# Sunny with a chance of stolen credentials: Malicious weather app found on Google Play

By Lukas Stefanko

Archived: 2026-04-06 01:27:12 UTC

ESET Research

ESET has spotted a new banking malware on Google Play. Disguised as a weather forecast app, it steals banking credentials and locks screens.

22 Feb 2017 • , 4 min. read

Android users were the target of new banking malware with screen locking capabilities, which was disguised as a weather forecast app on Google Play.

Detected by ESET as Trojan.Android/Spy.Banker.HU, the malware was a trojanized version of the otherwise benign weather forecast application Good Weather.

The malicious app managed to get around Google's security mechanisms and appeared in the store on February 4th, only to be reported by ESET two days later and consequently pulled from the store. During its short lifetime, the app found its way to devices of up to 5000 users.

Besides the weather forecast functionalities it adopted from the original legitimate application, the trojan is able to lock and unlock infected devices remotely and intercept text messages. Apart from doing so, the trojan targeted the users of 22 Turkish mobile banking apps, whose credentials were harvested using phony login forms.

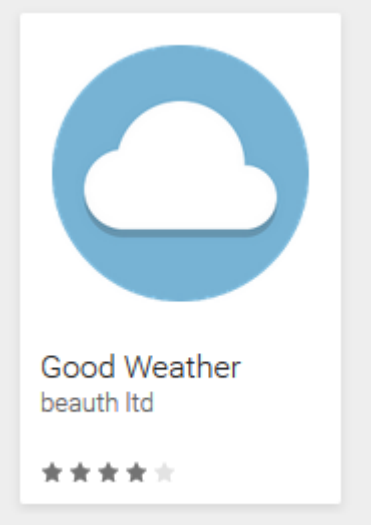



Figure 1: Trojanized Good Weather app on Google Play

# Good Weather

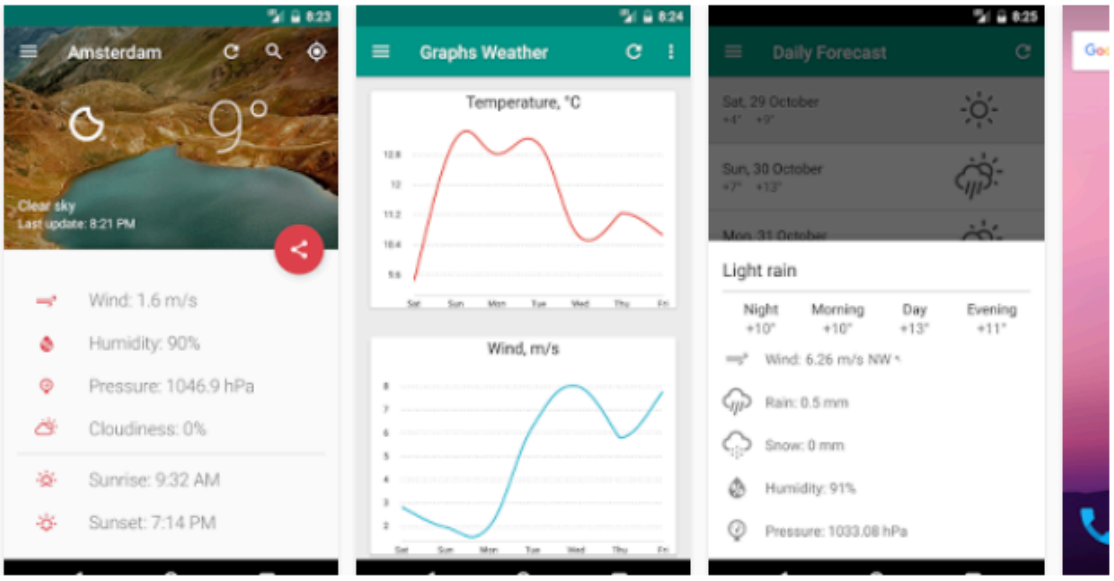
**beauth ltd** **Weather**

30

PEGI 3

This app is compatible with your device.

