CryptoRom Bitcoin swindlers continue to target vulnerable iPhone and Android users

Jagadeesh Chandraiah ⋮⋮ 16-3-2022

Romance scams have gotten some high-profile attention as late, thanks to the Netflix show Tinder Swindler. In some ways, the plot is similar to an organized crime campaign we dubbed CryptoRom, which we've been following since early 2021. The difference is that CryptoRom doesn't require in-person interaction.

This style of cyber-fraud, known as sha zhu pan (杀猪盘)—literally "pig butchering plate"—is a well-organized, syndicated scam operation that uses a combination of often romance-centered social engineering and fraudulent financial applications and websites to ensnare victims and steal their savings after gaining their confidence. While the scam initially focused on Asian victims, in October of 2021 we documented its global expansion.

This threat is still very active, and continues to impact victims around the world, in some cases costing them their life savings. Since our report in October, additional victims have reached out to us to report new CryptoRom apps and websites. In this post, we highlight those additional fake mobile apps and websites, as well as the social engineering techniques used by the malware operators—and another type of abuse of Apple iOS's software distribution to bypass the App Store's security screening.

iOS TestFlight abuse

Let's look at the new abuse vector first. Previously, we found CryptoRom's deceptive applications for iOS devices exploiting Apple's "Super Signature"application distribution scheme (a limited ad-hoc distribution method using a developer account) and abuse of Apple's enterprise application deployment scheme. We are now also seeing Apple TestFlight being abused by CryptoRom authors.

TestFlight is used for testing the "beta" version of applications before they are submitted to the App store for distribution. Apple supports use of TestFlight app distribution in two ways: for smaller internal application tests sent out by up to 100 users by email invitation, and larger public beta tests supporting up to 10,000 users. The smaller email-based distribution approach requires no App Store security review, while TestFlight apps shared by public web links require an initial review of code builds by the App Store.

Unfortunately, just as we've seen happen with other alternative app distribution schemes supported by Apple, "TestFlight Signature" is available as a hosted service for alternative iOS app deployment, making it all too simple for malware authors to abuse. These third-party services are extensively abused by CryptoRom authors.

A screen shot of a web site offering "TestFlight Signature" services to mobile developers.

TF Signature is cheaper to use than other schemes because all you need is an IPA file with a compiled app. The distribution is handled by someone else, and when (or if) the malware gets noticed and flagged, the malware developer can just move on to the next service and start again.

TF signature is preferred by malicious app developers in some instances over Super Signature or Enterprise Signature as it is bit cheaper and looks more legitimate when distributed with the Apple Test

Flight App. The review process is also believed to be less stringent than App Store review:

What should I do if the AppStore always fails to pass the review, TF signature will help you

