

Kripto Para Dolandırıcıları

written by Mert SARICA | 1 March 2023

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

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

2022 yılının Haziran ayında Twitter hesabımdan da duyurduğum üzere bu girişim, Anna isimli korumalı Twitter hesabından 14 Haziran 2022 tarihinde gelen bir mesaj ile başladı. Bu mesajda Anna, uzun zamandan beri beni görmediğinden bahsederek sohbete başladı. Adımı (Mark), nerede yaşadığımı (Türkiye’de yaşayan bir Belçikalı) ve çalıştığımı (Bir FinTek firmasında Finansal İşler Müdürü (CFO)) öğrendikten sonra konu nerelere nasıl yatırım yaptığımdan, Bitcoin kripto parasının o zamanlardaki değer kaybına geldi.



Anna

@Anna09339609

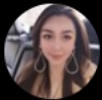


Anna @Anna09339609

Investment, one of the founders of import and export trading company,
photography enthusiast, travel is the truth of finding soul.

100 Following **19** Followers

Joined February 2022



Hello, long time no see

Jun 14, 2022, 5:06 AM

You accepted the request

Hello

Jun 14, 2022, 11:50 AM ✓

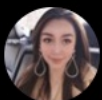


My friend, what are your plans for today?

Jun 14, 2022, 5:54 PM

Training.

Jun 14, 2022, 6:11 PM ✓



What kind of training do you do? What's it about?

Jun 14, 2022, 7:03 PM

Walking on the treadmill

Jun 14, 2022, 7:09 PM ✓



Start a new message



← → ↺ 🏠 🔒

twitter.com/Anna09339609

🐦

Home

Explore

🔔 1 Notifications

✉ Messages

🔖 Bookmarks

📄 Lists

👤 Profile

⋮ More

Tweet

← Anna 🔒

72 Tweets



⋮ ✉ Follow

Anna 🔒

@Anna09339609

Investment, one of the founders of import and export trading company, photography enthusiast, travel is the truth of finding soul.

📅 Joined February 2022

100 Following 19 Followers

These Tweets are protected

Only approved followers can see @Anna09339609's Tweets. To request access, click Follow. [Learn more](#)

Mert SARICA 🔒

@MertSARICA

⋮

← → ↺ 🏠 🔒

twitter.com/Anna09339609/photo

🔒 🔍 📄 ⚙️ 🌐 📱 🖨️ 🔄 Update ⋮

✕

🐦

Home

Explore

🔔 Notifications

✉ Messages

🔖 Bookmarks

📄 Lists

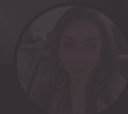
👤 Profile

⋮ More

Tweet

← Anna 🔒

72 Tweets



Follow

Anna 🔒

@Anna09339609

Investment, one of the founders of import and export trading company, photography enthusiast, travel is the truth of finding soul.

📅 Joined February 2022

100 Following 19 Followers

These Tweets are protected

Only approved followers can see @Anna09339609's Tweets. To request access, click Follow. [Learn more](#)

Mert SARICA 🔒

@MertSARICA

⋮

You might like

Steve Werby

@SteveWerby

Follow

LeDare Grossman

@LeDareGrossman

Follow

Hakan DIKMEN

@HakanDikmen

Follow

Show more

Trends for you

📈 Trending

Steam

📈 Trending

Christian

📈 Trending

#HandeErgel

📈 Trending

Mesal

📈 Trending

Messages



Anna



Finance is usually very sensitive to numbers. I guess you must have been exposed to cryptocurrency or stock investments.

Jun 14, 2022, 2:17 PM

Yes, I keep some amount of bitcoin and altcoins in my digital wallet. While bitcoin's price drops recently, I go on investing more coins for my bucket.

Jun 14, 2022, 2:20 PM

It seems that you invest in long-term holding.

Jun 14, 2022, 2:23 PM

Yes, I am a hodler

Jun 14, 2022, 2:23 PM

Yes, Bitcoin has been falling recently.

Jun 14, 2022, 2:24 PM

Although I invest in cryptocurrencies, I don't make long-term investments. As you know, the cryptocurrency market has been very unstable in recent years, and the risk of choosing any type of currency has also increased. I only do short-term bitcoin trading for 30 seconds, and get the data calculated by the head and shoulder formula and Kelly formula. And seize a good trading node and buy the ups and downs of Bitcoin within 30 seconds, so as to obtain a stable profit.

Jun 14, 2022, 2:26 PM



Sohbete bir süre ara verip bir yandan Anna'nın profilindeki fotoğrafının

sahte olduğunu düşünerek fotoğrafın gerçekte kime ait olduğunu bulmaya karar verdim. Bunun için Yandex arama motorunun Görsel Arama özelliğini kullanarak profil fotoğrafının Çinli Shasha Zhao isimli bir kişiye ait olduğunu tespit ettim. Shasha'nın profilinde paylaştığı fotoğraflara göz attığımda ise Anna'nın profil fotoğrafında yer alan fotoğrafı bulmam çok zor olmadı.

Yandex

Uploaded image x Search

Web Images Video News Translate Disk Mail Ads

videos do Instagram

instagram.com

Perfil do Instagram de COSMICKEE БРОВИ ИЗРАИЛЬ (@alina_beautymua) * 307 fotos e vídeos

Светлана Королева, Быково, Россия

liveuserpage.com

Ирина Алексанян

Instagram @zhaosasa 1P #zhaosasa, #chinese, 中国, #china, #asian, 亚洲, #asiangirls, #lamer, 美女, 正妹, #아름다움, #beauty, #cute #zhao

igirls.in

ID.

Instagram @zhaosasa 1P #zhaosasa, #lamer, 美女, 正妹, #아름다움, #beauty, #cute #zhaosasa #lamer 美女 正妹 #아름다움 #beauty #cute

socialgirls.im

Instagram @zhaosasa 1P #zhaosasa, #lamer, 美女, 正妹, #아름다움, #beauty, #cute #zhaosasa #lamer 美女 正妹 #아름다움 #beauty...

Хэрлэнзаяа (@kherlenzaya) Twitter

twitter.com

32. 21.

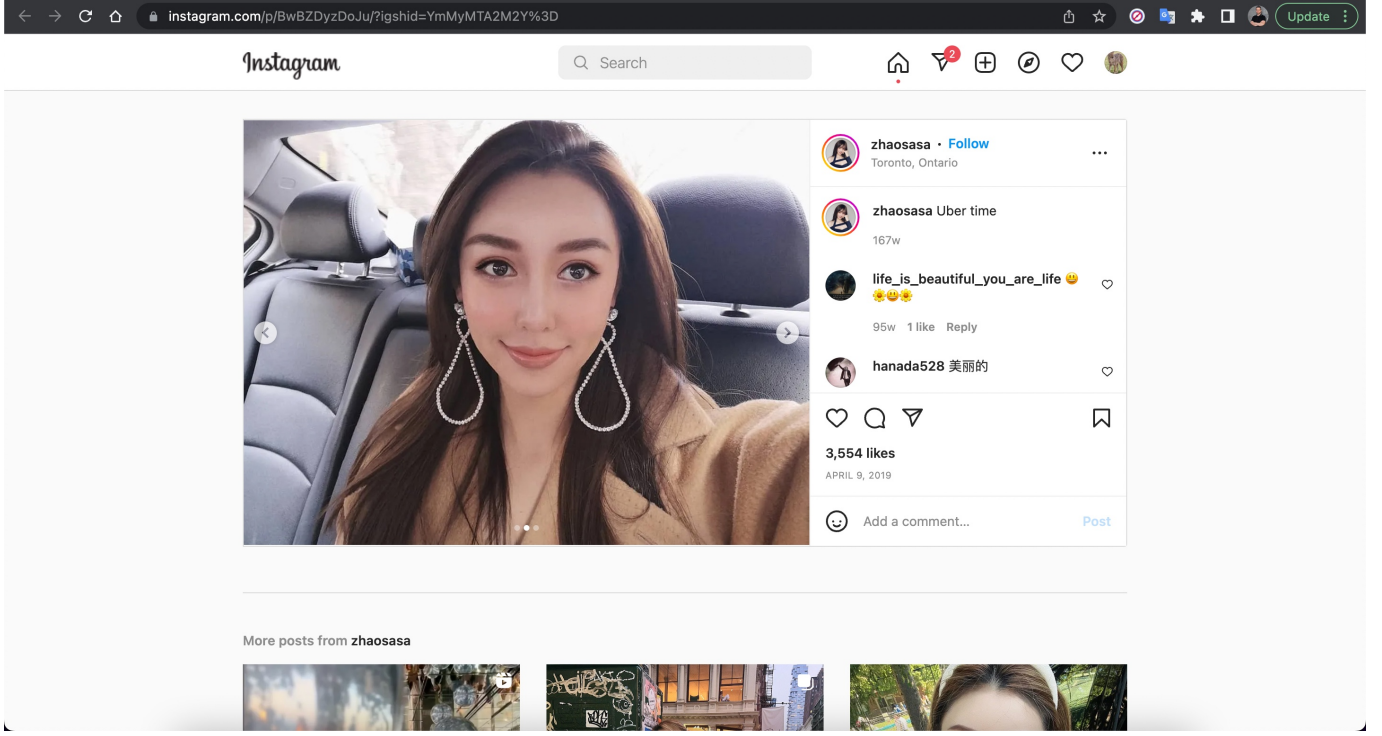
instagram.com/p/BwBZDyzDoJu/?igshid=YmMyMTA2M2Y%3D

Instagram

Search

Home Search Add Post Activity Heart Profile

Meta About Blog Jobs Help API Privacy Terms Top Accounts Hashtags Locations Instagram Lite Contact Uploading & Non-Users



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



Anna



Funds management

Total assets (USDT)

715460

≈ 714458.3560 USD



Recharge



Withdraw



Exchange



Transfer

Currency

Contract

Futures

Lock-up

USDT

Available

Frozen

Amount to (USD)

All the deals I made this month

I only used \$300,000 as the principal.

