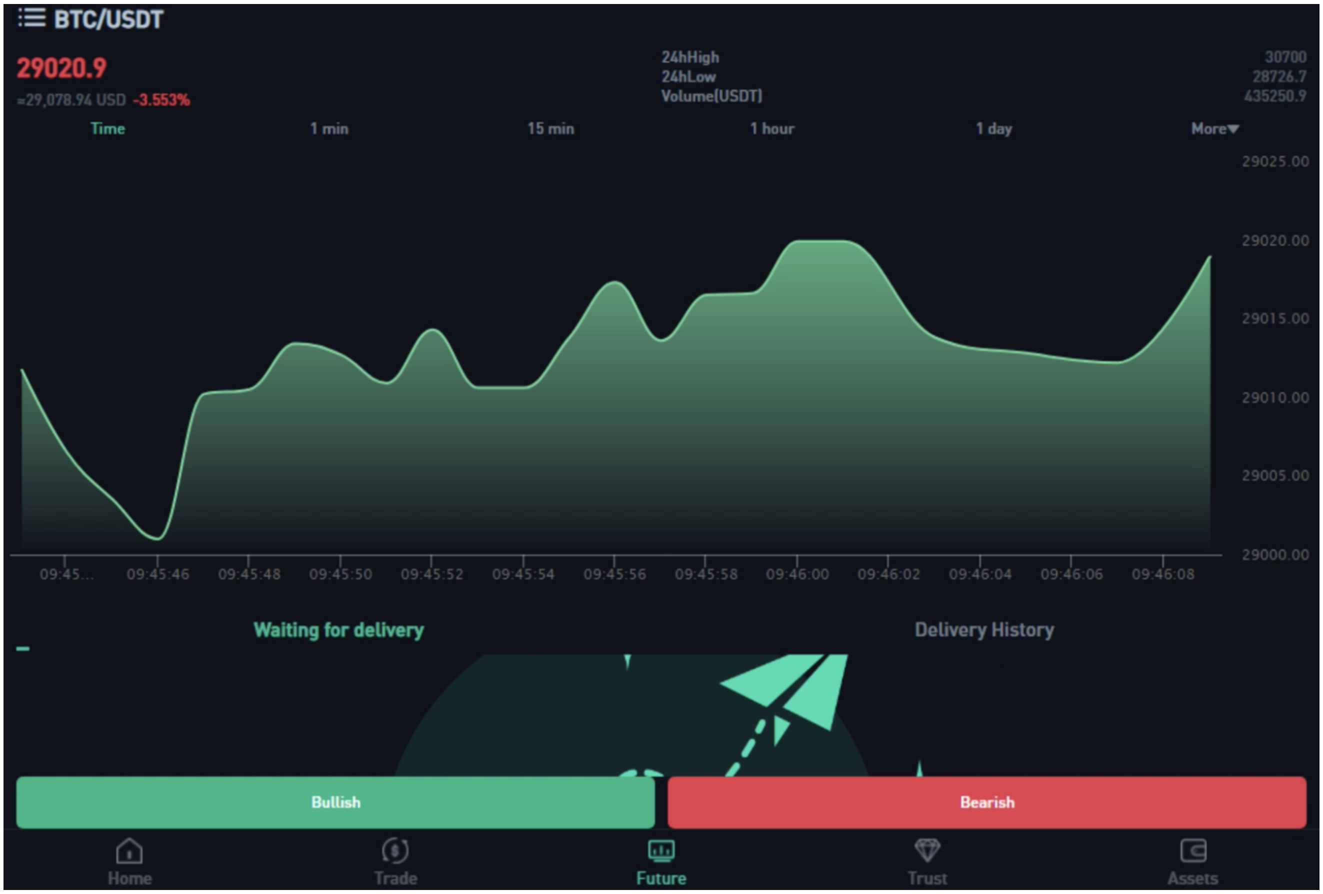
Fake Trading Apps

silentpush.com/blog/fake-trading-apps

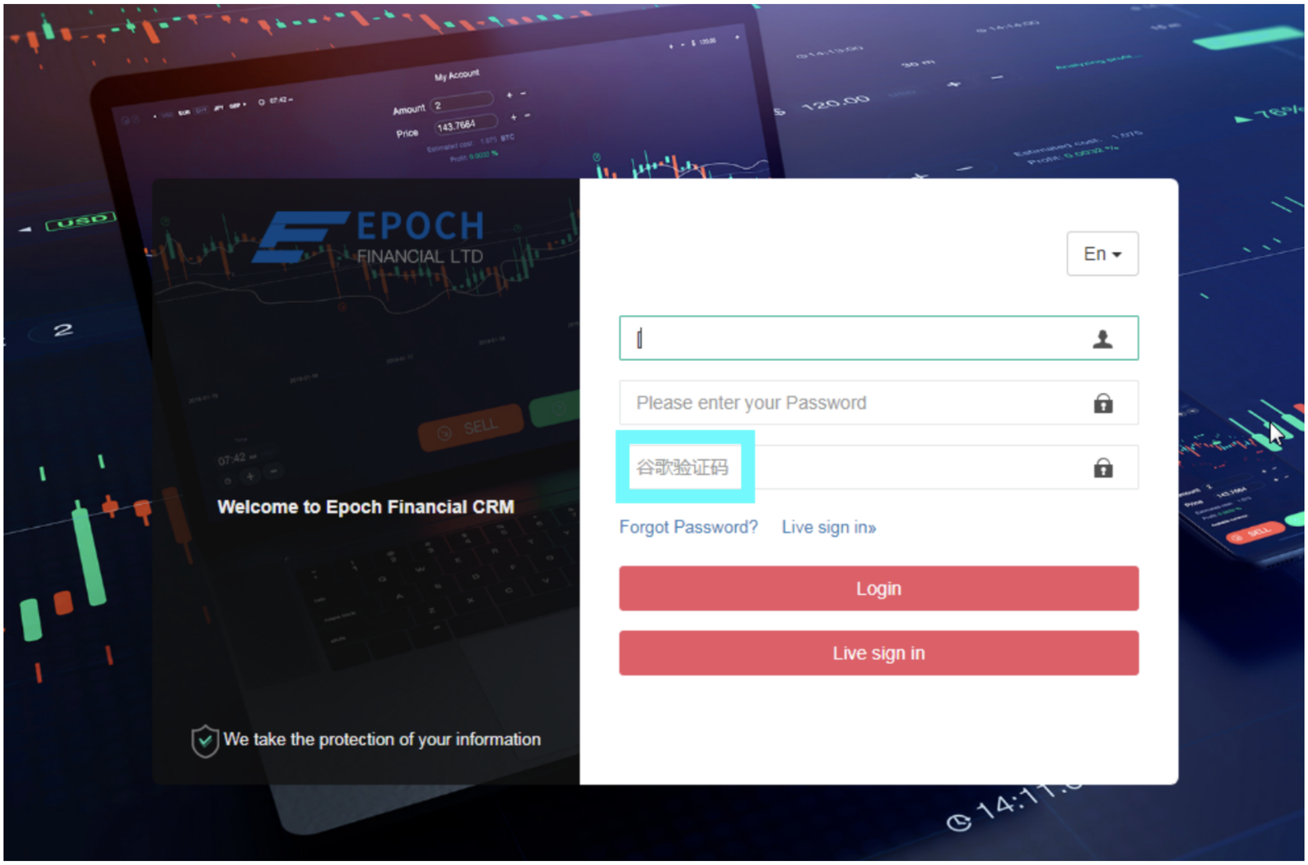
May 23, 2022



May 23
Written By Ken Bagnall

There is a very persistant fake mobile trading apps scam going on currently. This scam has been building in popularity for some time. It is spreading to a wider global victim base than before. A lot of money has been stolen from victims all over the world. In just Crypto scams the 2021 figure was over $7billion , however this scam includes more traditional trading plaforms as well.