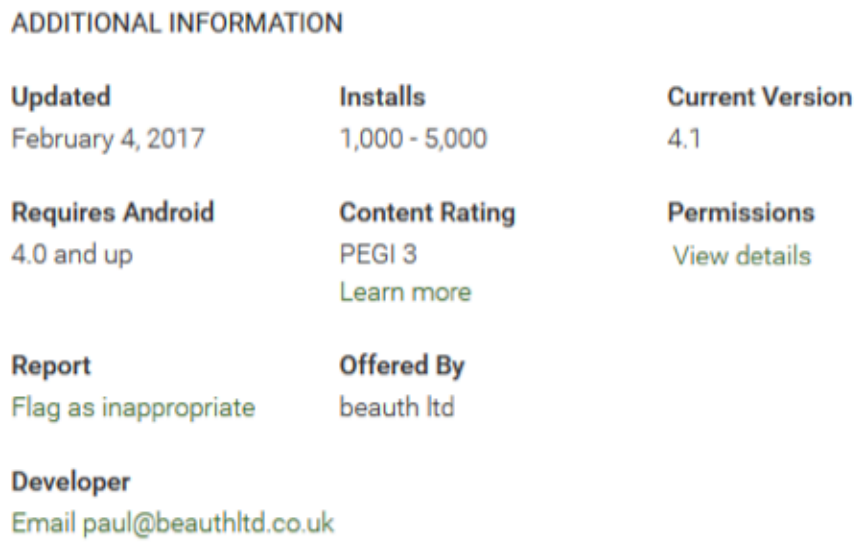
Add to Wishlist **Install**




Good Weather. The most beautiful weather app. Ever.

Don't let bad weather take you by surprise! Set the gorgeous animated wallpapers with live weather conditions on your home screen and be aware of any weather that is coming your way. Whether it is cloudy, rainy, snowy or even stormy outside, Weather Live will provide you with current weather conditions and forecast in your city and multiple locations all around the world.

READ MORE


ADDITIONAL INFORMATION

**Updated**
February 4, 2017

**Installs**
1,000 - 5,000

**Current Version**
4.1

**Requires Android**
4.0 and up

**Content Rating**
PEGI 3
Learn more

**Permissions**
View details

**Report**
Flag as inappropriate

**Offered By**
beauth ltd

**Developer**
Email paul@beauthltd.co.uk

Figure 2: Malicious app description as found on Google Play

## How does it operate?

After the app is installed by an unsuspecting user, its weather-themed icon disappears. The infected device then displays a fake system screen requesting device administrator rights on behalf of fictitious “System update”. By enabling these rights, the victim allows the malware to *Change the screen-unlock password* and *Lock the screen.*

