After Big Takedown Efforts, 20 More BankBot Mobile Malware Apps Make It Into Google Play

securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/

July 27, 2017

Home&nbsp/ Banking & Finance

After Big Takedown Efforts, 20 More BankBot Mobile Malware Apps Make It Into Google Play

Banking & Finance July 27, 2017

By Limor Kessem co-authored by Shachar Gritzman 7 min read

A flashlight app, fake videos or a fake gaming app? Any one of those could be malicious and harboring a mobile malware app, right there in a trusted official app store. In an ongoing trend, IBM X-Force noted that malicious apps manage to circumvent controls and infiltrate legitimate stores. And this is not about the plethora of adware apps infecting users in the app stores, which has almost become the norm, but rather that banking malware is now turning into somewhat of a resident in Google Play.

BankBot is one of the mobile banking Trojans that has taken to the Play store in the past few months, managing to get through in the guise of widgets and benign apps. After the discovery and takedown of these apps — hundreds of them, to be exact — it seems that BankBot still finds ways to get in and infect unwitting users.

In a recent discovery, IBM X-Force mobile researchers identified at least 20 different malicious Android apps that made it into Google's Play store delivering BankBot.

Landing a place in official app stores is both effective and profitable for cybercriminals who operate mobile malware. For one, they do not have to invest in the distribution of the malware. They can save on costs associated with spam lists, SMS messaging or sending mass emails, not knowing who would eventually click and bother fetching the app from a third-party store — provided they've already enabled side-loading. It's a longer shot.

Second, malicious apps will get all that much more exposure in an official store, where hundreds of millions of people search for apps daily. Botnets are always a numbers game. Beyond sheer traffic, malware that makes it into the official stores enjoys the trust factor that comes with downloading an app from a legitimate source, likely leading to more app permissions being granted to malicious applications.

A Dangerous, Rising Trend

Bad Android apps making it into the official app store is not new by any means. It appears that criminals manage to find their way into legitimate stores, concealing their malware or including it in app updates that comes later on.

The rising trend is this: While adware and other nuisance apps have been making in into official app stores for the past few years, now we are seeing banking malware increasingly showing up in those trusted download sources. This trend is extremely problematic because it introduces an entirely different threat level to the users of official stores, making them download a mobile banking Trojan, which can inevitably lead to a significant rise in fraudulent financial activity in the weeks and months following the installation.

BankBot — In Store and Ready for Fraud

The BankBot malware emerged in January 2017, initially identified in the wild as Android.BankBot.149, go_p00t, and later named BankBot and Mazain. In essence, all these malware names relate to the same code base that was leaked soon after it was discovered.

According to X-Force research, BankBot affects only Android-based mobile devices at this time. It is part of the overlay class of mobile banking Trojans, which uses fake activity screens on top of legitimate apps to lure users into divulging their banking and payment card credentials. BankBot is geared toward financial fraud, and used by cybercriminals to commit identity theft, account takeover and spamming of the malware to additional devices.