We will give the full details in this article and information on how to spot these fraudsters. There are a very large number of spoofed trading platforms involved in this scam. It involves both main stream regulated platforms like the worlds largest financial exchanges and reaches all the way down to very new crypto exchanges. The following report is provided by The Silent Push Labs team.


EPOCH
FINANCIAL LTD
Welcome to Epoch Financial CRM
We take the protection of your information
En
Please enter your Password
谷歌验证码
Forgot Password?
Live sign in»
Login
Live sign in

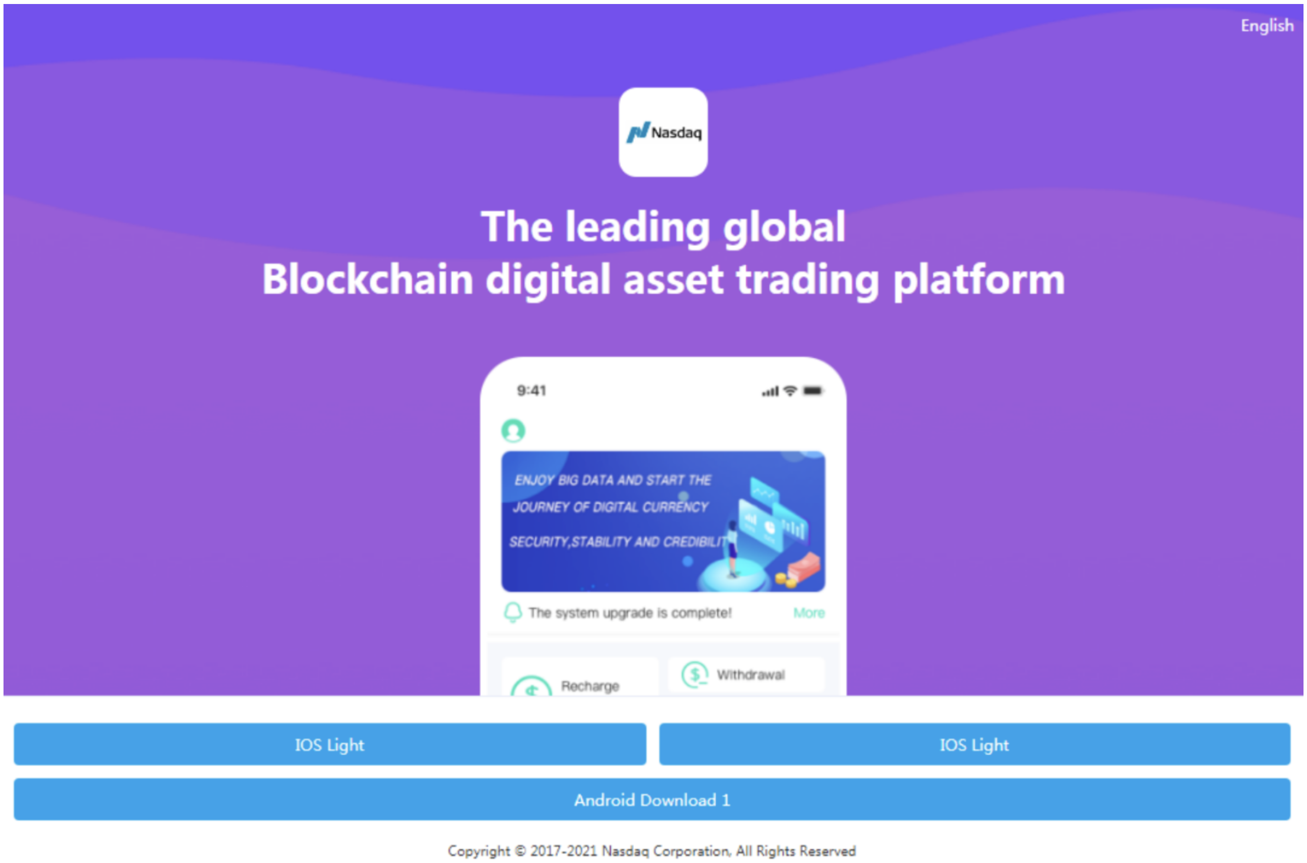
This is a fake trading platform pretending to be the legitimate platform Epoch Financial