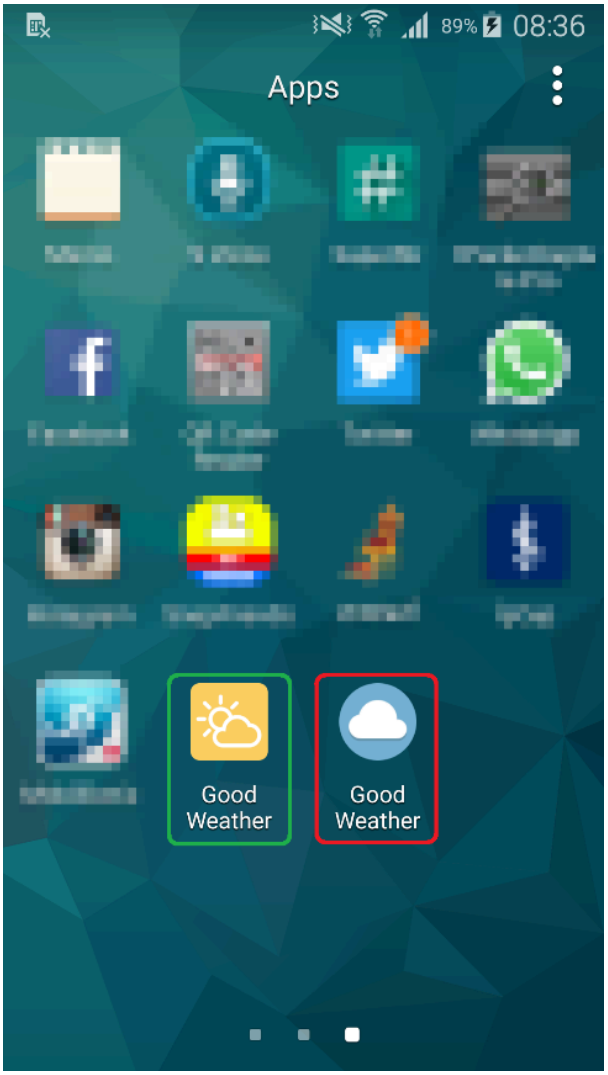



Figure 3: Green - legitimate Good Weather icon, Red – malicious version

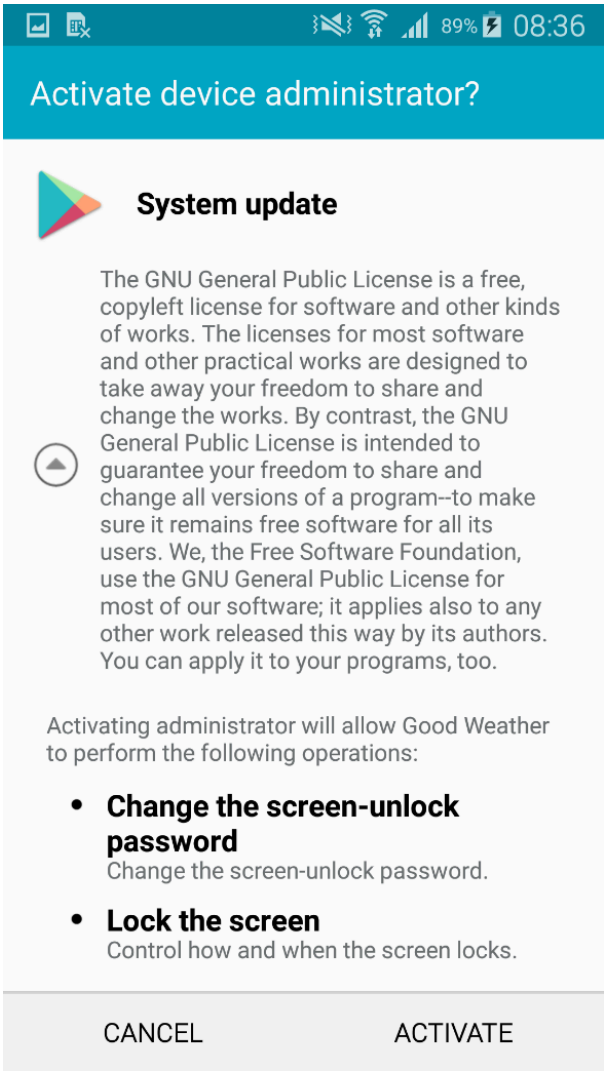



Figure 4: Fake “System update” demanding device administrator rights

Together with the permission to intercept text messages obtained during the installation, the trojan is now all set to start its malicious activity.

Users who are not alarmed at this point might be pleased with the new weather widget they can add to their home screens. However, in the background, the malware is getting to work sharing device information with its C&C server.

Depending on the command it gets in return, it can intercept received text messages and send them to the server, remotely lock and unlock the device by setting a lock screen password of the attackers’ choice, and harvest banking credentials.

The trojan displays a fake login screen once the user runs one of the targeted banking apps and sends entered data to the attacker. Thanks to the permission to intercept the victims’ text messages, the malware is also able to bypass SMS-based two-factor authentication.

