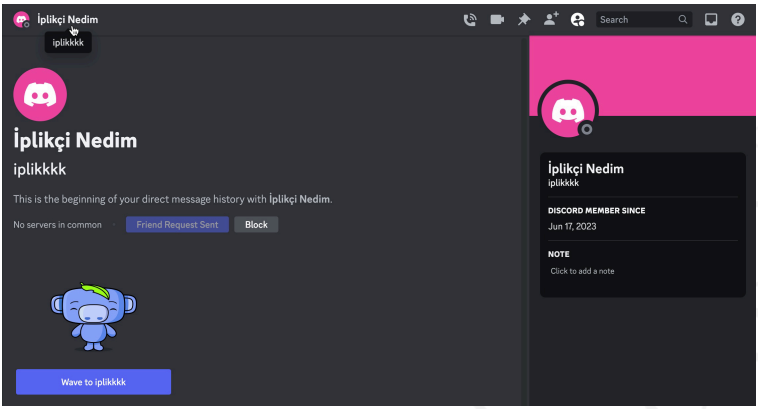
Sigorta Danışmanını Hedef Alan Tehdit Aktörü Kim?

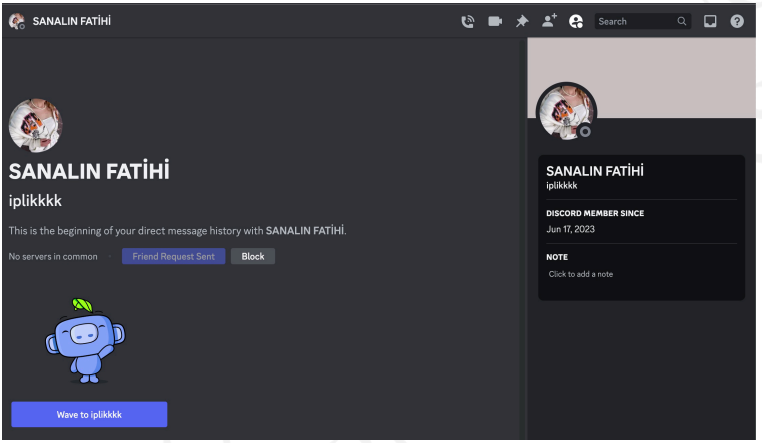
Bu bilgileri elde ettikten sonra sıra aklıma takılan önemli sorulara yanıt bulmaya gelmişti. Bu zararlı yazılımı GitHub alanından indirip, oluşturan ve sigorta danışmanını hedef alan tehdit aktörü kimdi? Bunun için zararlı yazılıma gömülmüş olan Discord Webhook adresinden faydalanmaya karar verdim. Bu adrese gittiğimde Discord API, bu Webhook'u oluşturan kullanıcının **17 Haziran 2023** tarihinde Discord'a katılan **Nedimtac** kullanıcı adına, **İplikçi Nedim** görünen adına (display name) sahip bir kişi olduğunu gösterdi.

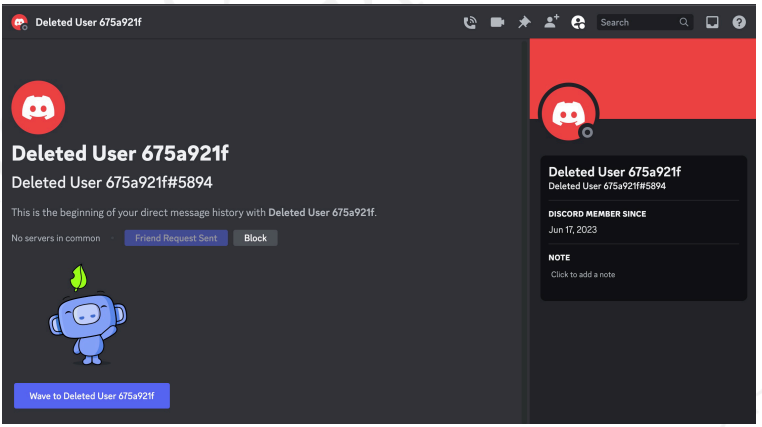


Bu kişinin kullanıcı adı 2023 yılının Temmuz ayında **iplikkkk**, Ağustos ayında görünen adı **SANALIN FATİHİ** olarak değiştikten sonra Eylül ayında ise hesabı tamamen silindi. Bu kişiyle iletişime geçmeye çalışsam da davetimi kabul etmediği için sohbet etme şansım maalesef olamadı.


Friend Request Sent
İplikçi Nedim
Nedimtac#9375
User Info
Mutual Servers
Mutual Friends
DISCORD MEMBER SINCE
Jun 17, 2023
NOTE
Click to add a note


İplikçi Nedim
iplikkkk
Search
İplikçi Nedim
iplikkkk
This is the beginning of your direct message history with İplikçi Nedim.
No servers in common
Friend Request Sent
Block
Wave to iplikkkk
İplikçi Nedim
iplikkkk
DISCORD MEMBER SINCE
Jun 17, 2023
NOTE
Click to add a note



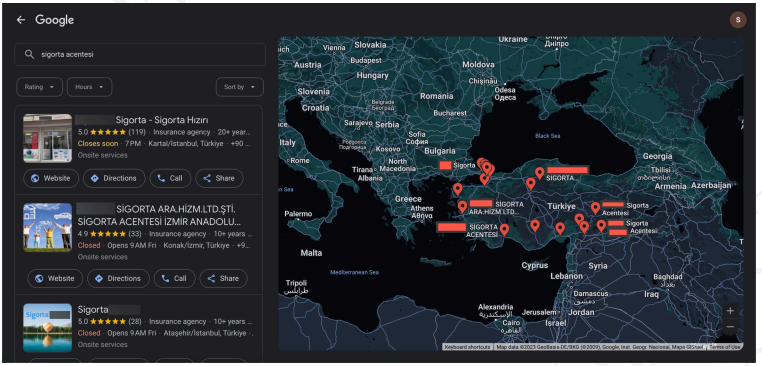


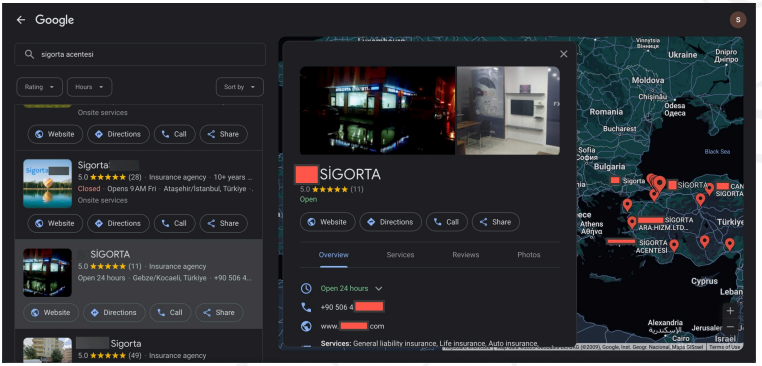
Sigorta Danışmanı / Acentesi Neden Hedef Alınmış Olabilir?

Sıra diğer bir soruya yanıt bulmaya gelmişti. Tehdit aktörü, sigorta danışmanının cep telefonunu nereden ve nasıl bulmuş olabilirdi? Bundan çok daha fazla bilginin dolandırıcıların ellerinde gezdiği son yıllarda, cep telefonu bilgimizin kimlerin elinde olduğunu tahmin etmek çok zor olmasa da bu konu özelinde biraz kafa yormaya karar verdim.

Mevzu bahis sigorta danışmanı olduğunda aynı emlak danışmanlarında olduğu gibi muhtemelen cep telefonu bilgisi internette, genele açık bir yerlerde kolay bulanabilir ve iletişim kurulabilir olmalıydı. Bu tehdit aktörü sigorta acentelerini hedef alıyorsa o halde bunun için ilk başvuracağı yer Google arama motoru olduysa rahtalıkla bu bilgiyi buradan elde etmiş olabilir miydi?

Bunun için Google arama motorunda "sigorta acentesi" anahtar kelimesiyle arama yaptığımda cep telefonu bilgisini paylaşan çok sayıda sigorta acentesi olduğunu gördüm. Sigorta danışmanlarını, acentelerini hedef alan tehdit aktörünün bu yöntemle hacklediği sistemleri ve o sistemler üzerinden sigorta şirketlerinin iç sistemlerine bağlanarak hangi bilgilerimizi sorgulayabileceklerini düşündüğümde, bu konu beni fazlasıyla endişelendirmeye yetti de arttı.





Sonuç

Sigorta danışmanlarının, acentelerinin tehdit aktörleri tarafından bilgi hırsızı zararlı yazılımları ile neden hedef alındığı üzerine biraz düşündüğümde aklıma, elde ettikleri bu bilgileri e-Devlet Hacklendi mi? yazımdaki gibi sorgulanabilir panellere dönüştürme ve/veya dolandırıcılara satma potansiyelinin oldukça yüksek olma ihtimali geldi. Bu ihtimal düşük de olsa yüksek de olsa, tehdit aktörlerinin kişisel verilerimize göz diktiği, bu verilere erişebilen kurumları hedef aldığı maalesef günümüzün yadsınamaz bir gerçeğidir.

Sonuç olarak siz siz olun, cep telefonunuza tanımadığınız kişilerden gelen bağlantı adreslerine (link) tıklamadan, dosyaları açmadan, çalıştırmadan önce iki defa düşünmeyi ihmal etmeyin.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

4. Yatırım Dolandırıcıları

Başlangıç

Hatırlayanlarınız varsa 2024 yılının Haziran ayında yayınlamış olduğum Deepfake Dolandırıcılarına Dikkat! başlıklı yazımda, Rusya merkezli olduğuna kanaat getirdiğim dolandırıcılık şebekesinin operasyonlarına dair detaylara, başka bir yazımda yer vereceğimi belirtmiştim.

O zamandan bu zamana kadar geçen sürede siber güvenlik araştırması ile elde ettiğim bilgiler öyle bir noktaya ulaştı ki hangi birini yazıya dökeceğim konusunda epey bir git gel yaşadıktan sonra farkındalık adına en çok faydası olacağına inandığım, dolandırıcılar ile aramda geçen telefon görüşmelerinin de yer aldığı kısımları yazıya dökmeye karar verdim.

Umuyorum ki benim için de önemli bir dönüm noktasına sahip olan bu **200.** araştırma yazım, farkındalık yaratma anlamında

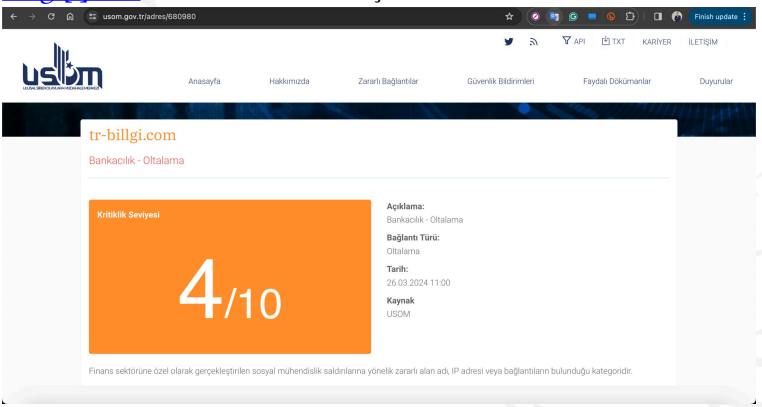
arzu ettiğim noktaya ulaşır ve bu araştırma ile ortaya koyduğum en ufak bir bilgi bile dolandırıcılık dosyalarını aydınlatmada, kurbanlardan emniyet güçlerine kadar geniş bir yelpazede fayda sağlar.

Lütfen sizler de daha az vatandaşın mağdur olması ve farkındalık yaratması adına bu yazıyı çevrenizdekilerle paylaşmayı ihmal etmeyin.

