Released Android malware source code used to run a banking botnet

welivesecurity.com/2017/02/23/released-android-malware-source-code-used-run-banking-botnet/

February 23, 2017

ESET researchers have discovered a new variant of botnet-forming Android banking malware based on source code made public a couple of months ago.

Lukas Stefanko
23 Feb 2017 - 02:00PM

ESET researchers have discovered a new variant of botnet-forming Android banking malware based on source code made public a couple of months ago.

Update (February 23rd): Following ESET's notice, the hosting company took the C&C server down.

The new Android banking malware ESET recently discovered on Google Play was spotted in the wild again, targeting more banks. Further investigation of this resurfacing threat has uncovered its code was built using source code that was made public a couple of months ago.

The previous version was detected by ESET as Trojan.Android/Spy.Banker.HU (version 1.1 – as marked by its author in the source code) and reported on February 6th. The malware was distributed via Google Play as a trojanized version of a legitimate weather forecast application Good Weather. The trojan targeted 22 Turkish mobile banking apps, attempting to harvest credentials using phony login forms. Moreover, it could lock and unlock infected devices remotely, as well as intercept text messages.

Last Sunday, we discovered a new version of the trojan on Google Play, masquerading as yet another legitimate weather app, this time World Weather. The trojan, detected by ESET as Trojan.Android/Spy.Banker.HW (version 1.2), was available in the Google Play store from February 14th until being reported by ESET and pulled from the store on February 20th.

Connecting the dots

The second discovery led to another round of investigation, which delivered some interesting revelations.

As it turns out, both of these Android trojans are based on a free source code that was made public online. Allegedly written from scratch, the "template" code of the Android malware, along with the code of the C&C server – including a web control panel – have been available on a Russian forum since December 19th, 2016.

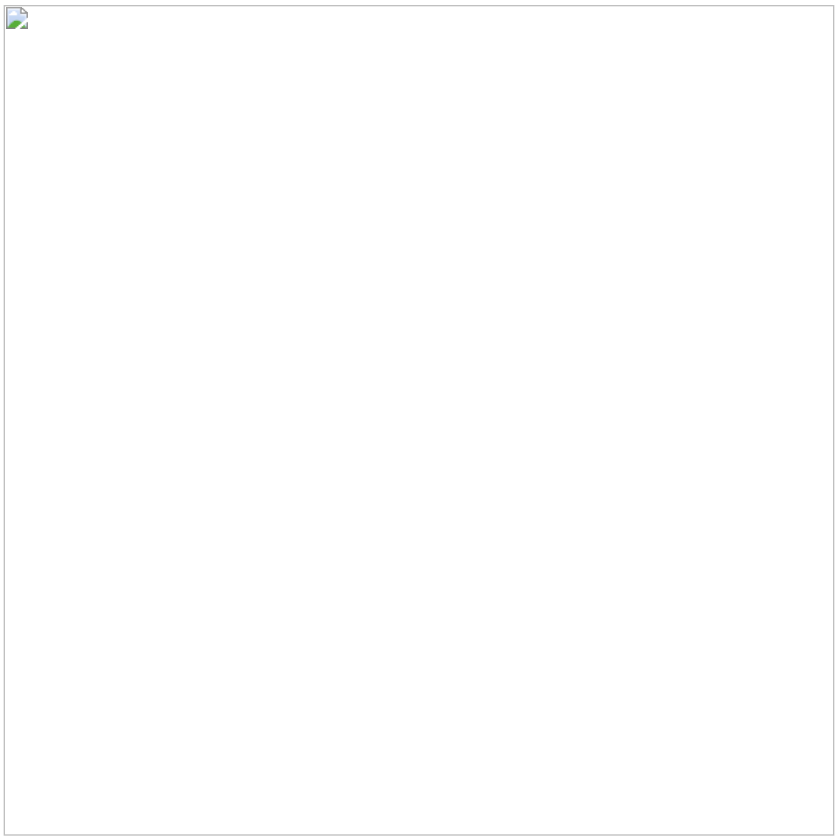
Figure 1 – Source code of the Android malware and of the C&C made public on a Russian forum