Outline

The Silent Push Labs team uncovered a threat actor launching several websites, Android and iOS applications with **counterfeit versions of trading platforms,** targeting not only regular stock based fintech companies but also cryptocurrency focused ones.
These meticulously designed fake platforms which mimic well known financial organizations such as *Australian Securities Exchange (ASX), AvaTrade, Bolsas y Mercados Españoles, Coinbase, CoinSmart, eToro, Eurex, itBitTradingView, Nasdaq, Rakuten Wallet, Saxo Bank, Timex Trading,* among others, purposely lure unsuspecting victims into trusting their services, only to **steal their investments.**

This group has scammed and stolen money from countless individuals worldwide.

Therefore, we have conducted a large investigation on this malicious actor, collecting hundreds of Indicators of Compromise, as well as reports from victims which allowed us to map their infrastructure and trace a profile on the course of their actions.



The leading global
Blockchain digital asset trading platform

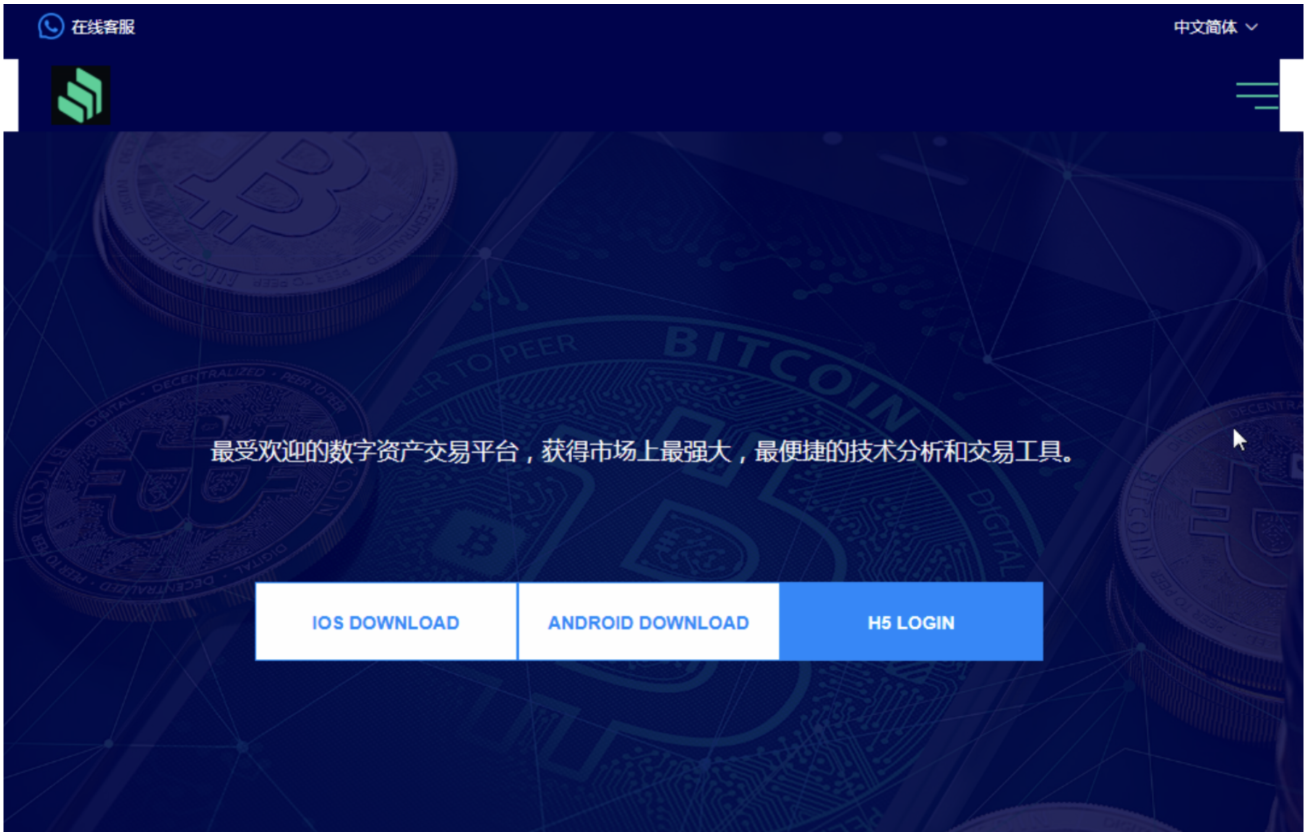
9:41
ENJOY BIG DATA AND START THE
JOURNEY OF DIGITAL CURRENCY
SECURITY,STABILITY AND CREDIBILIT
The system upgrade is complete!
More
Recharge
Withdrawal
IOS Light
IOS Light
Android Download 1

Copyright © 2017-2021 Nasdaq Corporation, All Rights Reserved

Example of a spoofed Nasdaq application download page- image 1

Threat actor profile and history

Although, we are unable to pin-point a date when this threat actor began its activity, we found that several active items of this malicious infrastructure were deployed in **early 2021.** Additionally, we had access to reports which described several occurrences with similar characteristics to this group **around that time period.** Given that these victims were **located on Asian countries** and that we found a small number of websites written in **Asian dialects**, we are compelled to claim that this threat actor is located in Asia.
On the other hand and after analyzing their current infrastructure, we consider that **American and European organizations and users are currently at the most risk.**