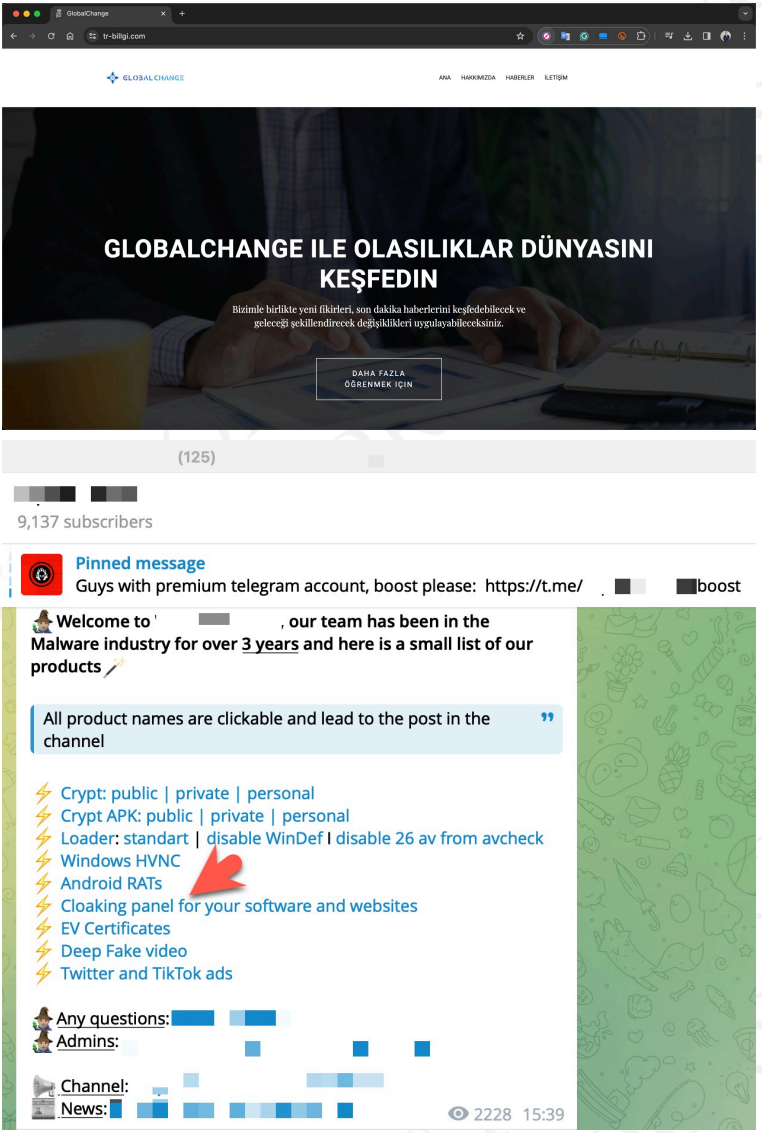
Teknik Araştırma

Keşif

2024 yılının Mart ayında USOM tarafından Zararlı Bağlantılar listesine **Bankacılık – Oltalama** açıklamasıyla eklenen tr-billgi[.]com alan adı dikkatimi çekti.



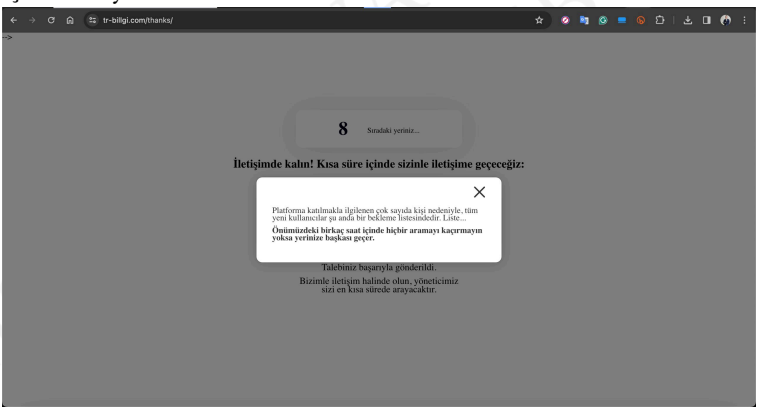
Web sitesini ziyaret ettiğimde karşılaştığım sayfa, oldukça sıradan ve zararsız görünüyordu. Olsa olsa bu sayfanın, tehdit aktörleri arasında oldukça popüler olup, asıl oltalama sayfasını gizlemek amacıyla oluşturulmuş sahte ana sayfa (cloaking) olduğunu düşünerek bu web sitesi üzerinde araştırma yapmaya karar verdim ve hikayemiz bu şekilde başlamış oldu.



Zararlı İçerik Tespiti

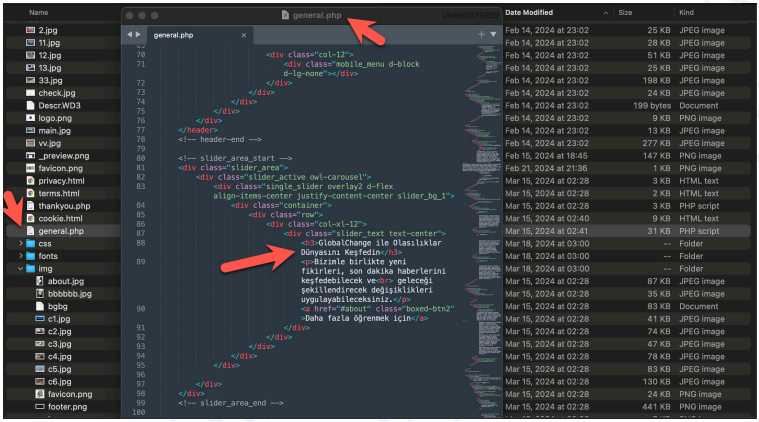
tr-billgi[.]com web sitesini biraz kurcaladığımda **/thanks**

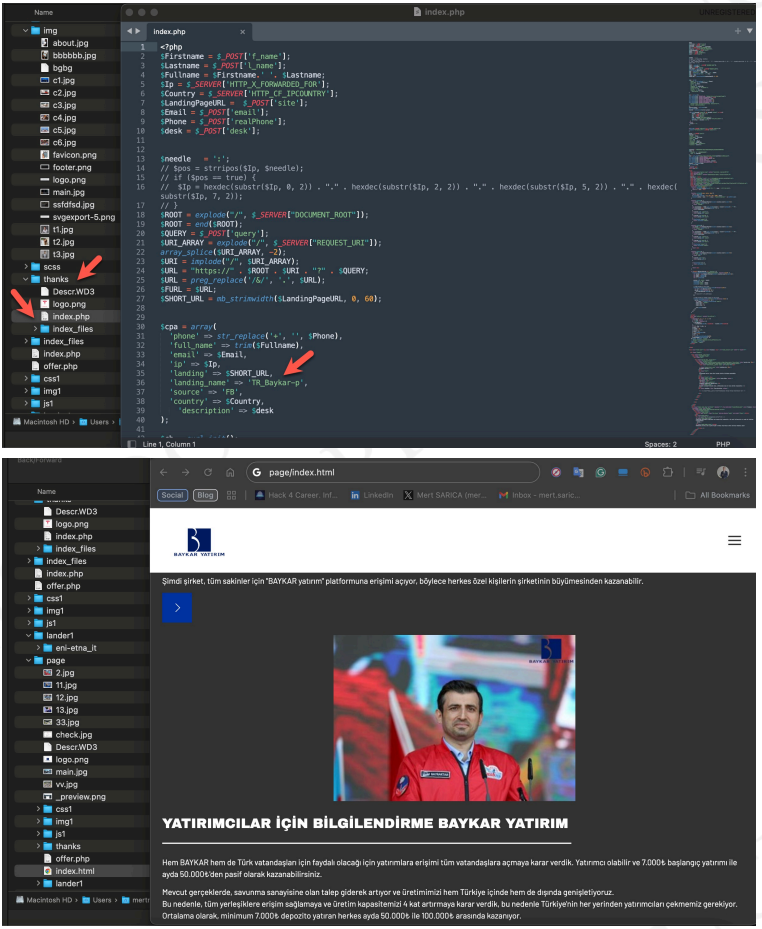
klasörü dikkatimi çekti. Bu sayfayı ziyaret ettiğimde, burasının web sitesinde yer alan herhangi bir formu dolduranların yönlendirildiği bir sayfa olduğunu düşünmeye başladım. Özellikle sayfada itinayla tekrarlanan "Hiçbir aramayı kaçırmayın", "Yöneticimiz sizi en kısa sürede arayacaktır" ifadeleri bu formu dolduranların birileri tarafından arandığına işaret ediyordu.



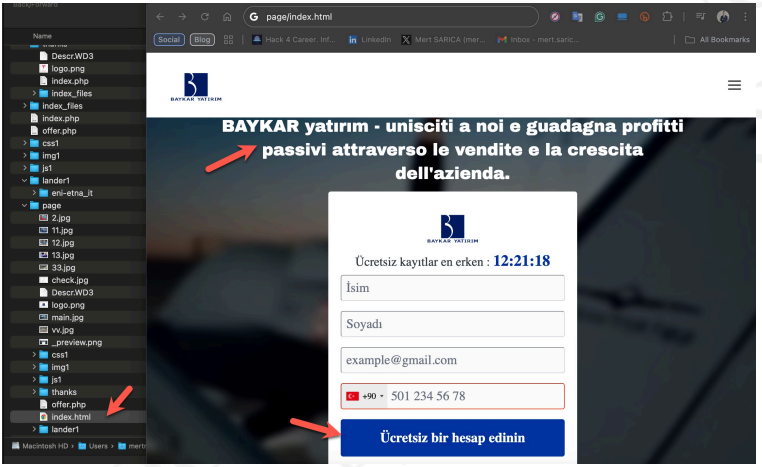
Bu web sitesini kurcalamaya devam ettiğimde bu tehdit aktörünün de, başka bir araştırma yazıma konu olanlar gibi Operasyon Güvenliği (OPSEC) noktasında hata yaptıklarını tespit ettim. Hatayı fırsata çevirip web sitesinin kaynak kodlarına eriştikten sonra kodları teker teker incelemeye başladım.

Kısa bir süre içinde **general.php** dosyasında sahte ana sayfaya ait kodları buldum. **Thanks** klasörü içinde yer alan **index.php** dosyasını, **page** klasöründe yer alan **offer.php**, **index.html** dosyalarını incelediğimde ise tehdit aktörleri tarafından bu oltalama sitesinin Baykar savunma şirketinin adını kötüye kullanarak kurbanlarını yatırım vaadiyle ağına düşürmek için tasarlandığını tespit ettim.



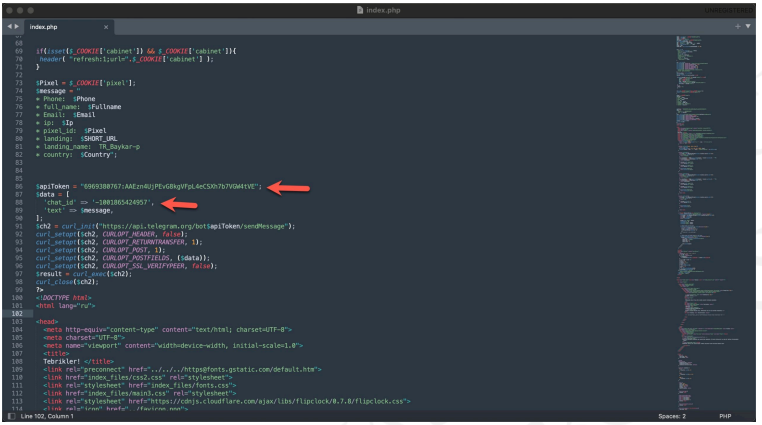


Oltalama sayfasındaki Türkçe metinlerin yanında İtalyanca metinlerin de yer alması bir yandan dikkatimi çekti. Tehdit aktörlerinin uluslararası kurumların adını (Slovnaft, INA d.d, Bosphorus Gaz, Baykar, Interpol) kullanarak dolandırıcılık girişiminde bulunduğunu Deepfake Dolandırıcılarına Dikkat! başlıklı yazımdan bildiğim için muhtemelen bu metin, İtalyan bir şirketi hedef almak için oluşturdukları İtalyanca oltalama sitesinden kalmış ve Türkçe'ye çevrilmesi unutulmuştu.



Teknik Takip

Bunların yanı sıra **thanks** klasörü içinde yer alan **index.php** dosyasında araştırmamı derinleştirecek çok önemli bir bilgiye daha ulaştım. O da tehdit aktörlerine ait olan Telegram Bot API jetonuydu (token).