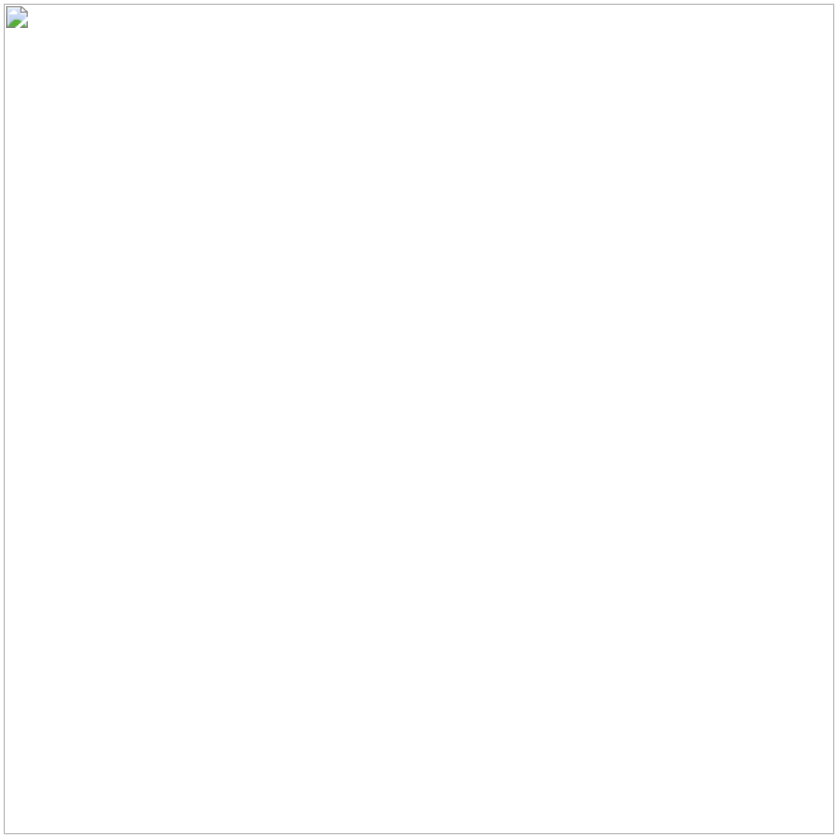
Subsequent investigation brought findings of Dr. Web to our attention , who analyzed one of the earlier variants of the malware (detected by our systems since December 26th, 2016 as Android/Spy.Banker.HH).

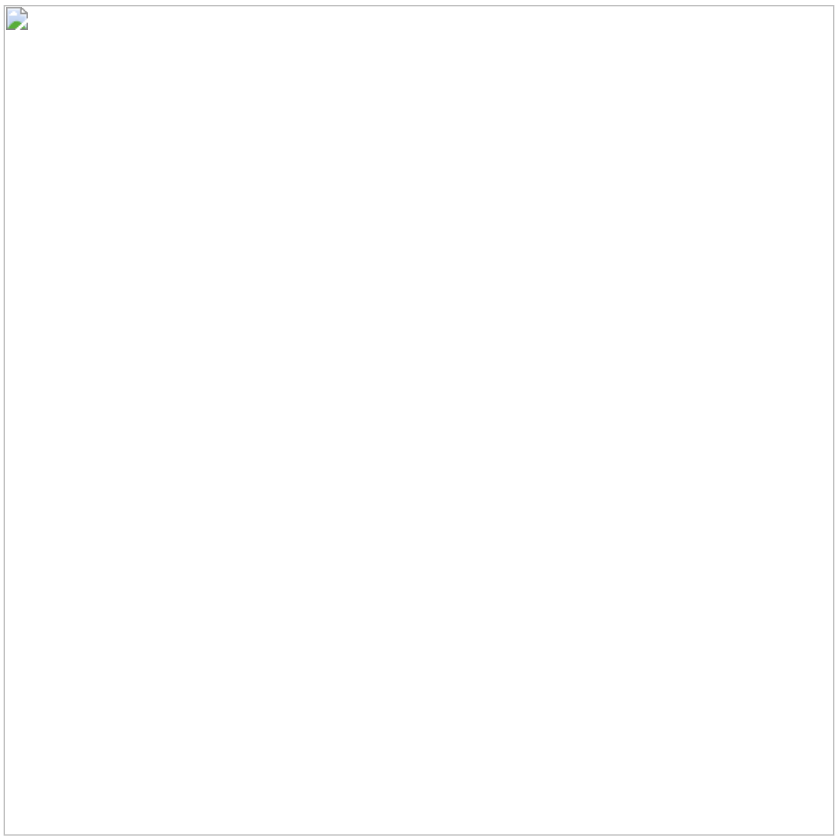
However, this variant is not directly connected to those we found on Google Play, even though we detected it under the same detection name as version 1.0. We were able to confirm this after getting access to the control panel of the botnet's C&C server, which was up and running at the time of our investigation. Through the control panel, we were able to collect information about malware versions of all of the 2800+ infected bots.