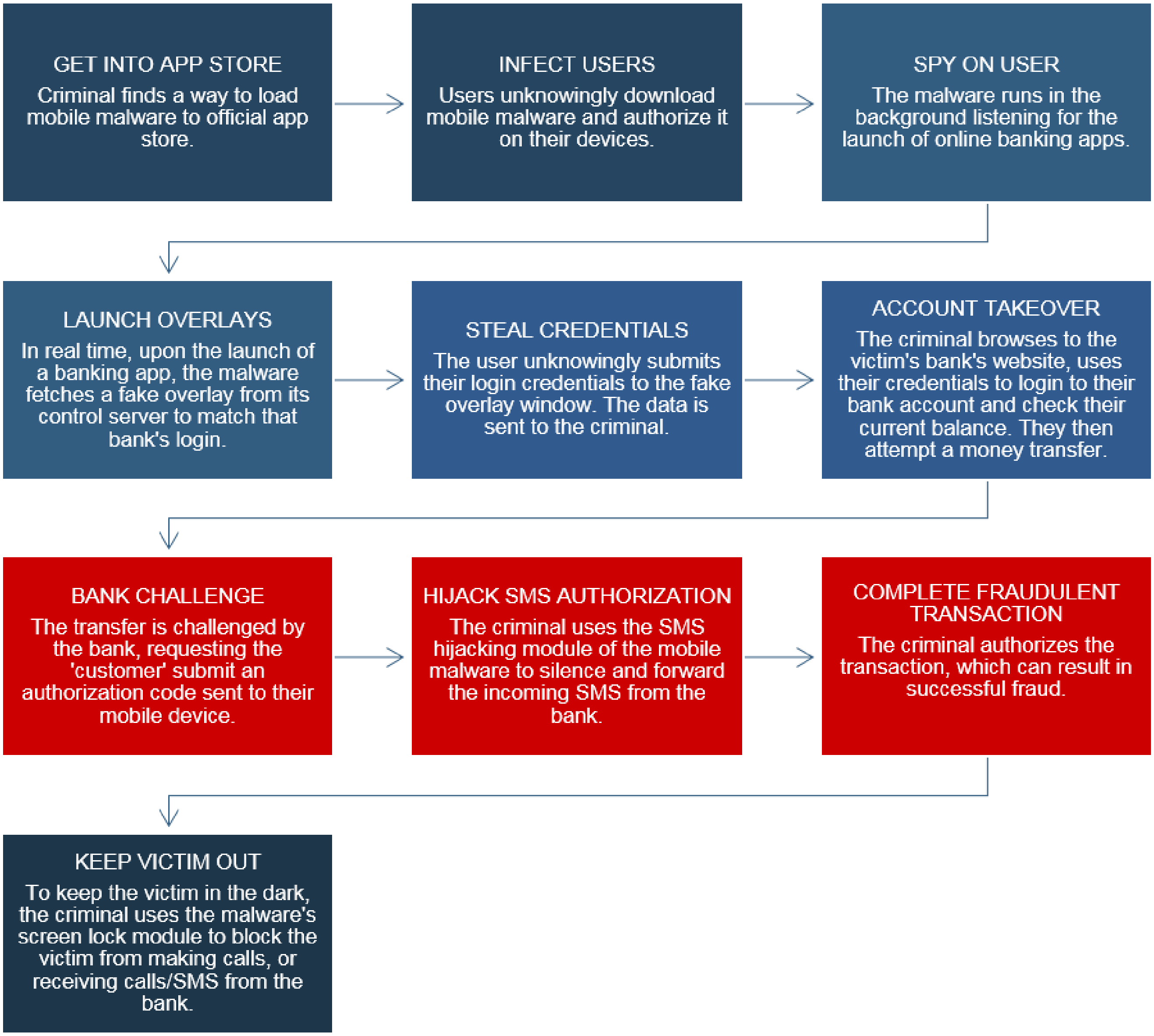
In April 2017, IBM X-Force researchers observed this malware use another notable manner to get into the official Play store. It started out as a benign application purporting to display funny videos. After downloading and executing it, the app would update itself, fetching and installing malware modules into the original application. This effectively turned the once benign app into a mobile banking malware complete with permissions and persistency on the device.

BankBot’s Fraud M.O.

Before mobile malware, cybercriminals looking to take over bank accounts for fraudulent transactions would run into SMS-based two-factor authentication and get stuck.

Those launching phishing attacks saw their attack capabilities quickly decline as more banks adopted out-of-band authentication challenges. To bypass this authentication method, they started writing SMS hijackers, convincing infected PC owners to download those apps to their smartphones. This social engineering worked for a while, but it required resources and a very convincing ploy to make victims enable side-loading and get the malicious app from a third-party store.

This is where mobile banking Trojans such as BankBot came in. They are a one-stop shop for authentication elements cybercriminals typically use to take over an account. The following is the takeover flow for criminals using malware like BankBot.



GET INTO APP STORE
Criminal finds a way to load mobile malware to official app store.

INFECT USERS
Users unknowingly download mobile malware and authorize it on their devices.

SPY ON USER
The malware runs in the background listening for the launch of online banking apps.

LAUNCH OVERLAYS
In real time, upon the launch of a banking app, the malware fetches a fake overlay from its control server to match that bank's login.

STEAL CREDENTIALS
The user unknowingly submits their login credentials to the fake overlay window. The data is sent to the criminal.