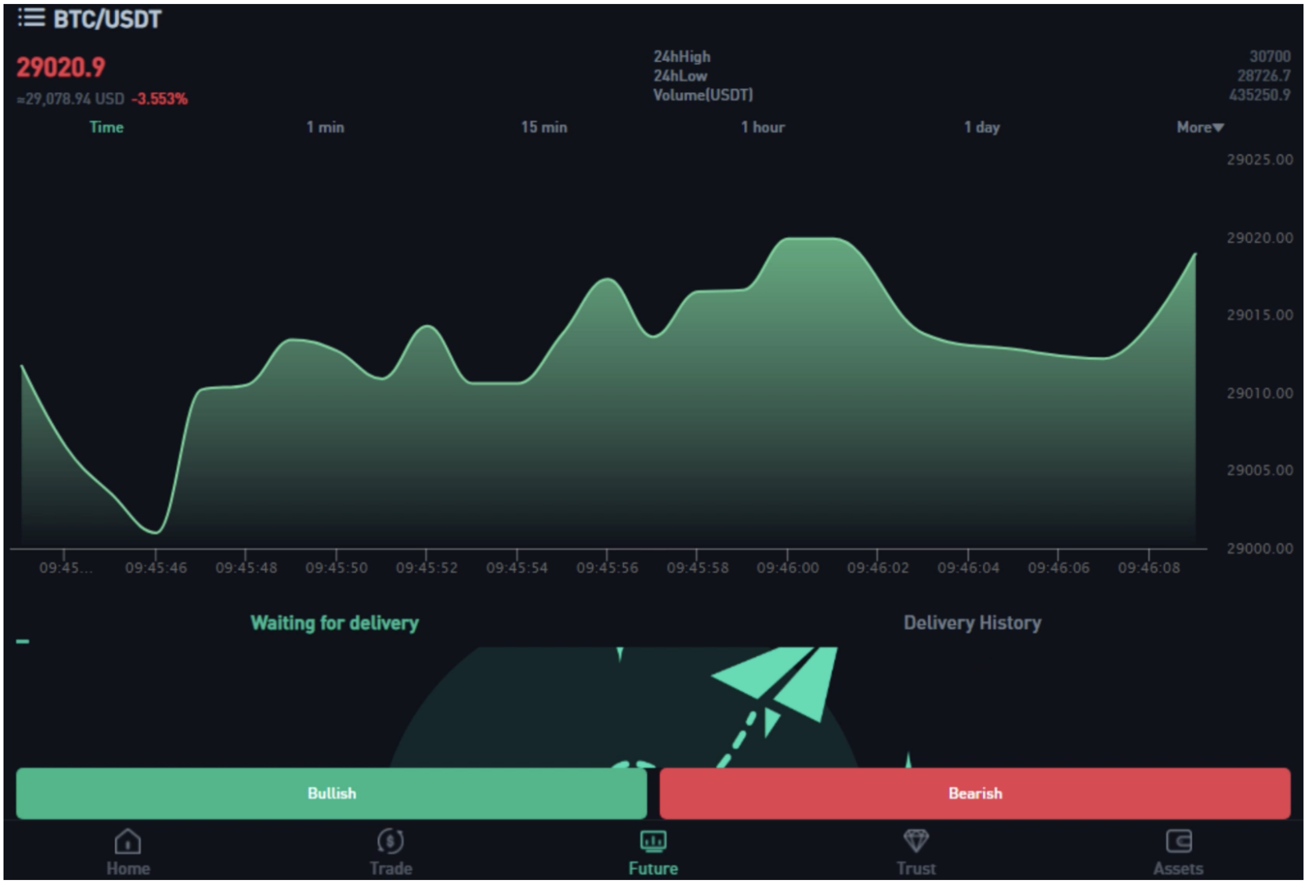
最受欢迎的数字资产交易平台，获得市场上最强大，最便捷的技术分析和交易工具。

Chinese version of a fake trading platform spoofing a known brand

Platform design -brandable kit

While navigating throughout this malicious infrastructure, an **evident visual pattern** emerged amongst the websites we investigated. Despite having a particular name and logo, the pages unfold in the same style: there is an initial website similar to the one displayed on *Image 5*, which is used as an initial landing page to attract possible victims. From this website, one can navigate to one of the following two pages:
- the app download page, similar to the one displayed on *Image 1;*
- or the website login page, where users can register and login into an account. We believe that this is a web version alternative to the app, which allows the users to transact funds and analyze fake stock indexes as can be seen on *Image 3.*

This fits into the Crime-as-a-service model with the fraudulent platform being distributed by different affiliate providers.

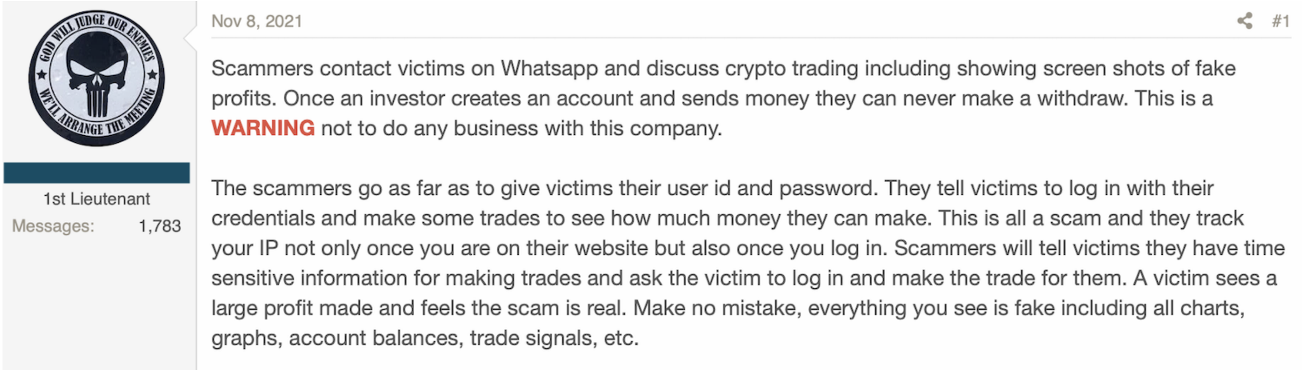


Example fake trading app content- image 3

Victims' reports

We **found many complaints concerning this malicious agent** surfacing on the internet. As suspected, the majority of them were **written by scammed individuals** but also by people who wish to take down this organization.

