Android trojans steal Facebook users' logins and passwords

news.drweb.com/show/

Doctor Web

Back to news

July 1, 2021

Doctor Web's malware analysts have discovered malicious apps on Google Play that steal Facebook users' logins and passwords. These stealer trojans were spread as harmless software and were installed more than 5,856,010 times.

In total, our specialists uncovered 10 of these trojan apps. Of them, 9 were available on Google Play:

1. a photo-editing software called Processing Photo. It is detected by Dr.Web Anti-Virus as **Android.PWS.Facebook.13** and was spread by the developer chikumburahamilton. It was installed over 500,000 times.

2. applications that enabled access limitations for using other software installed on Android devices: App Lock Keep from the developer Sheralaw Rence, App Lock Manager from the developer Implummet col, and Lockit Master from the developer Enali mchicolo—all detected as **Android.PWS.Facebook.13**. They were downloaded at least 50,000, 10 and 5,000 times respectively.
3. Rubbish Cleaner from the developer SNT.rbcl—a utility to optimize the Android device performance. It was downloaded over 100,000 times. Dr.Web detects it as **Android.PWS.Facebook.13**.
4. astrology programs Horoscope Daily from the developer HscopeDaily momo and Horoscope Pi from the developer Talleyr Shauna, also detected as **Android.PWS.Facebook.13**. The former had more than 100,000 installs while the latter—more than 1,000 installs.
5. a fitness program called Inwell Fitness, and detected as Android.PWS.Facebook.14 from the developer Reuben Germaine. It has more than 100,000 installs.
6. an image editing app called PIP Photo that was spread by the developer Lillians. Its various versions are detected as **Android.PWS.Facebook.17** and **Android.PWS.Facebook.18**. This app has over 5,000,000 downloads.

Upon Doctor Web's specialists report to Google, part of these malicious applications was removed from Google Play. However, at the time of this news release, some apps were still available for download.

During the course of analyzing of these stealer trojans, we discovered an earlier modification that was spread through Google Play under the guise of an image editing software called EditorPhotoPip, which has already been removed from the official Android app store but still available on software aggregator websites. This modification was added to the Dr.Web virus database as **Android.PWS.Facebook.15**.

While the **Android.PWS.Facebook.13**, **Android.PWS.Facebook.14**, and **Android.PWS.Facebook.15** are native Android apps, the **Android.PWS.Facebook.17** and **Android.PWS.Facebook.18** are utilizing the Flutter framework designed for cross-platform development. Despite this, all of them can be considered modifications of the same trojan since they use identical configuration file formats and identical JavaScript scripts to steal user data.

Processing Photo

chikumburahamilton Tools

★★☆☆☆ 809

Add to Wishlist

Install

This app will provide the beautification of images and special effect filters, and image processing functions such as clipping images.

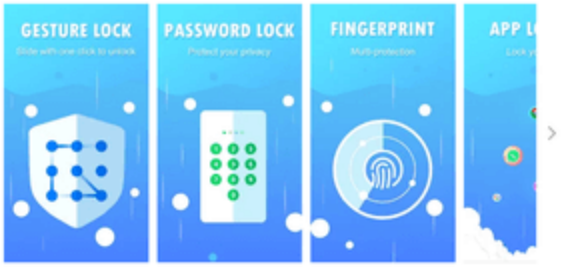
App Lock Keep

Sheralaw Rence Lifestyle

★★★★☆ 78

Add to Wishlist

Install



Main Features:
->AppLock: Lock any apps with privacy contents by using PIN lock & pattern lock
->Lock app: Lock social apps like Facebook, Instagram, WhatsApp & system apps like email, contacts and SMS
->Fake Lock: Force stop shows a fake crash screen to those who want to access your private apps
->Intruder Selfie: Snap a photo of who try to unlock your apps and record the date and time in

Rubbish Cleaner

SNT.rbcl Tools

★★★★☆ 323

This app is available for all of your devices

Add to Wishlist

Install

You can use this app to scan the cache files and junk files in the mobile phone, and clean them with one click to release the internal storage space of the mobile phone.You can also check the battery status of the mobile phone and clean up the background applications of the mobile phone.