Figure 2 – C&C web control panel listing victims of the malware

Below is an overview of user groups affected by the malware, based on the botnet data listed in the C&C control panel:







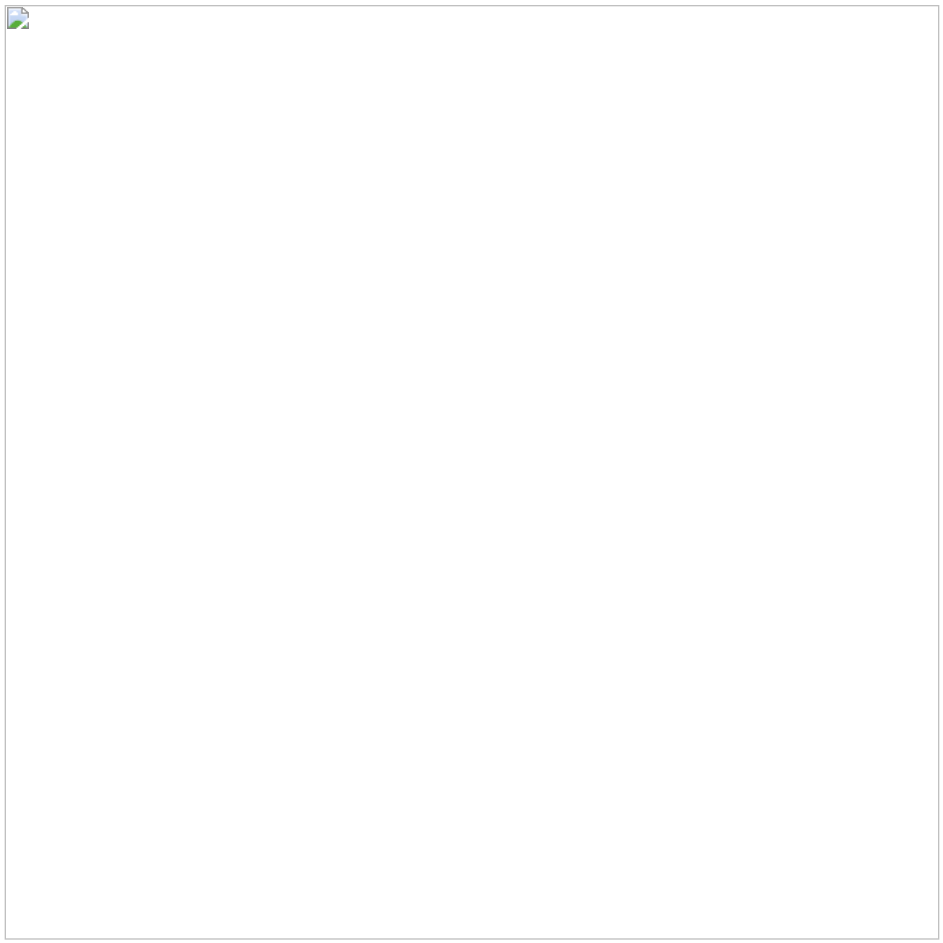
Interestingly enough, the C&C server itself, active since February 2, 2017, has been left accessible to whomever has the URL, without requiring any credentials.

Figure 3 – Investigation timeline

How does it operate?

The newly detected version has essentially the same functionalities as its predecessor. On top of the weather forecast functionalities it adopted from the original legitimate application, Trojan.Android/Spy.Banker.HW is able to lock and unlock infected devices remotely by setting the lock screen password and intercept text messages.

The only difference between the two appears to be a wider target group – the malware now affects users of 69 British, Austrian, German and Turkish banking apps – and a more advanced obfuscation technique.



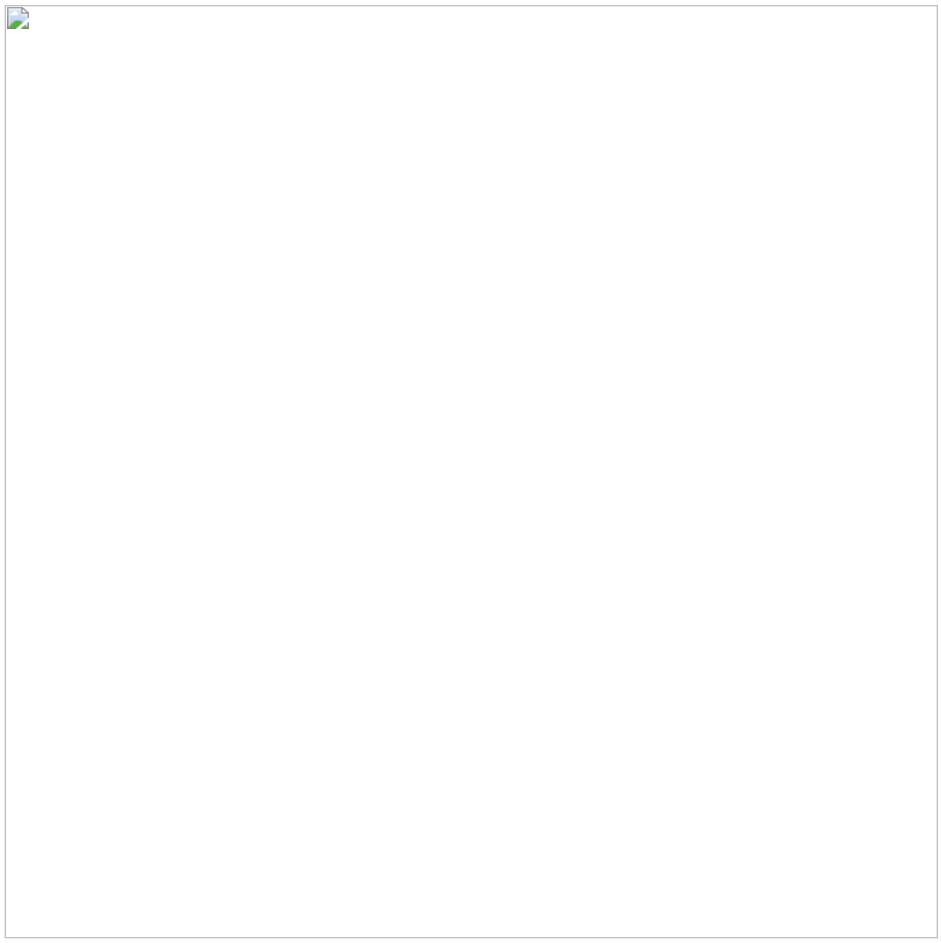


Figure 4 – The malicious app on Google Play

Figure 5 – Green – legitimate World Weather icon; Red – malicious version

The trojan also has an inbuilt notification functionality, the purpose of which could only be verified after having accessed the C&C server. As it turns out, the malware is able to display fake notifications on infected devices, prompting the user to launch one of the targeted banking apps on behalf of an “important message” from the respective bank. By doing so, malicious activity in the form of a fake login screen is triggered.

