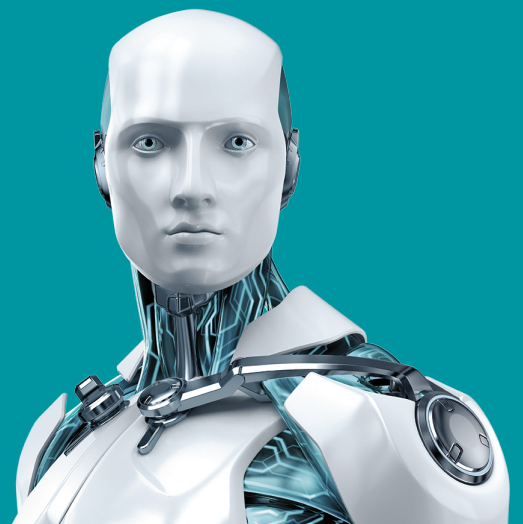


Cryptocurrency scams on Android

Lukáš Štefanko // ESET Malware Researcher



CONTENTS

Introduction	2
1. Fake cryptocurrency exchange apps	3
Fake Poloniex apps	3
2. Fake cryptocurrency wallet apps	4
Wallet address scams	4
Phishing & more phishing: Fake MyEtherWallet apps	5
A malicious mix: Cardano ADA Wallet	6
3. Android crypto-mining malware	7
Testing new revenue streams on millions of users: Bug Smasher	7
Mining Monero as promised, just not for you: Monero Miner (XMR)	9
4. Fake crypto-miners and free giveaways	10
5 stars for empty promises: Fake bitcoin miners	10
What do you mean it can't be mined? Fake Ripple miners	11
How to stay safe	12
Conclusion	13
IoCs	14
Endnotes	14

INTRODUCTION

In 2017, cryptocurrencies became a booming industry, attracting the attention of not only new users, but also cybercriminals.

As the fraudsters came rushing to the newly crowded cryptocurrency space, users, businesses, and exchanges have found themselves the target of various fraud schemes – from phishing scams, through hacks, to surreptitious crypto-mining on compromised devices and, as of late 2017, via browsers.

Cybercrime targeting cryptocurrency has recently become so rampant that regulators have issued multiple [warnings on cryptocurrency scams](#); Facebook [banned all cryptocurrency ads](#) on its platform; and insurers have started to offer [protection against cryptocurrency theft](#).

The Android platform hasn't been left out of the cryptocurrency frenzy, with users targeted by all kinds of deceptive cryptocurrency-related apps.

In this whitepaper, we'll look at the most prevalent types of cryptocurrency scams currently targeting Android users, and their go-to tricks and techniques. By identifying common red flags, we'll lay out tips for users to keep their devices – and virtual coins – safe from fraudsters.

1. FAKE CRYPTOCURRENCY EXCHANGE APPS

Fake Poloniex apps

Over the course of the last year, we have reported [two cases](#) where users of one of the world's leading cryptocurrency exchanges were targeted by credential-stealing apps. Both pretended to be mobile apps for the cryptocurrency exchange Poloniex, taking advantage of the exchange's lack of an official app. Apart from harvesting Poloniex login credentials, the fake apps also tried to trick victims into making their Gmail accounts accessible to the attackers.

Since then, the trend of creating fake apps for existing cryptocurrency exchanges or wallets has only intensified. For Poloniex alone, we have observed at least seven more instances of phishing apps. (Figure 1)

Besides the rather straightforward malicious behavior observed in these phishing apps, there are also third-party apps that merely open the official website of the impersonated legitimate exchange in a browser. A common motivation for creating such apps are referral programs offered by some exchanges: developers who drive new users to an exchange might be rewarded with discounts or bonuses.

While that alone can't be considered malicious, third-party apps for any legitimate services should be treated with caution, as there is no guarantee they won't be modified to contain malicious functionality later on.

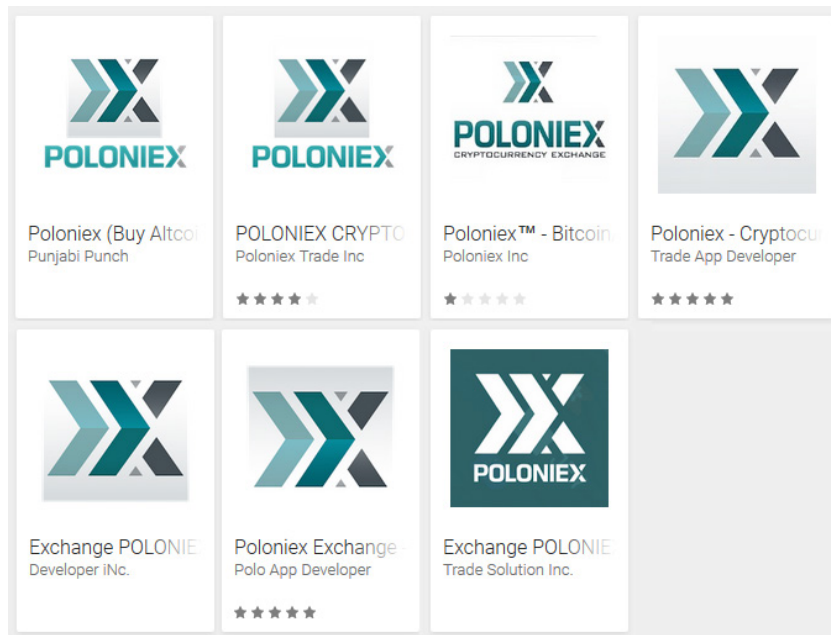
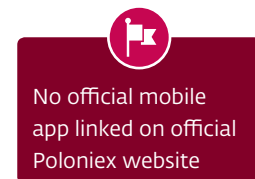