Jun 18, 2022, 10:17 PM

No, I ll move back to Belgium next month.

Jun 19, 2022, 12:59 AM

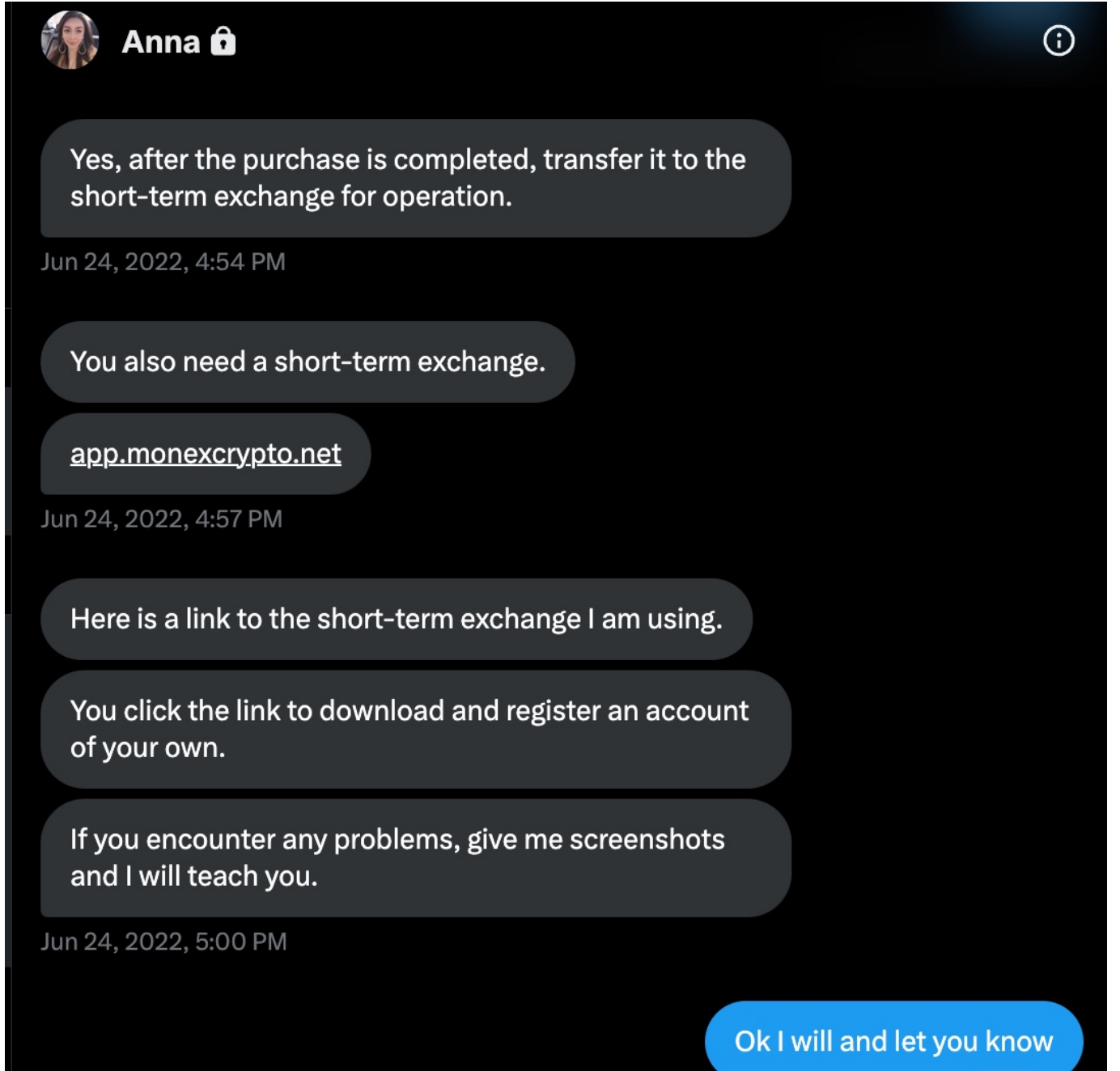
I have 500.000 USD to invest but I go on keeping eye on Bitcoin's price



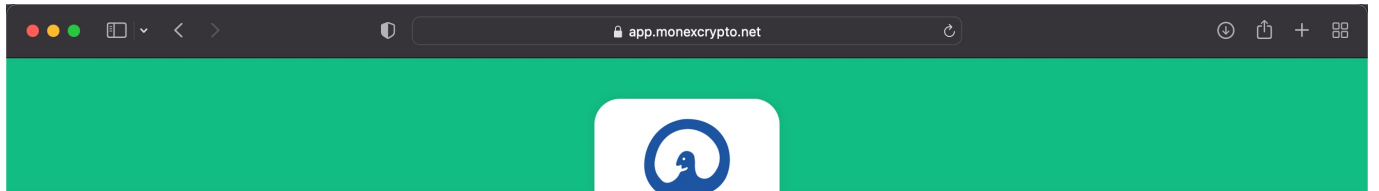
Jun 19, 2022, 12:59 AM

Kendisiyle onun çok iyi bir yatırımcı olduğunu ve onunla yatırım yapmak istediğimi paylaştıktan sonra kısa vadeli yatırım için MonexCrypto isimli

platforma girmem gerektiğini söyledi. Bunun için de [https://app\[.\]monexcrypto\[.\]net](https://app[.]monexcrypto[.]net) adresini ziyaret edip mobil uygulamayı indirip kayıt olmam gerektiğini paylaştı.



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



Developer tools interface showing the HTML structure and CSS styles for the 'download-btn' element.

HTML Structure:

```
<!DOCTYPE html>
<html lang="en">
<head>...</head>
<body>
  <div class="top-bg"></div>
  <div class="app-info">...</div>
  <a class="download-btn" onclick="btnClick();" href="/config/app.mobileconfig">Download and install</a> = $0
  
  <div class="scan-desc">Scan the QR code with the camera to download</div>
  <script src="/config/config.js"></script>
  <script src="/js/jr-qrcode.js"></script>
  <script src="/js/index.js"></script>
</body>
</html>
```

CSS Styles:

- .download-btn {** (index.css:1:555)
 - display: block;
 - width: fit-content;
 - margin: 28px auto 0;
 - padding: 0 50px;
 - line-height: 42px;
 - font-size: 18px;
 - font-weight: 400;
 - text-decoration: none;
 - color: #fff;
 - border-radius: 20px;
 - background: #157df1;
- a:any-link {** (User Agent Style Sheet)
 - color: -webkit-link;
 - text-decoration: underline;
 - cursor: auto;
- body {** (index.css:1)
 - font-family: helvetica,tahoma,arial,pingfang,sc,microsoft yahei,simsun,simhei,"sans-serif";

Box Model:

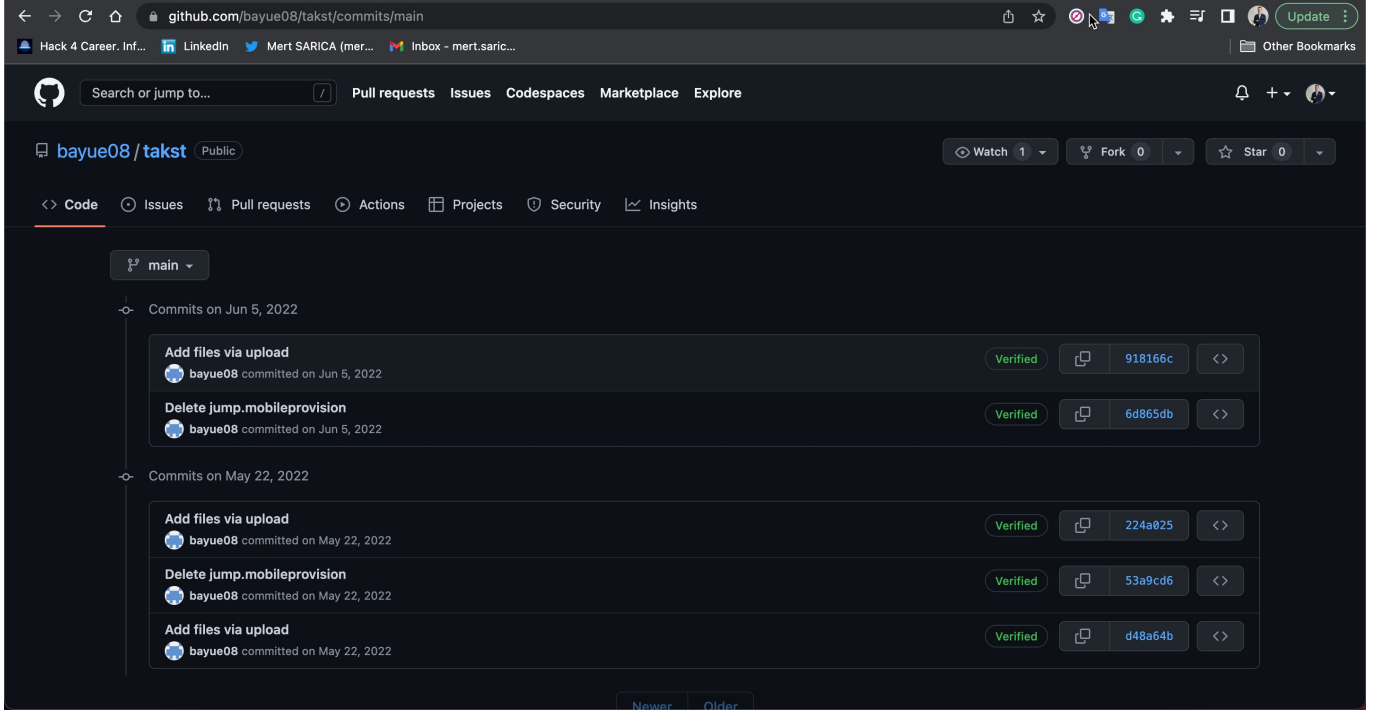
- margin: 28px auto 0 0
- padding: 0 50px
- border: 20px solid #157df1
- width: 166.11 x 42