ACCOUNT TAKEOVER
The criminal browses to the victim's bank's website, uses their credentials to login to their bank account and check their current balance. They then attempt a money transfer.

BANK CHALLENGE
The transfer is challenged by the bank, requesting the 'customer' submit an authorization code sent to their mobile device.

HIJACK SMS AUTHORIZATION
The criminal uses the SMS hijacking module of the mobile malware to silence and forward the incoming SMS from the bank.

COMPLETE FRAUDULENT TRANSACTION
The criminal authorizes the transaction, which can result in successful fraud.

KEEP VICTIM OUT
To keep the victim in the dark, the criminal uses the malware's screen lock module to block the victim from making calls, or receiving calls/SMS from the bank.

It’s important to note that the infection begins on a mobile device, usually unbeknownst to the common user. When the fraud attempt eventually takes place, it happens from an entirely different device. The attacker uses his or her own endpoint to access the victim’s bank’s website to initiate the fraudulent transaction, and the user will not always logically connect the dots and realize the two are linked.

When victims see their phones locked with a fake update message displayed by BankBot, they may think that there's a technical issue. They could reach out to a local mobile repair shop or call their service provider to ask about it. Even if they do realize they've been hit by malware, it's difficult to know what sort of malware and know that their bank account, and sometimes payment cards, have most likely been compromised at that point.

What makes this worse is that the malware prevents victims from receiving calls, and so prevents banks from being able to contact them about the suspicious transaction. By often resorting to a factory reset, victims unfortunately eliminate forensic information that can be useful for identification and analysis of the infection.

According to X-Force research, BankBot variants have been actively targeting banks in Spain and in France in July 2017. BankBot and the M.O. described in this post were detected and thwarted by IBM Trusteer Mobile SDK. The account takeover phase was detected with holistic cross-channel detection capabilities provided by IBM Trusteer Pinpoint Detect.

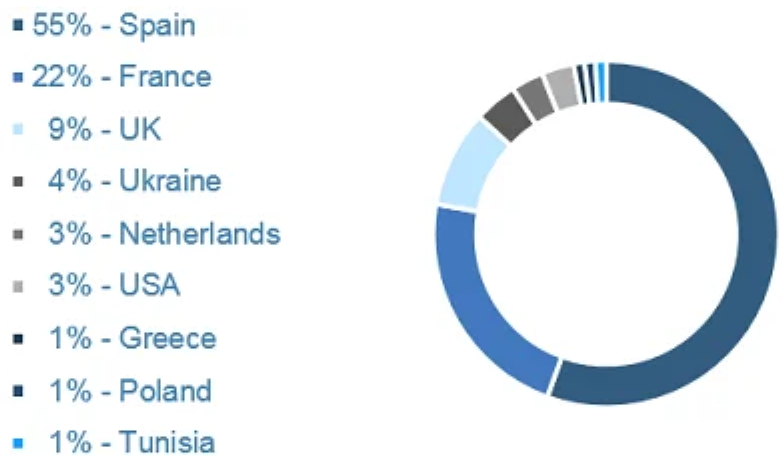


Figure 1: BankBot infected devices per device geography (Source: IBM Trusteer)

Additionally, recent BankBot target lists include banks in Australia, Germany and Romania.

X-Force research noted that BankBot is an overlay Android bot. It monitors for the launch of targeted banking applications on the infected device and then dynamically fetches a matching HTML overlay from its controller's server. The overlay is presented to users, hiding the original app they may have opened and requesting their online banking credentials, credit card details or login combination. Once entered, the malware sends the details to the attacker in cleartext.

Upon installation, this malware requests app administrator privileges on the device under the guise of a system update. Once installed, the application icon disappears, but the app continues to run in the background. BankBot will not operate if it detects that the infected device is located in CIS countries, alluding to its possible operator’s whereabouts.

BankBot can lock the device’s screen to keep the user out when it is performing fraudulent activity on the victim’s account; to do so, it displays a fake update message on screen to delay access attempts to the device. The malware further possesses data exfiltration capabilities that enable it to hijack incoming SMS messages and forward them to the attacker, thus compromising SMS-based two-factor authentication.