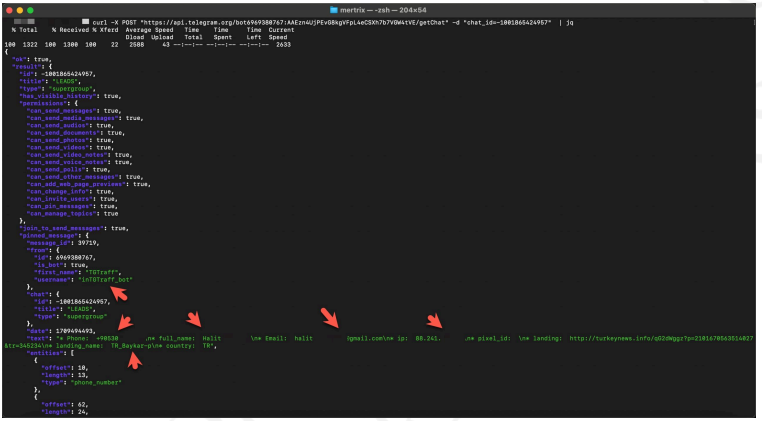
Telegram mesajlaşma uygulaması, hız, güvenlik ve dosya paylaşımı altyapısına sahip olması nedeniyle

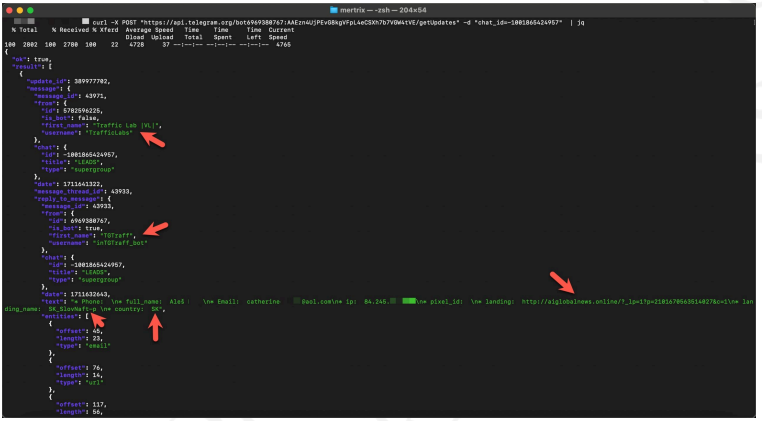
son yıllarda suç örgütlerinin, tehdit aktörlerinin, dolandırıcıların uğrak yeri olmaya devam ediyor.

Çoğu tehdit aktörü, Telegram Bot API'sinden faydalanarak oltaya düşürdükleri kişilerin çalınan bilgilerini anlık olarak oluşturdukları Telegram botları ile Telegram kanalları üzerinden takip etmektedirler. Bunun için yapmaları gereken ilk adım da botlarının jetonlarını (token) geliştirdikleri oltalama sitelerinin kaynak kodlarına yerleştirmektir.

Oltalama sitelerinin kaynak kodlarının başkalarının eline kolay kolay geçeceğini düşünmeyen tehdit aktörleri bu nedenle de bu jetonları aylarca değiştirmezler. Bu da emniyet güçlerinden, siber güvenlik araştırmacılarına kadar tehdit aktörlerinin Telegram üzerinden izlenmelerine olanak sağlar.

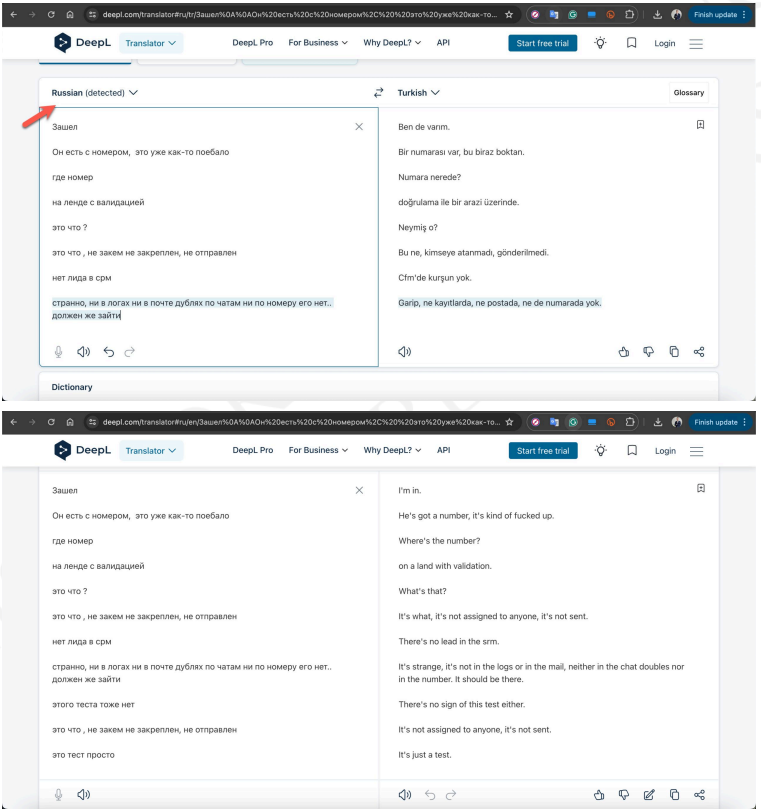
2024 yılının Mart ayı itibariyle bu jetonu kullanan Telegram botu üzerinden kanala gönderilen tüm mesajları mercek altına almaya başladığımda bu jetonun birden fazla oltalama sitesinde kullanıldığını gördüm. Oltalama sitesinde yer alan formu dolduran kurbanların ise **adları**, **telefon numaraları**, **e-posta adresleri**, **IP adresleri**, **hangi oltalama sitesini ziyaret ettikleri** ve **hangi ülkeden geldikleri** anlık olarak kanala iletiliyordu.


mertrix — -zsh — 204×54
curl -X POST "https://api.telegram.org/bot6969388767:AAEzn4UjPEvQ8kgVFpL4eCSKh7b7VOWktYE/getChat" -d "chat_id=-1001865424957" | jq
"ok": true,
"result": {
"id": -1001865424957,
"title": "LEADS",
"type": "supergroup",
"has_visible_history": true,
"permissions": {
"can_send_messages": true,
"can_send_media_messages": true,
"can_send_audios": true,
"can_send_documents": true,
"can_send_photos": true,
"can_send_videos": true,
"can_send_video_notes": true,
"can_send_voice_notes": true,
"can_send_polls": true,
"can_send_other_messages": true,
"can_add_web_page_previews": true,
"can_change_info": true,
"can_invite_users": true,
"can_pin_messages": true,
"can_manage_topics": true
},
"join_to_send_messages": true,
"pinned_message": {
"message_id": 39719,
"from": {
"id": 6969388767,
"is_bot": true,
"first_name": "TSTstaff",
"username": "InTSTstaff_bot"
},
"chat": {
"id": -1001865424957,
"title": "LEADS",
"type": "supergroup"
},
"date": 1709494493,
"text": "» Phone: +90530 »« full_name: Halit Halit »« Email: halit @gmail.com\n» ip: 88.241. »« pixel_id: \n» landing: http://turkeynews.info/qG2dWggzTp=2101670563514827&tr=340234\n» landing_name: TR_Baykar-p\n» country: TR",
"entities": [
{
"offset": 10,
"length": 13,
"type": "phone_number"
},
{
"offset": 62,
"length": 24,

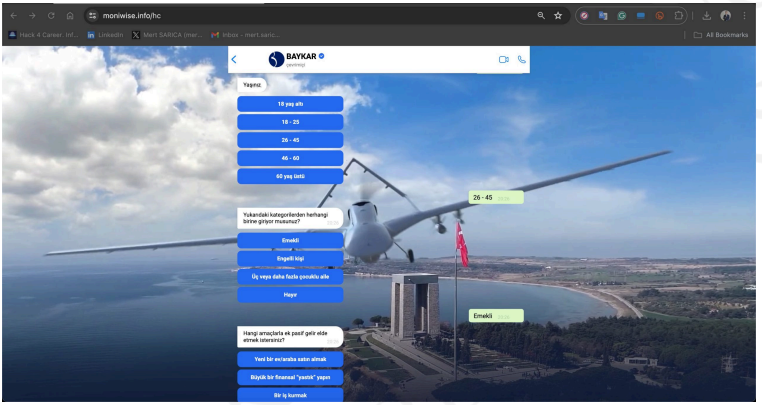


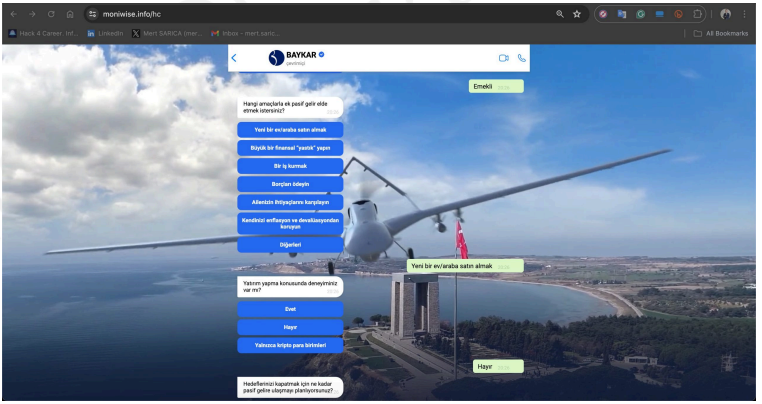
	A	B	C	D	E
1	**Phishing websites**		**Targeted Companies w/ Country Codes**		**Victim E-mails**
2	http://24main.news		CZ_Bitsoft-p		@mailcom
3	http://allinone-news.com		EN_BitGPT-p		adriana @gmail.com
4	http://ca-ai-world.pro		EU_Quantum-p		alex @centrum.sk
5	http://ca-profit-ai.com		HU_ImmediateConnect-p		alige @hotmail.com
6	http://hurriyet-tr.today		Ru_legion-g		ana @gmail.com
7	http://inone-news.com		SI_Petrol-l		ayem @yahoo.com
8	http://news-online.pro		SK_SlovNaft-p		aylir @gmail.com
9	http://news-online.wiki		TR-EU_Bosphorus-t		aysel @hotmail.com
10	http://news-proff.pro		TR_Baykar-l		cance @gmail.com
11	http://news-sheet.today		TR_Baykar-p		cihan @hotmail.com
12	http://official-tr-news.today		TR_Bosphorgaz-p		cure @gmail.com
13	http://sk-slnft.site		TR_Bosphorus-t		dogan @gmail.com
14	http://tr-bsfr.pro		TR_Kalyon-t		efehan @hotmail.com
15	http://tr-haberler.today				ejder @gmail.com
16	http://tr-inf.com				ekrem @gmail.com
17	http://tr-inform.com				fatma @gmail.com
18	http://tr-pro.info				fena @hotmail.com
19	http://turkeynews.info				fidan @gmail.com
20	https://ch-back-ltd.com				fm @gmail.com
21	https://tr-bkr.com				@ss.ss
22	https://tr-byr.com				gabriel @gmail.com
23	https://news-inform.site				gyula @gmail.com
24	https://baslangicnoktasi.online/				halil @gmail.com
25	https://proinfo-trader.site				havas @gmail.com
26	https://bilgihazinesi.online/				hilul @gmail.com
27	https://xn--hayalmezar-6ub.online				hj @dsd.dd
28	https://moniwise.info				h @gmail.com
29					jancobalog17@gmail.com

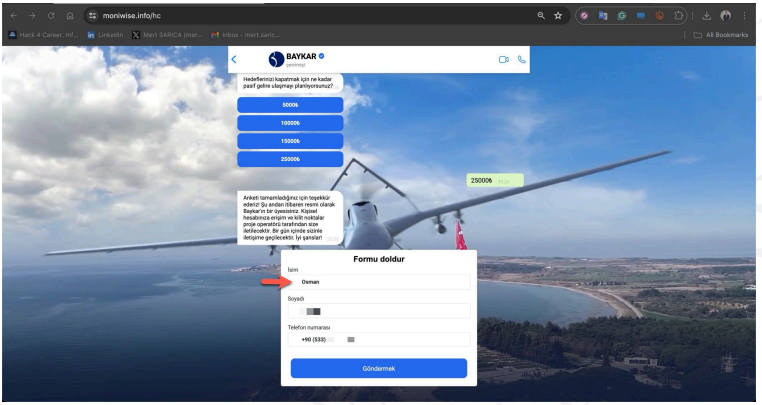
Kanalda yer alan kullanıcıların profillerine ve aralarında geçen yazışmalara baktığımda Rus mu yoksa Ukraynalı mı olduklarına kanaat getirmekte zorlandığım için son kararı Deepl çeviri uygulamasına bırakmaya karar verdim. Deepl, tüm bu metinlerin Rusça olduğunu belirtti. Bu kullanıcılar gerçekten bu oltalama sitelerini kuran, operasyonunu yürüten kişiler miydi yoksa sadece tehdit aktörlerine Telegram Botu hizmeti sağlayan aracı hizmet sağlayıcısının yöneticileri miydi bu kısımdan çok emin olamadım.