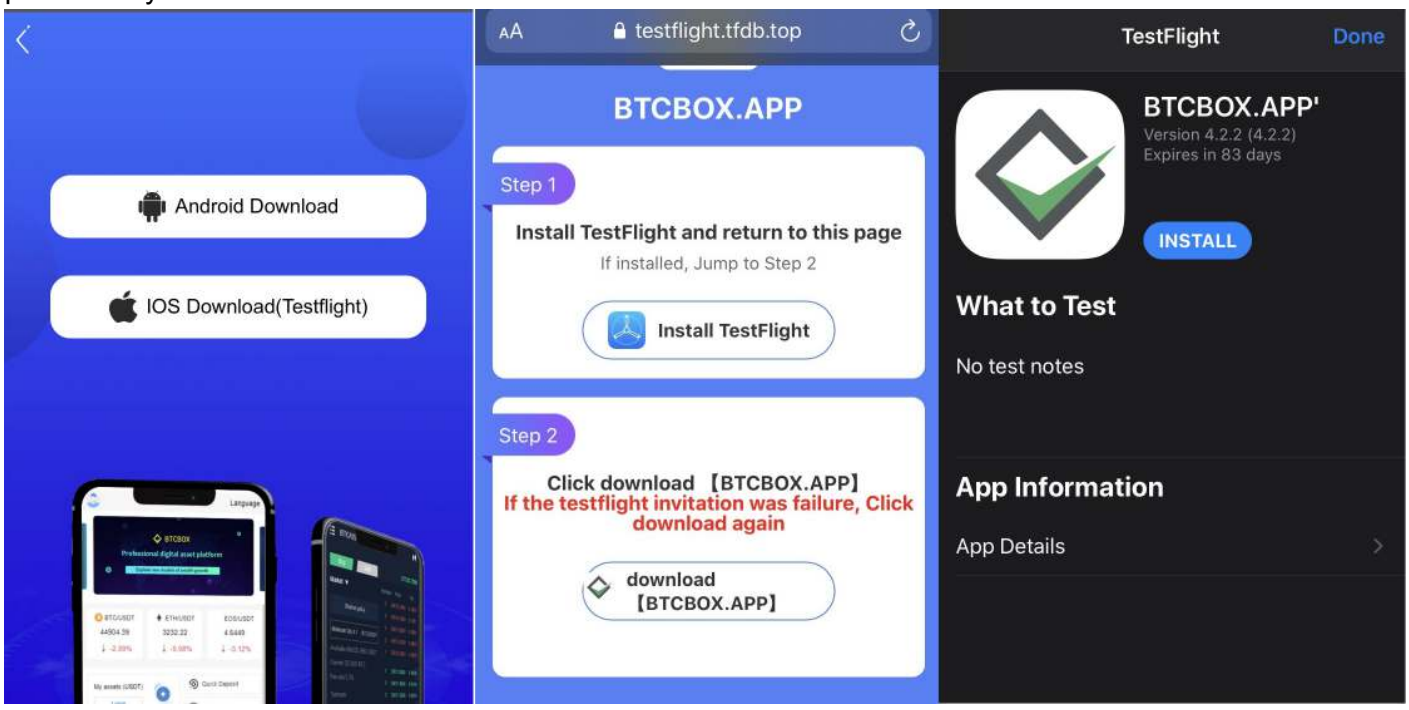
2021.11.02

Applications submitted to the Apple App Store for review are usually a result in most cases, because a review is not passed, and a review may take a month or more, which is not worth the loss. However, Apple's official internal beta application store gives APP developers a way to survive. In the case that they cannot be listed on the App Store, it is a good distribution method to complete the APP release through TF signature.

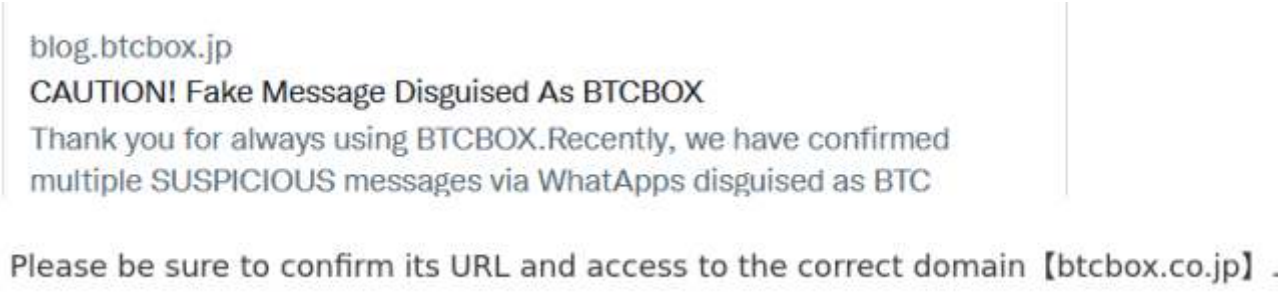
It usually takes 1-3 working days to complete the testflight on the Apple APP. If it goes well, it will be approved by Apple's official review within 20 minutes. Compared with the App Store, the advantage of the review cycle has far exceeded the review time of the App Store, and the TF signature still has a high pass rate.

Some of the victims who contacted us reported that they had been instructed to install what appeared to be BTCBOX, an app for a Japanese cryptocurrency exchange. We also found fake sites that posed as the cryptocurrency mining firm BitFury peddling fake apps through Test Flight. We continue to look for other CryptoRom apps using the same approach.

Apps for both Android and iOS were distributed through a fraudulent website. The iOS version of the fake application used TestFlight to deploy to victims' devices. We were able to reproduce this using links provided by victims:



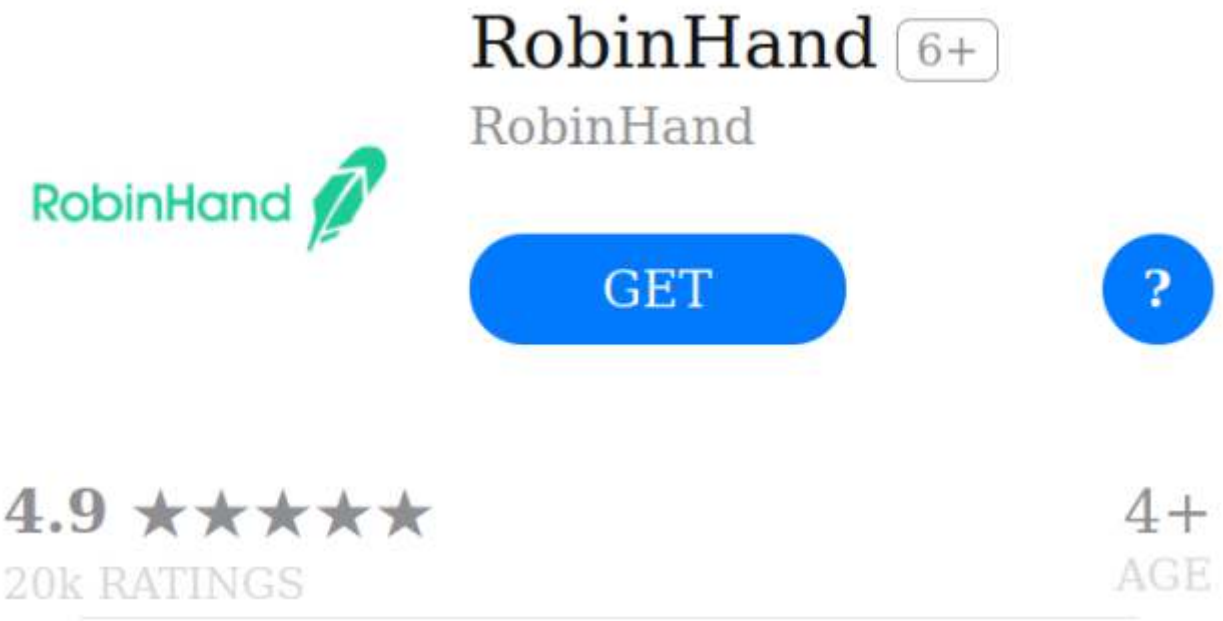
BTCBOX has warned of fake websites and asked users to use the right domains.