Initial interactions with the threat actors vary due to a possible affiliate scheme. We have seen varying reports from Romance Scams (hence Sophos referring to this as Cryptorom) to Forum recommendations**. Whatever the initial introduction and resulting conversation the victim eventually puts money into the fake account.** Unfortunately, once the victim tries to withdrawal the money, they see themselves logged out of their account and unable to log in, while the threat actors keep their funds and plan the next target.
We found similar messages on various websites as well as announcements from some fintechs reporting this robbery scheme.



1st Lieutenant
Messages: 1,783

Nov 8, 2021 #1

Scammers contact victims on Whatsapp and discuss crypto trading including showing screen shots of fake profits. Once an investor creates an account and sends money they can never make a withdraw. This is a **WARNING** not to do any business with this company.

The scammers go as far as to give victims their user id and password. They tell victims to log in with their credentials and make some trades to see how much money they can make. This is all a scam and they track your IP not only once you are on their website but also once you log in. Scammers will tell victims they have time sensitive information for making trades and ask the victim to log in and make the trade for them. A victim sees a large profit made and feels the scam is real. Make no mistake, everything you see is fake including all charts, graphs, account balances, trade signals, etc.

Messages concerning one of the distributions of this scam on the Forexpeacearmy website

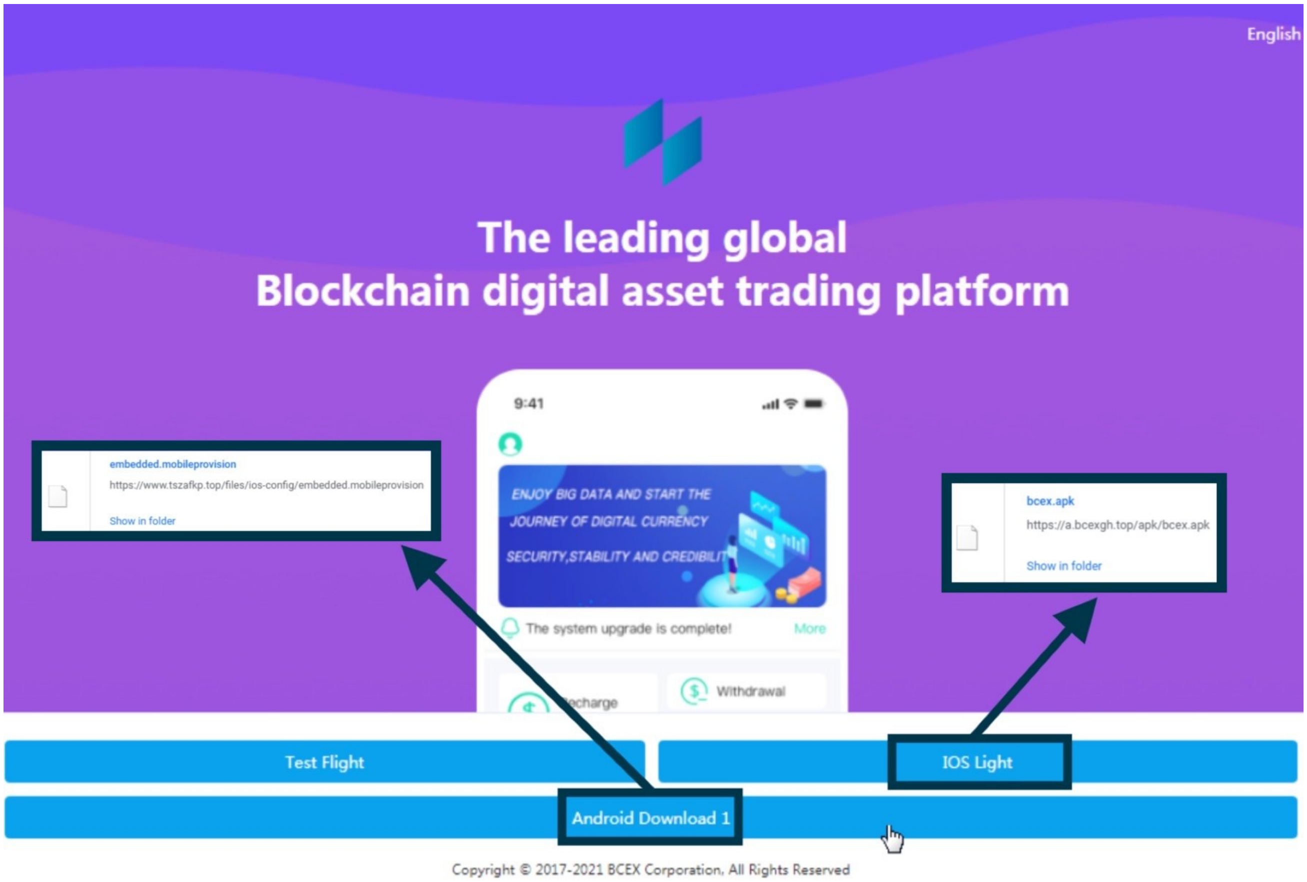
Installation process.

The primary target is mobile devices. The threat actors encourage users to download a mobile app or use a "Webapp". There are download links for iOS, and Android.

Analyzing the way the application is distributed on **iOS equipment,** it appears that the attackers exploit two main ways to get around the Apple approvals process:

1. The first one is done by simply creating a **Configuration profile**, which is a `.mobileconfig` **file** that can be easily shared.

2. The second one is through **Testflight,** a tool created by Apple, that allows developers to test their applications and provide Beta versions of new apps **without facing the severe verification protocols** found on Apple Store.
   This can allow **public direct link downloads to up to 10000 accounts**.