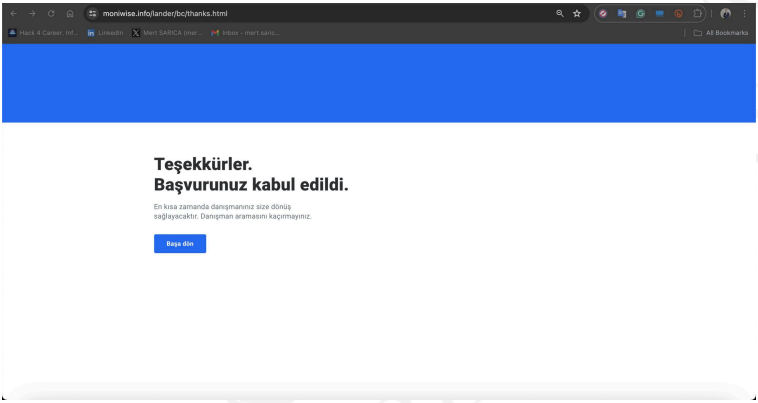


2024 yılının Temmuz ayına kadar dolandırıcıların oltalama amacıyla kullandığı web sitelerini yakın takibe aldıktan sonra bu web sitelerindeki formlara dolandırıcılarla iletişim kurabilmek için telefon numaramı girmeye başladım.


moniwise.info/hc
BAYKAR
Yaşınız
18 yaş altı
18 - 25
26 - 45
46 - 60
60 yaş üstü
26 - 45
Yukarıdaki kategorilerden herhangi birine giriyor musunuz?
Emekli
Engelli kişi
Üç veya daha fazla çocuklu aile
Hayır
Emekli
Hangi amaçlarla ek pasif gelir elde etmek istersiniz?
Yeni bir ev/araba satın almak
Büyük bir finansal "yastık" yapın
Bir iş kurmak

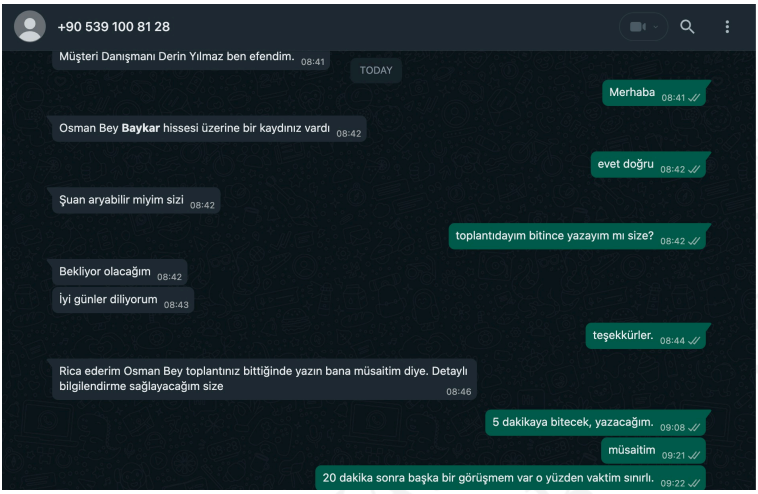

moniwise.info/hc
BAYKAR
Emekli
Hangi amaçlarla ek pasif gelir elde etmek istersiniz?
Yeni bir ev/araba satın almak
Büyük bir finansal "yastık" yapın
Bir iş kurmak
Borçları ödeyin
Ailenizin ihtiyaçlarını karşılayın
Kendinizi enflasyon ve devalüasyondan koruyun
Diğerleri
Yeni bir ev/araba satın almak
Yatırım yapma konusunda deneyiminiz var mı?
Evet
Hayır
Yalnızca kripto para birimleri
Hayır
Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz?


moniwise.info/hc
BAYKAR
Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz?
5000$
100000$
150000$
250000$
250000$
Anketi tamamladığınız için teşekkür ederiz! Şu andan itibaren resmi olarak Baykar'ın bir üyesisiniz. Kişisel bilgileriniz ve iletişim detaylarınız proje operatörü tarafından size iletilecektir. Bir gün içinde sizinle iletişime geçileceksiniz. İyi şanslar!
Formu doldur
İsim
Osman
Soyadı
Telefon numarası
+90 (533)
Göndermek



1. Dolandırıcılık Girişimi

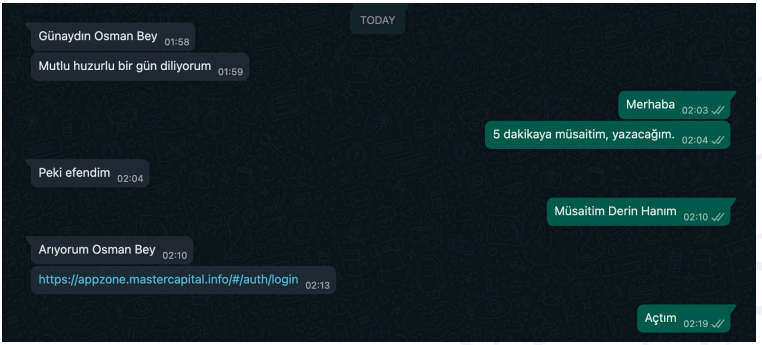
Takvimler **22 Temmuz 2024**'ü gösterdiğinde **+90 539 100 81 28** numaralı cep telefonundan kendisini müşteri danışmanı olarak tanıtan **Derin** isimli bir kişiden doldurduğum forma istinaden WhatsApp mesajı aldım.

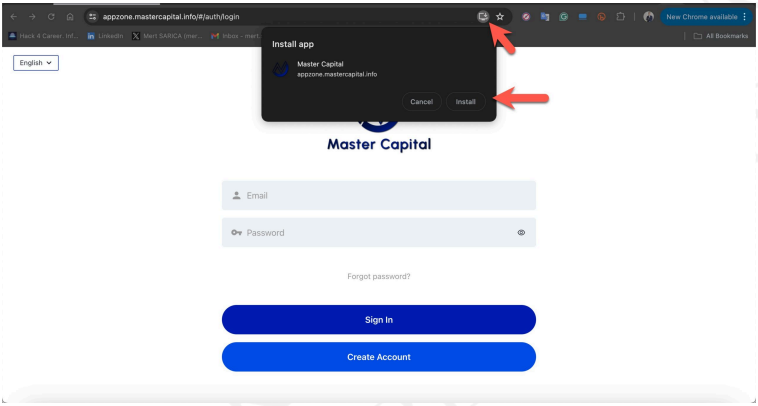


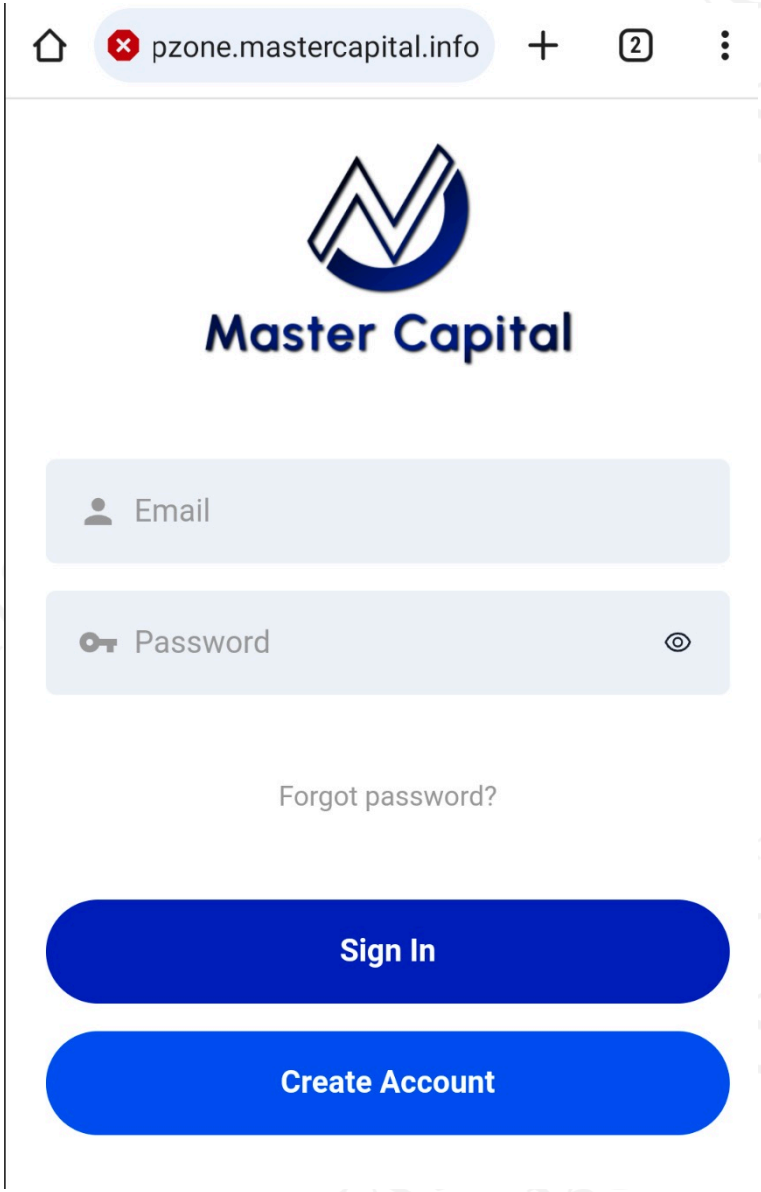
Amerika'da yaşadığım ve Türkiye ile saat farkı 7 saat olduğu için dolandırıcı ile iletişim kurmak zaman

> zaman zor oldu. Özellikle dolandırıcı Türkiye saati ile 9/6 çalıştığı (fazla mesai yapmayan bir meslek dalı :)) ve benimle iletişim kurmayı sabah saatlerinde yapmayı tercih ettiği için benim saatime göre çoğu görüşmemiz gece saat 02:00'dan sonra gerçekleşti. Amacım bu dolandırıcılık çarkını ortaya çıkarmak olduğu için gecenin körü de olsa tüm çağrılarını büyük bir motivasyonla yanıtlamayı başardım.

Dolandırıcı ile **23 Temmuz 2024** tarihinde yaptığım WhatsApp görüşmesinde, hisse alım satımı gerçekleştirebilmek için öncelikle mobil cihazıma bir uygulama yüklemem gerektiğini ve bunun için de **https://appzone[.]mastercapital[.]info/#/auth/login** web adresini ziyaret etmem gerektiğini belirtti. Her ne kadar dolandırıcı bunu mobil uygulama olarak adlandırsa da işin aslında bunun bir Progressive Web Apps (PWA) web uygulaması olduğunu gördüm.