Figure 1 // The fake Poloniex apps on Google Play



2. FAKE CRYPTOCURRENCY WALLET APPS

The fake wallet apps we've analyzed use different methods of defrauding victims of their virtual coins – some try to trick victims into transferring coins to the attackers' wallet, some phish for personal information tied to victims' wallets, others combine these or come up with further creative tricks.

Wallet address scams

Out of all the scams targeting users of cryptocurrency wallets, the wallet address scams are likely the easiest to see through.

The apps using this trick are based on a simple principle: right after being launched, and without requiring any kind of registration, the apps pretend to generate a public key for a new wallet, presented as copyable text and/or a scannable QR code. If users follow the instructions and send currency to this

wallet, they will find that they can't do any further actions with the amount they had sent – they don't own the private key necessary for accessing the wallet. The attackers, however, do, and the sent amount is now at their full disposal.

We've seen this technique in apps targeting Bitcoin as well as other cryptocurrencies. Rather than being isolated cases, the apps often come in batches, tied to a single attacker either by developer name, or shared wallet addresses. We've found dozens of apps with this kind of fraudulent behavior and reported them to Google's security teams which promptly removed them from Google Play. (Figures 2, 3, 4)

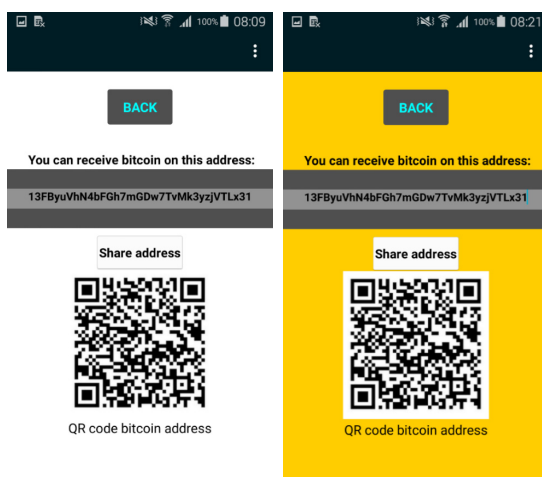


Figure 2 // Two separate fake bitcoin wallet apps using the same wallet address

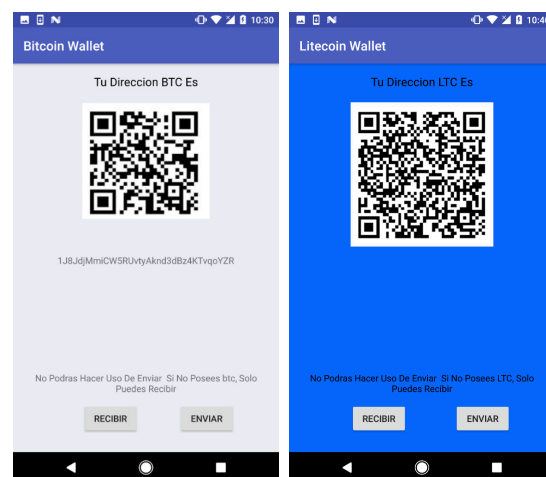


Figure 3 // Two of the eleven fake wallets targeting Spanish users

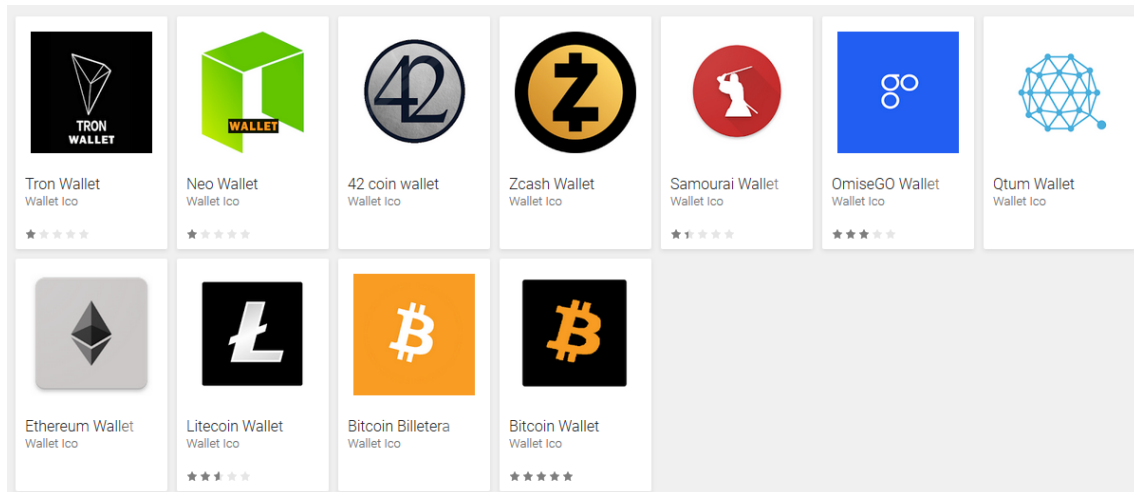


Figure 4 // Eleven fake wallets for various cryptocurrencies uploaded under the same developer name, targeting Spanish users



Unknown developers; no registration required; no private key provided to the user

Phishing & more phishing: Fake MyEtherWallet apps

Users of both cryptocurrency exchanges and wallets are frequently targeted by phishing apps. With wallets, however, there is usually even more at stake than with exchanges – a stolen password situation can potentially be resolved with the help of the exchange holding the user's private key, but in case of a wallet, it's the private key that gets compromised, with no one else to save the day.

An example of a cryptocurrency wallet we've observed as being continuously impersonated by scammers is MyEtherWallet, a popular open-source Ethereum wallet. Like the Poloniex exchange, MyEtherWallet doesn't offer an official Android app, to date, and is thus an easy target. (Figure 5)

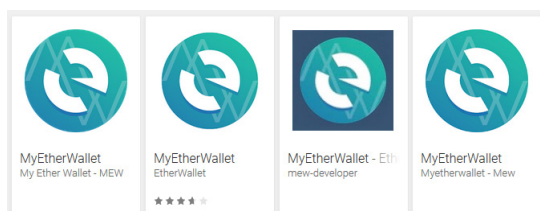


Figure 5 // The fake MyEtherWallet apps on Google Play

The phishing app misusing the wallet's name, reuploaded to Google Play multiple times under different developer names, tries to trick victims into giving away the private key or mnemonic phrase tied to their MyEtherWallet account. While obtaining either the key or the phrase is enough to gain control over the victim's wallet, some variants of the fake MyEtherWallet we've analyzed play it safe and "double phish" for both items, in two sequential forms. (Figure 6)

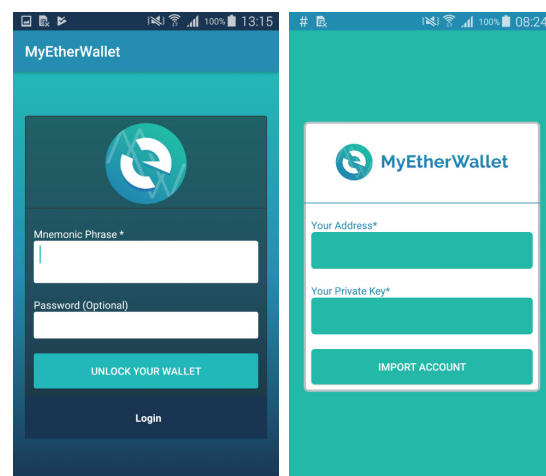
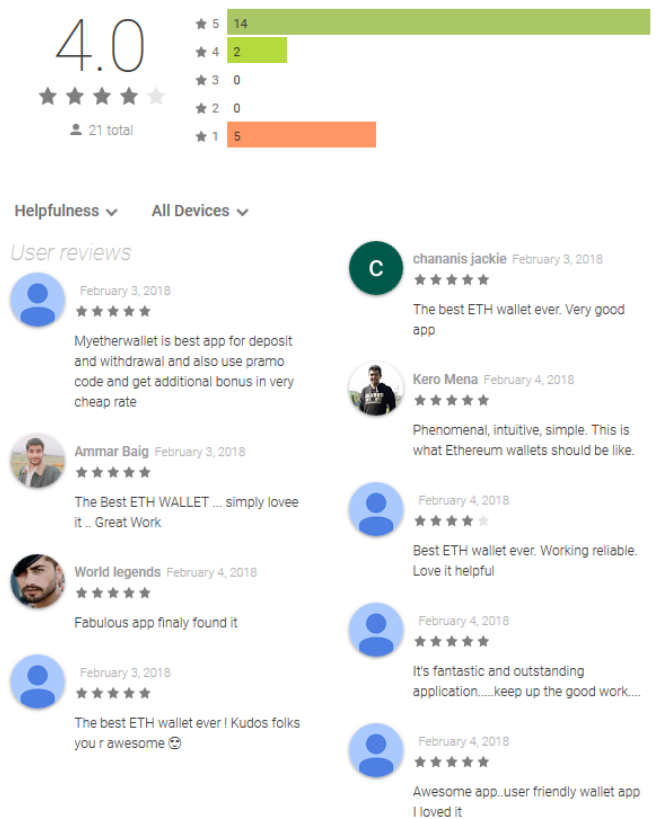


Figure 6 // Phishing forms used by some fake MyEtherWallet apps

To increase the chances of their app being downloaded, scammers also tend to make sure the app has a good initial rating and at least a dozen highly positive reviews. This was no different with the fake MyEtherWallet apps, as seen in [Figure 7](#).

No official mobile app linked on MyEtherWallet's website; generic positive reviews



[Figure 7](#) // Fake positive reviews for one of the bogus MyEtherWallet apps

A malicious mix: Cardano ADA Wallet

The app we discovered on Google Play as “Cardano ADA Wallet”, uploaded under the developer name “Cardano inc”, is an example of scammers combining “a bit of everything” to increase their success rate. ([Figure 8](#))

The malicious app pretends to be a wallet for Ada, an alternative cryptocurrency run on the blockchain platform Cardano¹. Once launched, the app starts out much as the previously described wallet address scams, luring victims into transferring Ada coins to the attackers’ wallet. ([Figure 9](#))

Next, the fraudsters try their luck with phishing, using a trick presented as a desktop wallet recovery function. The desktop wallet is promised to be transferred to the app once

users enter their wallet address and phrase. As in the case of the malicious MyEtherWallet, the stolen phrase can be used for accessing and controlling victims’ wallets. ([Figure 10](#))

Apart from these tricks, the app also seemingly offers an exchange function between a wide array of cryptocurrencies (namely Bitcoin, Litecoin, Dash, Bitcoin Cash, Bitcoin Gold, Dogecoin and Ripple) and Cardano (Ada). In reality, users are directed to the attacker’s own deposit address when submitting coins for exchange. The only difference to the previously described wallet address scams is that by using the guise of an exchange, the attackers don’t have to limit themselves to a single currency per app. ([Figure 11](#))

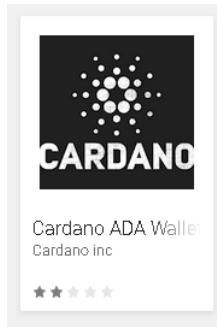


Figure 8
The malicious
“Cardano ADA Wallet”
on Google Play

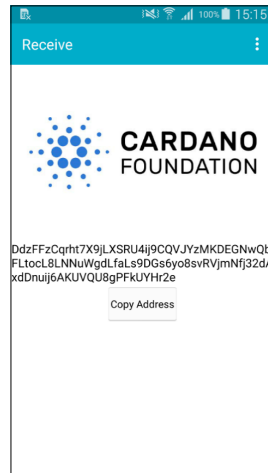


Figure 9
Opening screen of the
malicious “Cardano
ADA Wallet”

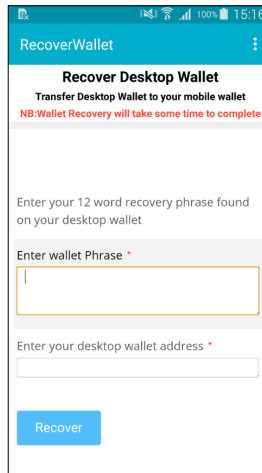


Figure 10
“RecoverWallet” phishing
trick used by the malicious
“Cardano ADA Wallet”

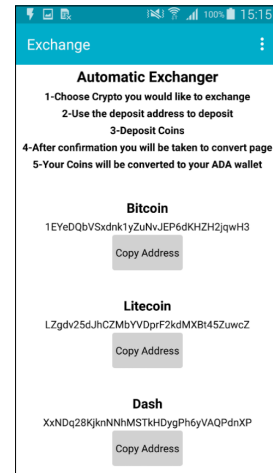


Figure 11
“Exchange” trick used by
the malicious “Cardano
ADA Wallet”



No official mobile app linked on Cardano's website

3. ANDROID CRYPTO-MINING MALWARE

With the overall surge in cryptocurrency mining observed over recent months, the number of Android-based miners has also been rising. While the effectiveness of using smartphones for resource-intensive mining is questionable to say the least, the trend shown in Figure 12 indicates that malware authors seem determined to try it regardless. (Figure 12)

Whether a crypto-mining app is considered malicious is essentially a question of consent – are users deliberately downloading an app with the intention to use their device's processing power to mine cryptocurrency, or is the device being hijacked with someone else making the profit? When the latter is the case, we speak of crypto-mining malware.

The mining functionality of Android crypto-mining malware is achieved either by including a crypto-mining framework in apps or by running crypto-mining scripts in mobile browsers, also known as in-browser mining or cryptojacking.

Testing new revenue streams on millions of users: Bug Smasher

A recent example of an app that was caught misusing victims' devices to covertly mine cryptocurrency is Bug Smasher, a popular game from the developer “aleksaant2”. This simple bug smashing game had been available on Google Play since November 2011 and had been installed between 1 and 5 million times before being removed upon our notification in January 2018.

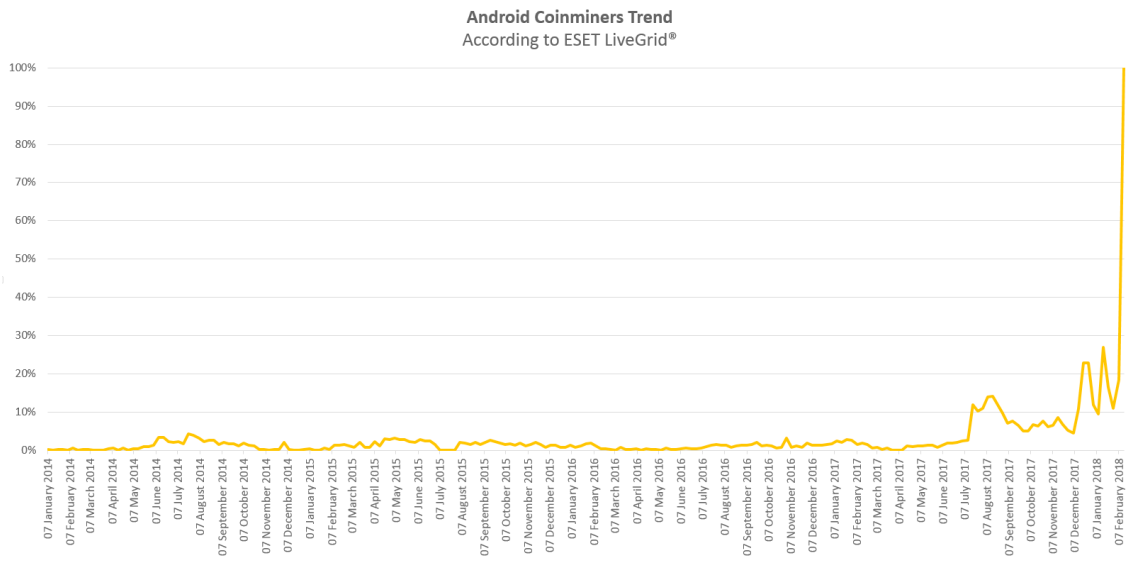
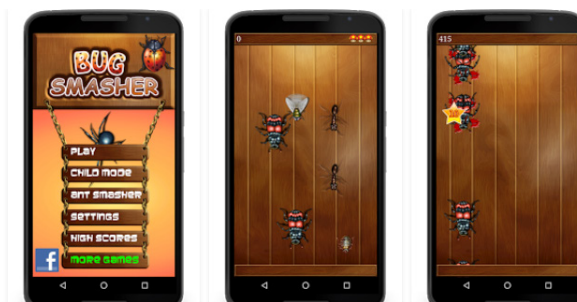
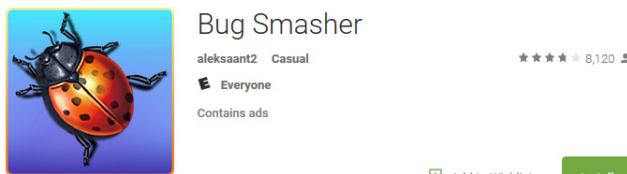


Figure 12 // Android/Coinminer trend according to ESET LiveGrid®

At the time of our discovery, the game contained a mining package that used a library to mine the cryptocurrency Monero. It is unclear when the functionality was implemented, but it was likely done through one of the more recent updates.

A common motivation for such a change is the promise of new revenue streams, which, apparently, is sometimes alluring enough to risk reputational damage. (Figure 13)



Bug Smasher
Best Bug smashing game on Android .
Smash various bugs : ants, beetles, spiders, cockroaches, flies, ladybug, shield bug.
Cool graphics. Child mode for your kids. They will love it.
Smash all those bugs. Have fun.
Don't touch the scorpion and bomb.



Reduced phone performance
– lagging, overheating, shorter battery life, etc.

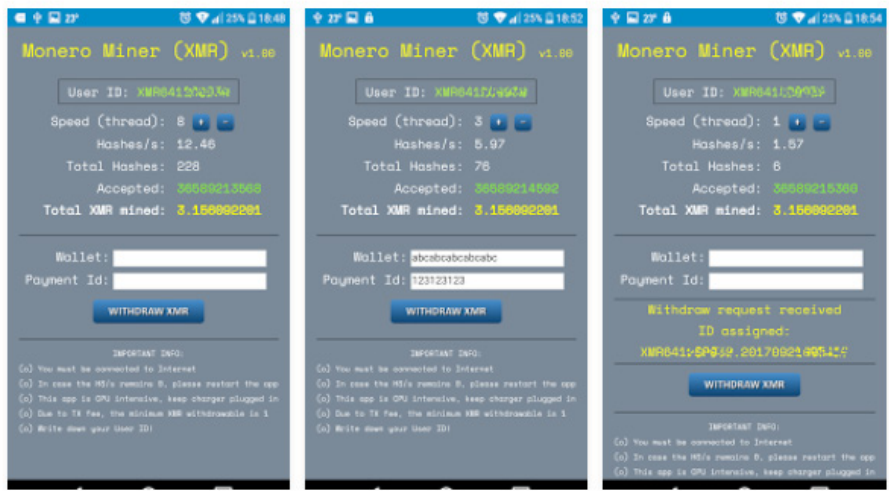
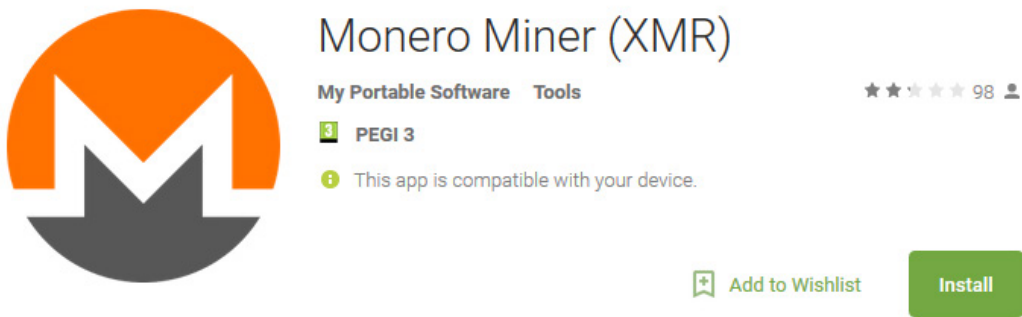
Figure 13 // The Bug Smasher app with hidden crypto-mining functionality

Mining Monero as promised, just not for you: Monero Miner (XMR)

While some scammers try to take advantage of unsuspecting users and hide the mining in apps with other functionalities, others go after cryptocurrency enthusiasts specifically looking for mobile mining apps.

The app named “Monero Miner (XMR)” by the developer “My Portable Software”, that we

recently discovered on Google Play promises to mine Monero inside a browser, and it does just that – only the reward is not sent to the device user, but to the app developer. The deceptive app had reached between 10,000 and 50,000 installs since September 2017 and was removed from the Google Play store in February 2018 based on ESET’s notification. (Figure 14)



**** NEWS **** now you can mine Monero directly from your web browser using the power of your desktop CPU!

Visit our site: www.monerowebminer.com

A simple and smart app for mining Monero coins (XMR) with your smartphone.

Figure 14 // “Monero Miner (XMR)” on Google Play



Unknown developer; low rating and negative reviews

4. FAKE CRYPTO-MINERS AND FREE GIVEAWAYS

Unlike apps that don't disclose their mining intentions are apps that pretend to be mining (or in some other way "obtaining") cryptocurrency for the user, but in reality don't do much else than display ads. And to maximize the effect of the ads, these scam apps are often built in a way that incentivizes users to open them on a regular basis – to continue with mining or to receive more "free" coins every day. While these apps aren't malware per se, we consider them unwanted due to their deceptive nature.

5 stars for empty promises: Fake bitcoin miners

Due to its increasing difficulty, bitcoin mining nowadays can't be feasibly done using regular CPUs found in PCs, let alone mobile devices². That, however, isn't enough to stop scammers from disguising their ad-riddled apps as Android bitcoin miners.

As the "mining" inside these apps progresses, the user's earnings balance seemingly increases. In some of the fake miners we've analyzed, the fake mining was interrupted with pop-ups promising a reward for leaving 5-star ratings for the app. In the pop-ups we've seen during our analysis of "Bitcoin Miner Android" from the developer "Miner Coin" and "Bitcoin Miner Automatic – Earn free Bitcoins" from the developer "Mining and Utility Apps", the reward was set to 50,000 Satoshi³. (Figure 15)

The number displayed to the user as their earnings balance is arbitrarily set by the operators of the apps. In one of the apps

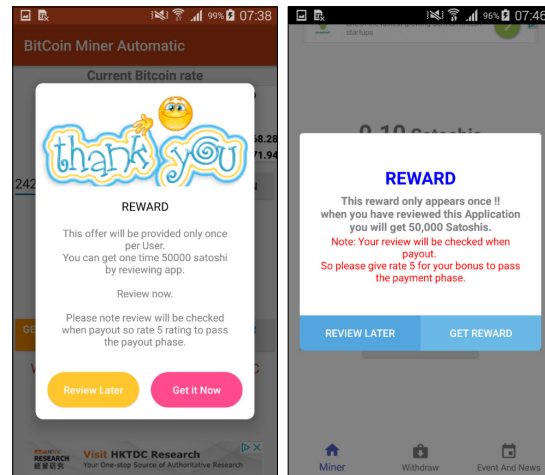


Figure 15 // Fake reward offered in exchange for 5-star ratings in "Bitcoin Miner Automatic – Earn free Bitcoins" and "Bitcoin Miner Android"

("Bitcoin Miner – Earn Free BTC" from the developer "Honey Corporation"), this number could even be altered by the user in the configuration file in shared preferences. Without wading through a barrage of ads, we conveniently changed our earnings from zero to two hundred BTC (Figure 16).