English
The leading global
Blockchain digital asset trading platform
embedded.mobileprovision
https://www.tszafkp.top/files/ios-config/embedded.mobileprovision
Show in folder
9:41
ENJOY BIG DATA AND START THE JOURNEY OF DIGITAL CURRENCY
SECURITY,STABILITY AND CREDIBILIT
The system upgrade is complete!
More
Recharge
Withdrawal
bcex.apk
https://a.bcexgh.top/apk/bcex.apk
Show in folder
Test Flight
IOS Light
Android Download 1
Copyright © 2017-2021 BCEX Corporation, All Rights Reserved

On the other hand, when it comes to **Android users,** an `.apk` **file** with a tailored name matching the specific website gets downloaded. If at first glance this file appears to be authentic, a more careful look reveals some **obfuscated information** using a combination of a tool called **String Fog, base 64 and a XOR operation** to encrypt suspicious data. However, our team was able to decrypt some of this information, namely a few servers and config URLs.

There are some claims online that mention the **existence of malware (Trojan) on the apps.** Unfortunately, we can not assuredly deny or confirm this information, at the time of the publication of this blog post.

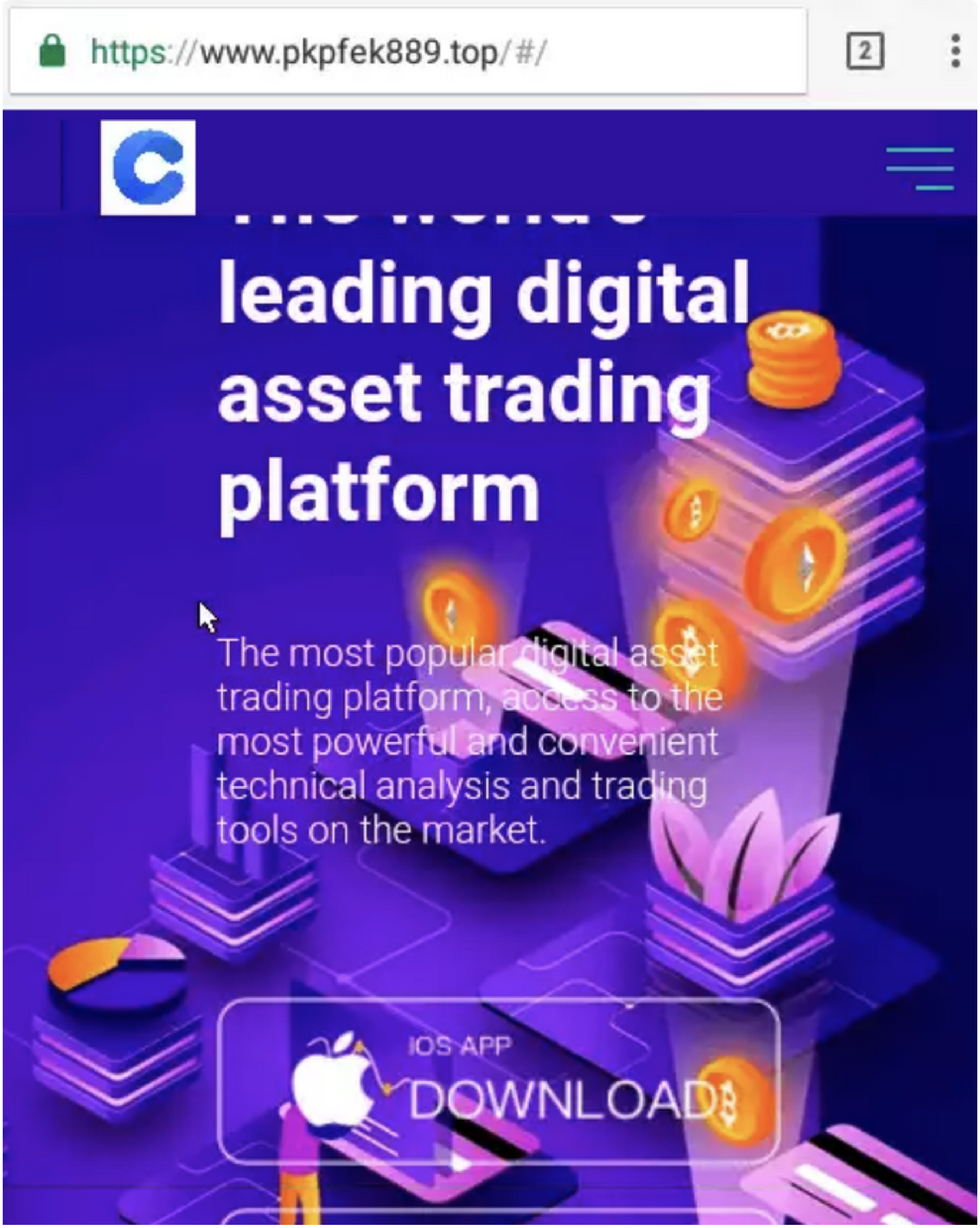
Final remarks

Taking everything into account, we are confident that this threat actor will continue to develop and distribute trading platforms, in order to exploit and steal funds from individuals.

The methods of delivery will vary as expected with an affiliate program.

We recommend blocking access to the uderlying app download infrastructure.