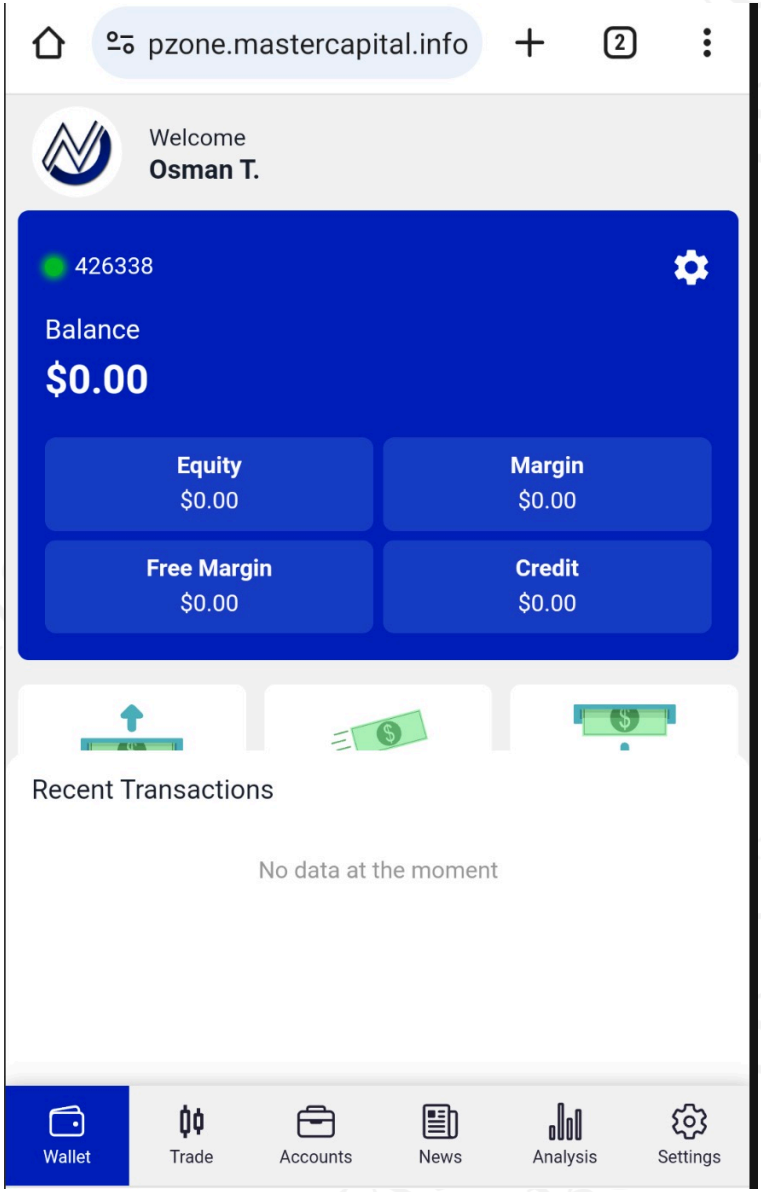


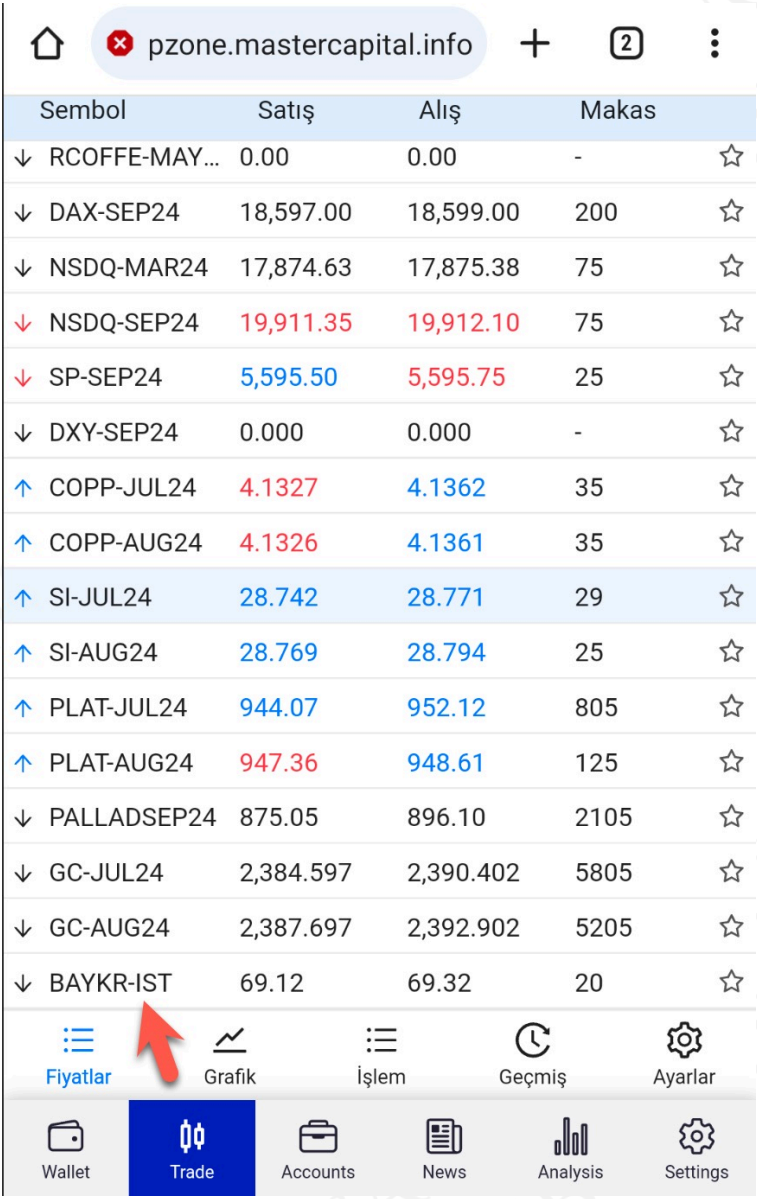




Web uygulamasına giriş yaptığımda karşılaştığım ekranlar Kripto Para Dolandırıcıları başlıklı yazıma konu olan sahte

borsaya oldukça benziyordu. Farklı olan kısım, dolandırıcılar tarafından uygulamada yer alan sembol listesine sahte Baykar hisse senedi sembolünü (**BAYKR-IST**) eklemiş olmalarıydı.


pzone.mastercapital.info
Welcome
Osman T.
426338
Balance
$0.00
Equity
$0.00
Margin
$0.00
Free Margin
$0.00
Credit
$0.00
Recent Transactions
No data at the moment
Wallet
Trade
Accounts
News
Analysis
Settings

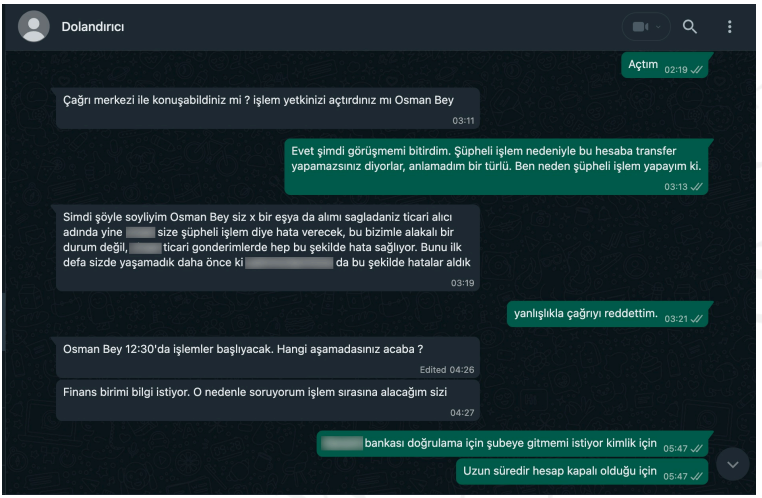


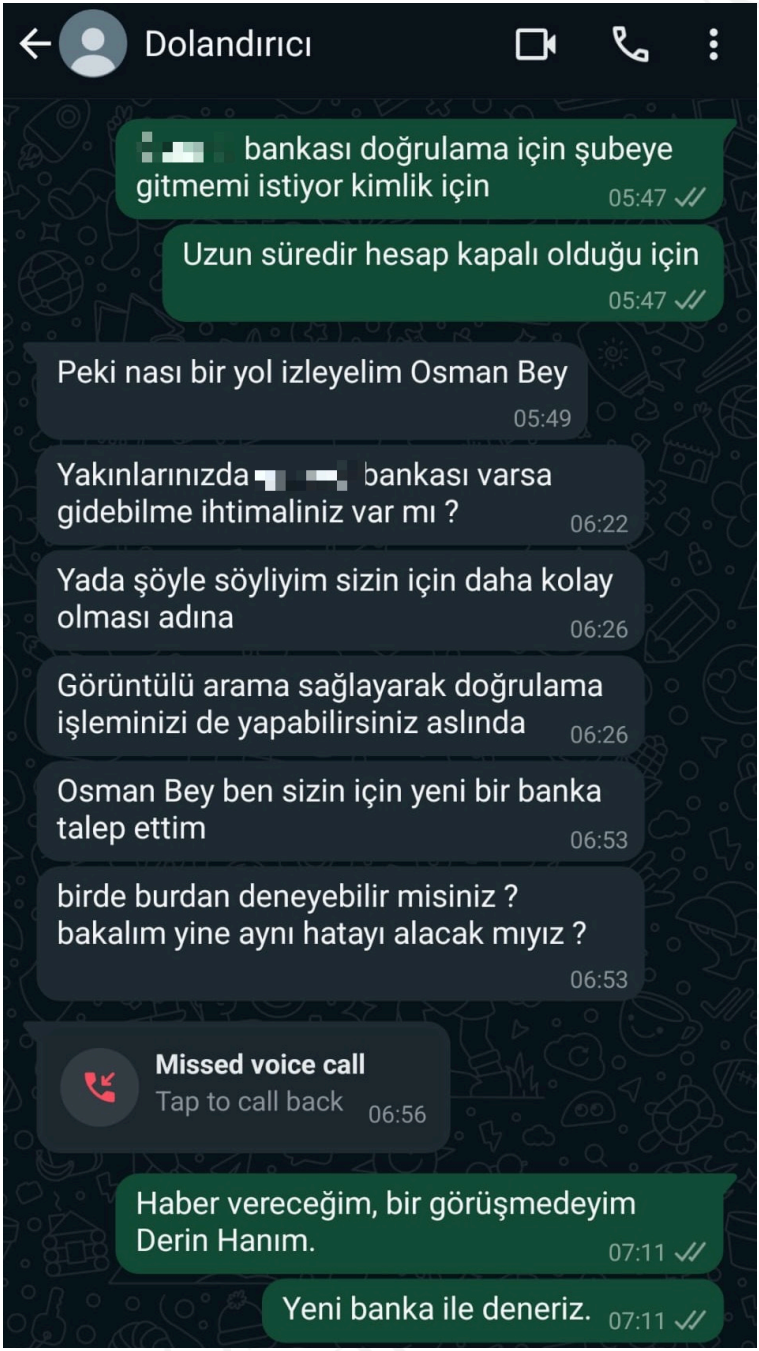
Görüşmenin devamında dolandırıcı, bu borsaya para gönderebilmem ve sözde Baykar hissesini satın alabilmem için

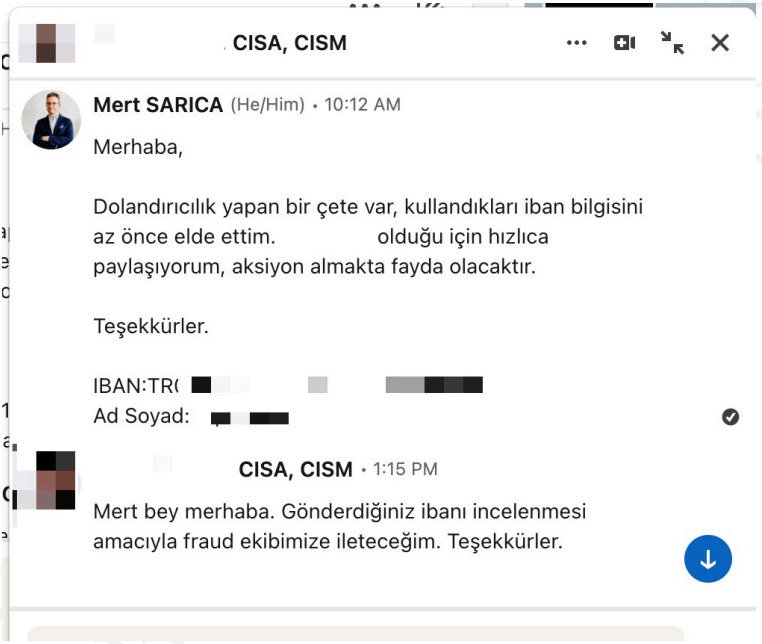
benden paylaşmış olduğu banka hesaplarına para transferi yapmam gerektiğini söyledi. Ana amacım hem dolandırıcıların yöntemini öğrenmek hem de WhatsApp Dolandırıcıları başlıklı yazımda yaptığım gibi kötüye kullanılan banka hesap bilgilerini öğrenip banka yetkilileri ile paylaşmak olduğu için bir mizansen kurgulamaya karar verdim.

> Benimle harcadıkları her bir dakikanın, masum vatandaşları dolandırmak için ayıracakları zamandanın eksildiğini bildiğim için mizansenin uzun ve gerçekçi olmasına gayret ettim.

Büyük bir hevesle para transferi yapmaya çalışan ama sürekli hata alan bir kurban rolüne büründükten sonra dolandırıcıya hata aldığımı belirttim. Dolandırıcı da bir zaman sonra yeni bir banka hesap bilgisini benimle paylaştı. Ben de vakit kaybetmeden elde ettiğim bilgileri banka yetkilileri ile paylaştım.




Dolandırıcı
[redacted] bankası doğrulama için şubeye gitmemi istiyor kimlik için
05:47
Uzun süredir hesap kapalı olduğu için
05:47
Peki nası bir yol izleyelim Osman Bey
05:49
Yakınlarınızda [redacted] bankası varsa gidebilme ihtimaliniz var mı ?
06:22
Yada şöyle söyliyim sizin için daha kolay olması adına
06:26
Görüntülü arama sağlayarak doğrulama işleminizi de yapabilirsiniz aslında
06:26
Osman Bey ben sizin için yeni bir banka talep ettim
06:53
birde burdan deneyebilir misiniz ?
bakalım yine aynı hatayı alacak mıyız ?
06:53
Missed voice call
Tap to call back
06:56
Haber vereceğim, bir görüşmedeyim Derin Hanım.
07:11
Yeni banka ile deneriz.
07:11



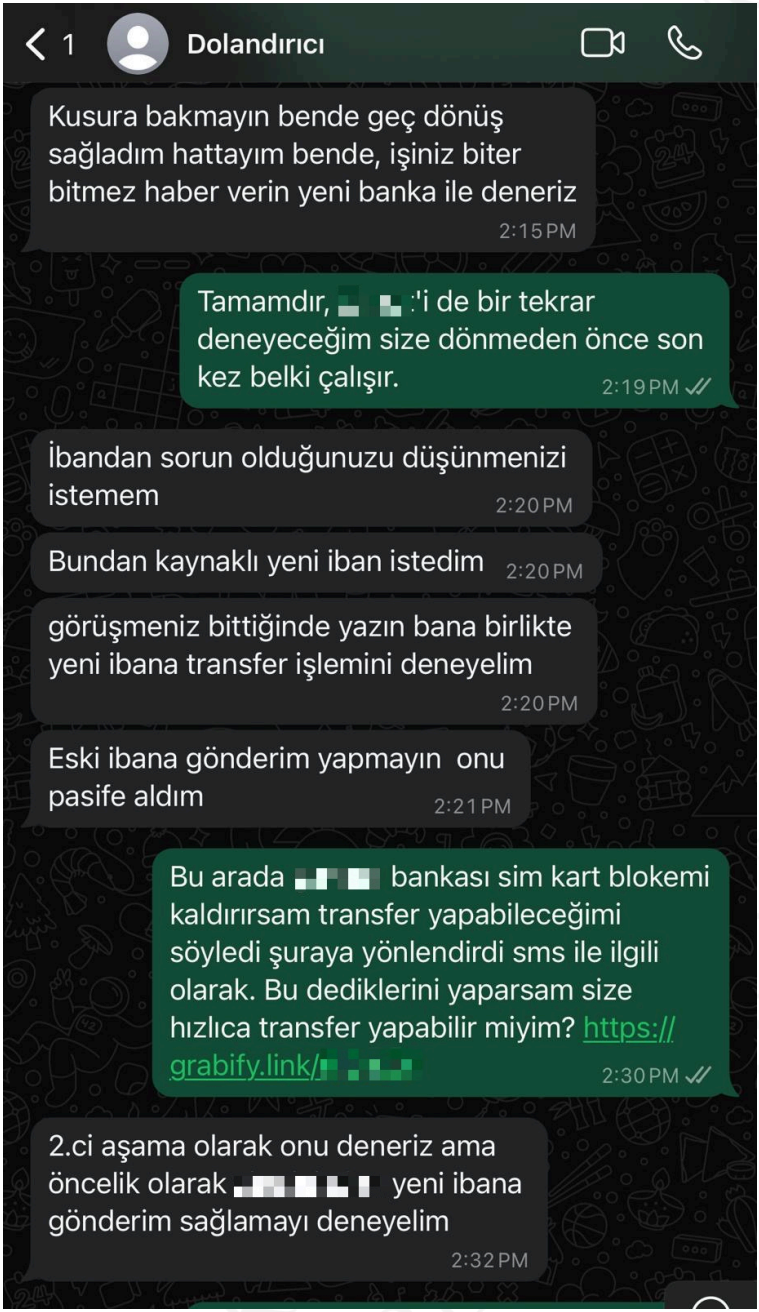
Aldığım hatalardan yaka silken **Derin** isimli dolandırıcı beni vakit kaybetmeden bankaların internet/mobil şube ekranları konusunda çok daha bilgili ve tecrübeli olduğunu düşündüğüm **Demir** isim dolandırıcıya (**+90 539 105 14 31**) yönlendirse de şans pek yüzüne gülmedi.

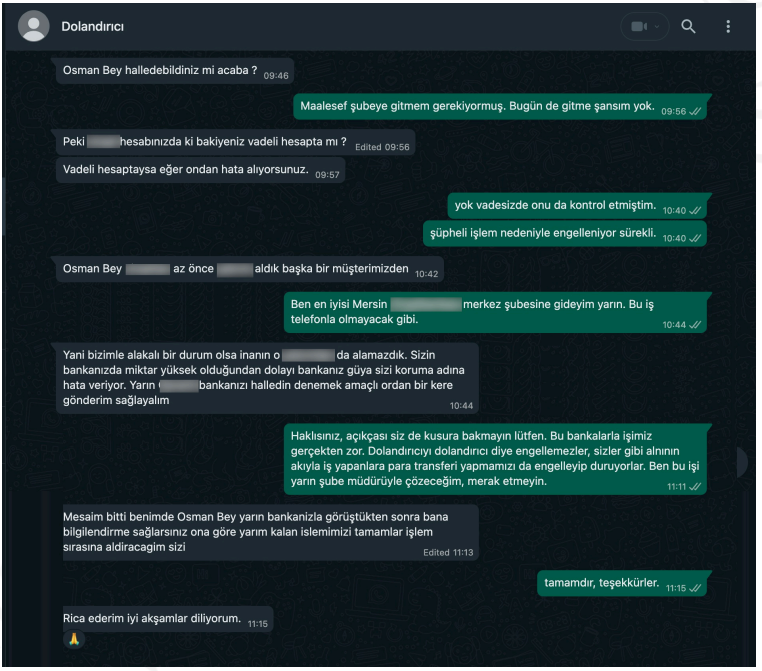
IP Tespiti

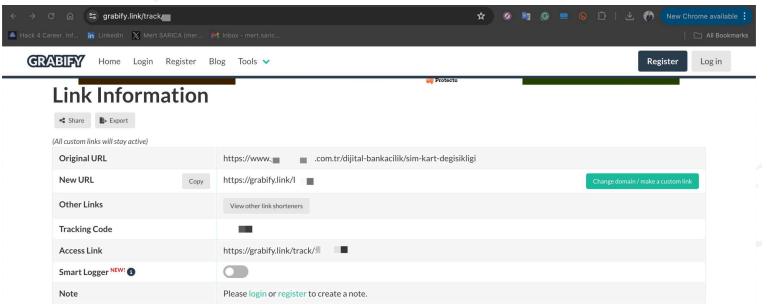
Görüşmenin ilerleyen dakikalarında benimle WhatsApp üzerinden iletişim halinde olan dolandırıcının IP adresini öğrenmek için Grabify IP Logger uygulamasından faydalanmaya karar verdim.

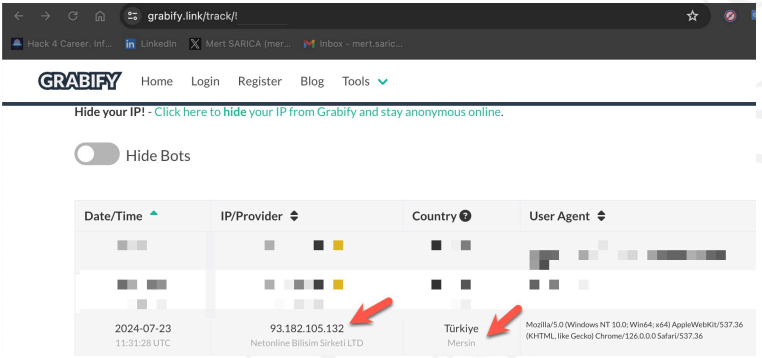
Grabify üzerinde, ziyaret edildiğinde X bir bankanın SIM kartı bloke kaldırma sayfasına yönlendiren bir bağlantı adresi (link) oluşturduktan sonra bunu dolandırıcı ile paylaştım. Sohbetin

gidişatına göre doğru zamanda bağlantı adresini dolandırıcıya gönderdiğim için çok geçmeden dolandırıcının IP adresini ve bağlandığı şehri Grabify üzerinden tespit edebildim. (**93.182.105.132** – **Mersin**)

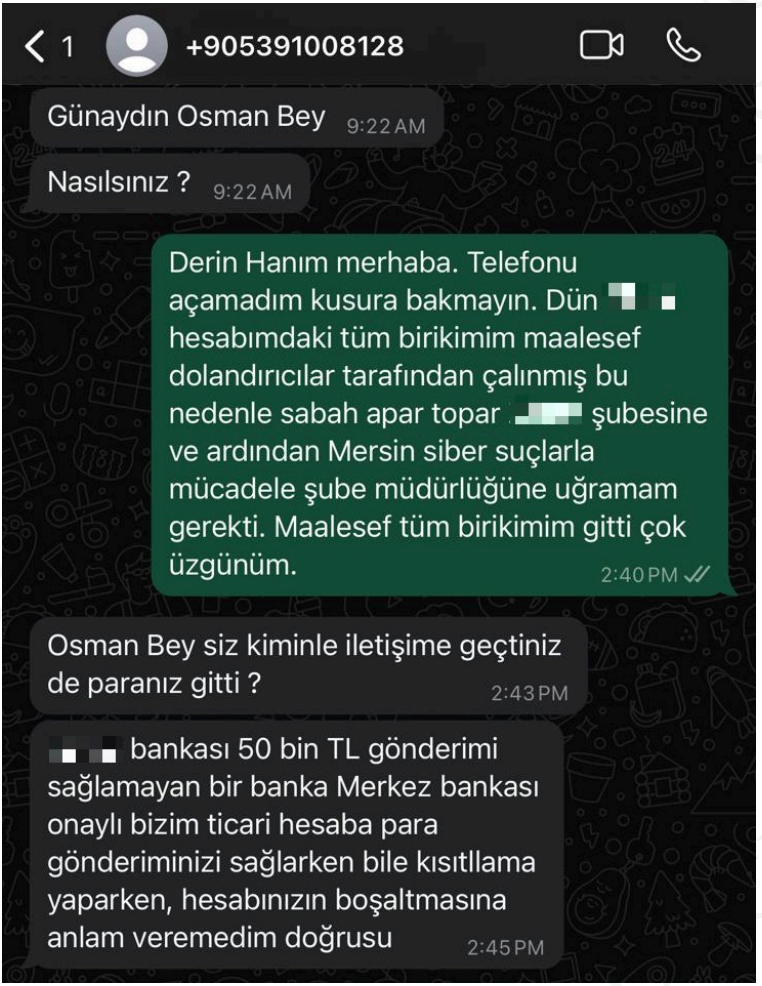

1
Dolandırıcı
Kusura bakmayın bende geç dönüş sağladım hattayım bende, işiniz biter bitmez haber verin yeni banka ile deneriz
2:15 PM
Tamamdır, [redacted]'i de bir tekrar deneyeceğim size dönmeden önce son kez belki çalışır.
2:19 PM
İbandan sorun olduğunuzu düşünmenizi istemem
2:20 PM
Bundan kaynaklı yeni iban istedim
2:20 PM
görüşmeniz bittiğinde yazın bana birlikte yeni ibana transfer işlemini deneyelim
2:20 PM
Eski ibana gönderim yapmayın onu pasife aldım
2:21 PM
Bu arada [redacted] bankası sim kart blokemi kaldırırsam transfer yapabileceğimi söyledi şuraya yönlendirdi sms ile ilgili olarak. Bu dediklerini yaparsam size hızlıca transfer yapabilir miyim? https://grabify.link/[redacted]
2:30 PM
2.ci aşama olarak onu deneriz ama öncelik olarak [redacted] yeni ibana gönderim sağlamayı deneyelim
2:32 PM