Horoscope Daily

HscopeDaily momo Personalization

★★☆☆☆ 486

This app is available for all of your devices

Add to Wishlist

Install

Detailed astrological predictions available for all signs of the zodiac: Aries, Taurus, Gemini, Cancer, Leo, Virgo, Libra, Scorpio, Sagittarius, Capricorn, Aquarius, Pisces

★ View zodiac compatibility – select the zodiac sign of your special someone and discover aspects of happiness and harmony in your relationship, success in mutual business and outlook on family.
★ Set custom push notifications and never miss an update

Horoscope Pi

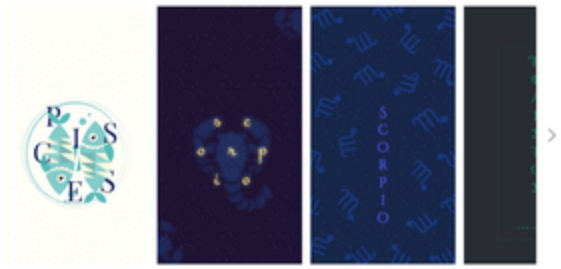
Talleyr Shauna Lifestyle

★★☆☆☆ 8

This app is available for all of your devices

Add to Wishlist

Install



Discover what the future holds for you with accurate and free daily horoscope, personalized tarot reading and love compatibility test. Get an insight on what to expect for love, money, work, health for today and tomorrow.