Properties:

- webkit-font-smoothing: antialiased;
- background-attachment: scroll;
- background-clip: border-box;
- background-color: rgb(21, 125, 241);
- background-image: none;
- background-origin: padding-box;
- background-position-x: 0%;

app.monexcrypto.net/config/config.js

```
var appConfig = {
  name: '',
  ios: './config/app.mobileconfig',
  jump: 'https://github.com/bayue08/takst/raw/main/jump.mobileprovision',
  android: './download/update.apk',
};
```



3. parti uygulamaların iOS işletim sistemi üzerinde çalışmasına imkan tanıyan mobileprovision dosyasının GitHub üzerinde saklandığını gördükten sonra Apple'ın Geliştirici Programı'na kayıtlı, imza yetkisi olan yazılımcı/firma (QuanLi Network Technology Co., Ltd. (SRD7J8LLBV)) ile ilgili bilgileri görüntüledim.

wql220604

Expired 7 months ago

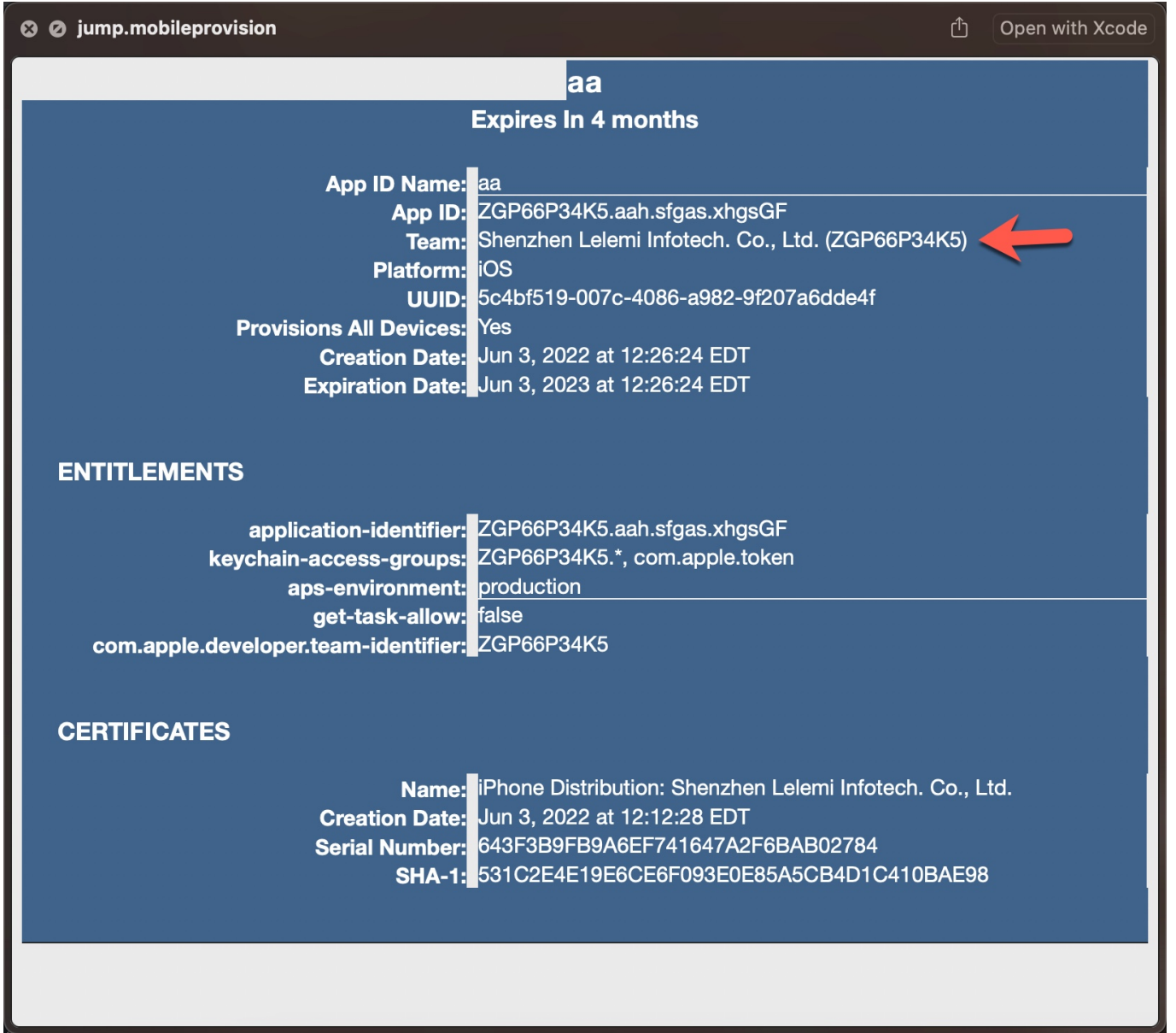
App ID Name: iosplayer
App ID: SRD7J8LLBV.com.wei quanli.iosplayer
Team: QuanLi Network Technology Co., Ltd. (SRD7J8LLBV) 
Platform: iOS
UUID: f464148a-77ac-4a72-a15e-f1ed214212f8
Provisions All Devices: Yes
Creation Date: Jun 4, 2021 at 03:02:28 EDT
Expiration Date: Jun 4, 2022 at 03:02:28 EDT

ENTITLEMENTS

keychain-access-groups: SRD7J8LLBV.*, com.apple.token
com.apple.external-accessory.wireless-configuration: true
com.apple.developer.healthkit.access: health-records
com.apple.developer.ubiquity-container-identifiers: SRD7J8LLBV.*
get-task-allow: false
com.apple.developer.default-data-protection: NSFileProtectionComplete
com.apple.developer.healthkit: true
com.apple.developer.associated-domains: *
com.apple.developer.team-identifier: SRD7J8LLBV
com.apple.security.application-groups: Unknown
application-identifier: SRD7J8LLBV.com.wei quanli.iosplayer
com.apple.developer.ubiquity-kvstore-identifier: SRD7J8LLBV.*
com.apple.developer.homekit: true

CERTIFICATES

Name: iPhone Distribution: QuanLi Network Technology Co., Ltd. 
Creation Date: Apr 9, 2020 at 10:39:23 EDT
Serial Number: 04F4A485C1B2F933
SHA-1: F4AD79B2285828A32B124AC7EB4D664013F8CCC5



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

Web klipleri: Web kupürü, aygıtın Ana Ekran'ında bir web sitesine veya URL'ye bağlantı sağlayan bir simgedir. Web klipleri isteğe bağlı olarak tam ekran web uygulamalarını başlatabilir ve HTML5 yerel saklama alanını kullanarak çevrimdışı çalışabilir. Konfigürasyon profilleri özel bir başlık ve simge kullanan ve isteğe bağlı olarak silinemez yapılabilen web klipleri içerebilir. Web klipleri, öğrencileri eğitim amacıyla belirli web sitelerine yönlendirebilir. Bir aygıttaki web kupürlerini ayarlama hakkında daha fazla bilgi için Apple Geliştirici belgelerindeki WebClip profil sayfasına bakın.



1:05



Bu web sitesi bir konfigürasyon profili
göstermek istiyor. İzin vermek
istiyor musunuz?

Yok Say

İzin Ver

p/YeniYazi/Monex/app.mobileconfig





1:06



< Genel

Aygıt Yönetimi

İNDİRİLEN PROFİL



MonexCrypto





1:06



Vazgeç

Profili Yükle

Yükle



MonexCrypto

İmzalayan iPhone Distribution: gang dai
(83A48V8PWY)

Doğrulandı ✓

İçeriyor Web Klibi

Daha Fazla Ayrıntı



İndirilen Profili Sil



1:06



< Profili Yükle MonexCrypto

WEB KLİBİ



Web Klibi

URL: <https://www.monexcrypto.net>
Etiket: MonexCrypto



İMZALAMA SERTİFİKALARI



iPhone Distribution: gang dai
(83A48V8PWY)

Sertifika Veren: Apple Worldwide
Developer Relations Certification
Authority
Bitiş: 11 Mart 2023



Apple Worldwide Developer
Relations Certification
Authority

Sertifika Veren: Apple Root CA
Bitiş: 20 Şubat 2030





1:06



< MonexCrypto Web Clip

Etiket MonexCrypto

URL <https://www.monexcrypto.net>

Silinebilir Evet

Tam Ekran Evet

Bildiri Kapsamını Göz Ardı Et Evet



1:06



iPhone Distribution: gang dai (83A48...