iOS WebClips, changing Icons and Websites

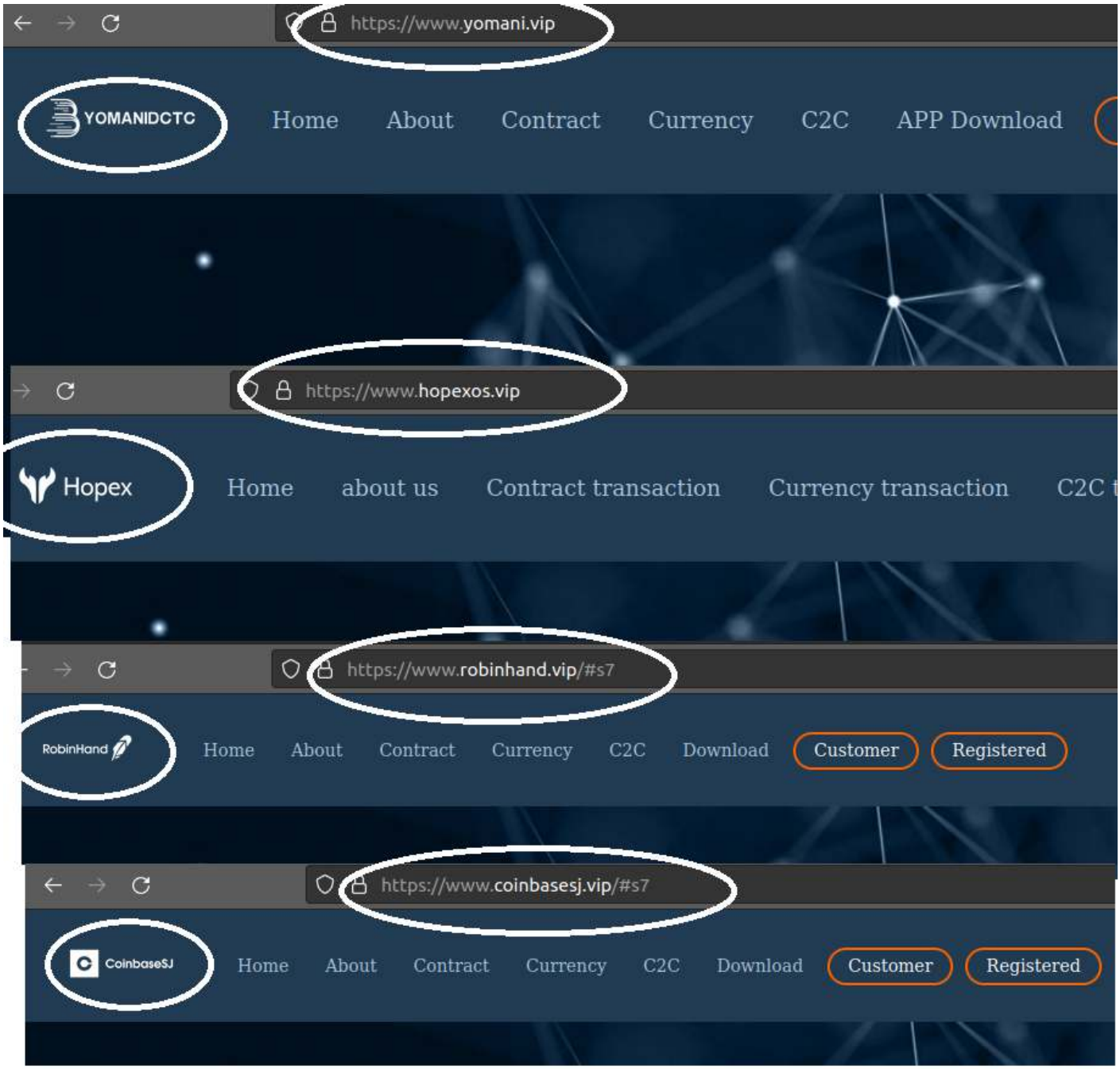
The majority of the iPhone users we spoke with who had encountered these fraudulent apps were lured with another approach to bypassing the App Store: they were sent URLs serving iOS WebClips. WebClips are a mobile device management payload that adds a link to a web page directly to the iOS device's home screen, making it look to less sophisticated users like a typical application.