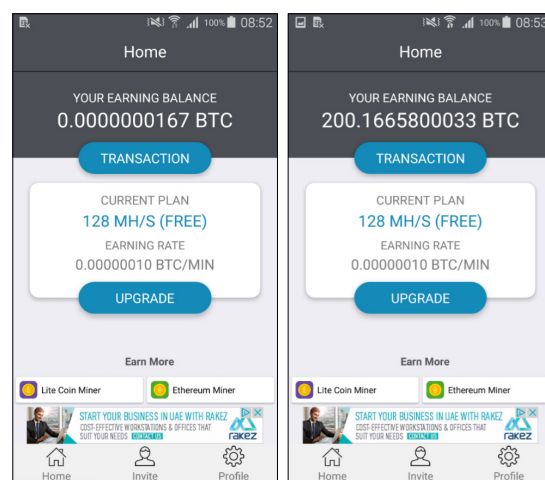


Figure 16 // Arbitrary earnings balance altered in the configuration file of "Bitcoin Miner – Earn Free BTC"

Needless to say, there is no amount of bitcoin to be redeemed. In spite of the obvious, the scammers made some effort to appear trustworthy – once the request for withdrawal to a bitcoin wallet address is submitted, the app informs the user that the payment will take three to four working days to proceed (Figure 17). The amount submitted for withdrawal is then seemingly subtracted from the user’s earnings balance.

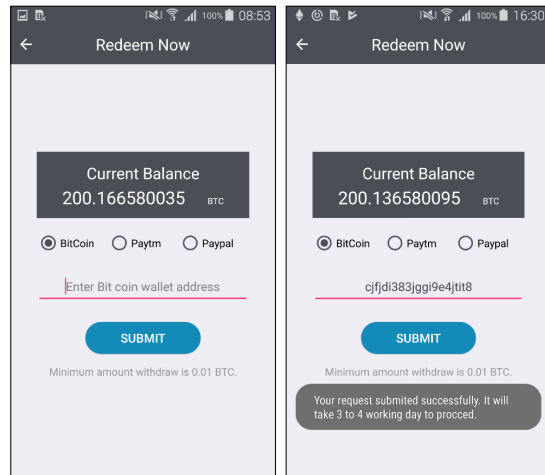


Figure 17 – Fake bitcoin withdrawal screen in “Bitcoin Miner – Earn Free BTC”

 Infeasibility of bitcoin mining on Android

What do you mean it can't be mined? Fake Ripple miners

An especially daring attempt at fooling users into viewing ads are apps that promise to mine the cryptocurrency Ripple (XRP) – a non-minable currency by definition⁴. Despite this, ESET has

found and reported a number of “Ripple mining” ad-displaying apps on Google Play, often with thousands of installs. (Figures 18, 19)

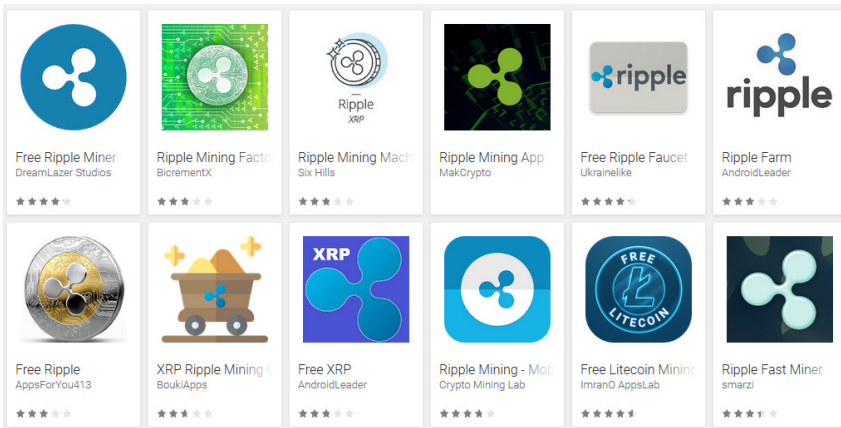


Figure 18 // Fake Ripple miners on Google Play

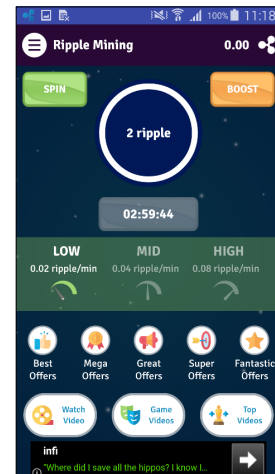


Figure 19 // Deceptive “mining” screen in one of the fake Ripple miners

 Ripple non-minable by definition

HOW TO STAY SAFE

Seeing the many ways cybercrooks have been misusing the current cryptocurrency craze on the Android platform, it is important to be aware of their tricks and to take preventive measures.

Here's what you can do to stay safe:

1. First and foremost, treat cryptocurrency exchanges and wallets and their security and legitimacy with the same level of caution as your mobile banking apps.
2. If you'd like to download a mobile app for a cryptocurrency exchange or wallet, first make sure the service **really offers a mobile app**. If that's the case, the app should be linked on the service's official website, redirecting you to a legitimate download source.
3. If the option is available, use 2-factor-authentication to protect your exchange or wallet accounts with an extra layer of security.
4. When downloading apps from Google Play, pay attention to the number of downloads, as well as app ratings and reviews. Be extra careful with newly published apps with generic-sounding positive reviews and read also their negative counterparts.
5. If something sounds too good to be true, it most probably is – an Android app is not very likely to award you with free bitcoins or any other cryptocurrency.
6. Keep your Android device updated and use a reliable mobile security solution to protect it from the latest threats.

CONCLUSION

Based on the threats described above, we can conclude that cybercrooks have recently put a great deal of effort into targeting cryptocurrency enthusiasts with deceptive mobile apps.

Scammers have several reasons to do so – users might for example be vigilant when downloading unknown software on their computer, but not think twice before installing a handy-looking app. There's also the significant advantage of "unclaimed territory" in cases where a popular service doesn't offer a mobile app. Finally, fake ratings and reviews increase the attackers' chance of deceiving unsuspecting users.

In this whitepaper, we have identified the most dominant cryptocurrency-related threats currently targeting Android users, dividing them into four categories:

1. Fake cryptocurrency exchange apps
2. Fake cryptocurrency wallet apps
3. Android crypto-mining malware
4. Fake crypto-miners and free giveaways

It is important to note that all the apps discussed within these categories are detected and blocked by ESET systems and have been suspended from the Google Play store. Users with Google Play Protect enabled are protected via this [mechanism](#).

IOCS

Package name	Hash	Detection name
com.myportablesoftware.minermonero	2041EE5D49D55767EC7994F184649C85	Android/Coinminer.AB
com.puissantapps.bugsmasher.free	289E8B3D442BA3B6E3826604D35AC37B	Android/Coinminer.Q
com.thunkable.android.cryptodevapp.ADA_Daedalus_Walletg	2043A5C7959A9CC264EFE491225EE220	Android/FakeApp.HX
com.appybuilder.amal_zaki_meka212.BitcoinWallet	2778B8493E0E71E5AA3CF70E3BB2A3D0	Android/FakeApp.HM
com.appybuilder.amal_zaki_meka212.BitPhonex	955D2E3D4F765BEBE95570AC5581379D	Android/FakeApp.HM
com.appybuilder.amal_zaki_meka212.blockchaincoin	C1EB276F805F93D5BCE3FCBB722E55AE	Android/FakeApp.HM
com.bitcoin.btc.neowallelt	F811C48C500A3A01F45334740B74D40C	Android/FakeApp.HZ
com.criptomoendas.fa.ethwallet	4AB2E39EC35A6D08CE3249359C504520	Android/FakeApp.HZ
com.libretriunfo.fa.billeterabitcoin	E5171496DCDB335379F5F51B576FEB39	Android/FakeApp.HZ
com.libretriunfo.fa.btcwallets	66658D4F035699057E0271960B3F49F5	Android/FakeApp.HZ
com.libretriunfo.fa.litecoinwallet	57A6F8EADAE0D514FA33C92D91629944	Android/FakeApp.HZ
com.wallet.a42coin42.coin4242	C0C9B28ABE57F8FBC71516205AE67F9D	Android/FakeApp.HZ
com.wallet.omisego.omisego	A964ACED6978BA202CA7B8D98434528A	Android/FakeApp.HZ
com.wallet.qtum.qtumwallet	C275D99C6CD664FB7B811255114F174D	Android/FakeApp.HZ
com.wallet.samouraiwallet.samouraiwallet	B15C2140E8DAC2E6799A0C9FDC1857ED	Android/FakeApp.HZ
com.wallet.trx.tronwallet	969D36420F64A7B4FD9725711FAFE5D1	Android/FakeApp.HZ
com.wallet.zcashwallet.zcash	9CDFE189E3E3FF0DAC95B60CFF71B58A	Android/FakeApp.HZ
com.ether.etherwallet	C9D4175E61EBCB22BA8F028F141E18C2	Android/FakeApp.HT
com.myetherwallet	B73E2436954C088E5EA0C3FE683EBB48	Android/FakeApp.HV
com.wallet.ether.myetherwallet	05BFD8C85224A680512CB75BD46B8CB4	Android/FakeApp.HV
com.myetherwalletproject	3F85490F886755B6E1BDEAA4BE1F70A4	Android/FakeApp.HV
com.poloniex.PoloApps	49EB93C6DB5858BC692F3C270D0ADA8B	Android/FakeApp.HK
com.cryptocurrencytrade.app	290CDFDAEA6BA6F53D60E52EA5C418C2	Android/FakeApp.HK
com.devpolo.app	AD4A5355193643AF0169C24911155407	Android/FakeApp.HK
com.poloniex.buysell	EA31ABE6E01B1DBB1F4D9EE0A2C0277B	Android/FakeApp.HK
com.poloniextrade.com	CB5E264A445A83FEA399AC5811FB28EB	Android/FakeApp.HK

Endnotes

- 1 The only official wallet for Ada to date is named Daedalus, and is only available on desktop.
- 2 Specialized hardware known as an ASIC (Application-Specific Integrated Circuit) is needed for profitable bitcoin mining.
- 3 One Satoshi is currently the smallest unit of the bitcoin currency recorded on the block chain, amounting to 0.00000001 BTC.
- 4 The reason for this is that Ripple (XRP) wasn't designed as a standard cryptocurrency, but rather as a native part of the digital payment network created by the company Ripple.