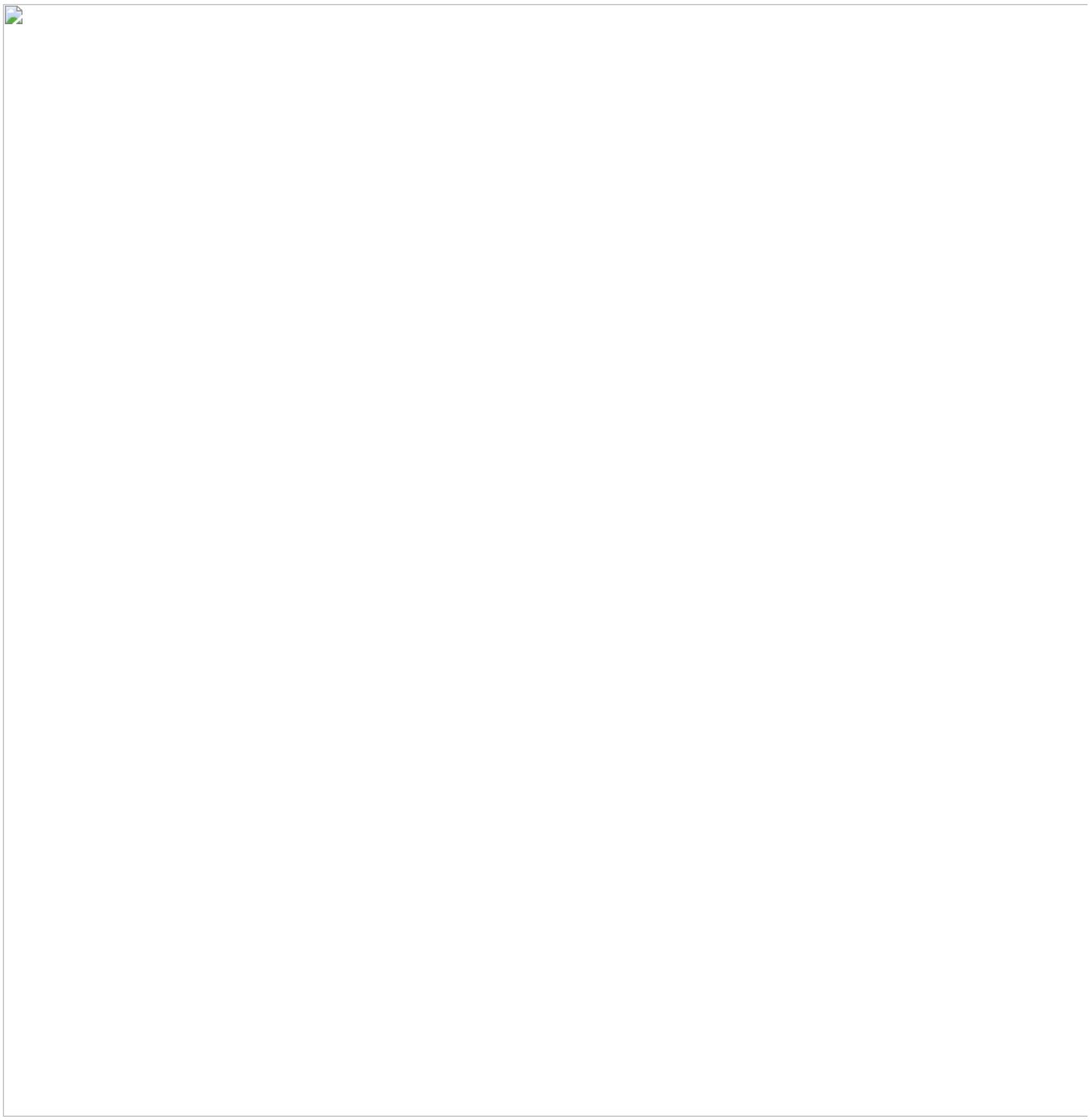


Figure 6 – C&C sending fake notification message to infected device

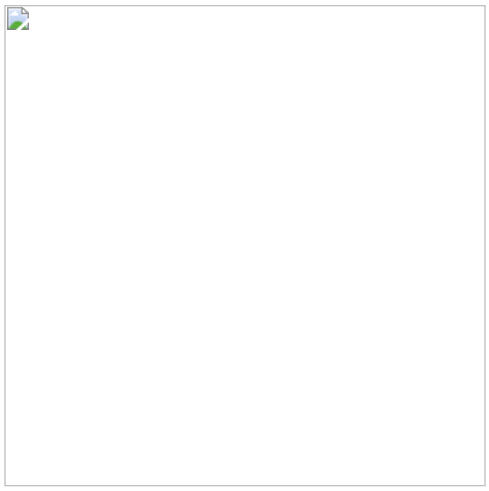


Figure 7 – fake banking app notification sent from C&C

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

If you have 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 Weather, look for it under Settings -> Application Manger. If you see the app depicted in Fig. 8, and also find "System update" under Settings -> Security -> Device administrators (Fig. 9), your device has been infected.

To clean your device, we recommend that you turn to a mobile security solution, 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 -> Weather.