ÖZNE ADI

Kullanıcı Kimliği 83A48V8PWY

Genel Ad

iPhone Distribution: gang dai
(83A48V8PWY)

Kuruluş Birimi 83A48V8PWY

Kuruluş gang dai

Ülke veya Bölge CN

SERTİFİKA VERENİN ADI

Genel Ad

Apple Worldwide Developer Relations
Certification Authority

Kuruluş Birimi G3

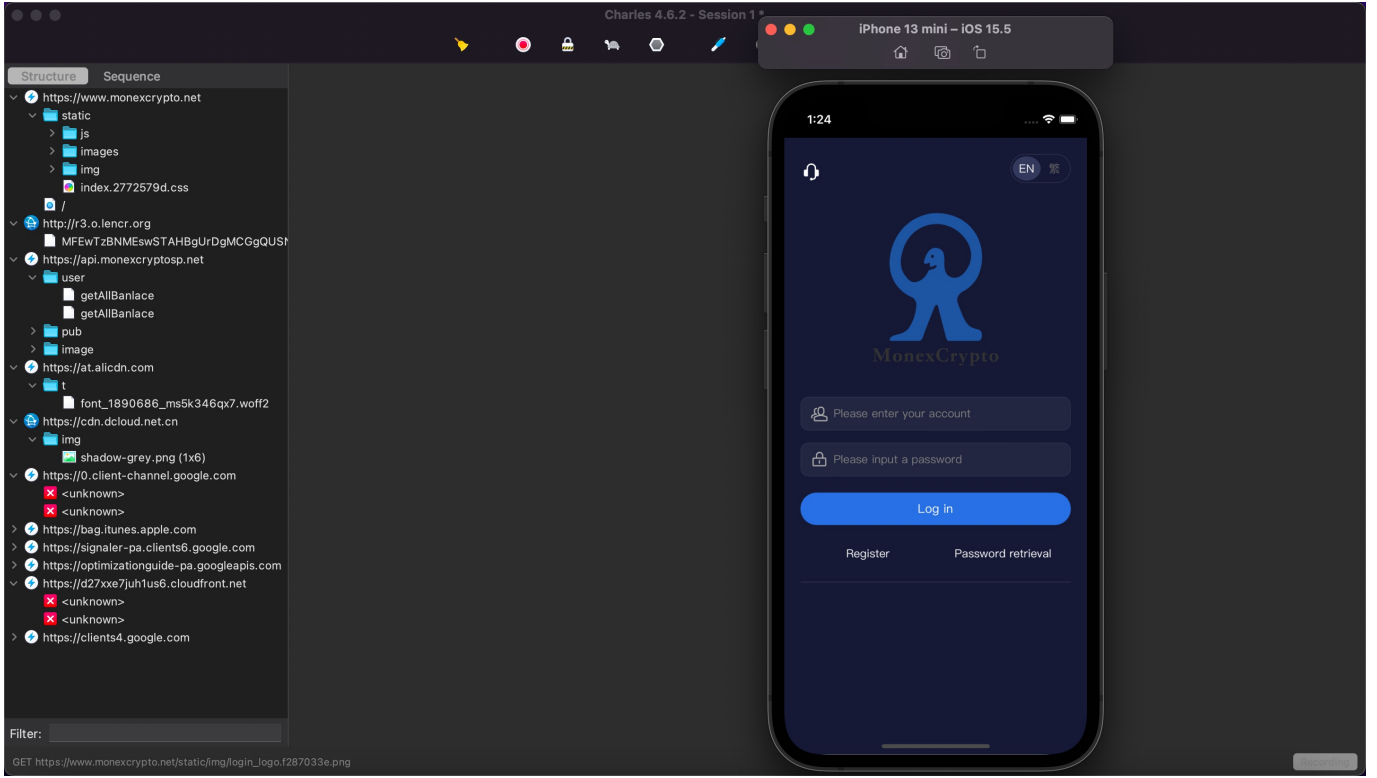
Kuruluş Apple Inc.

Ülke veya Bölge US

SERİ NUMARASI

Seri Numarası

7C 48 07 65 DE 89 A8 85 40 88 05 AF



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

Register

Phone E-mail

1 - USA Please input mobile phone number

Please input verification code

Please input a password

Please confirm password.

Please input rganization code

Submit

☒ I have read and agree 《User Agreement》

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



Anna



I can not able to install it to my iPhone, do not know why.

Jun 25, 2022, 2:39 PM

Can be installed

You may not have found the installation package.



Jun 25, 2022, 2:43 PM

It will prompt that the description file has been downloaded. After the download is completed, click Settings to see the description file and click Install.

Jun 25, 2022, 2:45 PM

Profile Downloaded >



Airplane Mode



Wi-Fi

Not Connected >



Bluetooth

On >





Anna



I have installed it.

Jun 26, 2022, 6:21 AM

I can not able to register as it asks me an organization code which I have no idea what it is

Jun 26, 2022, 7:18 AM



我找找我之前用的你可不可以用

Jun 26, 2022, 4:36 PM

Try the 768919 I used.

Jun 26, 2022, 4:39 PM

This is the organization code I used.

You try

Jun 26, 2022, 4:40 PM

It worked. Now what is next ? :)

Jun 27, 2022, 12:37 AM

Next, buy and transfer.





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



12:08

 MonexCrypto

Everyone is looking forward
to the shining debut

**MonexCrypto mining pool is newly
launched**

 BTC/USDT

21481.13

+0.49%

 ETH/USDT

1252.59

+2.77%

 NEO/USDT

10

+2.35%

Quick recharge

Support BTC, USDT,
ETH and etc.



Contract transac...