As for the device locking, we suspect this function enters the picture when cashing out the compromised bank account, to keep the fraudulent activity hidden from the user. Once locked out, all victims can do is wait until the

malware receives a command to unlock the device.

## Has my device been infected? How do I clean it?

If you've recently installed a weather app from the Play Store, you might want to check if you haven't been one of the victims of this banking trojan.

In case you think you might have downloaded an app named Good Weather, check for its icon under your apps. See the yellow icon from Fig. 3? Your app is safe. Can't find any icon and the app only works as a widget? Search further under Settings -> Application Manger. If you find the app with its blue icon in your Application Manager, as depicted below, you have downloaded the malicious Good Weather imitation.

To clean your device, you can turn to a renowned mobile security solution, such as ESET Mobile Security, or you can remove the malware manually.

To manually uninstall the trojan, it is first necessary to deactivate its device administrator rights found under Settings -> Security -> System update. With that done, you can uninstall the malicious app in Settings -> Application Manger -> Good Weather.

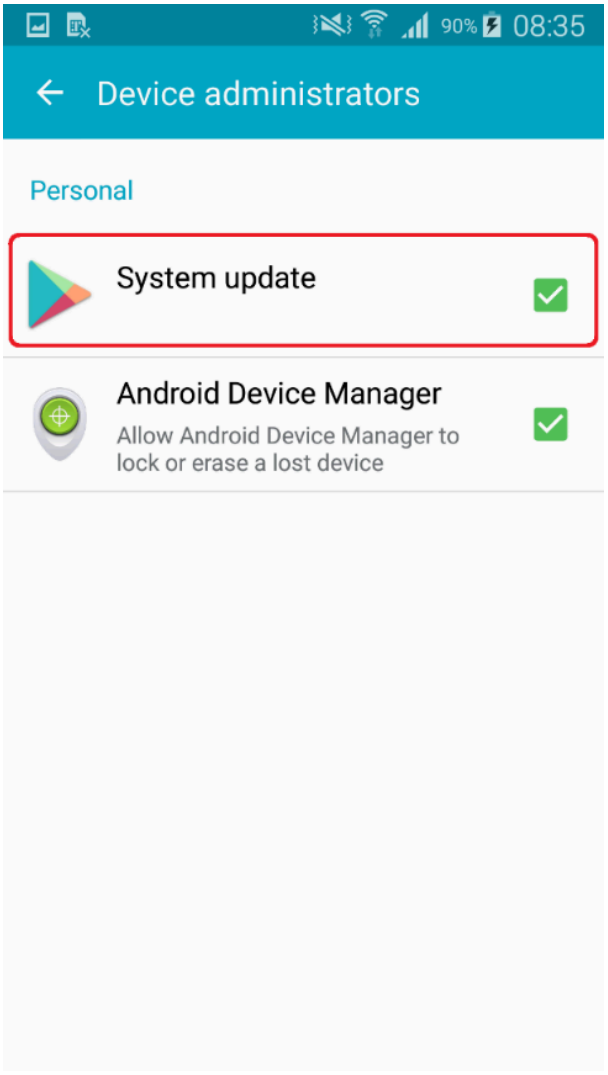


Figure 5: Malware disguised as System update under active Device administrators

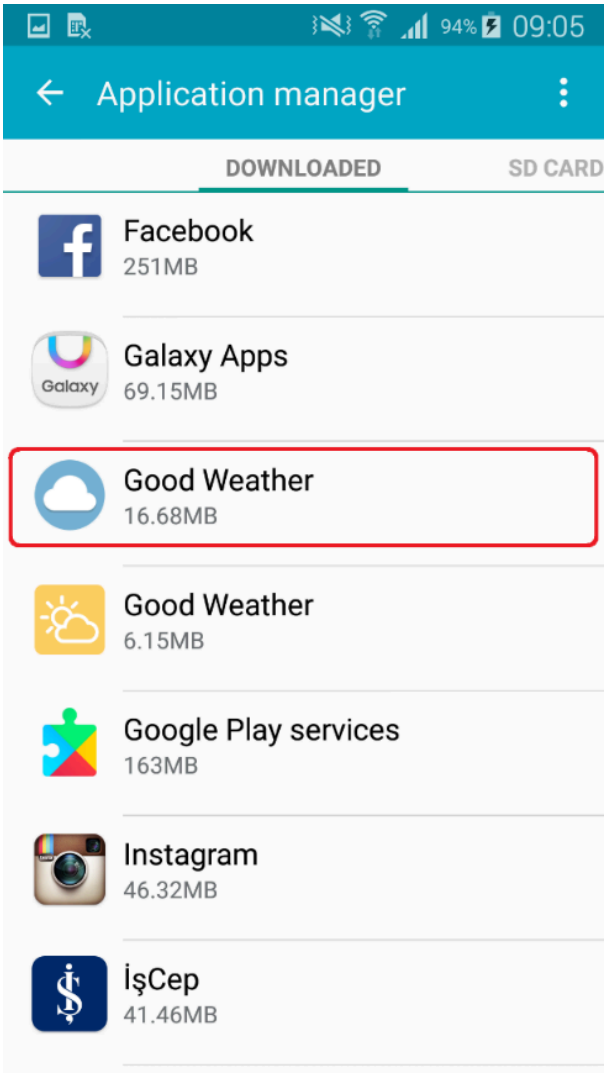



Figure 6: The trojan in Application Manager

## How to stay safe

Since the trojanized version of the app has already been pulled from the store, it is safe to download Good Weather, as originally delivered to Google Play by the developer AsdTm.

However, as malicious fakes of legitimate apps continue to infiltrate the Play Store, it’s good to stick to some basic principles to keep you from encountering them first-hand.

Although not flawless, Google Play does employ advanced security mechanisms to keep malware out. As this may not be the case with alternative app stores or other unknown sources, opt for the official Google Play store whenever possible.

While downloading from the Play store, make sure to get to know the app permissions before installing or updating. Instead of automatically giving an app the permissions it demands, consider what they mean for the app

as well as your device. If anything seems out of line, read what other users write in their reviews and rethink downloading accordingly.

After running anything you've installed on your mobile device, keep paying attention to what permissions and rights it requests. An app that won't run without advanced permissions that aren't connected to its intended function might be an app you don't want installed on your phone.

Last but not least, even if all else fails, a reputable mobile security solution will protect your device from active threats.

If you'd like to find out more about Android-based malware, look into our latest research on the topic.

You're also welcome to stop by ESET's stand at this year's Mobile World Congress.

## Analyzed sample's Indicators of Compromise (IoCs)

| Package Name | Hash | Detection |
|---|---|---|
| goodish.weather | A69C9BAD3DB04D106D92FD82EF4503EA012D0DA9 | Android/Spy.Banker.HU |

## Targeted applications

com.garanti.cepsubesi
com.garanti.cepbank
com.pozitron.iscep
com.softtech.isbankasi
com.teb
com.akbank.android.apps.akbank_direkt
com.akbank.softotp
com.akbank.android.apps.akbank_direkt_tablet
com.ykb.androidtablet
com.ykb.android.mobilonay
com.finansbank.mobile.cepsube
finansbank.enpara
com.tmobtech.halkbank
biz.mobinex.android.apps.cep_sifrematik
com.vakifbank.mobile
com.ingbanktr.ingmobil
com.tmob.denizbank
tr.com.sekerbilisim.mbank
com.ziraat.ziraatmobil
com.intertech.mobilemoneytransfer.activity
com.kuveytturk.mobil
com.magiclick.odeabank

---

Source: https://www.welivesecurity.com/2017/02/22/sunny-chance-stolen-credentials-malicious-weather-app-found-google-play/