App Lock Manager

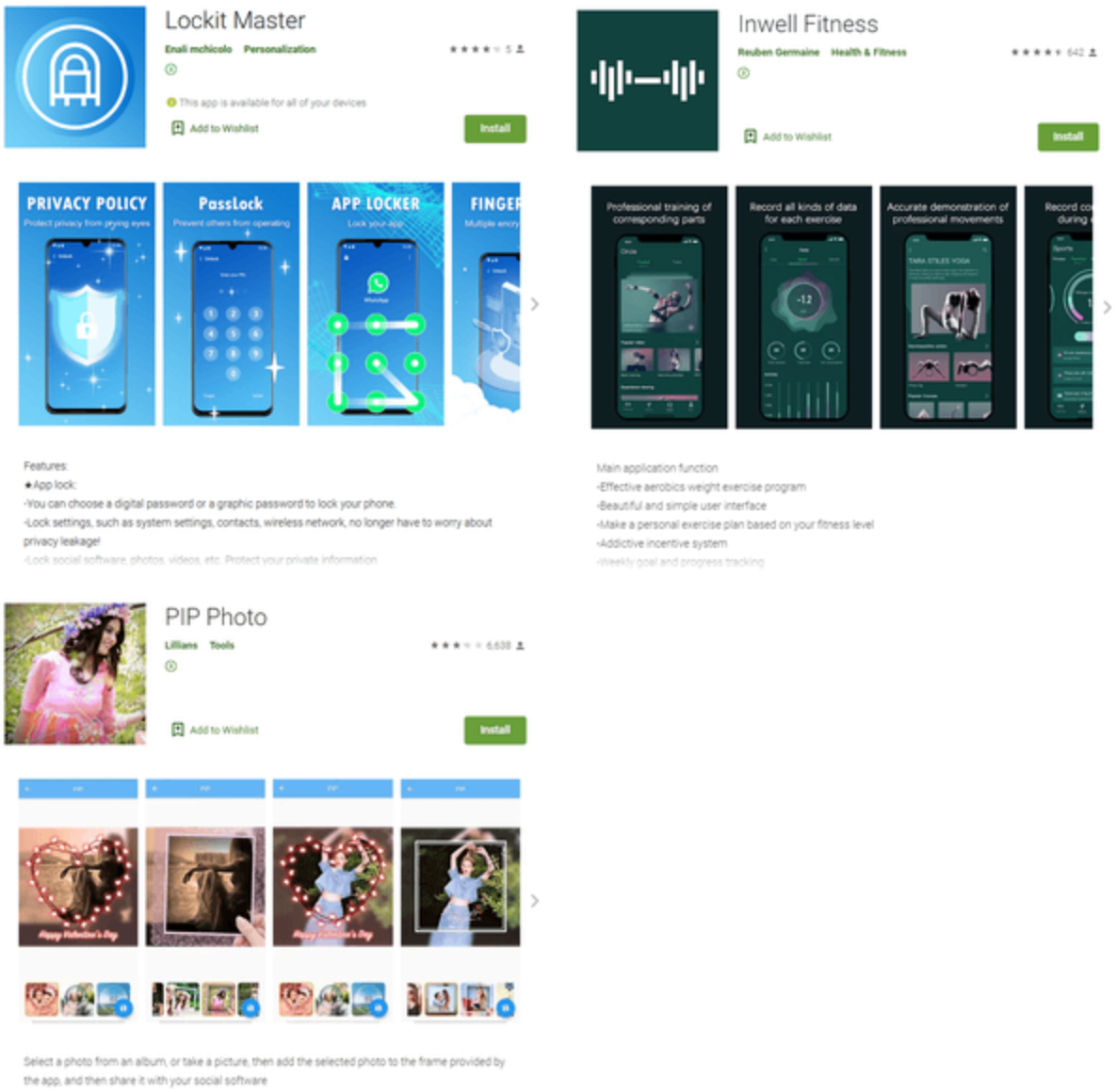
Implummet col Lifestyle

This app is available for all of your devices

Add to Wishlist

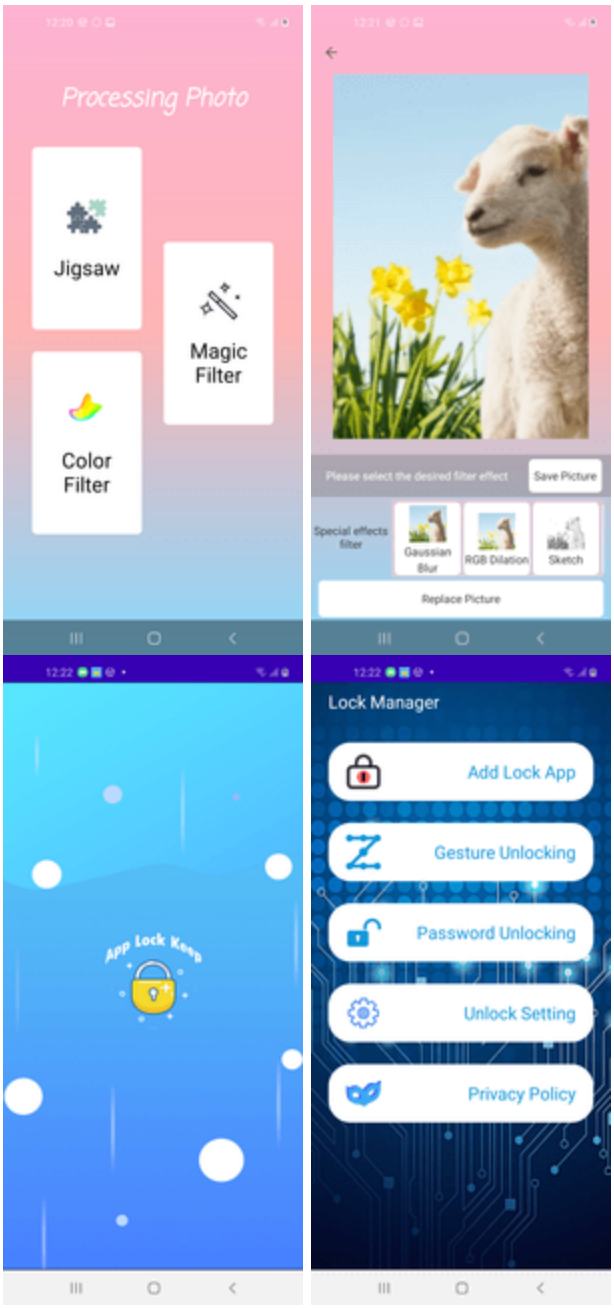
Install

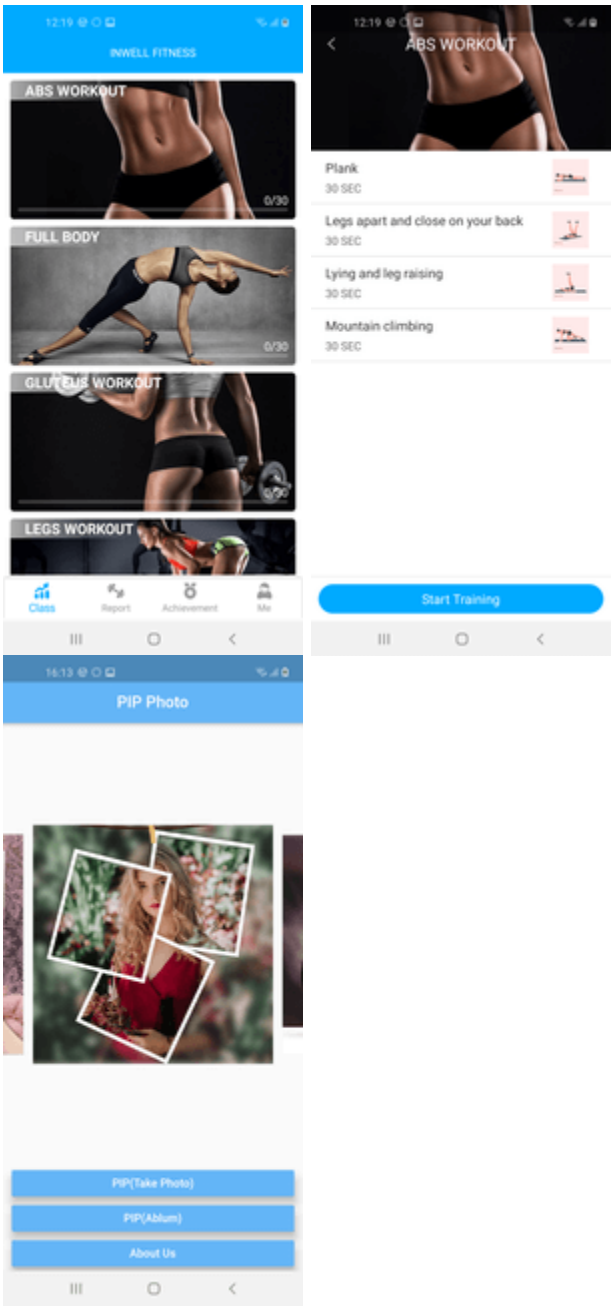
● Protect your privacy
Hide your personal pictures and videos by locking gallery and photo apps with AppLocker (App Lock)



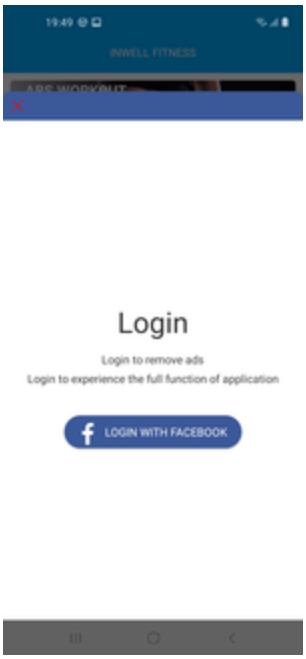
The applications were fully functional, which was supposed to weaken the vigilance of potential victims. With that, to access all of the apps' functions and, allegedly, to disable in-app ads, users were prompted to log into their Facebook accounts. The advertisements inside some of the apps were indeed present, and this maneuver was intended to further encourage Android device owners to perform the required actions.