Since it is commercially available in underground forums and code-sharing sites, BankBot targets include a long list of banks across Europe, especially in Spain, Australia, New Zealand and some banks in Argentina. In some cases, the malware targets both Android smartphone and Android tablet versions of the banking apps it is after, depending on the botnet’s operator’s goals.

More to Come?

According to ongoing research by X-Force, mobile malware has been rising in sophistication in the past few years, making it less surprising to see its operators manage to circumvent automated security controls on legitimate app stores.

With various code leaks in the mobile malware scene, the number of malicious actors has also been steadily growing — especially since unlike PC botnets, mobile malware does not require a high level of technical savvy. Together, these factors make for a continually rising threat that now reaches more users than ever, turning them into potential fraud victims.

Indicators of Compromise

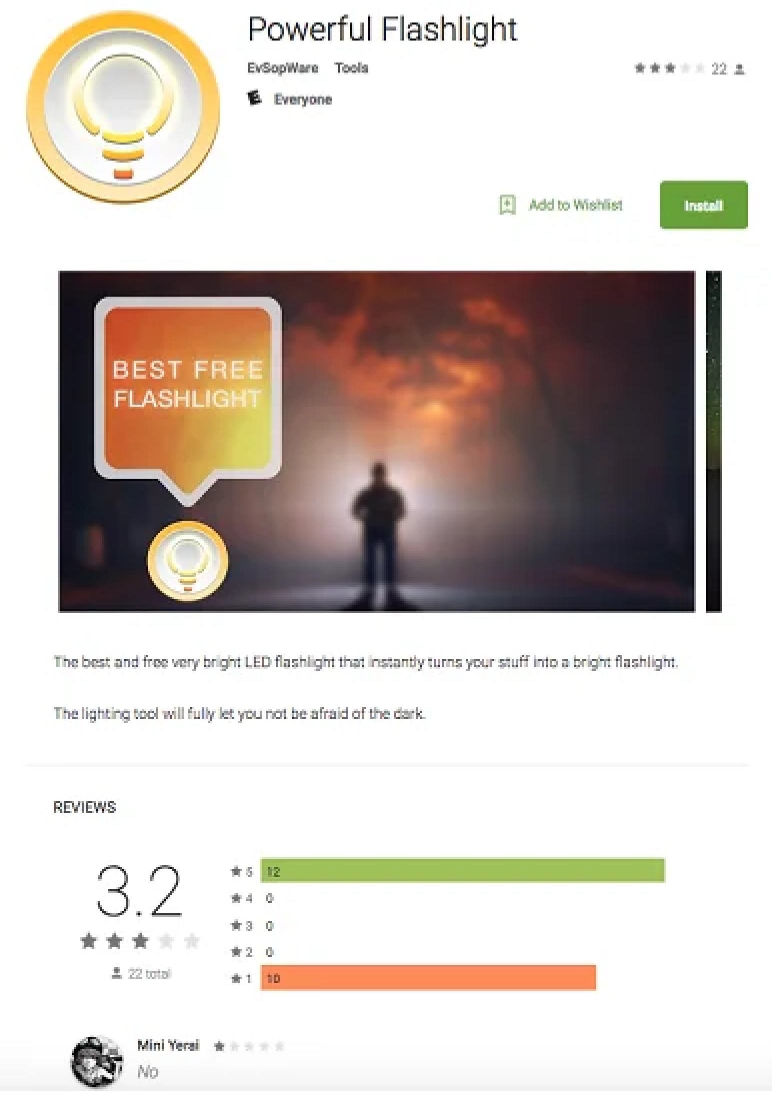
X-Force identified the following apps as the malicious BankBot apps that made it into the Google Play store:

	APK MD5	**Package Name**	**Date Entered Google Play**
1	34D70B6A2C2B1B07128726499FAC19B1	com.detective.wid	22-Jul-17
2	4D51687ADB3B75DD18DD68A70204AE56	com.ak47fl.wid	21-Jul-17
3	FEFACA64DFE0BF6D7081CBBF6A05CCD5	com.comfl.wid	18-Jul-17
4	210B717194C265739F055B9D8BF4F5F2	com.defl.wid	13-Jul-17
5	0F996382F01E4502BCA36EF48A87BE86	com.simfl.wid	9-Jul-17
6	069BF2F0B21DA3579F7C76EF2B9284D1	com.safarifl.widg	26-Jun-17

	APK MD5	Package Name	Date Entered Google Play
7	5d68069e8d258c796af5011e27c11423	com.tactflashlight.widget	22-Jun-17
8	832ABF77D80FD9A204ABBEB7E7CA9E4A	com.spyflashlight.widg	17-Jun-17
9	F4A0D659C8F7F79D0CD629296CA95478	com.flashdet.widg	17-Jun-17
10	3AE09A3D86BC1083A7B67C7827F510B1	com.ledflash.widg	11-Jun-17
11	69D0286289A18A2BCF8C1BAFD431B2B7	com.flashmarines.widget	9-Jun-17
12	A36FA1C70BB238A83547580ED013F8F7	com.flashwar.widg	8-Jun-17
13	A1007FCB2F238B1A0E63E6B195446086	com.goldflash.widg	7-Jun-17
14	F16FE16ACD942AA1AF79BE2BD1C1F923	com.goldwidg.flashlight	5-Jun-17
15	B534F3CA69BBDE1299CCDDDCB3591E5B	com.pwidget.flashlight	4-Jun-17
16	F59D91BCF3CFC8C94E4345C218D9E41C	com.eco.fwidget	31-May-17
17	9515BA4A7D3E9113402DE9F858E001A4	com.funfl.wid	Unknown
18	9698340576e27fd11643e6869a192bd0	com.warfl.widget	Unknown
19	DF22128F3C66BCC8074538E47DEC7544	com.flashpolice.widg	Unknown
20	A543A7FE67C99EAC11F5E6B8C5F6B5FB	com.flashlight.army	Unknown

Most apps have already been removed from the Play store at the time of this writing. Those that were live at the time of writing were disclosed to Google Play.

X-Force captured some examples of the apps that contained BankBot:



Powerful Flashlight

EvSopWare Tools ★★★☆☆ 22 👤

Everyone

Add to Wishlist

Install

The best and free very bright LED flashlight that instantly turns your stuff into a bright flashlight.

The lighting tool will fully let you not be afraid of the dark.

REVIEWS

3.2

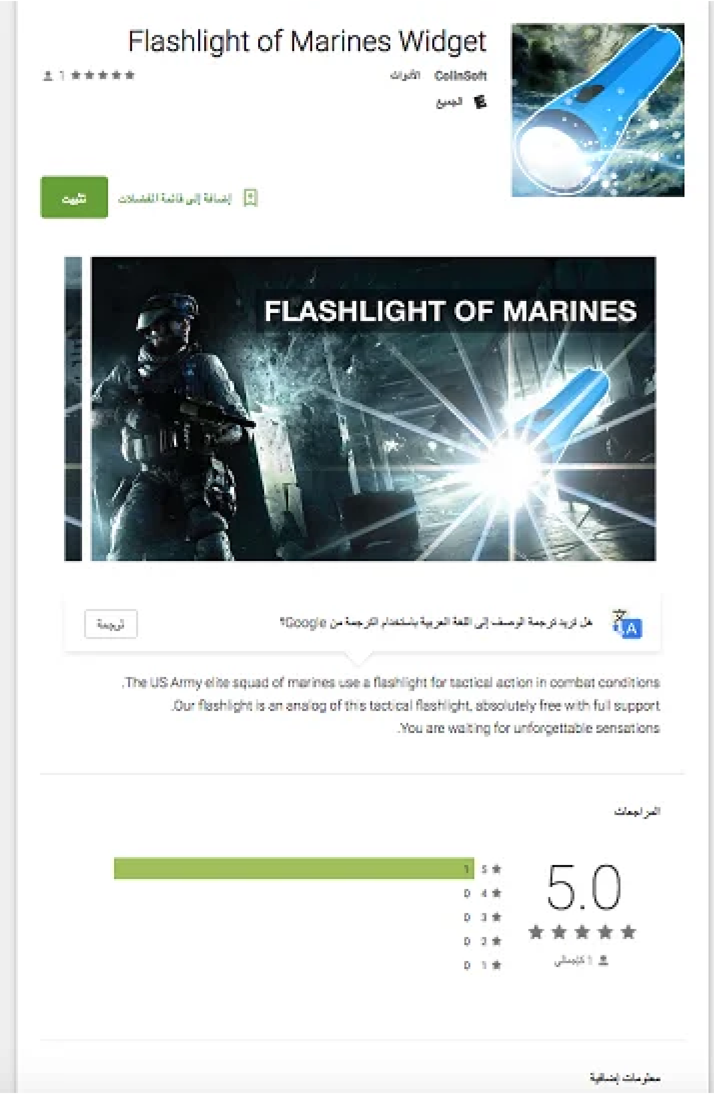
★★★☆☆

👤 22 total

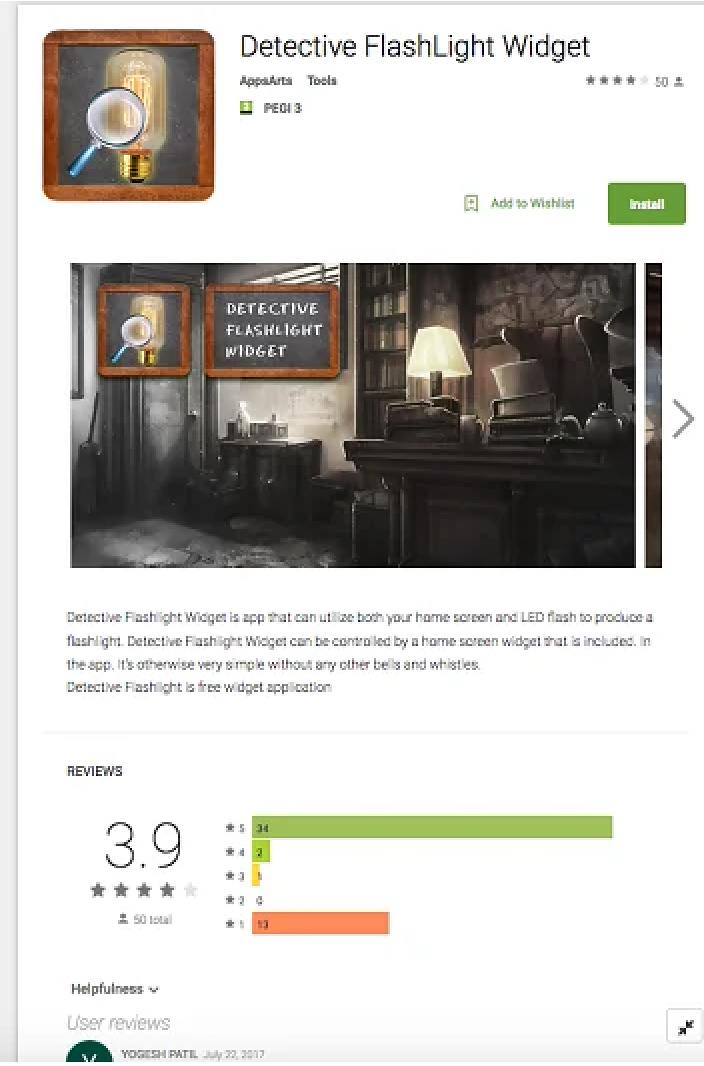
★ 5	12
★ 4	0
★ 3	0
★ 2	0
★ 1	10

Mini Yerai ★☆☆☆☆

No


Flashlight of Marines Widget
CollnSoft الأدوات
الجميع
1 ★★★★★
إضافة إلى قائمة المفضلات
تثبيت
FLASHLIGHT OF MARINES
هل تريد ترجمة الوصف إلى اللغة العربية باستخدام الترجمة من Google؟
ترجمة

.The US Army elite squad of marines use a flashlight for tactical action in combat conditions
.Our flashlight is an analog of this tactical flashlight, absolutely free with full support
.You are waiting for unforgettable sensations



Detective FlashLight Widget

AppsArts Tools

PEGI 3

Detective Flashlight Widget is app that can utilize both your home screen and LED flash to produce a flashlight. Detective Flashlight Widget can be controlled by a home screen widget that is included. In the app. It's otherwise very simple without any other bells and whistles.
Detective Flashlight is free widget application

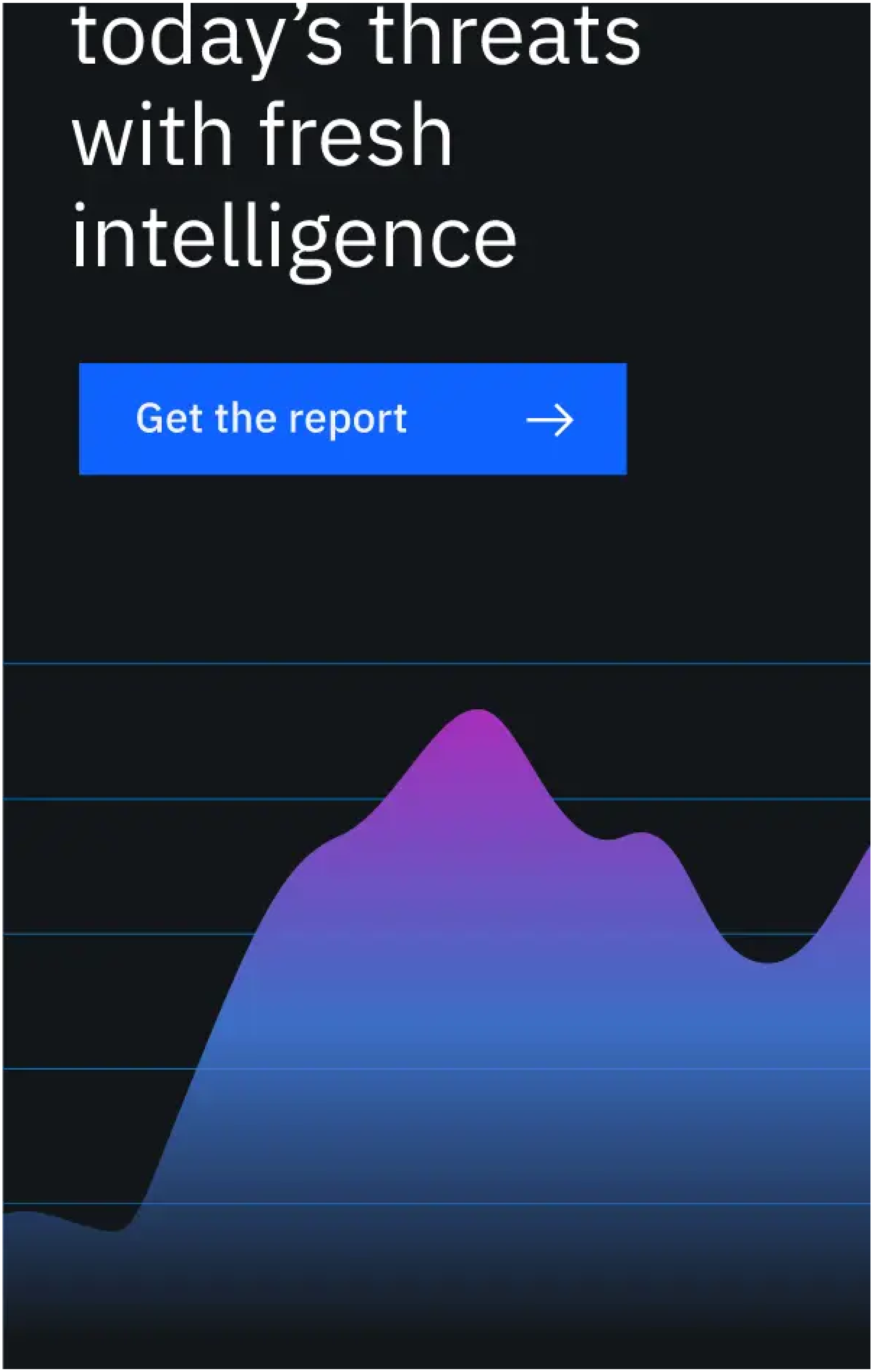
REVIEWS

Mobile malware can turn customers of reputable app stores into fraud victims. IBM Trusteer Mobile SDK customers have full detection of all variants and overlay malware designed for financial fraud with the same M.O. IBM Trusteer Pinpoint Detect offers customers detection via the account takeover module.

Worried about mobile security? Read this white paper

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...



today’s threats with fresh intelligence

Get the report →

IBM **Security**