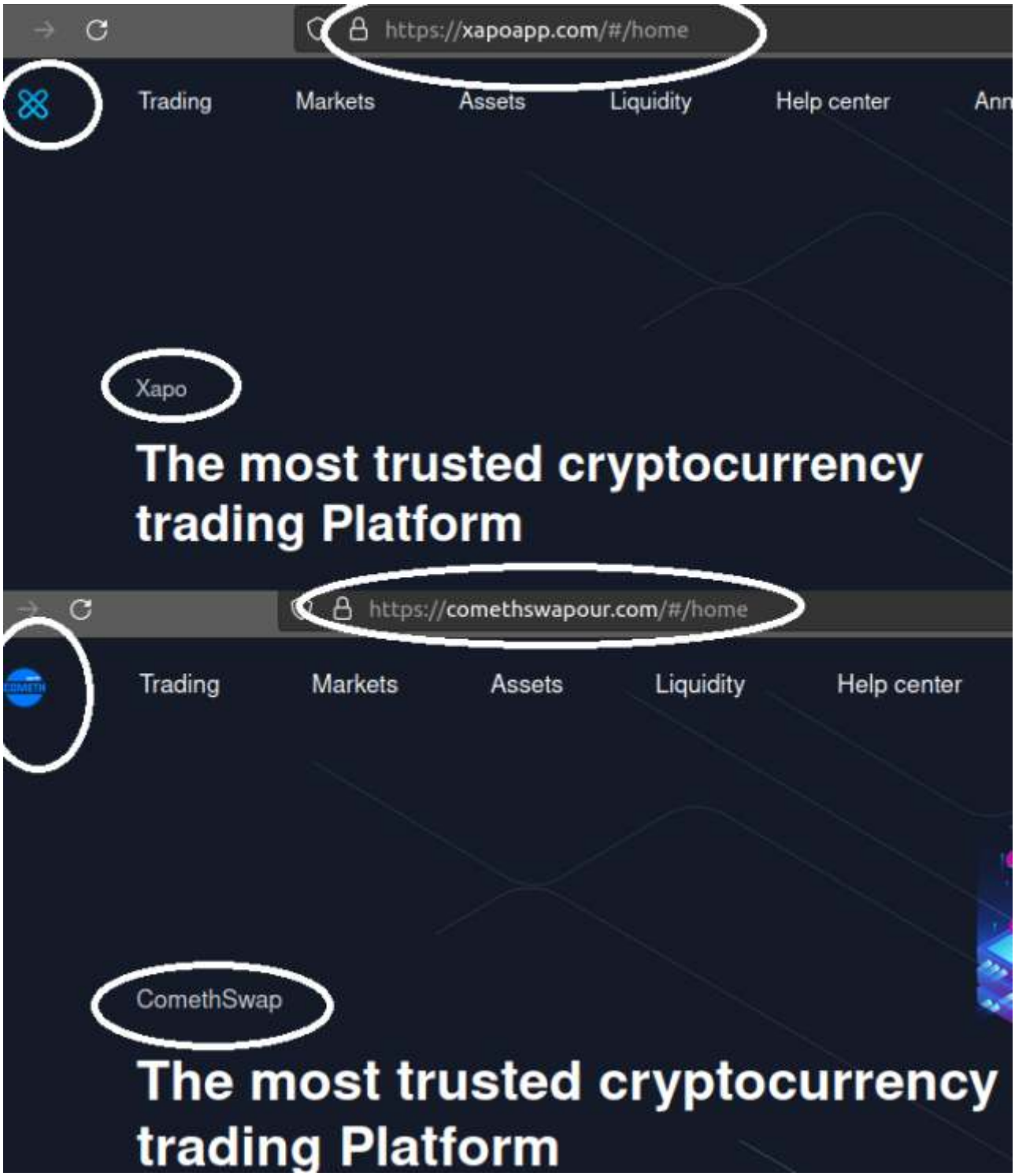
While investigating one of the CryptoRom URLs, we found related IPs that were hosting App store lookalike pages with a similar template, but with varying names and icons. The "apps" included one that mimics the popular Robinhood trading application, called 'RobinHand.' Its logo is similar to that of Robinhood.



In addition to App store pages, all these fake pages also had linked websites with similar templates to convince users—different brands and icons, but similar web content and structure. This is probably done to move on from one brand to another when they get blocked or found out. This shows how cheap and easy it is to mimic popular brands while siphoning thousands of dollars from victims.

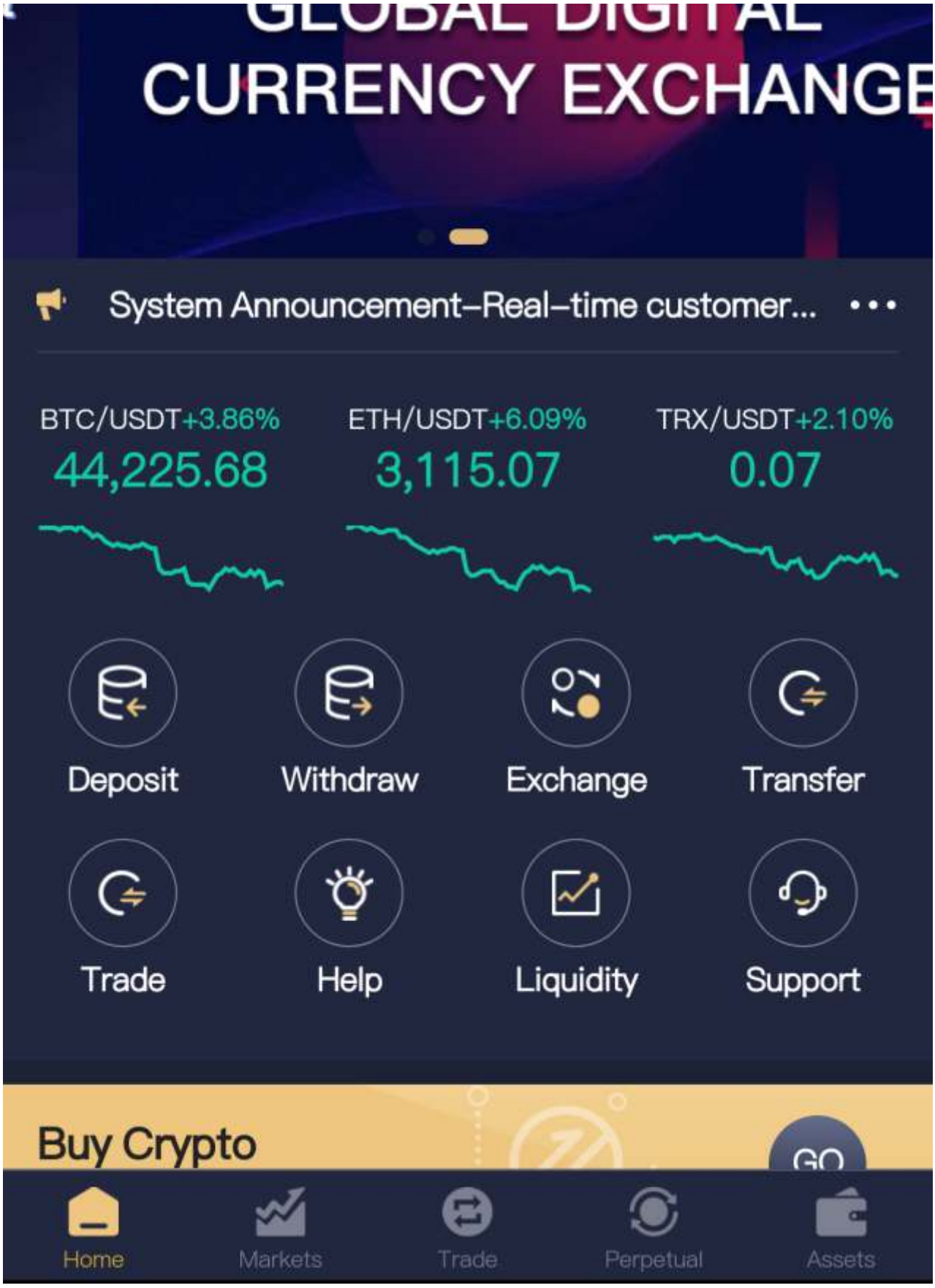
The following images show copying of well-known cryptocurrency, trading, and exchange platforms with web templates where they change only icon, URL, and brand name.


https://www.yomani.vip
YOMANIDCTC
Home
About
Contract
Currency
C2C
APP Download
https://www.hopexos.vip
Hopex
Home
about us
Contract transaction
Currency transaction
https://www.robinhand.vip/#s7
RobinHand
Home
About
Contract
Currency
C2C
Download
Customer
Registered
https://www.coinbasesj.vip/#s7
CoinbaseSJ
Home
About
Contract
Currency
C2C
Download
Customer
Registered

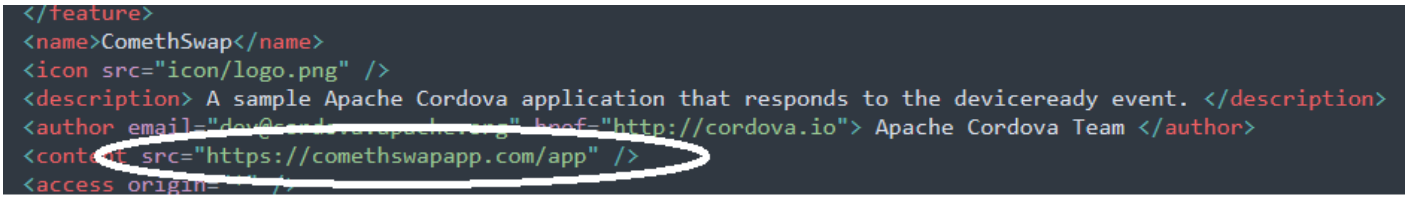


Android applications

As for the Android versions of these fake apps, the trend of using easy, low effort app development tools continues. Most of the CryptoRom-connected Android applications we have seen have been essentially wrapped web applications with minimal code. The URLs that the apps connect to vary.



The following image shows the app config file with the CryptoRom URL; the app in this case was developed using Apache Cordova.



Gaining trust, ruining lives

Since our initial report, we have been contacted by victims of CryptoRom scams from around the world. Many of them provided details of the scams that allowed us to collect samples and other threat data. Most also reported that they had lost thousands of dollars in personal savings to the crooks behind the scams, though some saw our previous reports and recognized the scam before being drawn into it too deeply. In some cases, victims have lost their entire savings and even taken out loans with the hope that they will get their money back:

```
Hello, sorry suddenly sent you a message, I know you from shopos news and
there you were writing an article about cryptoroom fake [apps].
I am one of the victims of this fake crypto that has lost more than $20,000 I
want to ask you about this application, this is the application the suspect
sent to me, can you help me to check if this is fake or not?
```

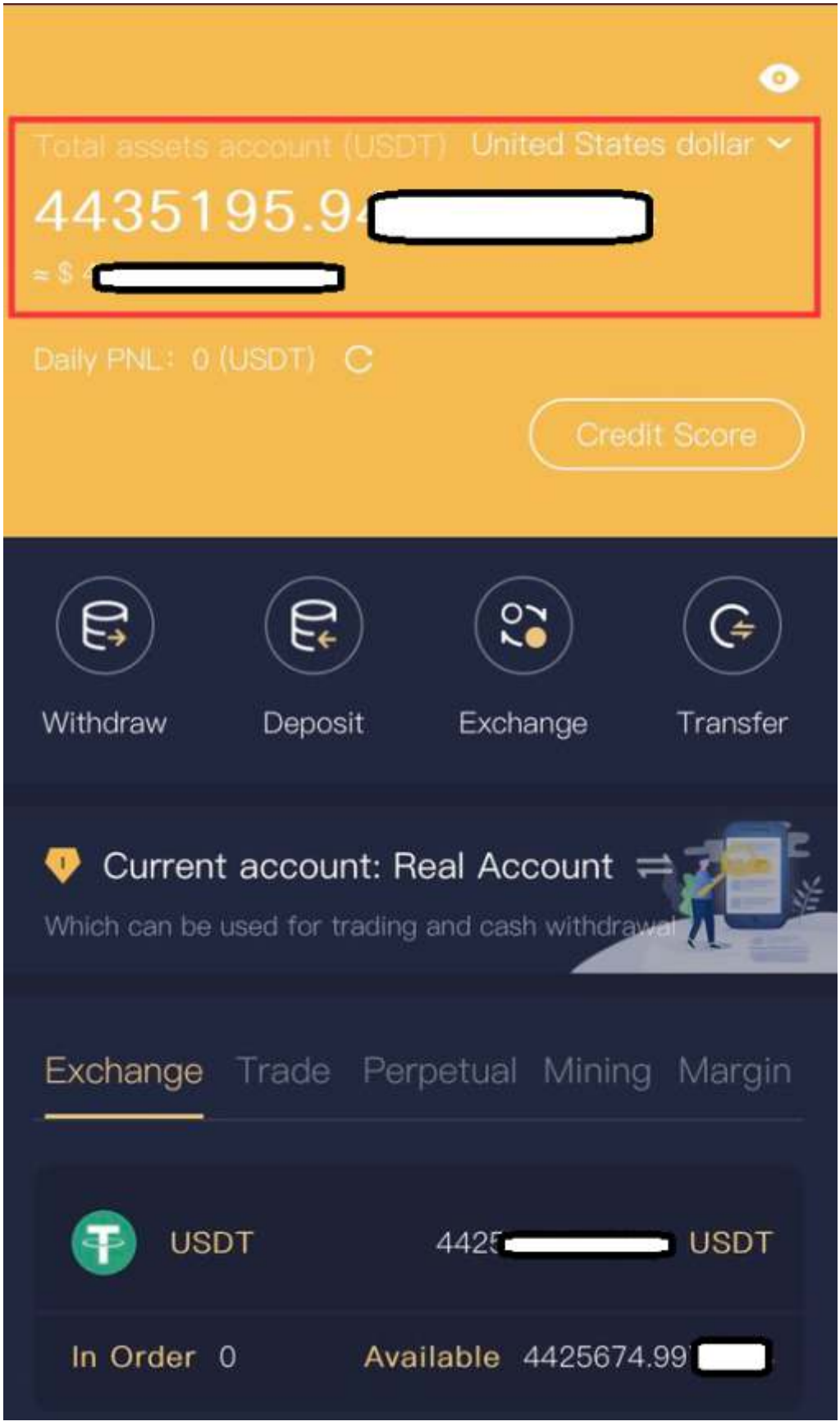
```
Hi,Found your ID from comments section of fake crypto app article. One of my
friend is using similar app called 'UBS global' + binance. They are providing
trading in crypto. now when he tried to withdraw amount, they are asking for
paid membership of $6000.Can you help check if this app is legal.
```

