Banking malware on Google Play targets Polish banks

welivesecurity.com/2017/12/11/banking-malware-targets-polish-banks/

December 11, 2017

Besides delivering the promised functionalities, the malicious apps can display fake notifications and login forms seemingly coming from legitimate banking applications, harvest credentials entered into the fake forms, as well as intercept text messages to bypass SMS-based 2-factor authentication.

Lukas Stefanko
11 Dec 2017 - 02:58PM

Besides delivering the promised functionalities, the malicious apps can display fake notifications and login forms seemingly coming from legitimate banking applications, harvest credentials entered into the fake forms, as well as intercept text messages to bypass SMS-based 2-factor

authentication.

Another set of banking Trojans has found its way past Google Play's security mechanisms, this time targeting a number of Polish banks. The malware managed to sneak into Google Play disguised as seemingly legitimate apps "Crypto Monitor", a cryptocurrency price tracking app, and "StorySaver", a third-party tool for downloading stories from Instagram.

Besides delivering the promised functionalities, the malicious apps can display fake notifications and login forms seemingly coming from legitimate banking applications, harvest credentials entered into the fake forms, as well as intercept text messages to bypass SMS-based 2-factor authentication.

The same trojan, only under a different disguise, was recently spotted on Google Play by researchers at RiskIQ, who published their analysis of the threat in a November 9 report.

The malicious apps

The first of the malicious apps we came across, "Crypto Monitor", was uploaded to the store on November 25, 2017 under the developer name walltestudio. The other app, "StorySaver" with the developer name kirillsamsonov45, appeared on Google Play on November 29.

Together, the apps had reached between 1000 and 5000 downloads at the time we reported them to Google on December 4. Both apps have since been removed from the store.

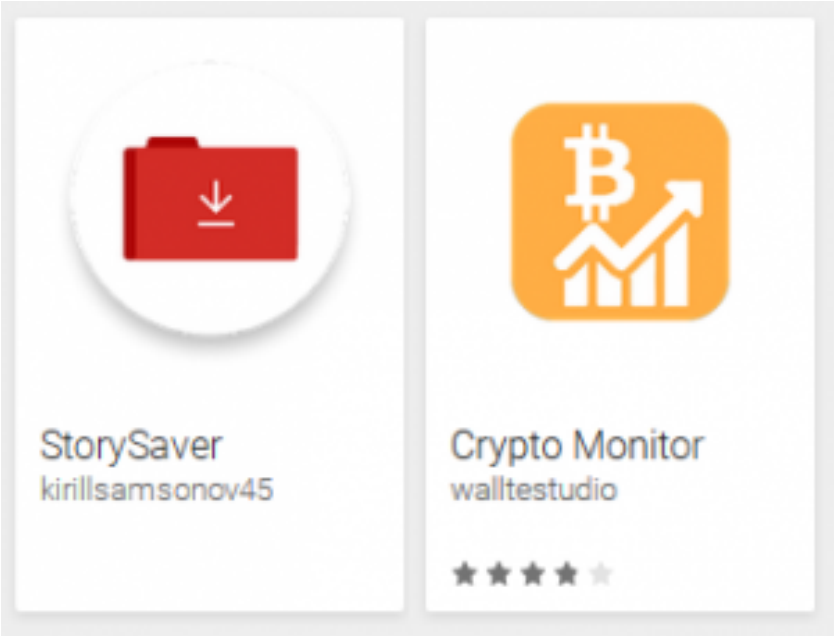

Figure 1 – The malicious apps discovered on Google Play

After the malicious apps are launched, they compare the apps installed on the compromised device against a list of targeted banking apps – in this case, the official apps of fourteen Polish banks (the list of specific banking apps can be found at the end).

If any of the fourteen apps are found on the device, the malware can display fake login forms imitating those of the targeted legitimate apps. This may happen without any action on the user's side, or after the user clicks on a fake notification displayed by the malware, seemingly on behalf of the bank.

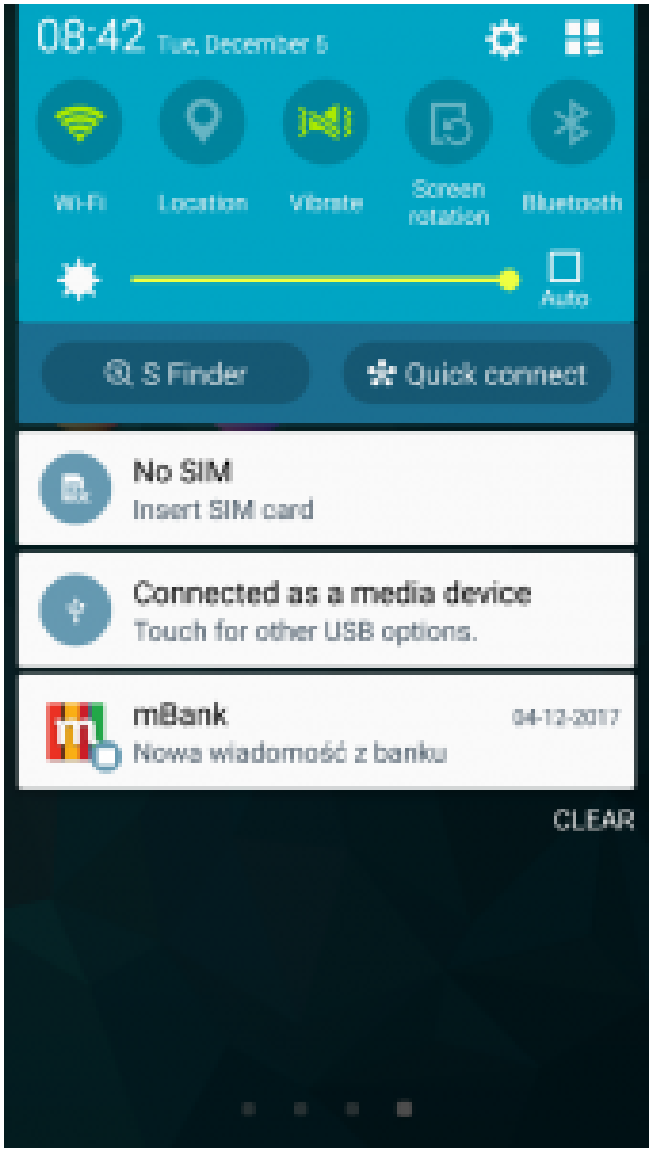

Figure 2 – Fake notification displayed by the malicious "StorySaver" app

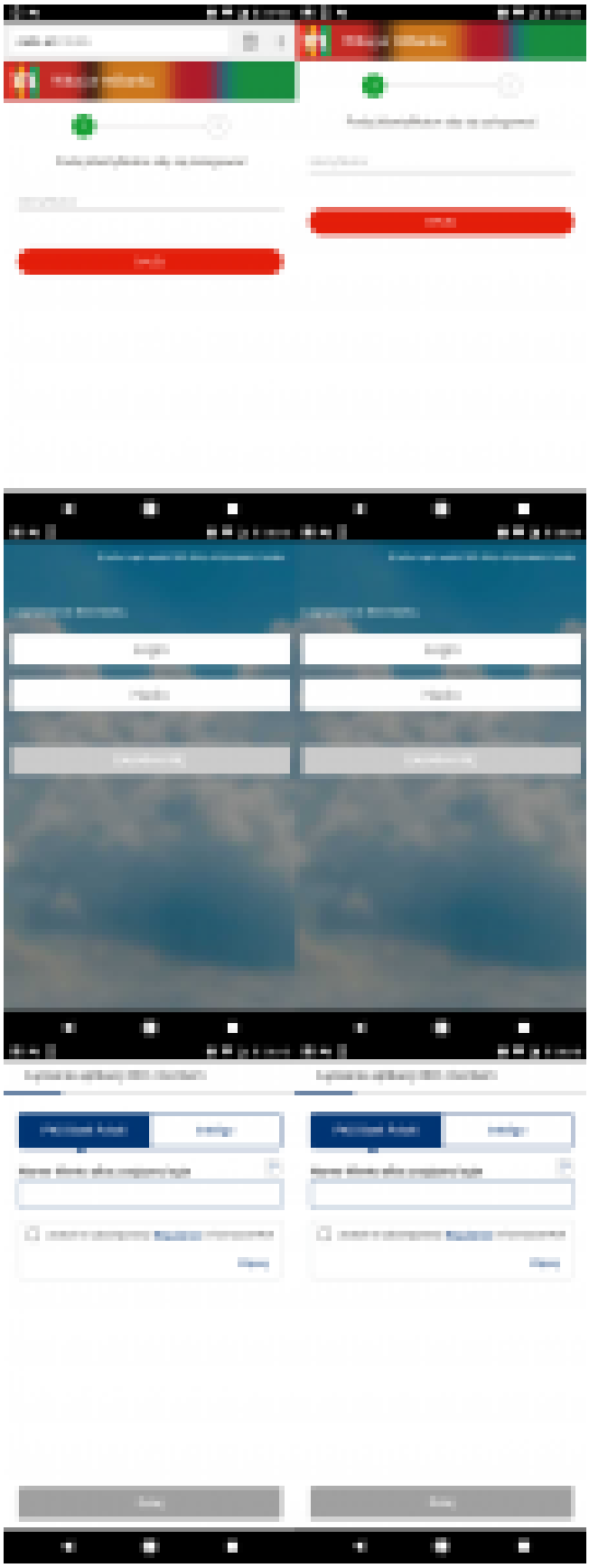

Figure 3 – Left: Fake login form; Right: legitimate login form

ESET's security systems detect the threat as Android/Spy.Banker.QL and prevent it from getting installed.

ESET telemetry shows that 96% of the detections come from Poland (the remaining 4% from Austria), apparently due to local social engineering campaigns propagating the malicious apps.

How to stay safe

The good news is that this particular banking malware doesn't use any advanced tricks to ensure its persistence on affected devices. Therefore, if you've installed any of the above described malicious apps, you can remove them by going to **Settings** > (**General**) > **Application manager/Apps**, searching for either "StorySaver" or "Crypto Monitor" and uninstalling them.

The bad news, however, is that if you have installed one of the apps on a device on which you use any of the fourteen targeted banking apps listed below, the crooks might already have access to your bank account. We advise you to check your bank account for suspicious transactions and seriously consider changing pin codes.

To avoid falling prey to mobile malware in the future, make sure to always check app ratings and reviews, pay attention to what permissions you grant to apps, and use a reputable mobile security solution to detect and block latest threats.

Targeted banking apps

App name	Package name
Alior Mobile	com.comarch.mobile
BZWBK24 mobile	pl.bzwbk.bzwbk24
Getin Mobile	com.getingroup.mobilebanking
IKO	pl.pkobp.iko
Moje ING mobile	pl.ing.mojeing
Bank Millennium	wit.android.bcpBankingApp.millenniumPL
mBank PL	pl.mbank
BusinessPro	pl.bph
Nest Bank	pl.fmbank.smart
Bank Pekao	eu.eleader.mobilebanking.pekao
PekaoBiznes24	eu.eleader.mobilebanking.pekao.firm
plusbank24	eu.eleader.mobilebanking.invest
Mobile Bank	eu.eleader.mobilebanking.raiffeisen
Citi Handlowy	com.konylabs.cbplpat

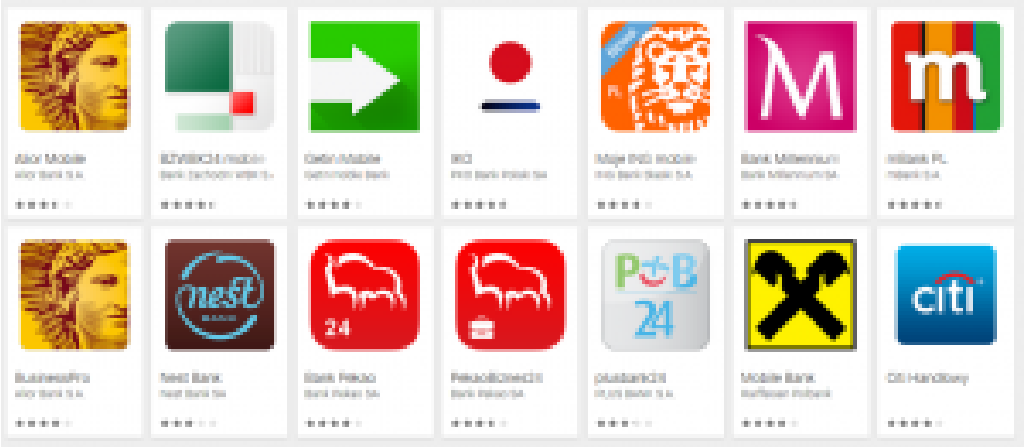

Figure 4 – Icons of the targeted banking apps

IoCs

Package Name	Hash	Phishing server
in.crypto.monitor.coins	57A96D024E61F683020BE46173D74FAD4CF05806	nelis.at
com.app.storysavernew	757EA52DB39E9CDBF5E2E95485801E3E4B19020D	sdljfkh1313.win

Special thanks to Witold Precikowski for bringing one of the malicious apps to our attention.

11 Dec 2017 - 02:58PM

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

Newsletter

Discussion