This is how some of these apps looked upon launch:

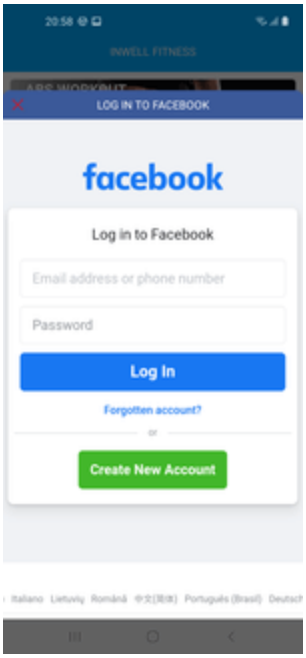

Processing Photo
Jigsaw
Magic Filter
Color Filter
Please select the desired filter effect
Save Picture
Special effects filter
Gaussian Blur
RGB Dilation
Sketch
Replace Picture
App Lock Keep
Lock Manager
Add Lock App
Gesture Unlocking
Password Unlocking
Unlock Setting
Privacy Policy



And this is the message encouraging potential victims to log into their Facebook account:



If users agreed and clicked the login button, they saw standard social network login form as shown on the next screenshot:



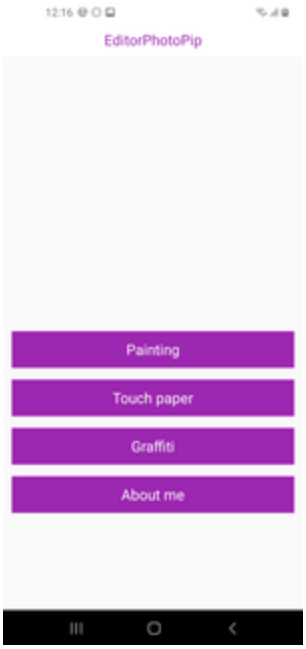
With that, the displayed form was genuine. These trojans used a special mechanism to trick their victims. After receiving the necessary settings from one of the C&C servers upon launch, they loaded the legitimate Facebook web page https://www.facebook.com/login.php into WebView. Next, they loaded JavaScript received from the C&C server into the same WebView. This script was directly used to highjack the entered login credentials. After that, this JavaScript, using the methods provided through the JavascriptInterface annotation, passed stolen login and password to the trojan applications, which then transferred the data

to the attackers' C&C server. After the victim logged into their account, the trojans also stole cookies from the current authorization session. Those cookies were also sent to cybercriminals.

Analysis of the malicious programs showed that they all received settings for stealing logins and passwords of Facebook accounts. However, the attackers could have easily changed the trojans' settings and commanded them to load the web page of another legitimate service. They could have even used a completely fake login form located on a phishing site. Thus, the trojans could have been used to steal logins and passwords from any service.

The **Android.PWS.Facebook.15** malicious program that turned out to be an earlier modification of the trojans, is identical to the others. However, it contains additional functionality to output the data into the log in Chinese, which may indicate its possible origin.

The appearance of the **Android.PWS.Facebook.15** trojan with examples of its output to the log file are shown below:




```
MyCLog.log("上报条件未达到，请求参数不完整，不执行>>>");
MyCLog.log("没有登录>>>");
MyCLog.log("cookies上报已执行>>>");
MyCLog.log("page上报已执行>>>");
MyCLog.log("bm上报已执行>>>");
MyCLog.log("BM,Page 检测js为空，不再继续>>>");
MyCLog.log("初始化js");
```

Doctor Web recommends Android device owners install applications only from known and trusted developers, as well as to pay attention to other user reviews. The reviews cannot provide an absolute guarantee that the apps are harmless but can still alarm you about potential threats. You should also pay attention to when and which apps ask you to login into your account. If you are not sure that what you are doing is safe, it would be better for you not to proceed any further and uninstall the suspicious program.

Dr.Web Anti-Virus products for Android successfully detects and deletes all known modifications of the **Android.PWS.Facebook.13**, **Android.PWS.Facebook.14**, **Android.PWS.Facebook.15**, **Android.PWS.Facebook.17**, and **Android.PWS.Facebook.18** trojan applications, so they pose no threat to our users.

Indicators of compromise

More details on **Android.PWS.Facebook.13**

More details on **Android.PWS.Facebook.14**

More details on **Android.PWS.Facebook.15**

More details on **Android.PWS.Facebook.17**

More details on **Android.PWS.Facebook.18**

Your Android needs protection.

Use Dr.Web

- The first Russian anti-virus for Android
- Over 140 million downloads—just from Google Play
- Available free of charge for users of Dr.Web home products

Free download

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments