Romance scams with a cryptocurrency twist – new research from SophosLabs

13 OCT 2021 1

Apple, Cryptocurrency, iOS

Previous: Apple quietly patches yet another iPhon...

Next: S3 Ep54: Another 0-day, double Apache pat...

by Paul Ducklin

Sadly, we've needed to write and warn about romance scams and romance scammers many times in recent years.

Indeed, in February 2021 we published an article entitled Romance scams at all-time high: here's what you need to know, following a report from the US Federal Trade Commission (FTC), America's official consumer protection watchdog, warning that romance scammers are making more money than ever before.

Victims in the US were tricked out of more than $300 million in 2020, up from $200 million in 2019.

Conventional romance scams are what we often refer to as "long game" confidence tricks, where someone you meet online, typically on a dating site, manages to convince you: [a] that they're a real person with the life history they claim; [b] that they're love with you; and, most importantly of all, [c] that you are in love with them.

After weeks, perhaps months, of careful ground work, the illusory lover turns the talk towards money, and gradually convinces you to part with more and more of it, thanks to an ever-evolving series of ruses, abuses and excuses that practised cyberscammers can sometimes maintain for weeks, months or even years.

Putting money before love

Well, there's another angle that dating-site scammers are taking these days, where the crooks quite deliberately put money before love.

They still use dating sites to select, stalk and groom their victims, but instead of investing weeks or months progressing from friendship, through love, romance and perhaps even fraudulent betrothal, to the "fleecing" phase...

...they strike up a friendship, using the dating game as a ruse, but then quickly move to money, this time in the guise of them doing you a big favour by offering you a chance to join an "unbeatable" investment opportunity.

As you can imagine, the "investment" that they propose typically involves cryptocoins, but to add a veneer of legitimacy, these **CryptoRom crooks**, as we've dubbed them (crypto- from "cryptocurrency" and -rom from "romance scam"), invite you to install an "official" app in order to join the scheme.

All those dubious excuses needed by traditional romance scammers to talk you into using wire transfer services to send money, or into buying them gift cards and sending through the redemption codes, are replaced by a sense of structure: there's a genuine app for this investment!

In fact, the cryptorom scammers will even offer you an app if you have an iPhone, where Apple's "walled garden" approach of requiring all consumer app downloads to come from the Apple App Store almost certainly persuades many victims that the cryptorom app must indeed have some sort of official authorisation or approval.

The App Store, like Google's Play Store equivalent for Android, is by no means immune to malware, fleeceware and other badware apps.

But totally bogus cryptocurrency trading apps, based on totally bogus trading platforms, rarely make it through. (Generally speaking, trading apps and platforms are supposed to comply with a whole bunch of regulations in additional to Apple's own.)

So these crooks **bypass the App Store entirely**, using a series of tricks explained in a new SophosLabs research report entitled **CryptoRom fake iOS cryptocurrency apps hit US, European victims for at least $1.4 million**.

CryptoRom fake iOS cryptocurrency apps hit US, European victims for at least $1.4 million

Scammers combine romantic lures with crypto scams, abusing Apple's ad-hoc app distribution to steal millions from people around the world.

"Pretend that your phone really is our phone"

The technological basis for these scam apps is surprisingly simple: the crooks persuade you, for example on the basis of a friendship carefully cultivated via a dating site, into giving them the same sort of administrative power over your iPhone that is usually reserved for companies managing corporate-owned devices.

Companies who enrol staff devices into Apple's remote management system, by means of what's known as an MDM (mobile device management) profile, do so in order to take an active role in the protection, monitoring and control of those devices.

Typically, they can remotely wipe them, unilaterally or on request, block access to company data, enforce specific security settings such as lock codes and lock timeouts…

…and (this is the feature the crooks are after!) they can install bespoke corporate apps intended for employees only.

This "loophole" allows companies to bypass the App Store for proprietary apps that aren't supposed to be available for anyone to download.

So, the cryptorom crooks exploit this Enterprise Provisioning feature by tricking you into treating them as if they were your employer, and as if they had a reasonable need or right to exercise almost complete control over your device.

In one fraudulent app deployment process that SophosLabs investigated, the criminals even used the "Description" field in the their fake app to claim that their off-market software was "authorised by Apple to be safe and reliable":

1. Fake "Apple" 5-star reviews.
2. Fake "Apple" name on management certificate.
3. Fake "Apple" endorsement in bogus app.

Of course, the app isn't a trading program at all.

There's no trading platform behind it; your "investments" aren't used to buy any sort of cryptocurrency, not even a volatile or little-known one; any "trades" and "profits" reported by the app are imaginary; if you are ever allowed to withdraw any of your "profits" in order to built up trust, the crooks will simply give you a tiny bit of your own money back; and when you want to cash out your "investment"...

...you realise that it's all smoke and mirrors, what's known in the jargon as a pyramid or Ponzi scheme.

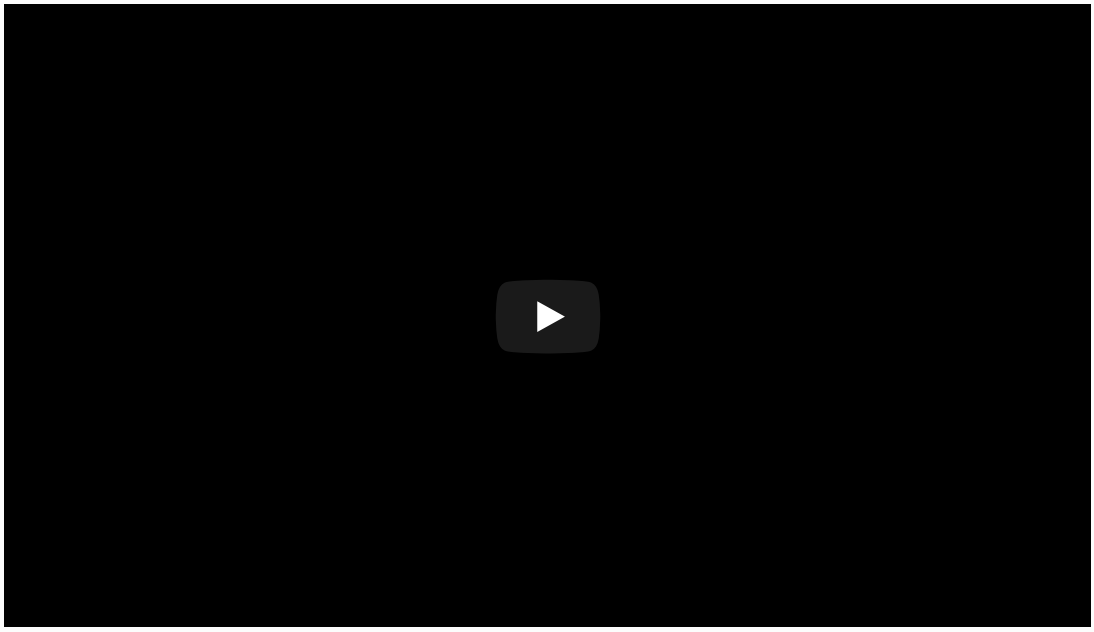
What to do?

- **Take your time when "dating site" talk turns from friendship, love or romance to money.** It's Cybersecurity Awareness Month right now, and one of the catch phrases of #Cybermonth is: Stop. Think. Connect. Don't be swayed by the fact that your new "friend" happens to have a lot in common with you. That needn't be down to serendipity or because you have a genuine match. The other person could simply have read your various online profiles carefully in advance.
- **Never give administrative control over your phone to someone with no genuine reason to have it.** Never click `[Trust]` on a dialog that asks you to enrol in remote management unless it's from someone you already have an employment contract with who, the conditions have been clearly explained to you in advance, and you understand and accept the reasons for enrolling your phone.
- **Don't be fooled by app descriptions that claim approval from Apple.** Description text, unofficial reviews, and text shown by screens in the app itself are just that: text. Relying on what an app says about itself is like emailing someone you aren't sure about and

asking “Are you genuine?” If they are truthful, then the answer will be “Yes”. If they are lying, then the answer will be “Yes.”

- **Listen openly to your friends and family if they try to warn you.** Criminals who use romance or dating as a lure think nothing of deliberately setting you against your family as part of their scams. They may even “counsel” you not to let your friends and family in on your “secret”, pitching their romantic interest or their investment proposal as something that conservative, hidebound people will simply never understand. Don’t let the scammers drive a wedge between you and your family as well as between you and your money.

YOU MIGHT ALSO LIKE:



Original video here: https://www.youtube.com/watch?v=_nO77xWeO4o
Click the cog icon to speed up playback or show live subtitles.
[BY POPULAR DEMAND!] Read a **TRANSCRIPT** of the video.

Follow @NakedSecurity on Twitter for the latest computer security news.

Follow @NakedSecurity on Instagram for exclusive pics, gifs, vids and LOLs!

Free tools

Sophos Home
Protect personal PCs and Macs

Previous: Apple quietly patches yet another iPhon...

Next: S3 Ep54: Another 0-day, double Apache pat...

One comment on “Romance scams with a cryptocurrency twist...

David Lawlor October 14, 2021 at 11:17 pm

Yes this article is true started chatting with a Chinese woman of a dating app then WhatsApp come out in conversation that am into crypto then the badgering about investing with her began quickly become a pain said she was a model lol I saw through it tho haven't heard of her for months

3 0 Rate This

Reply

What do you think?

Comment

Name

Email

Website

Post Comment

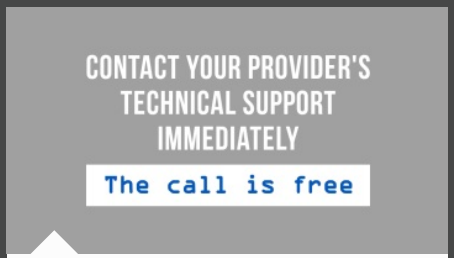
Recommended reads

OCT
07 BY PAUL DUCKLIN 6

S3 Ep53: Apple Pay, giftcards, cybermonth, and ransomware busts [Podcast]

AUG
06 BY PAUL DUCKLIN 6

Conti ransomware affiliate goes rogue, leaks “gang data”



AUG
16 BY PAUL DUCKLIN 6

Copyright scammers turn to phone numbers instead of web links

SOPHOS