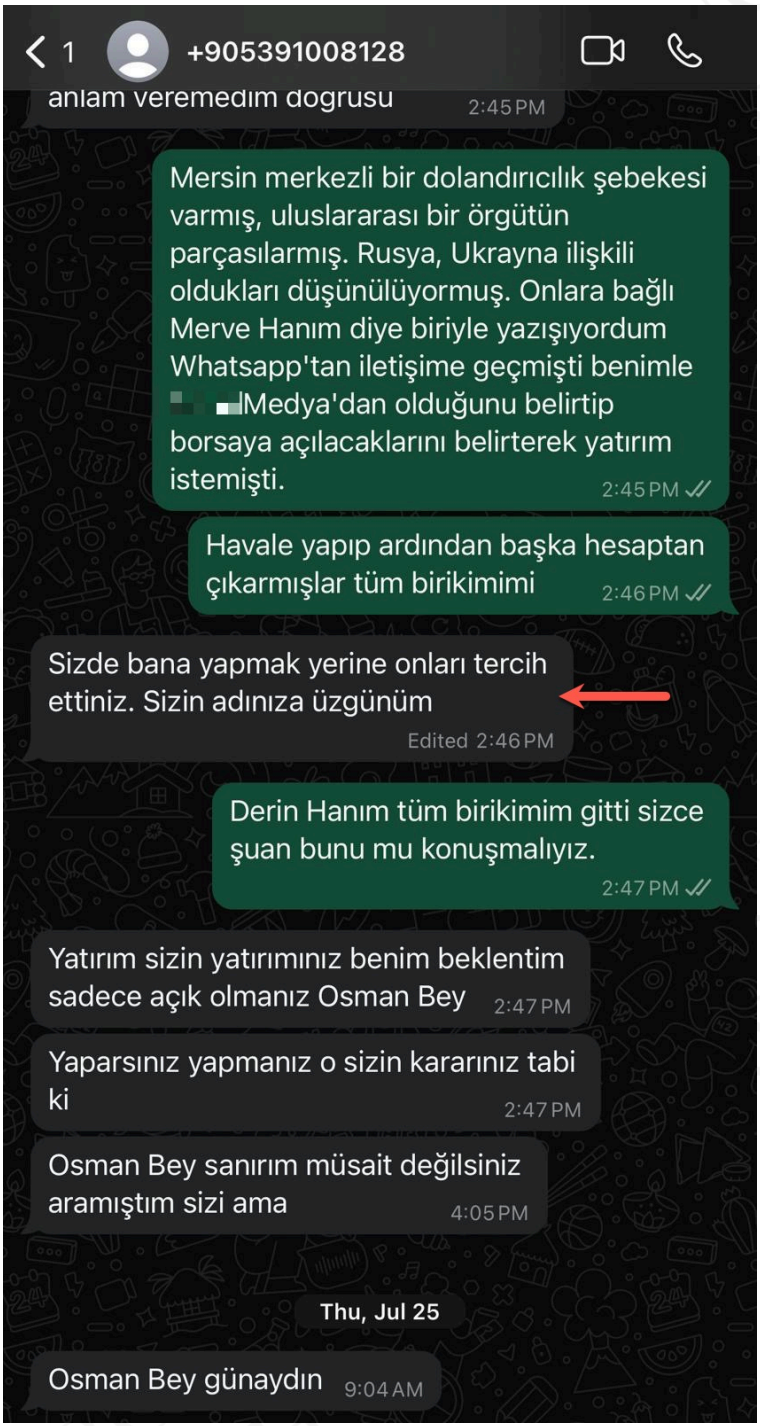

Dolandırıcı
Osman Bey halledebildiniz mi acaba ? 09:46
Maalesef şubeye gitmem gerekiyormuş. Bugün de gitme şansım yok. 09:56
Peki [redacted] hesabınızda ki bakiyeniz vadeli hesapta mı ? Edited 09:56
Vadeli hesaptaysa eğer ondan hata alıyorsunuz. 09:57
yok vadesizde onu da kontrol etmiştim. 10:40
şüpheli işlem nedeniyle engelleniyor sürekli. 10:40
Osman Bey [redacted] az önce [redacted] aldık başka bir müşterimizden 10:42
Ben en iyisi Mersin [redacted] merkez şubesine gideyim yarın. Bu iş telefonla olmayacak gibi. 10:44
Yani bizimle alakalı bir durum olsa inanın o [redacted] da alamazdık. Sizin bankanızda miktar yüksek olduğundan dolayı bankanız güya sizi koruma adına hata veriyor. Yarın [redacted] bankanızı halledin denemek amaçlı ordan bir kere gönderim sağlayalım 10:44
Haklısınız, açıkçası siz de kusura bakmayın lütfen. Bu bankalarla işimiz gerçekten zor. Dolandırıcıyı dolandırıcı diye engellemezler, sizler gibi alnının akıyla iş yapanlara para transferi yapmamızı da engelleyip duruyorlar. Ben bu işi yarın şube müdürüyle çözeceğim, merak etmeyin. 11:11
Mesaim bitti benimde Osman Bey yarın bankanizla görüştükten sonra bana bilgilendirme sağlarsınız ona göre yarım kalan islemimizi tamamlar işlem sırasına aldiracagim sizi Edited 11:13
tamamdır, teşekkürler. 11:15
Rica ederim iyi akşamlar diliyorum. 11:15

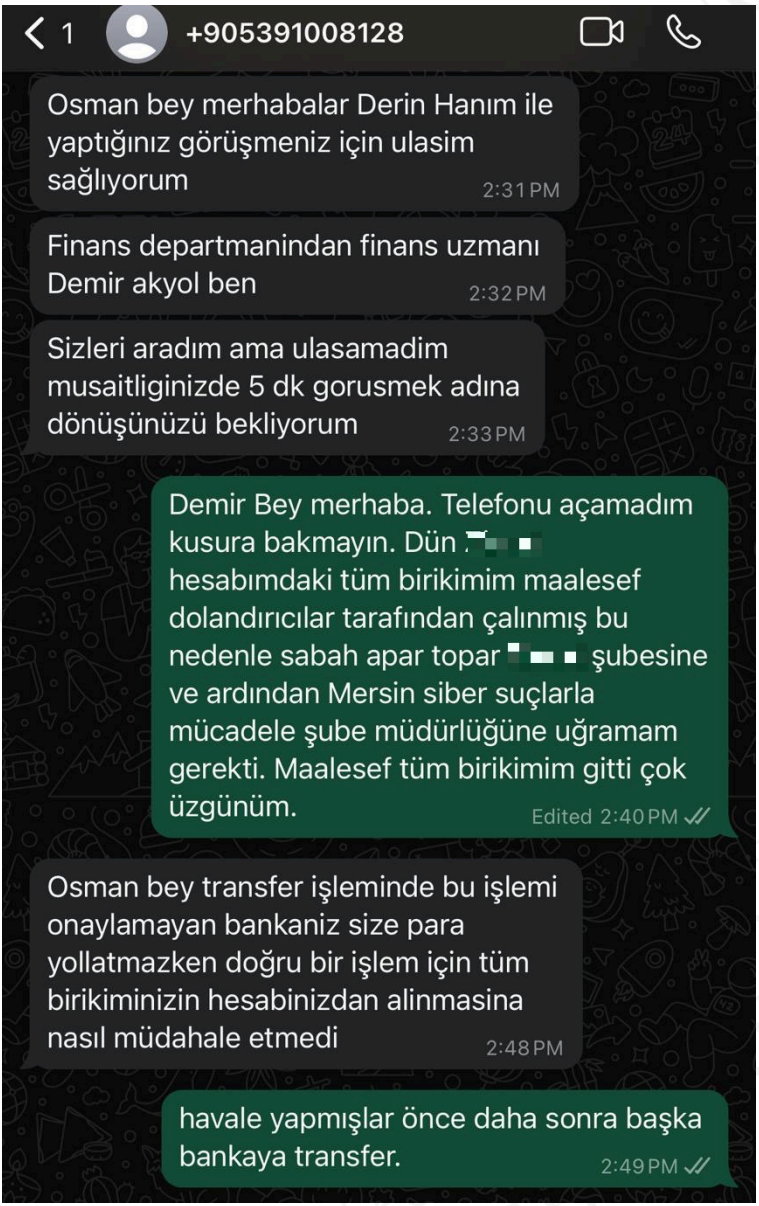

grabify.link/track
GRABIFY
Home
Login
Register
Blog
Tools
Register
Log in
Link Information
Share
Export
(All custom links will stay active)
Original URL
https://www. .com.tr/dijital-bankacilik/sim-kart-degisikligi
New URL
Copy
https://grabify.link/l
Change domain / make a custom link
Other Links
View other link shorteners
Tracking Code
Access Link
https://grabify.link/track/
Smart Logger NEW!
Note
Please login or register to create a note.



İstediğim bilgileri elde ettikten sonra dolandırıcılara soğuk duş etkisi yaratmak için başka dolandırıcı tarafından dolandırılan kurban senaryosu ile ilerlemeye karar verdim. Yazdığım mesajlar sonucunda, dolandırıcılar arasındaki rekabete yenik düştüklerini düşünen dolandırıcılar, sırasıyla sitem dolu mesajlar göndermeye başladılar.

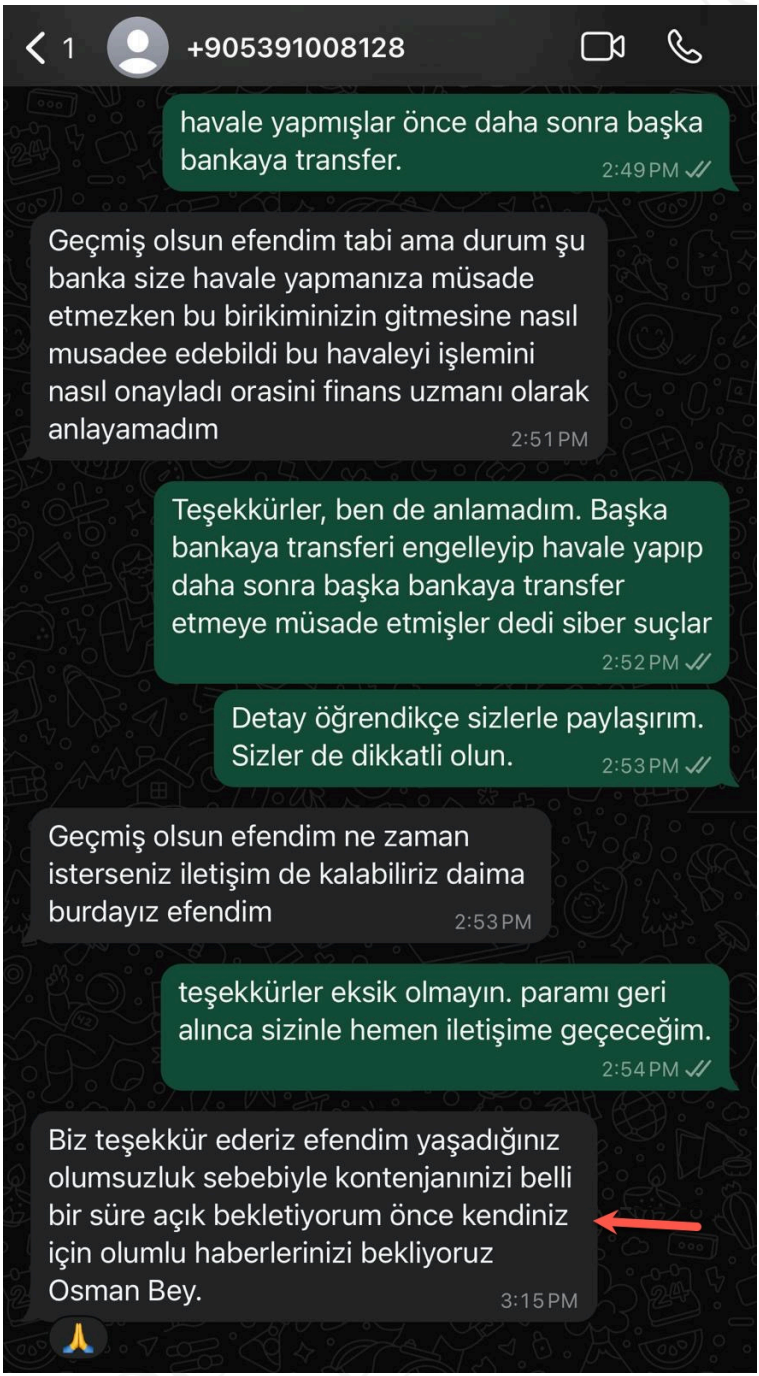

1
+905391008128
Günaydın Osman Bey 9:22 AM
Nasılsınız ? 9:22 AM
Derin Hanım merhaba. Telefonu açamadım kusura bakmayın. Dün [redacted] hesabımdaki tüm birikimim maalesef dolandırıcılar tarafından çalınmış bu nedenle sabah apar topar [redacted] şubesine ve ardından Mersin siber suçlarla mücadele şube müdürlüğüne uğramam gerekti. Maalesef tüm birikimim gitti çok üzgünüm. 2:40 PM
Osman Bey siz kiminle iletişime geçtiniz de paranız gitti ? 2:43 PM
[redacted] bankası 50 bin TL gönderimi sağlamayan bir banka Merkez bankası onaylı bizim ticari hesaba para gönderiminizi sağlarken bile kısıtllama yaparken, hesabınızın boşaltmasına anlam veremedim doğrusu 2:45 PM


1
+905391008128
anlam veremedim dogrusu
2:45 PM
Mersin merkezli bir dolandırıcılık şebekesi varmış, uluslararası bir örgütün parçasılarmış. Rusya, Ukrayna ilişkili oldukları düşünülüyormuş. Onlara bağlı Merve Hanım diye biriyle yazışıyordum Whatsapp'tan iletişime geçmişti benimle [redacted]Medya'dan olduğunu belirtip borsaya açılacaklarını belirterek yatırım istemişti.
2:45 PM
Havale yapıp ardından başka hesaptan çıkarmışlar tüm birikimimi
2:46 PM
Sizde bana yapmak yerine onları tercih ettiniz. Sizin adınıza üzgünüm
Edited 2:46 PM
Derin Hanım tüm birikimim gitti sizce şuan bunu mu konuşmalıyız.
2:47 PM
Yatırım sizin yatırımınız benim beklentim sadece açık olmanız Osman Bey
2:47 PM
Yaparsınız yapmanız o sizin kararınız tabi ki
2:47 PM
Osman Bey sanırım müsait değilsiniz aramıştım sizi ama
4:05 PM
Thu, Jul 25
Osman Bey günaydın
9:04 AM



Yazdıklarıma rağmen beni ikinci defa dolandırma umutlarını sonuna kadar koruyan ve iletişimi devam ettirmeye motive

olmuş vicdansız, serin kanlı dolandırılarıcıların mesajları ben yanıt vermeyi bıraktıktan bir süre sonra kesildi.


1
+905391008128
havale yapmışlar önce daha sonra başka bankaya transfer.
2:49 PM
Geçmiş olsun efendim tabi ama durum şu banka size havale yapmanıza müsade etmezken bu birikiminizin gitmesine nasıl musadee edebildi bu havaleyi işlemini nasıl onayladı orasini finans uzmanı olarak anlayamadım
2:51 PM
Teşekkürler, ben de anlamadım. Başka bankaya transferi engelleyip havale yapıp daha sonra başka bankaya transfer etmeye müsade etmişler dedi siber suçlar
2:52 PM
Detay öğrendikçe sizlerle paylaşırım. Sizler de dikkatli olun.
2:53 PM
Geçmiş olsun efendim ne zaman isterseniz iletişim de kalabiliriz daima burdayız efendim
2:53 PM
teşekkürler eksik olmayın. paramı geri alınca sizinle hemen iletişime geçeceğim.
2:54 PM
Biz teşekkür ederiz efendim yaşadığınız olumsuzluk sebebiyle kontenjanınizi belli bir süre açık bekletiyorum önce kendiniz için olumlu haberlerinizi bekliyoruz Osman Bey.
3:15 PM
🙏

Tüm bu olup bitenler devam ederken Baykar şirketi de 2024 yılının başından bu yana vatandaşları uyarmak için yazılı, görsel ve sosyal medya hesaplarından bu konuda uyarılar (#1, #2, #3) yayınlamaya hız kesmeden devam etti.

Ses Kayıtları

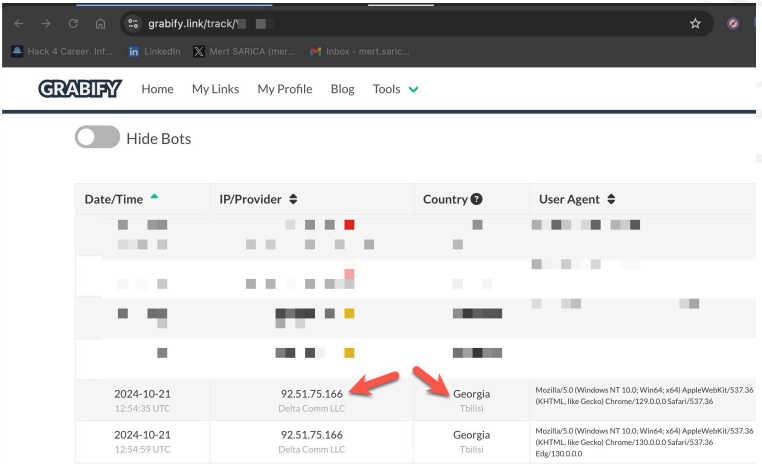
> Merak edenleriniz dolandırıcılarla gerçekleştirmiş olduğum akıllara durgunluk veren görüşmelerin ses kayıtlarını aşağıda, YouTube kanalım üzerinden dinleyebilirler.

2. Dolandırıcılık Girişimi

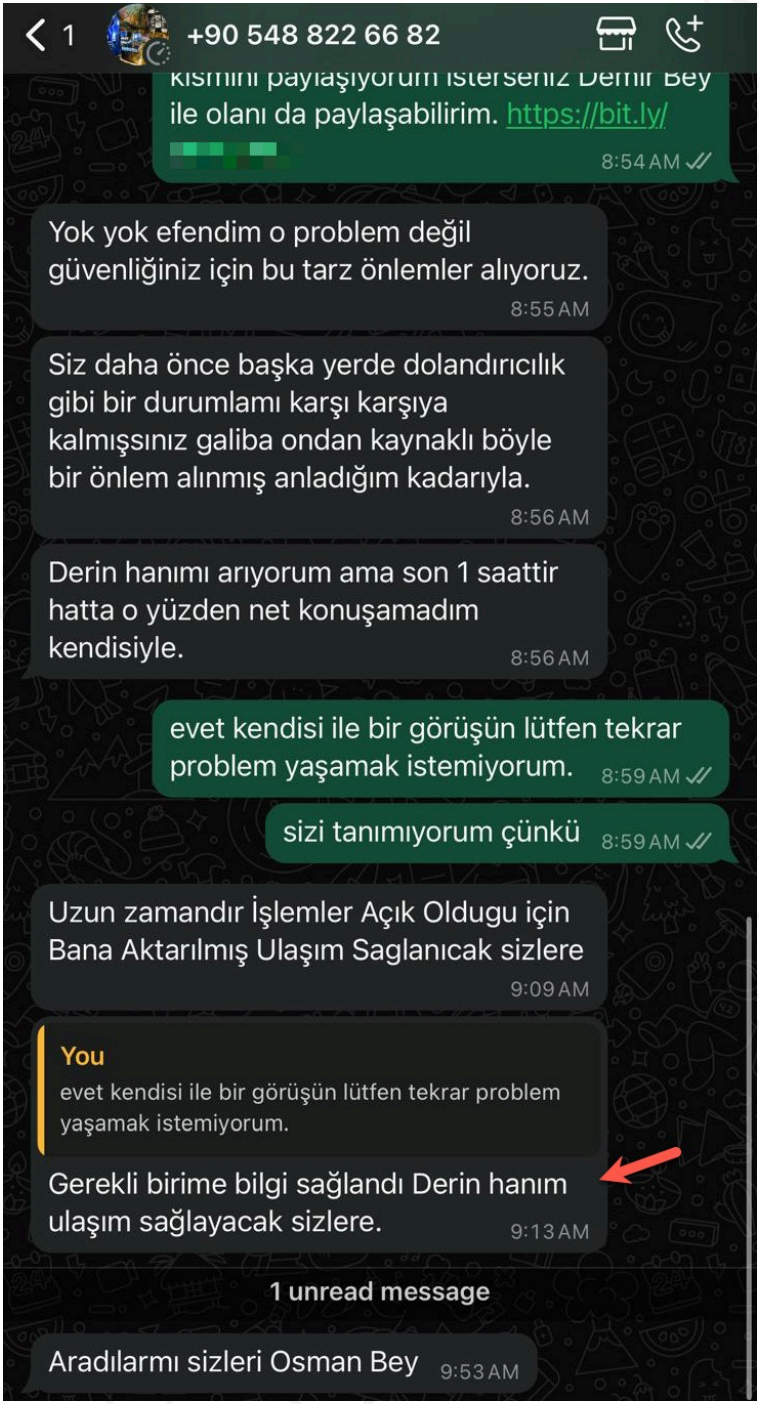
IP Tespiti

Takvimler 2024 yılının **Ekim** ayını yani bir önceki dolandırıcılık girişiminden neredeyse 3 ay sonrasını gösterdiğinde bu defa **+90 548 822 66 82** numaralı cep telefonundan **İpek** isimli başka bir dolandırıcı yine aynı senaryo ile benimle iletişime geçti. Ben de fırsat bu fırsat daha önceki yöntemle bu dolandırıcının da IP adresini elde etmeye karar verdim. Yine benzer bir şekilde dolandırıcıyı yemledikten sonra bu dolandırıcının öncekinin aksine **Mersin** yerine Gürcistan'ın başkenti **Tiflis**'ten bağlantı kurduğunu tespit ettim. (Dolandırıcının vekil sunucu (proxy) kullanmadığını varsaydım.)


3
+90 548 822 66 82
Today
Günaydınlar hayırlı haftalar Osman bey.
1:32 AM
Demir bey yıllık izinde. Sistem uzman olarak beni atamış sizlere müsait olduğunuzda aramak isterim.
1:33 AM
Açıkçası onlar tembih etmişler başkası ile konuşmamam için o nedenle onları beklemek isterim.
8:02 AM
Efendim yanlışlık olmasın benim danışmanım onlar aynı kuruma hizmet vermekteyiz. Aradığımda görebilirsiniz aynı numara ile arama gerçekleştiriyorum zaten. 100 adet danışmanız mevcut.
8:08 AM
Missed voice call
Tap to call back
8:24 AM
bit.ly
https://bit.ly/40c3kxC
bit.ly
Açıkası o zaman ufak bir problem yaşamıştım ve kesinlikle Derin Hanım kaynaklı değildi fakat yine de başkası ile görüşmemem gerektiğini paylaşmıştı güvenliğim için. Yazışmamımızın bir kısmını paylaşıyorum isterseniz Demir Bey ile olanı da paylaşabilirim. https://bit.ly/
8:54 AM



Bir önceki dolandırıcılık girişiminin baş aktörlerinden **Derin** veya **Demir**'in hala görevlerinin başında olup olmadıklarını da bir yandan merak ettiğim için bu dolandırıcıya Derin veya Demir'den başka kimseyle görüşmeyeceğimi ısrarla dile getirdikten sonra dolandırıcı ısrarlarıma yenik düşüp Derin'e ulaşmaya ve bana yönlendirmeye karar verdi. Bu sayede dolandırıcıların son 3 aydır operasyonlarına aynı kadro ile hız kesmeden devam ettiğini öğrenmiş oldum.


1
+90 548 822 66 82
kısmını paylaşıyorum isterseniz Demir Bey ile olanı da paylaşabilirim. https://bit.ly/
8:54 AM
Yok yok efendim o problem değil güvenliğiniz için bu tarz önlemler alıyoruz.
8:55 AM
Siz daha önce başka yerde dolandırıcılık gibi bir durumlamı karşı karşıya kalmışsınız galiba ondan kaynaklı böyle bir önlem alınmış anladığım kadarıyla.
8:56 AM
Derin hanımı arıyorum ama son 1 saattir hatta o yüzden net konuşamadım kendisiyle.
8:56 AM
evet kendisi ile bir görüşün lütfen tekrar problem yaşamak istemiyorum.
8:59 AM
sizi tanımıyorum çünkü
8:59 AM
Uzun zamandır İşlemler Açık Oldugu için Bana Aktarılmış Ulaşım Saglanıcak sizlere
9:09 AM
You
evet kendisi ile bir görüşün lütfen tekrar problem yaşamak istemiyorum.
Gerekli birime bilgi sağlandı Derin hanım ulaşım sağlayacak sizlere.
9:13 AM
1 unread message
Aradılarmı sizleri Osman Bey
9:53 AM

Sonuç

Sonuç itibariyle bu güvenlik araştırması ile Slovnaft, INA d.d, Bosphorus Gaz gibi petrol rafineri, gaz dağıtım şirketlerinden, Baykar gibi savunma şirketlerine hatta Interpol'e kadar önde gelen kurumların adını kullanarak dolandırıcılık girişiminde bulunan uluslararası dolandırıcılık çetesinin arka planda kurbanlarını nasıl ağlarına düşürdüklerini öğrenmiş oldum. Umuyorum ki masum vatandaşların paralarına göz diken bu dolandırıcılar en kısa sürede yakalanır ve hak ettikleri cezayı alırlar.

Yazının başında da belirttiğim üzere çok iyi kurgulanmış bu organize dolandırıcılık çarkına daha fazla masum insanın düşmemesi, kurban olmaması adına bu yazıyı çevrenizdekilerle ve tüm sevdiklerinizle paylaşmanızı gönülden rica ederim.

Bu yazı vesilesiyle de yeni yılınızı kutlar, 2025 yılının hem sizlere hem de tüm sevdiklerinize önce sağlık sonra mutluluk ve başarı getirmesini dilerim.