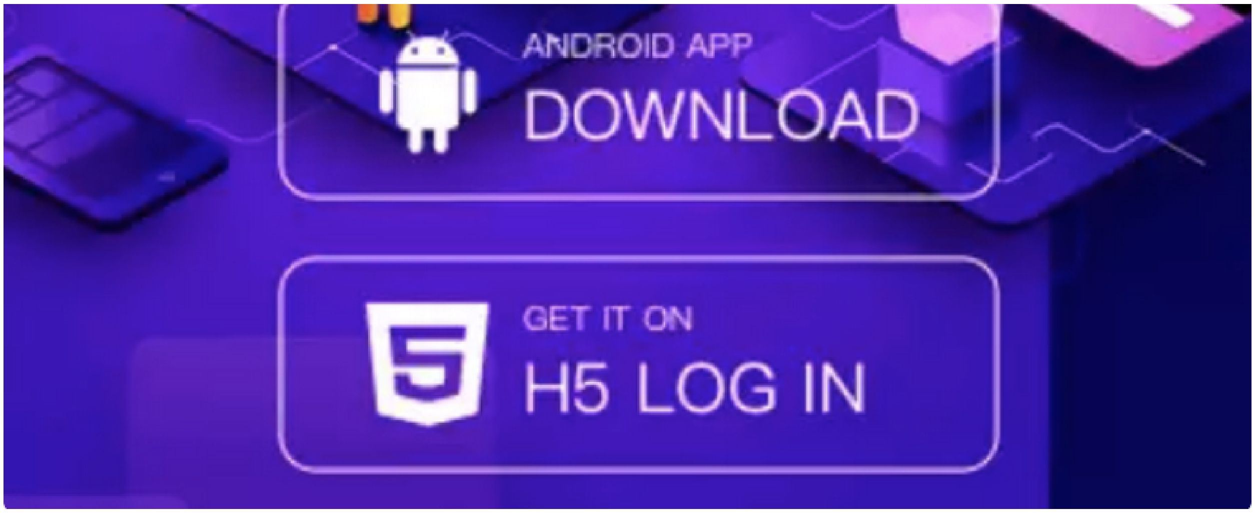
With that in mind, we have collected an extensive **list of Indicators of Compromise**, which are available for the Silent Push costumers. Additionally, these users have access to **pre-built modifiable queries** that allow them to **navigate through this operating infrastructure,** as well as access to **whois information, server information, curated risk scores and other innovative functionality.**

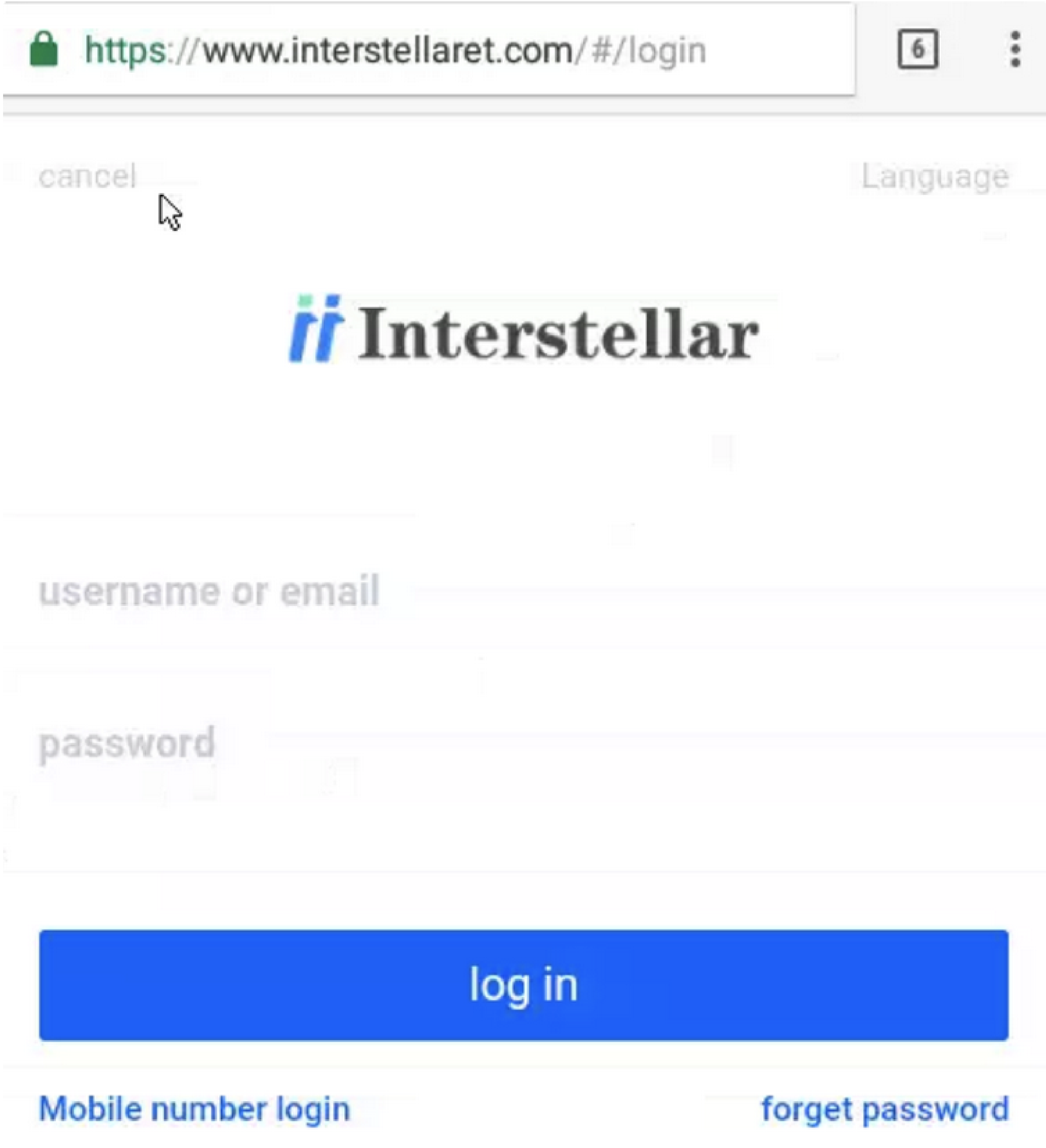


https://www.pkpfek889.top/#/

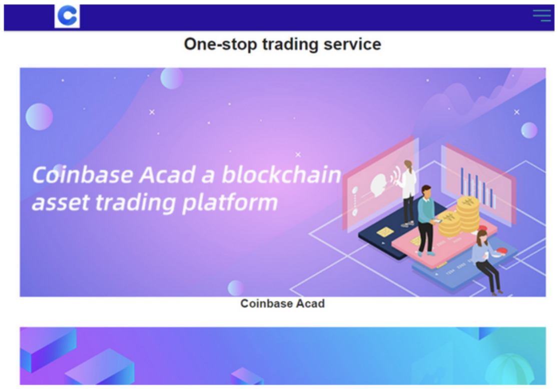
The world's leading digital asset trading platform

The most popular digital asset trading platform, access to the most powerful and convenient technical analysis and trading tools on the market.

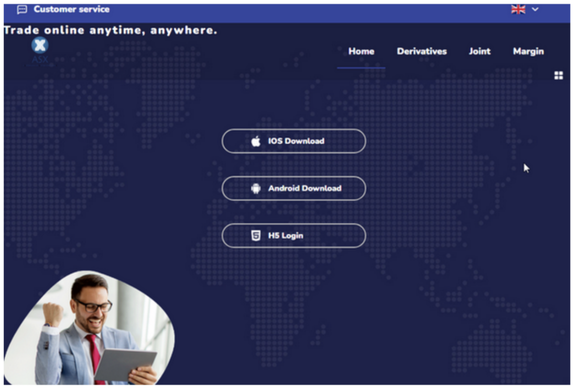

ANDROID APP
DOWNLOAD
GET IT ON
H5 LOG IN



https://www.interstellaret.com/#/login



`www.pkpfek889.top` website



`www.qgwhte24561.top` website

Another fake Coinbase site

IOCs of Fake Trading Apps

These IOCs are relevant on the day of publication, but for ongoing dynamic lists that stay up to date every day please subscribe to our service.

Subdomains:

`d.appk12036[.]xyz`

`d.appk56295[.]xyz`

`d.appkoi65y[.]xyz`

`d.appl8965[.]xyz`

`d.appl9035[.]xyz`

`d.appr6552[.]xyz`

`d.atfxwqe[.]xyz`

`d.avatradewqd[.]xyz`

`d.bbexsbcv[.]xyz`

`d.bitcudbf[.]xyz`

`h5.amcoinbhd.buzz`

`h5.ascifgm[.]top`

`h5.asxnvds[.]cc`

`h5.biupsdfe[.]cc`

`h5.blyg367[.]top`

`h5.bqsbkomh[.]net`

`h5.bsxkiso[.]cc`

`h5.cnfalwk[.]top`

`h5.coinbasekp.buzz`

`h5.coindealmip[.]cc`

`h5.dbag-prot[.]com`

`h5.dbagde[.].cc`

`h5.dcgbyre[.]shop`

`h5.dcgtbh[.]com`

`h5.eurexvky[.]cc`

`h5.fegeh42415[.]top`

`www.hifly01569[.]top`

`www.hifly22787[.]top`

`www.hifly22878[.]top`

`www.hifly27702[.]top`

`www.hifly38283[.]top`

`www.hifly56982[.]top`

`www.hifly76862[.]top`

`www.hifly85086[.]top`

`www.hiflyk47344[.]top`

`www.hiflyk87327[.]top`

Android apk file download URLs:

`hxxps://a.digitalsurgeno[.]top/apk/digitalsurge[.]apk`

`hxxps://a.edgecryptoge[.]top/apk/edgecrypto[.]apk`

`hxxps://a.etorodes[.]buzz/apk/etoro[.]apk`

`hxxps://a.exnessge[.]top/apk/exness[.]apk` `hxxps://a.ftxano[.]top/apk/ftx[.]apk`

`hxxps://a.jubinok[.]top/apk/jubi[.]apk`

`hxxps://a.masteryptge[.]top/apk/masterypto[.]apk`

`hxxps://a.okcoinge[.]top/apk/opkcoin[.]apk`

`hxxps://a.olymptradeno[.]top/apk/olymptrade[.]apk`

`hxxps://a.opkcoinno[.]top/apk/opkcoin[.]apk`

`hxxps://a.parvestano[.]top/apk/parvesta[.]apk`

`hxxps://a.timexdes[.]buzz/apk/timex[.]apk`

`hxxps://a.tycoonsege[.]top/apk/tycoonse[.]apk`

Apple Configuration profile download URLs:

`hxxps://www.bfefe96b[.]top/files/ios-config/olymptrade[.]mobileconfig`

`hxxps://www.gniyfe35f[.]xyz/files/ios-config/opkcoinabc[.]mobileconfig`

`hxxps://www.grgrnt55y[.]top/files/ios-config/parvesta[.]mobileconfig`

`hxxps://www.hifly69972[.]xyz/files/ios-config/timex[.]mobileconfig`

`hxxps://www.hiflyf14255[.]top/files/ios-config/tycoonse[.]mobileconfig`

`hxxps://www.hiflyg41344[.]top/files/ios-config/exness[.]mobileconfig`

`hxxps://www.hiflyg66779[.]xyz/files/ios-config/etoro123[.]mobileconfig`

`hxxps://www.hutyfr688[.]top/files/ios-config/okcoin1[.]mobileconfig`

`hxxps://www.kod89h5[.]top/files/ios-config/ftx[.]mobileconfig`

`hxxps://www.lkqv215[.]xyz/files/ios-config/masterypto[.]mobileconfig`

`hxxps://www.niyfe35f[.]xyz/files/ios-config/opkcoinabc[.]mobileconfig`

`hxxps://www.pade00bg[.]top/files/ios-config/digitalsurge[.]mobileconfig`

`hxxps://www.pkofe675[.]top/files/ios-config/jubi[.]mobileconfig`

`hxxps://www.tvao183[.]xyz/files/ios-config/edgecrypto123[.]mobileconfig`

If you have been affected by the Counterfeit Trading scams please share the details with us so we can keep trying to get them taken down as we find them. Contact us using [email protected] or the form below.

Name *
Must be a work account
Thank you!

Ken Bagnall