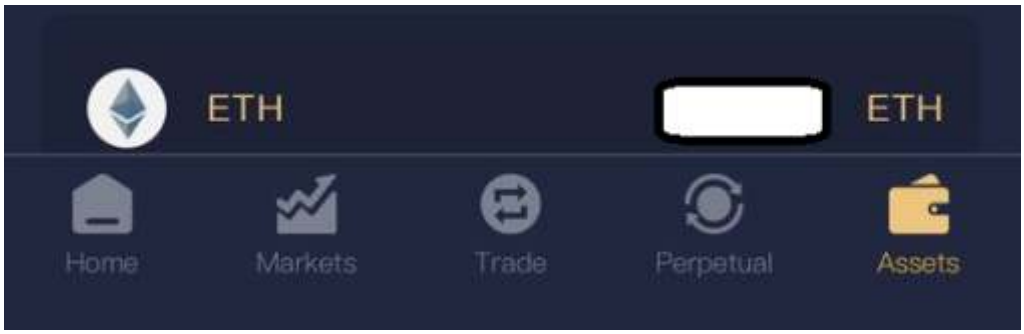
```
I have invested wrongly on one fake trading app. Invested 100k , and my
brother and their friends it's huge more than 10lakhs..and they looting more
innocent people.
```

As we've noted in our previous reports, these scams use a number of approaches to build a relationship with their targets without ever meeting them face to face. In previous reports, we noted that crooks had used dating sites and dating applications, as well as other social networking platforms, to find new victims. But in some instances, they were initiated through seemingly random WhatsApp messages offering the recipients investment and trading tips, including links to CryptoRom site URLs. Often these messages included promises of huge financial returns. We suspect that the crooks obtained contact information for their targets either through their own social media accounts or through compromised websites. They also seem to obtain publicly available information and target those who are already into investment and cryptocurrency.

Because the fake apps targets are directed to mimic popular brands, the targets are often convinced that they are transacting with legitimate companies just as they do with mobile banking applications. But the most important factor in these scams, based on online conversations, appears to be that the crooks allow targets to initially make withdrawals from the fake accounts after taking "profits." Victims are allowed to

withdraw their initial investment as a confidence-building measure, just as in classic Ponzi schemes—but then the fake romantic partner or “friend” urges the victim to reinvest even more for a big event. To sweeten the pot, they even offer to “lend” the target a huge sum to increase the investment; since they control the back-end of the app, they can inject fake deposits on accounts and create imaginary profits at will. For example, in the following image you can see that in case they have increased the total assets to be over $4 million:





Because the crooks control the back end of the app, they can artificially inflate or deflate what the app displays to reinforce the con; this also seems to be an important factor in convincing victims that they are making money. Based on the circumstances and situation, the crooks deflate or inflate deposits and profits to increase the confidence of victims.

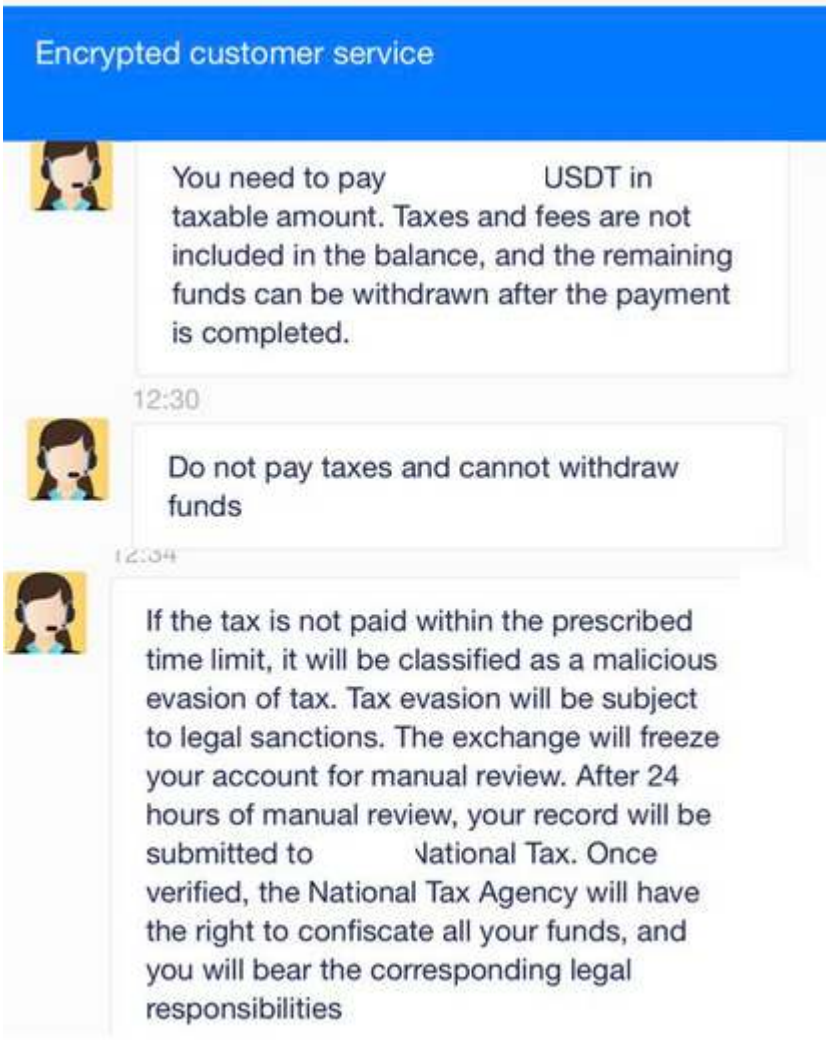
Leeching every penny by fake lending

The scam doesn't end with just fooling victims into investing. When victims try to withdraw funds from their big "profit," the crooks use the app to inform them that they need to pay a "tax" of 20% of their profits before funds can be withdrawn—and threaten that all their investments will be confiscated by tax authorities if they do not pay, as some victims have reported:

"Hello I have come this app that one friend suggested me. It's a trading app, but I don't know if it's real or now [because] I have to recharge lot of money there but they don't allow me to withdraw without paying taxes and I can't pay with the existing money I have."

"Hello, I found your contact info online from the Sophos News article about fake iOS apps disguise as trading and cryptocurrency apps. I am a victim of a romance scam and the article describes an exactly what I'm currently experiencing. Unfortunately, I already deposited a lot of money in the trading app and after several successful trades with double gains, my account has been frozen until I pay an enormous 20% tax fee on the profits."

"I have invested all my retirement money and loan money , about $1,004,000. I had no idea that they would freeze my account, requiring me to pay $625,000, which is 20% taxes on the total profits before they will unfreeze my account."

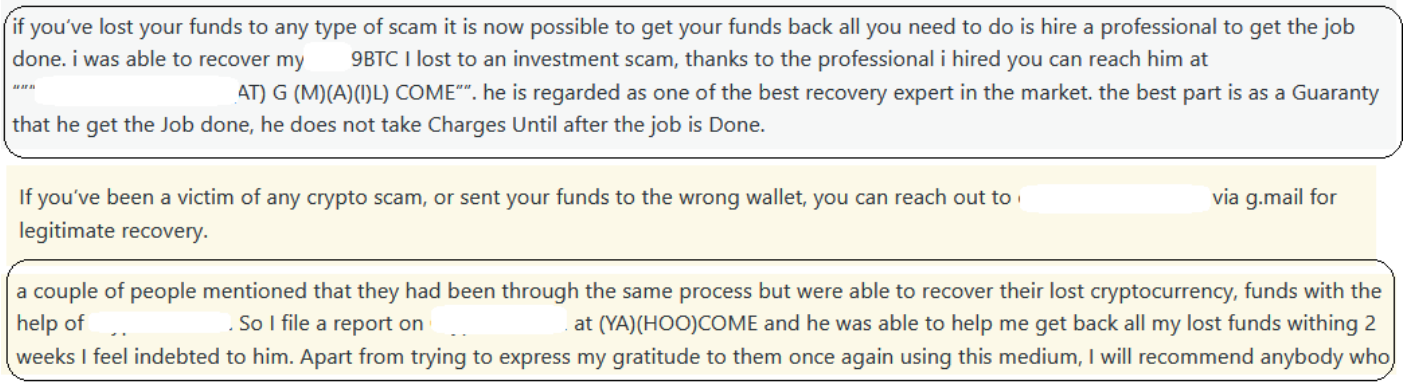


A screen shot of an in-app “customer service” chat telling a “customer” that taxes must be paid before withdrawals can be made.

When victims have tapped out their personal capital and do not have any money to pay the tax, the crooks continue to squeeze every last penny from them. In the translated screenshot shown below, the fake romantic interest is telling the victim that the funds they had lent them have also been frozen, and that the victim needs to pay tax—but they are willing to lend part of the money required (up to $300,000) and the victim needs to find the rest to get the money back. By pretending to lend, they offer fake support to the victim, while at the same time manipulating the victim to pay even more to the crooks.

Recovery Scams targeting CryptoRom victims

CryptoRom victims are frequently desperate to find a way to get their money back after they realize they've been taken by criminals. But because of the nature of cryptocurrency and the fact that cross-border foreign transactions are involved, it is difficult at best to recover funds through law enforcement or other legal channels. Exploiting this desperation, a number of bogus cryptocurrency recovery services have sprung up that specifically target CryptoRom victims. We've found a number of offerings for these services on the web via responses in discussion groups and social media; many of the messages are typo-laden. The vast majority of these services are fake, and it is highly unlikely that any service would be able to get victims' money back.



The best approach is to contact local and national law enforcement for assistance.

Conclusion

CryptoRom scams continue to flourish through the combination of social engineering, cryptocurrency, and fake applications. These scams are well-organized, and skilled in identifying and exploiting vulnerable users based on their situation, interests, and level of technical ability. Those who get pulled into the scam have lost tens of thousands of dollars.

SophosLabs has reported all of the CryptoRom-related websites and apps to Apple and Google, but the only long-term fix to prevent these scams is a collective response. Banks and financial organizations need to provide traceability for cryptocurrency transactions. Social media companies should alert users about these scams, and should spot patterns and remove fake profiles committing this fraud. Finally, Apple and Google should alert users that newly installed “side-loaded” apps are not from official sources.

If you have experienced this type of fraud or wish to report applications or URLs connected to CryptoRom scams, please comment on this post or reach out via Twitter to @jag_chandra. A full list of IOCs for the apps we’ve analyzed is available on SophosLabs’ Github.

SophosLabs would like to acknowledge Xinran Wu for his contribution to this article