New purchase



USDT Flexible earnings

DEPOSIT ANYTIME, TAKE ANYTIME
DAILY SETTLEMENT OF EARNINGS

Rising rank

Transaction rank

Name

Latest price

Rising rank



TES/ USDT

1.7178

+11.04%



TradeZone



Pool



Futures

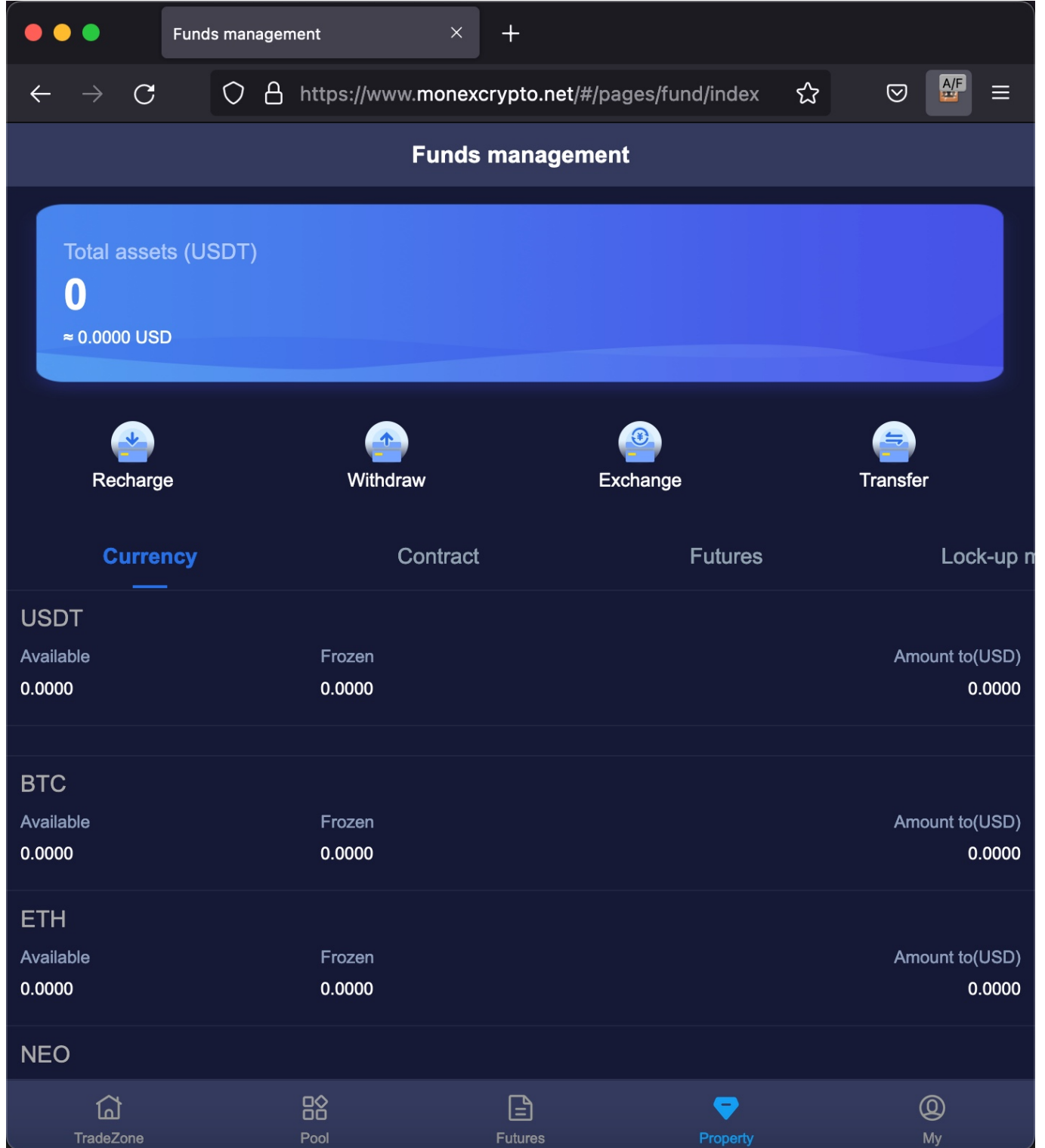


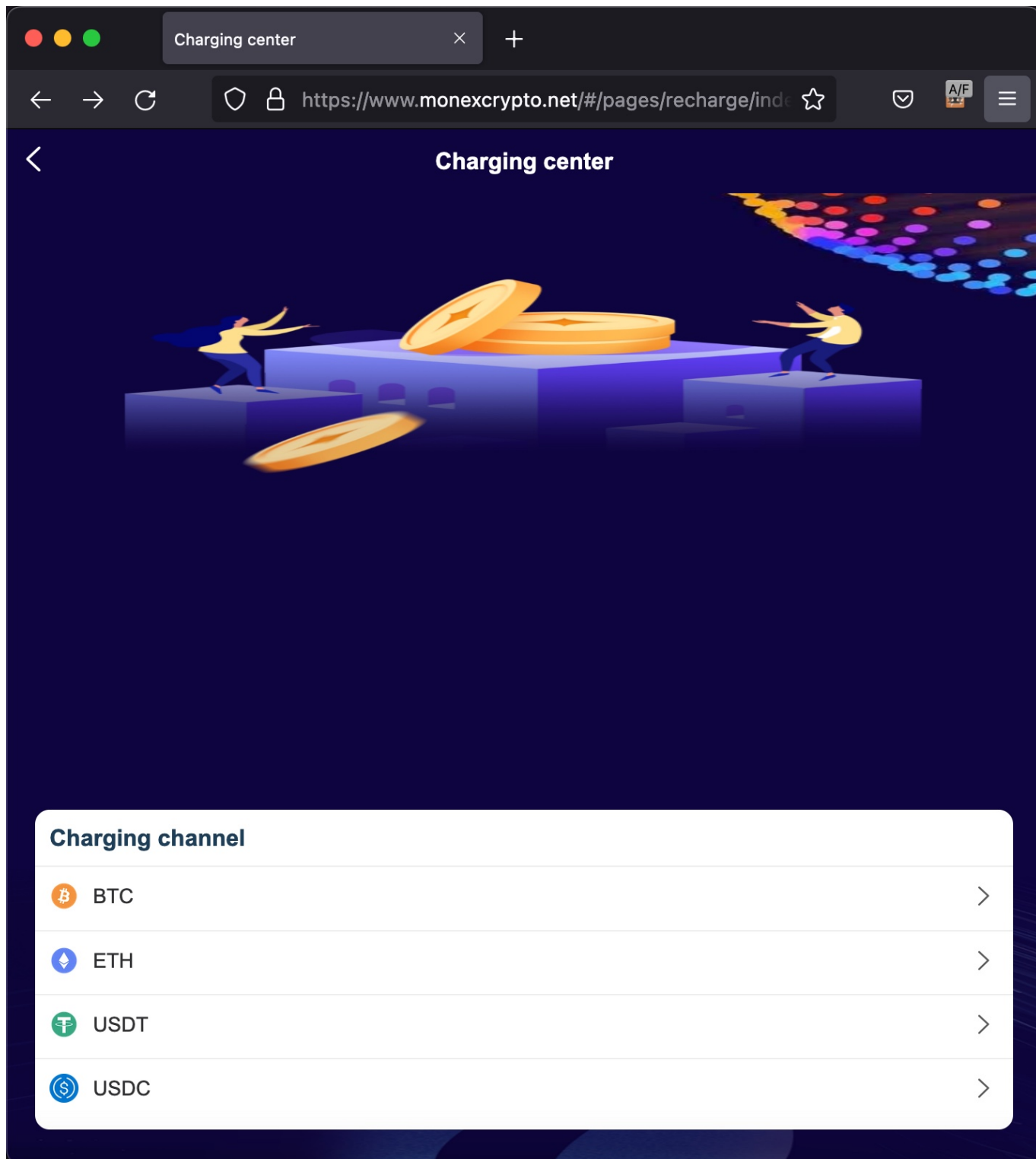
Property

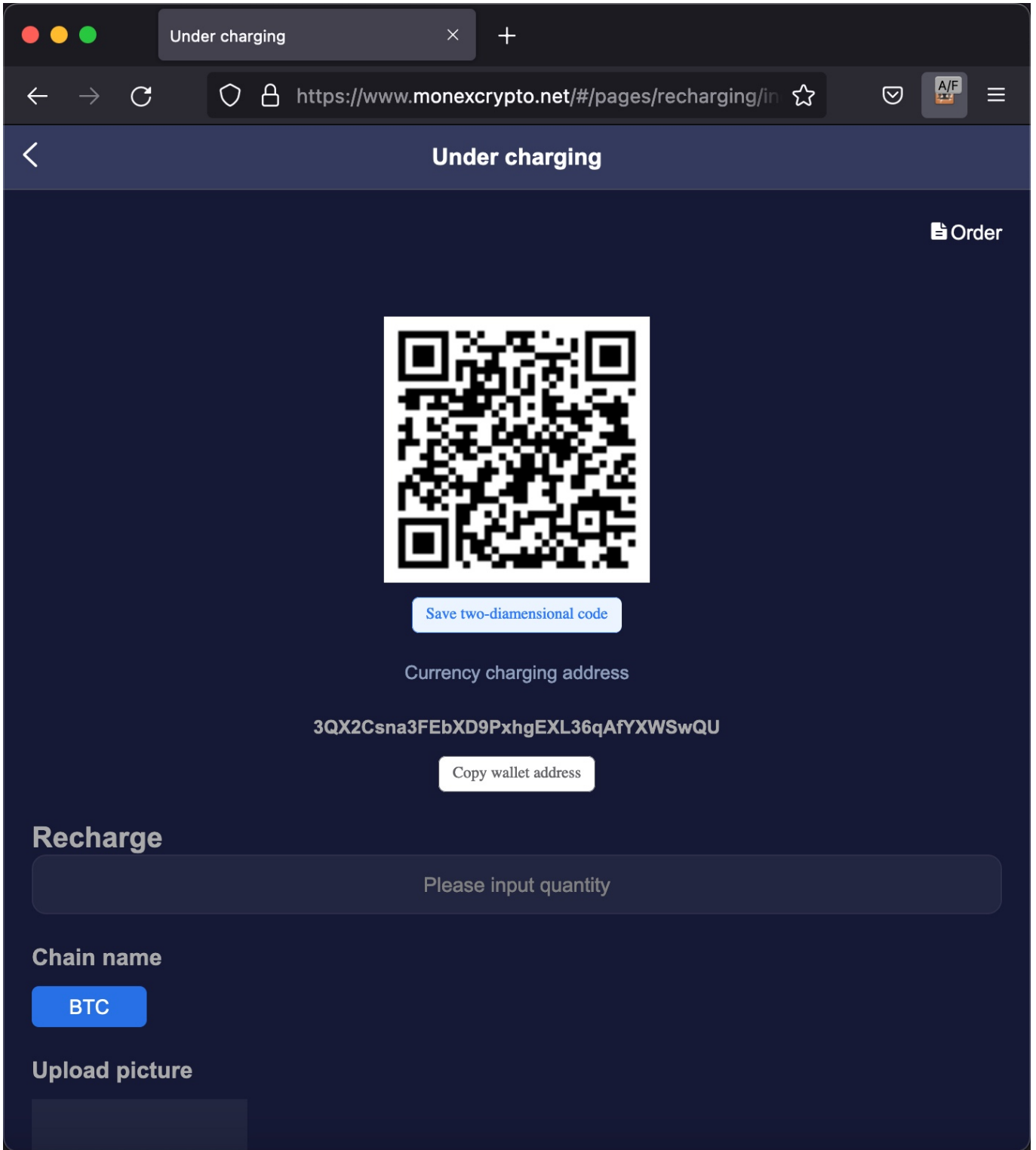


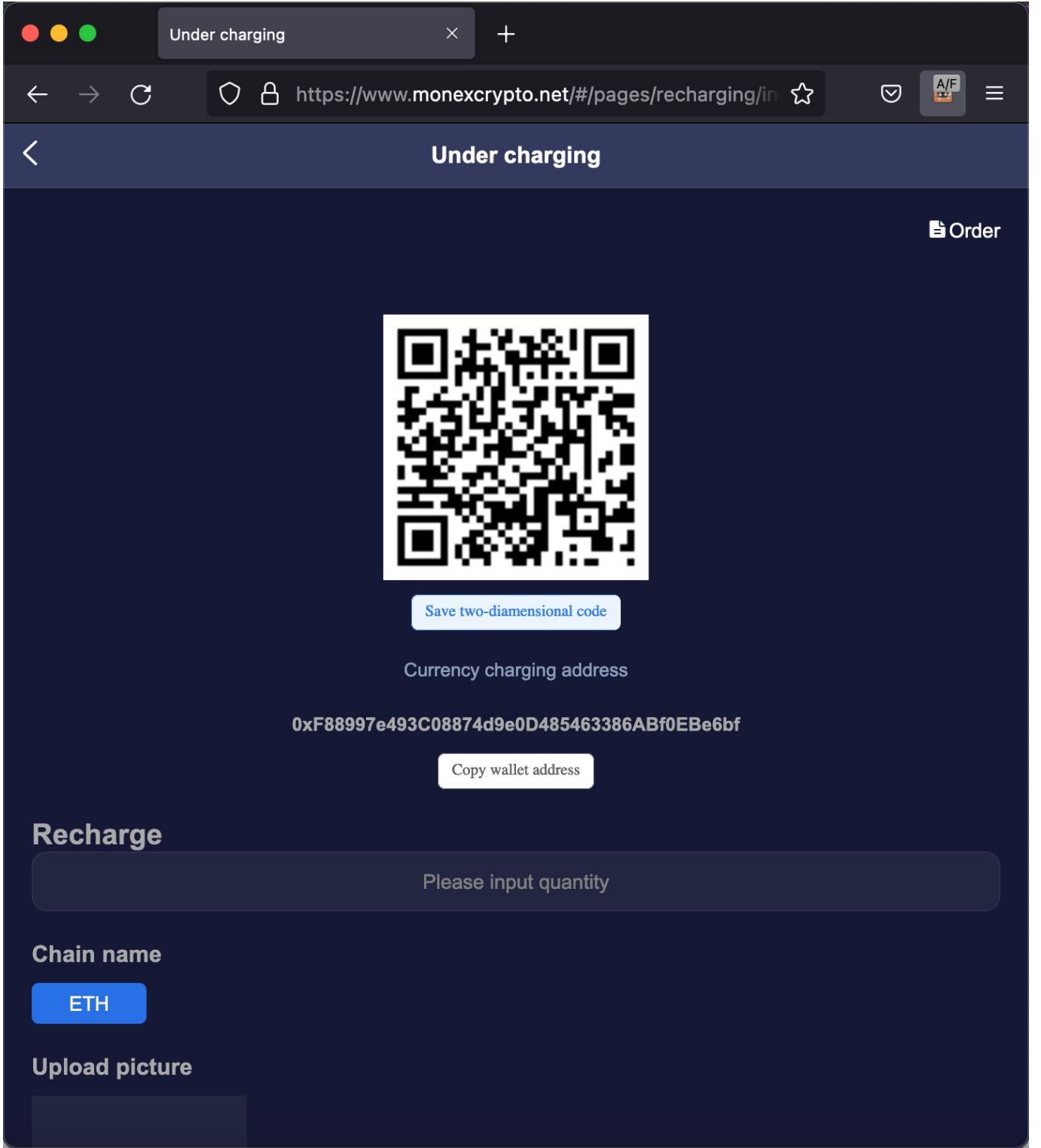
My

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









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



Anna



If you are herebinancel you have coins, you don't need to buy them. You just need to convert them into USDT and transfer them.

Jun 28, 2022, 12:43 PM

Direct purchase is also possible, but then it needs to be purchased by wire transfer. The minimum purchase amount is \$3,000, and it will be more convenient to purchase and transfer with the traditional exchange.

I usually do the same thing, and then transfer back to the traditional exchange after the transaction.

Jun 28, 2022, 12:49 PM

Where is my USDT wallet address I cant find it.

Jun 28, 2022, 1:31 PM

Give me a screenshot.

I'll show you how to find him.

Jun 28, 2022, 1:45 PM

Just give me the screenshot of the main page of the exchange.



Anna



Click on it and give me a screenshot.

I'll teach you the next step

Jun 28, 2022, 2:08 PM

Order



Save two-dimensional code

Currency charging address

0xF88997e493C08874d9e0D485463386ABf0EB6bf

Copy wallet address

Recharge

Please input quantity

Chain name

ERC20 TRC20

Upload picture

Jun 28, 2022, 2:21 PM

Order



0xF88997e493C08874d9e0D485463386ABf0EB6bf

Copy wallet address

Recharge

Please input quantity

Chain name

ERC20 TRC20

Upload picture

Copy wallet address

Jun 28, 2022, 2:26 PM

Got it.

Jun 28, 2022, 2:27 PM

Then open your Binanc screenshot and send it to me,
I will teach you how to transfer the injected funds

How much money do you plan to start investing?

Jun 28, 2022, 2:29 PM



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

Anna, paylaştığım 3 tane bit.ly adresine tıklamaktan zerre kadar imtina etmediği için SOCRadar IOC Radar üzerinden kısa sürede Hong Kong'da yer alan 45.204.66.140 IP adresinden benimle iletişim kurduğunu öğrenmiş oldum.



Anna



That is a bit complicated, let me share the screenshots with you.

Jul 2, 2022, 1:15 PM

okay

Let's start with the transfer.

Jul 2, 2022, 1:18 PM

You openbinanceGive me a screenshot of the homepage and I'll tell you what you should do.

Jul 2, 2022, 1:20 PM

is this the address of USDT wallet that I have to send from Binance ? [bit.ly/](#)

Jul 2, 2022, 1:29 PM

Yes

Jul 2, 2022, 1:34 PM

After copying, open Binance to find the transfer, then paste the wallet address you copied and transfer it.

After successful transfer, go back to the short-term exchange and upload the certificate of successful transfer.

You can start trading.

Jul 2, 2022, 1:37 PM

If you have any questions, please take screenshots and ask me.

Jul 2, 2022, 1:38 PM

After the transfer, I ll see the amount of the USDT on this area, is that correct ? [bit.ly/](#)

Jul 2, 2022, 1:43 PM

Yes

Jul 2, 2022, 1:44 PM

If you want to finish it in a few minutes

You can take a screenshot for me.

After all, it's your first time, and I'm afraid you'll make a mistake during the transfer.

Jul 2, 2022, 1:48 PM

At Binance, this is where I should buy USDT ? [bit.ly/](#)

Jul 2, 2022, 1:55 PM

:o)

Why is your screenshot like this?

45.204.66.140 - [02/Jul/2022:17:32:55 +0000] "GET /images/wallet1.jpg HTTP/1.1" 200 116233 "https://t.co/..." "Mozilla/5.0 (iPhone; CPU iPhone OS 14_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/15E148 Safari/604.1"

45.204.66.140 - [02/Jul/2022:17:56:40 +0000] "GET /images/wallet3.jpg HTTP/1.1" 200 464081 "https://t.co/..." "Mozilla/5.0 (iPhone; CPU iPhone OS 14_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/15E148 Safari/604.1"

45.204.66.140 - [02/Jul/2022:17:57:27 +0000] "GET /images/wallet3.jpg HTTP/1.1" 304 183 "https://t.co/..." "Mozilla/5.0 (iPhone; CPU iPhone OS 14_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/15E148 Safari/604.1"

45.204.66.140 - [02/Jul/2022:17:59:28 +0000] "GET /images/wallet3.jpg HTTP/1.1" 200 464081 "https://t.co/..." "Mozilla/5.0 (iPhone; CPU iPhone OS 14_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/15E148 Safari/604.1"

SOCradar LABS

Dark Web Report

Threat Intel Snapshot Report

External Attack Surface

IOC Radar Results

45.204.66.140

Details **Completed**

ASN: 132513

Name: SKYTELLAO-AS-AP Sky Telecom State Compan...

Description: MU

Country Code: HK

Subnet: 45.204.66.0/24

RAW: 45.204.66.0 - 45.204.66.255 aaof_data.internati...

Latitude: 22.28552

Longitude: 114.15769

Country Code: HK

Region Name: Hong Kong

SOCradar

Threat intelligence. Extended.

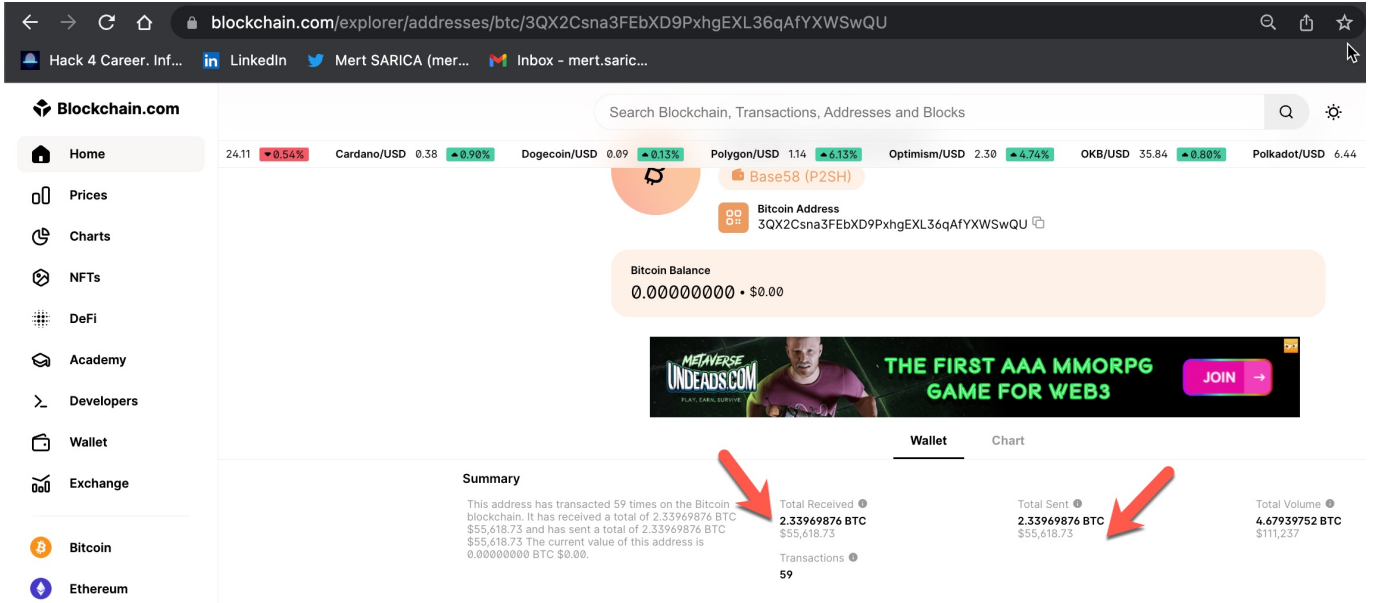
We empower you to know the unknowns.

REQUEST DEMO **FREE ACCESS**

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

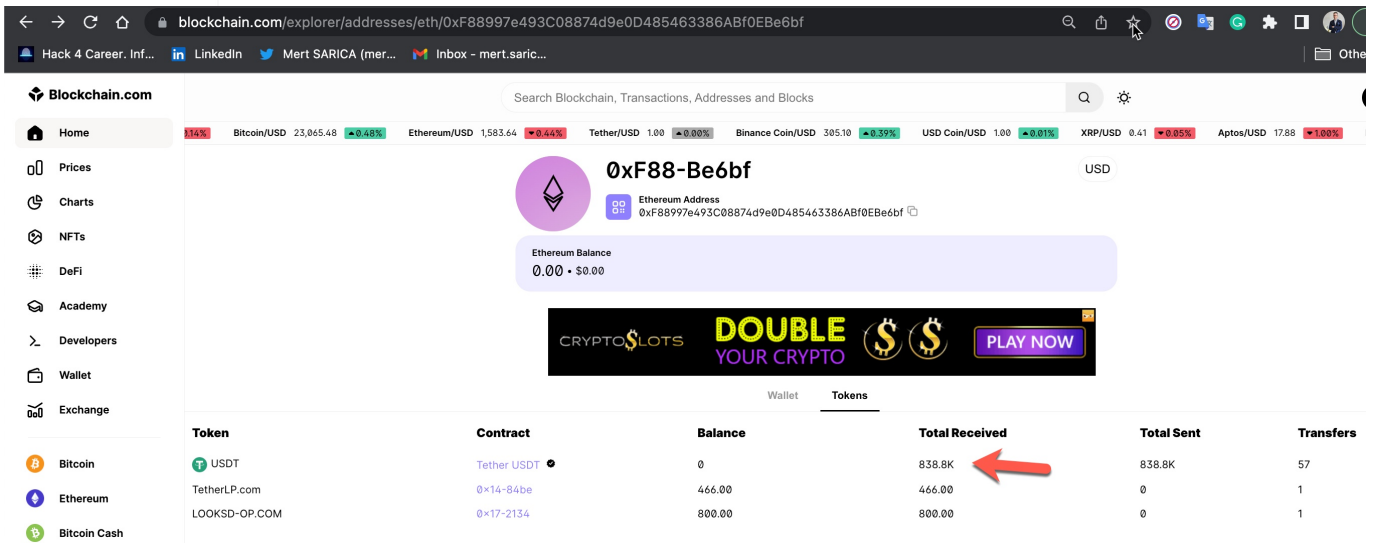
1. 28 Haziran 2022 tarihinde Bitcoin cüzdan adresimi (3QX2Csna3FEbXD9PxbhgEXL36qAfYXWSwQU) Blockchain.com web sitesi üzerinde sorguladığımda, bu cüzdanın 6 Haziran 2022 tarihinde oluşturulduğu ve 29 Eylül 2022 tarihine dek bu cüzdana 55,618.73\$ değerinde Bitcoin aktarıldığı ve daha sonrasında çekildiği görülmüyordu.
2. Aynı tarihte Ethereum cüzdan adresimi (0xF88997e493C08874d9e0D485463386ABf0EBE6bf) aynı yerde sorguladığımda bu cüzdanın da 26 Haziran 2022 tarihinde oluşturulduğu ve 23 Kasım 2022 tarihine dek bu cüzdana ~839.000\$ değerinde Ethereum ve USDT aktarıldığı görülmüyordu.
3. Yine aynı tarihte bu defa USDC cüzdan adresimi (0xcfd9df006ec9f4af5bf34a6f71af41655fb7d4167) sorguladığımda bu cüzdanın 17 Haziran 2022 tarihinde oluşturulduğu ve 16 Ağustos 2022 tarihine dek bu cüzdana da ~46.000\$ değerinde Ethereum ve USDT aktarıldığı görülmüyordu.

Blockchain.com explorer showing Bitcoin address: 3QX2Csa3FEbXD9PxbgEXL36qAFYXWswQU. The address has a balance of 0.00000000 BTC and \$0.00. The summary shows 59 transactions, with a total received of 2.33969876 BTC (\$55,618.73) and a total sent of 2.33969876 BTC (\$55,618.73). The total volume is 4.67939752 BTC (\$111,237).



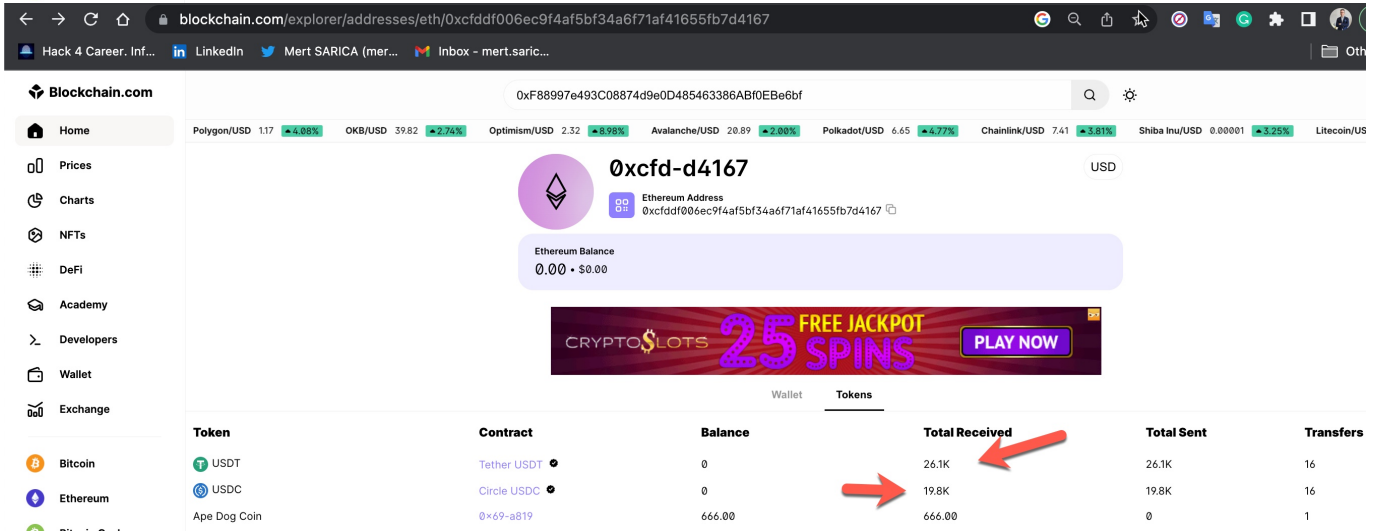
Blockchain.com explorer showing Ethereum address: 0xF88997e493C08874d9e0D485463386ABf0EB6bf. The address has a balance of 0.00 ETH and \$0.00. The tokens table shows the following data:

Token	Contract	Balance	Total Received	Total Sent	Transfers
USDT	Tether USD	0	838.8K	838.8K	57
TetherLP.com	0x14-84be	466.00	466.00	0	1
LOOKSD-OP.COM	0x17-2134	800.00	800.00	0	1



Blockchain.com explorer showing Ethereum address: 0xcfd-d4167. The address has a balance of 0.00 ETH and \$0.00. The tokens table shows the following data:

Token	Contract	Balance	Total Received	Total Sent	Transfers
USDT	Tether USD	0	26.1K	26.1K	16
USDC	Circle USDC	0	19.8K	19.8K	16
Ape Dog Coin	0x69-a819	666.00	666.00	0	1



Feragatname: Herhangi bir hataya karşı Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency kitabında olduğu gibi uçtan uca kripto para transferlerini takip edebilecek bir IRS ajanı veya Blockchain uzmanı olmadığımı hatırlatmış olayım. :)

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

A	B	C
Blockchain Type	Wallet Address	~Stolen Amount (USD)
Bitcoin	3QX2Csna3FEbXD9PxbgEXL36qAfYXWSwQU	\$55,618.73
Ethereum	0xF88997e493C08874d9e0D485463386ABf0EBE6bf	\$818,800.00
Ethereum	0xCFDDF006EC9F4AF5BF34A6F71AF41655FB7D4167	\$46,000.00
Ethereum	0x392667b0CDf9B04Ce5C48754Ea4185056A65DD31	\$246,000.00
Ethereum	0x66FD1C86ae25BDd278bb90f1174f668392EBB540	\$675,000.00
Ethereum	0xA9434DFb0fa3f29fc6324AA60DB377C863022f13	\$204,000.00
Ethereum	0xC495928233A6E4433c151B7A552e34A3d7Af54D7	\$564,000.00
Ethereum	0xaE7A6F74c09BDB3E1e17e51040C070A65ACf7859	\$134,000.00
	Total Stolen Amount (USD)	\$2,743,418.73

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

2021 yılında FBI'nın İnternet Suçları Şikayet Merkezi'ne bu dolandırıcılık yöntemiyle ilgili olarak 4.300'den fazla başvuru yapılmış ve toplamda 429 milyon dolardan fazla kayıp yaşanmıştır. Kasım ayının sonunda ise ABD Adalet Bakanlığı, 2022 yılında dolandırıcılar tarafından kullanılan yedi alan adına el koyduğunu açıkladı. (Kaynak: Wired)

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



Anna



Haven't you finished your authentication yet?

Jul 5, 2022, 12:41 PM

Not yet. :/

I am on vacation, do it on next week.

Jul 6, 2022, 1:50 AM

awfully sorry

I can't understand.

Jul 6, 2022, 7:33 AM

Why do people always have the habit of procrastinating about such little things? It's justIt's just verification. You can be ready.

I can't understand why things that can be done in a few minutes should be delayed.

Jul 6, 2022, 7:35 AM

What is wrong 1 week ?

Jul 6, 2022, 7:35 AM





Anna



It's nothing

Jul 6, 2022, 11:30 AM

I just don't understand why such simple things have to be delayed.

Isn't it best to do such a thing when you have a rest?

Sorry, Maybe it's because I don't like to procrastinate, and I can't understand such things.

People always like to put off the simplest things until the end.

Jul 6, 2022, 11:33 AM

Don't invest in cryptocurrency, I thought you weren't suitable for it. You can't even do such a simple thing well.

Enjoy your vacation, sir,

Jul 6, 2022, 11:35 AM

After a period of conversation, I feel that you are not suitable for investing in cryptocurrency. You always procrastinate when you can't even do such a simple thing well. I don't like people who procrastinate. Maybe





Anna



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

Jul 6, 2022, 11:42 AM

Sorry to hear that

Jul 6, 2022, 2:30 PM

You can study it yourself.

Or find someone else to teach you.

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

Jul 6, 2022, 2:33 PM

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

Jul 6, 2022, 2:49 PM

How do you do ?

Jul 22, 2022, 10:28 AM

hello

What's the matter?

Aug 1, 2022, 11:58 AM



bleepingcomputer.com

FBI warns of fake cryptocurrency apps used to defraud investors

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

Have you read this article ?

Aug 1, 2022, 2:53 PM

What is this?

Aug 8, 2022, 9:10 PM

Read and tell me that is it familiar to you ? ;)

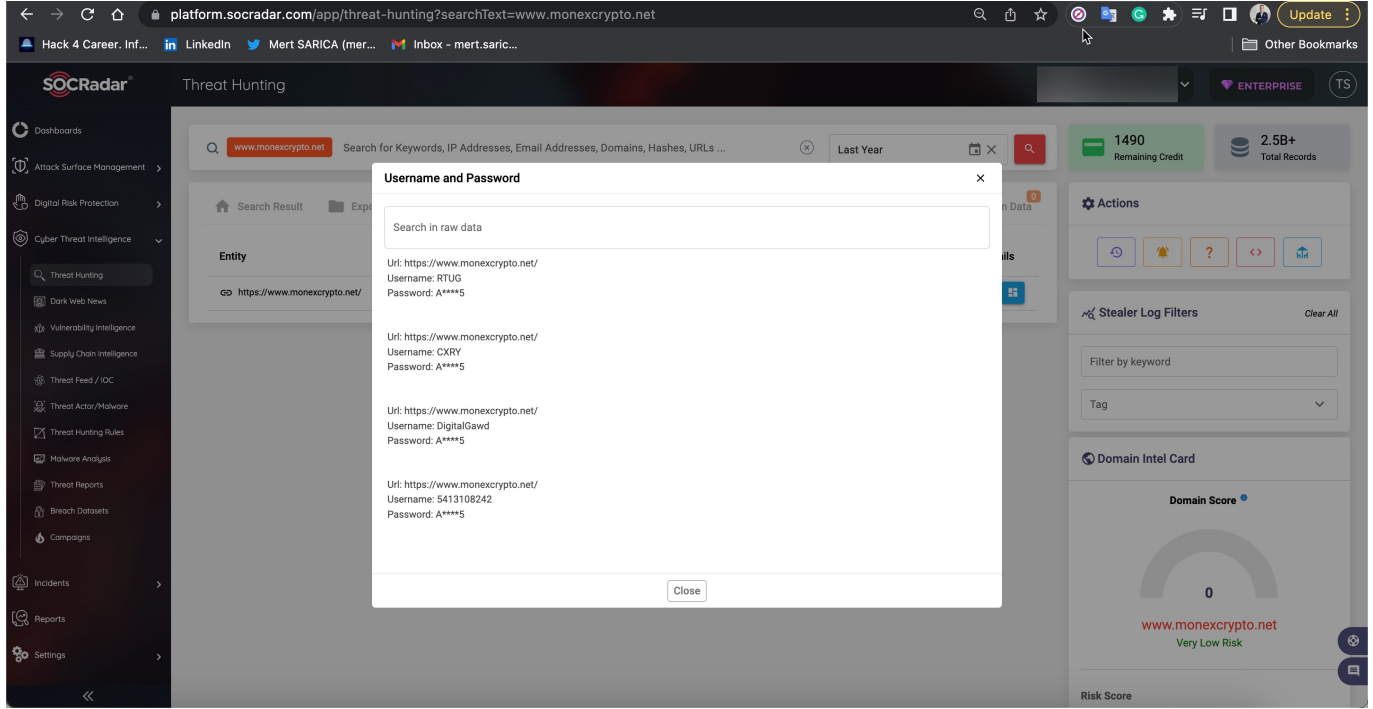
Aug 9, 2022, 12:16 AM

never heard

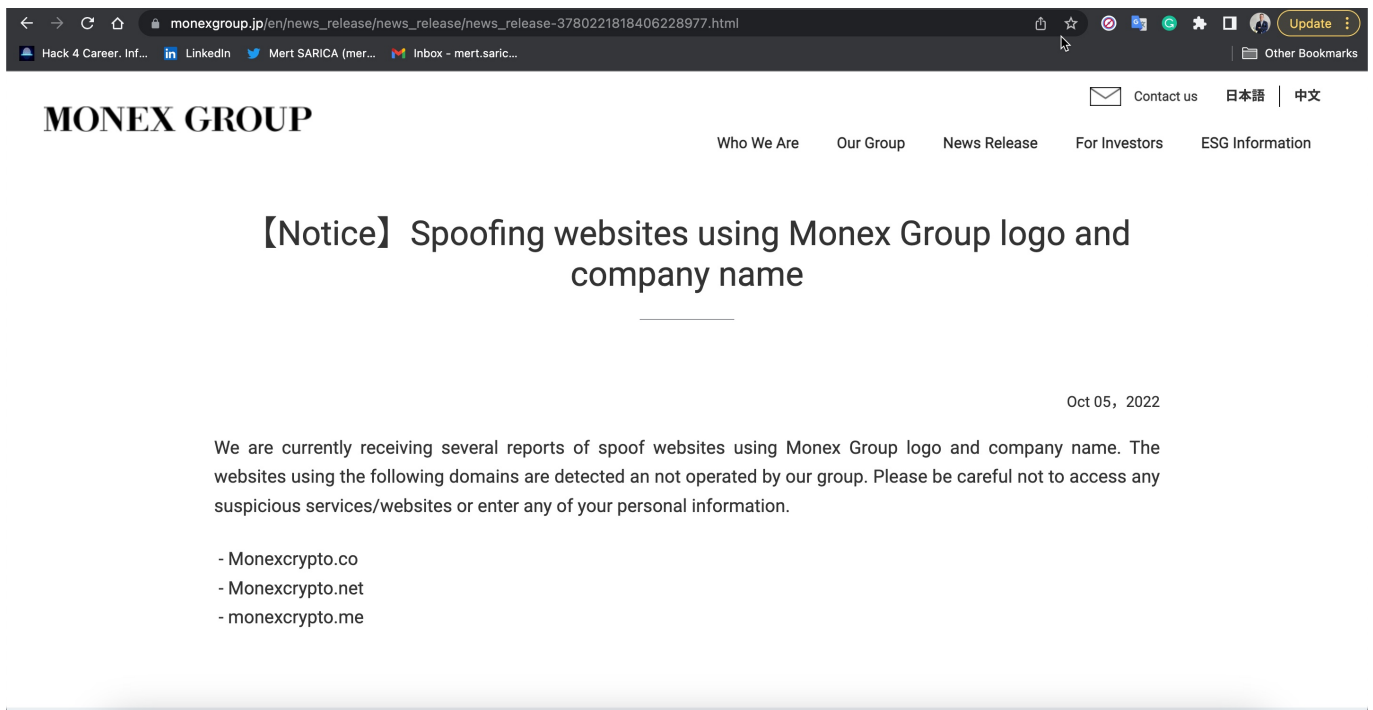
Aug 9, 2022, 12:41 PM



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



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



Sonuç itibariyle Anna ve klavye arkadaşlarının Pig Butchering Scam adı verilen, iyi kurguladıkları bu dolandırıcılık yöntemi ile nasıl milyonlarca dolar vurgun yaptıklarını, Apple App Store ve Google Play Store'dan indirdiğimiz uygulamalardan, sosyal medya üzerinden gelen mesajlara kadar neden çok dikkat etmemiz gerektiğini diğer yazılarımda da olduğu üzere detaylı bir şekilde öğrenmiş olduk.

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