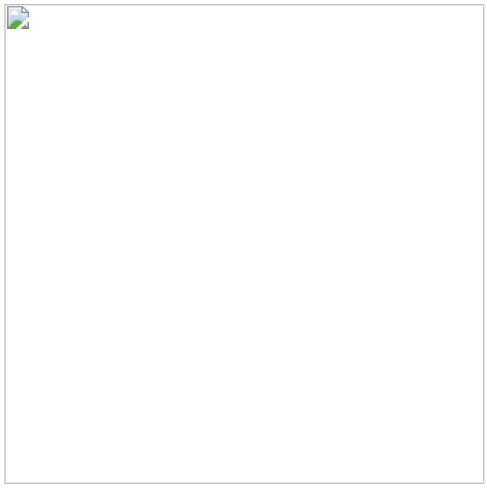


Figure 8: The trojan in Application Manager

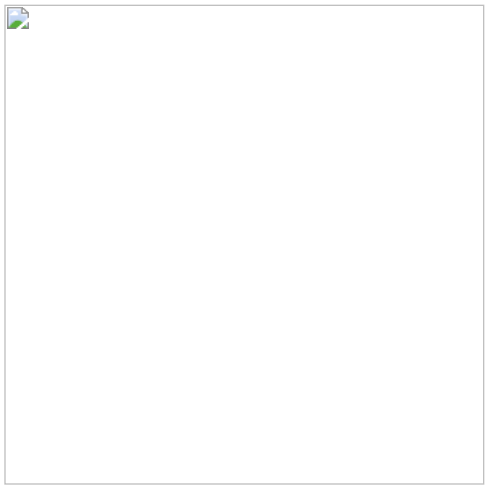


Figure 9: Malware disguised as System update under active Device administrators

How to stay safe

While the particular group of attackers behind this botnet chose to spread the malware through trojanized weather apps and target the banks listed at the bottom of this article, there is no guarantee the code isn't or won't be used elsewhere.

With that in mind, it's good to stick to some basic principles to stay protected from mobile malware.

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.

Samples

Package Name	Hash	Detection
goodish.weather	CA2250A787FAC7C6EEF6158EF48A3B6D52C6BC4B	Android/Spy.Banker.HH
goodish.weather	A69C9BAD3DB04D106D92FD82EF4503EA012D0DA9	Android/Spy.Banker.HU
follon.weather	F533761A3A67C95DC6733B92B838380695ED1E92	Android/Spy.Banker.HW

Targeted applications

Android/Spy.Banker.HH and Android/Spy.Banker.HU:

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

Android/Spy.Banker.HW:

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.android
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
com.isis_papyrus.raiffeisen_pay_eyewdg
at.spardat.netbanking
at.bawag.mbanking
at.volksbank.volksbankmobile
com.bankaustria.android.olb
at.easybank.mbanking
com.starfinanz.smob.android.sfinanzstatus
com.starfinanz.smob.android.sbanking
de.fiducia.smartphone.android.banking.vr
com.db.mm.deutschebank
de.postbank.finanzassistent
de.commerzbanking.mobil
com.ing.diba.mbbr2
de.ing_diba.kontostand
de.dkb.portalapp
com.starfinanz.mobile.android.dkbpushtan
de.consorsbank
de.comdirect.android
mobile.santander.de
de.adesso.mobile.android.gad
com.grppl.android.shell.BOS
uk.co.bankofscotland.businessbank
com.barclays.android.barclaysmobilebanking
com.barclays.bca
com.ie.capitalone.uk
com.monitise.client.android.clydesdale
com.monitise.coop
uk.co.northernbank.android.tribank
com.firstdirect.bankingonthego
com.grppl.android.shell.halifax
com.htsu.hsbcpersonalbanking
com.hsbc.hsbcukcmb
com.grppl.android.shell.CMBlloydsTSB73
com.lloydsbank.businessmobile
uk.co.metrobankonline.personal.mobile
co.uk.Nationwide.Mobile
com.rbs.mobile.android.natwest
com.rbs.mobile.android.natwestbandc
com.rbs.mobile.android.rbsm
com.rbs.mobile.android.rbsbandc
uk.co.santander.santanderUK
uk.co.santander.businessUK.bb
com.tescobank.mobile

uk.co.tsb.mobilebank
com.rbs.mobile.android.ubn
com.monitise.client.android.yorkshire

23 Feb 2017 - 02:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion