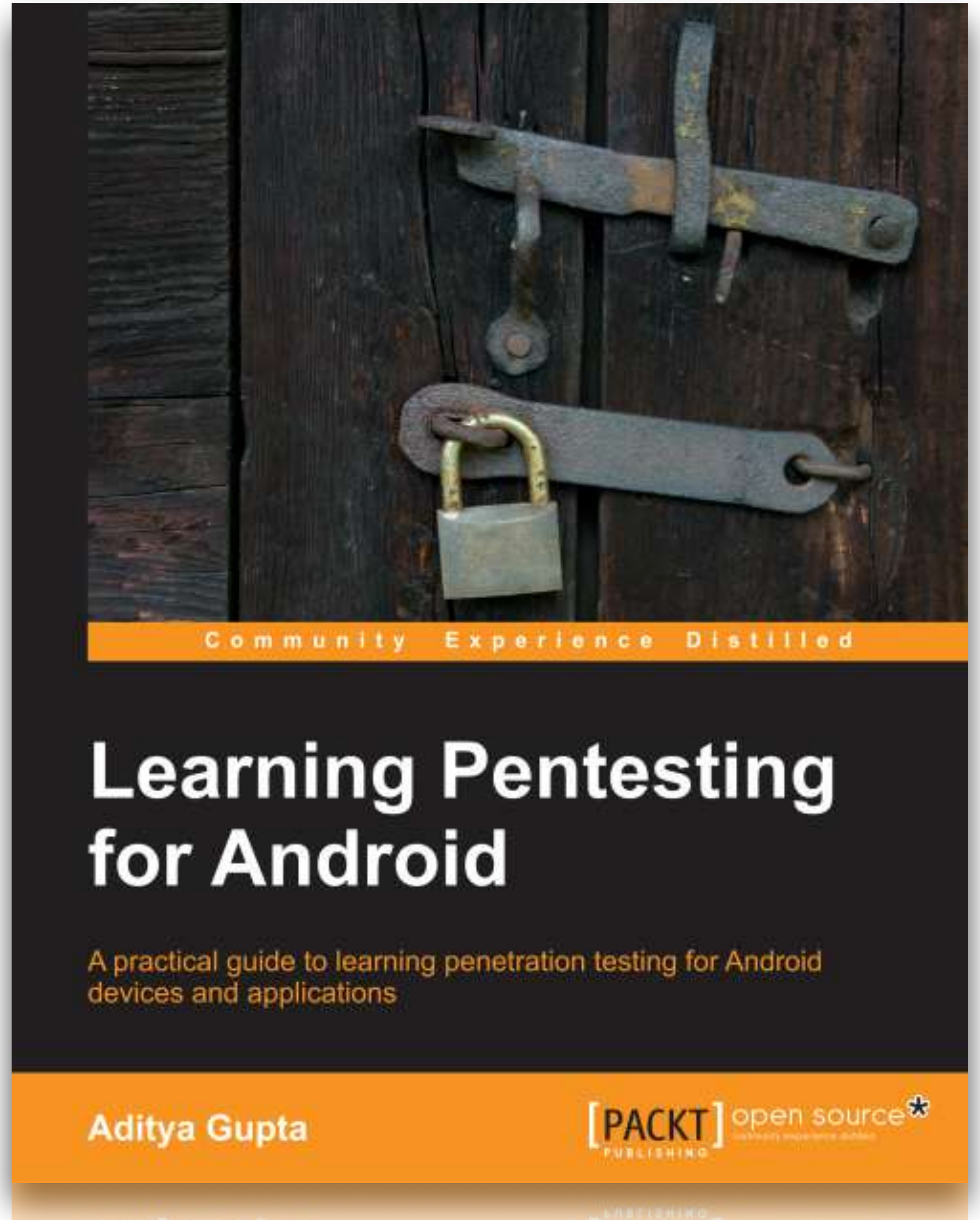
Breaking and Securing Mobile Apps

Aditya Gupta

@adi1391 | adi@attify.com | +91-9538295259

Who Am I?

- The Mobile Security Guy
- Attify
- Security Architecture, Auditing, Trainings etc.
- Ex Rediff.com Security Lead
- <3 Python
- Active Member at null meetups and Humlas - Bangalore and Mumbai



Community Experience Distilled

Learning Pentesting for Android

A practical guide to learning penetration testing for Android devices and applications

Aditya Gupta

[PACKT] PUBLISHING open source* community experience distilled

Learning Pentesting for Android

Previously Discovered vulns

Microsoft
facebook
Adobe
YAHOO!
skype
tumblr.
rediff.com
PayPal
And more..

Also given trainings and talks at

Agenda

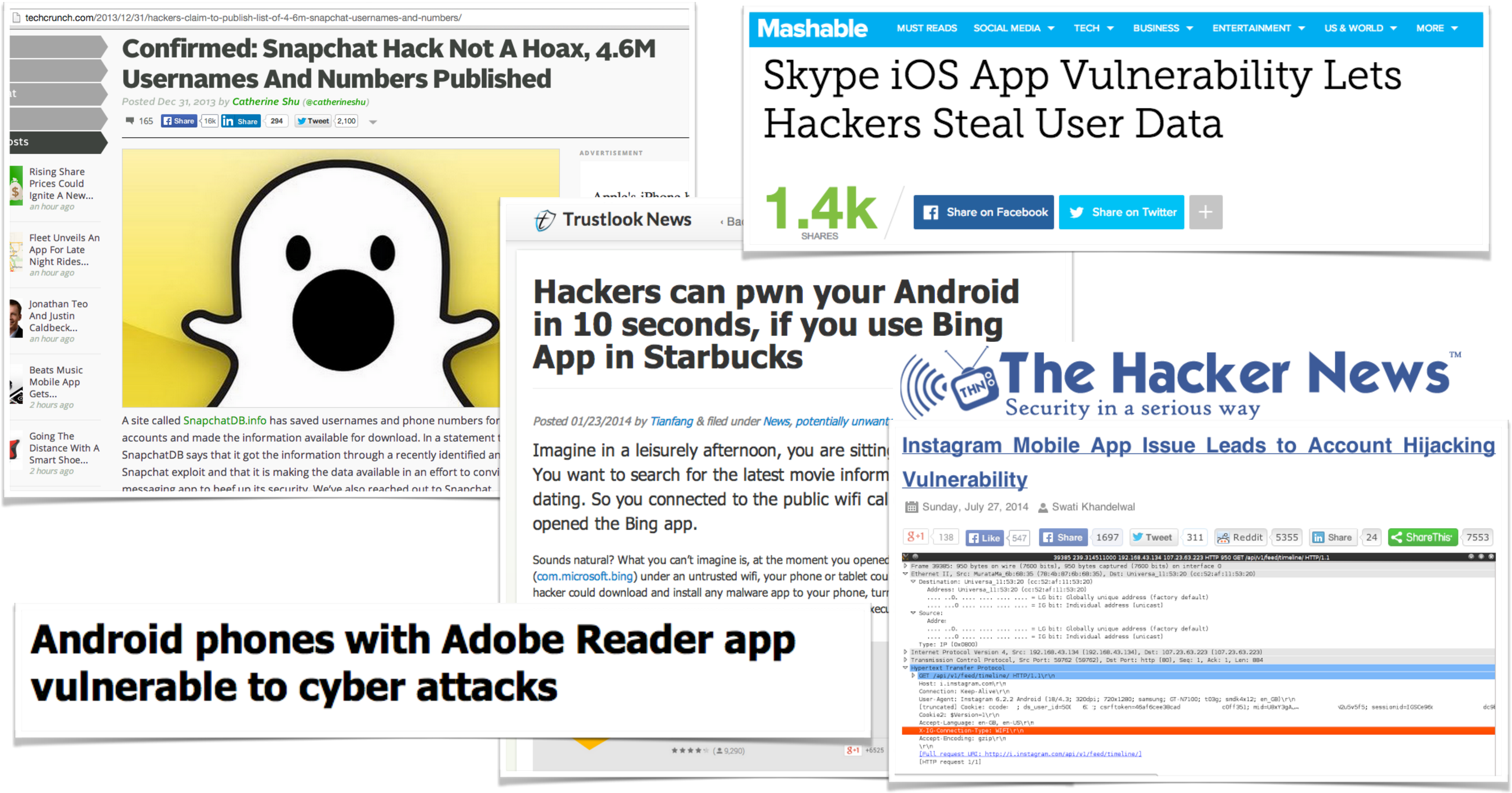
- Android and iOS Security Overview
- Experiences over the past few years
- Finding vulnerabilities in Mobile Apps
- Automating Security Analysis
- AppWatch - The Community Edition

Why Smartphones?

We are in the POST PC era

Why Smartphones?

- Present almost everywhere
- Contains the most sensitive information
- Not much attention paid to its security by enterprises
- People love apps ('There's an app for that')
- AVs not that efficient



techcrunch.com/2013/12/31/hackers-claim-to-publish-list-of-4-6m-snapchat-usernames-and-numbers/

Confirmed: Snapchat Hack Not A Hoax, 4.6M Usernames And Numbers Published

Posted Dec 31, 2013 by Catherine Shu (@catherineshu)

165 Share 16k Share 294 Tweet 2,100

A site called SnapchatDB.info has saved usernames and phone numbers for accounts and made the information available for download. In a statement t SnapchatDB says that it got the information through a recently identified an Snapchat exploit and that it is making the data available in an effort to convi messaging app to beef up its security. We've also reached out to Snapchat

ADVERTISEMENT

Apple's iPhone h

t
osts
Rising Share Prices Could Ignite A New...
an hour ago
Fleet Unveils An App For Late Night Rides...
an hour ago
Jonathan Teo And Justin Caldbeck...
an hour ago
Beats Music Mobile App Gets...
2 hours ago
Going The Distance With A Smart Shoe...
2 hours ago

Mashable

Skype iOS App Vulnerability Lets Hackers Steal User Data

1.4k SHARES

Trustlook News ‹ Ba

Hackers can pwn your Android in 10 seconds, if you use Bing App in Starbucks

Posted 01/23/2014 by Tianfang & filed under News, potentially unwant

Imagine in a leisurely afternoon, you are sittin You want to search for the latest movie inform dating. So you connected to the public wifi cal opened the Bing app.

Sounds natural? What you can't imagine is, at the moment you opened (com.microsoft.bing) under an untrusted wifi, your phone or tablet cou hacker could download and install any malware app to your phone, turr xecu

★★★★☆ (9,290) +1 +6525

The Hacker News™

Security in a serious way

Instagram Mobile App Issue Leads to Account Hijacking Vulnerability

Sunday, July 27, 2014 Swati Khandelwal

```
39385 239.314511000 192.168.43.134 107.23.63.223 HTTP 950 GET /api/v1/feed/timeline/ HTTP/1.1
▷ Frame 39385: 950 bytes on wire (7600 bits), 950 bytes captured (7600 bits) on interface 0
▽ Ethernet II, Src: MurataMa_6b:68:35 (78:4b:87:6b:68:35), Dst: Universa_11:53:20 (cc:52:af:11:53:20)
  ▽ Destination: Universa_11:53:20 (cc:52:af:11:53:20)
      Address: Universa_11:53:20 (cc:52:af:11:53:20)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▽ Source:
      Addre:
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
▷ Internet Protocol Version 4, Src: 192.168.43.134 (192.168.43.134), Dst: 107.23.63.223 (107.23.63.223)
▷ Transmission Control Protocol, Src Port: 59762 (59762), Dst Port: http (80), Seq: 1, Ack: 1, Len: 884
▽ Hypertext Transfer Protocol
  ▷ GET /api/v1/feed/timeline/ HTTP/1.1\r\n
    Host: i.instagram.com\r\n
    Connection: Keep-Alive\r\n
    User-Agent: Instagram 6.2.2 Android (18/4.3; 320dpi; 720x1280; samsung; GT-N7100; t03g; smdk4x12; en_GB)\r\n
    [truncated] Cookie: ccode:  ; ds_user_id=50(    6: ; csrftoken=46af6cee38cad           c0ff351; mid=U8xY3gA...          V2u5v5f5; sessionid=IGSCe96          dc9
    Cookie2: $Version=1\r\n
    Accept-Language: en-GB, en-US\r\n
    X-IG-Connection-Type: WIFI\r\n
    Accept-Encoding: gzip\r\n
    \r\n
    [Full request URI: http://i.instagram.com/api/v1/feed/timeline/]
    [HTTP request 1/1]
```

Android phones with Adobe Reader app vulnerable to cyber attacks

Android Security Architecture

- Two-tier security model : Linux and Android
- Each app in its own DVM
- App Sandbox

Android Security Overview

- Apps data stored at /data/data/[package-name]/
- Apps stored in /data/app and /system/app
- AndroidManifest.xml plays an important role

Android Apps Security Primer

- Reversing using Apktool / Dex2Jar + JD-GUI / JEB
- Look for security issues in source code
- IDA Pro for Native Apps

Android Vulnerabilities

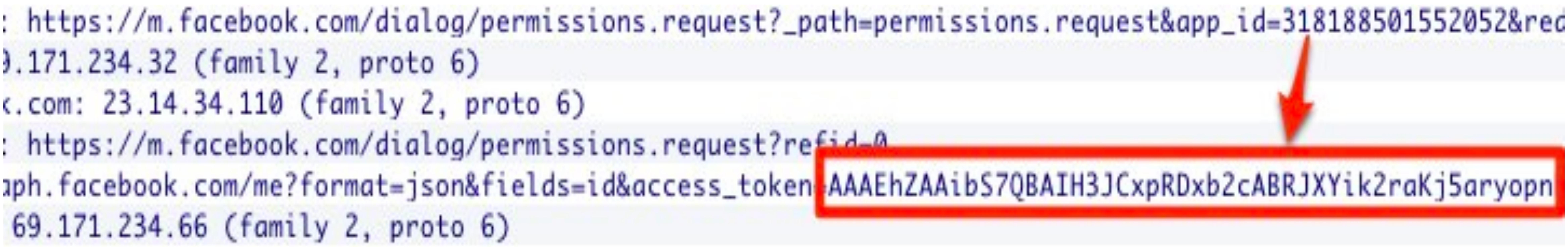
- Most of the applications vulnerable by default
- Developers don't often know how to secure mobile apps
- Apps get compromised, sensitive info leaked

Hard coded sensitive info

- Really common in many apps
- API Key / Username & Passwords / server credentials found in app code
- No Binary protection as well

Logging Sensitive Info

Logging Sensitive Info



```
: https://m.facebook.com/dialog/permissions.request?_path=permissions.request&app_id=318188501552052&red
).171.234.32 (family 2, proto 6)
<.com: 23.14.34.110 (family 2, proto 6)
: https://m.facebook.com/dialog/permissions.request?refid=0
aph.facebook.com/me?format=json&fields=id&access_token=AAAEhZAAibS7QBAIH3JCxpRDxb2cABRJXYik2raKj5aryopn
 69.171.234.66 (family 2, proto 6)
```

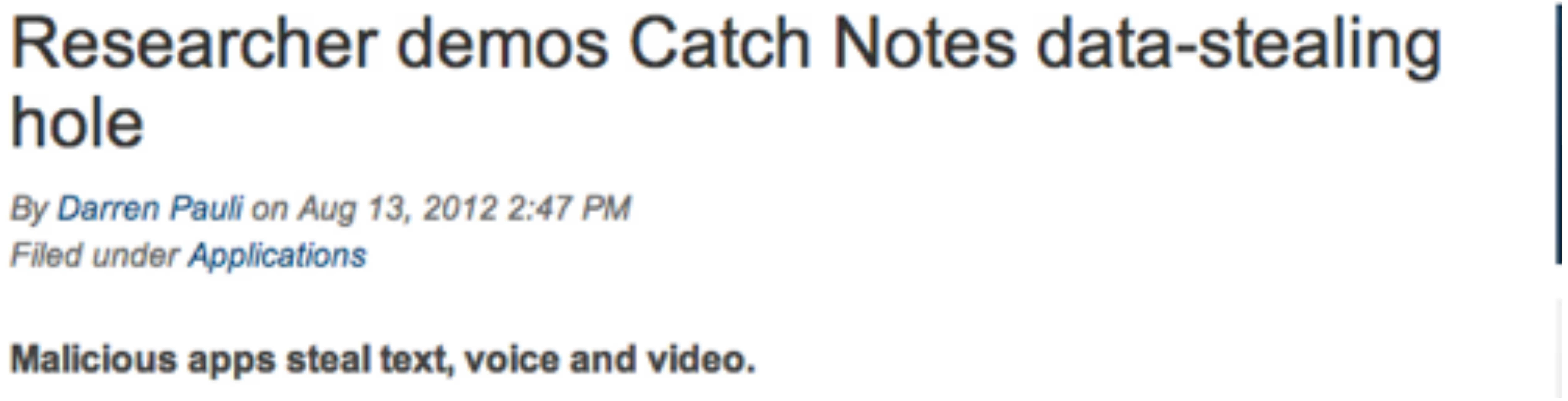
Logging Sensitive Info

```
Log.d("Facebook-authorize", "Login Success! access_token="
        + getAccessToken() + " expires="
        + getAccessExpires());
```

Leaking Content Providers

- Used to share data between apps
- Few by default
- Apps could define their own
- By default exported

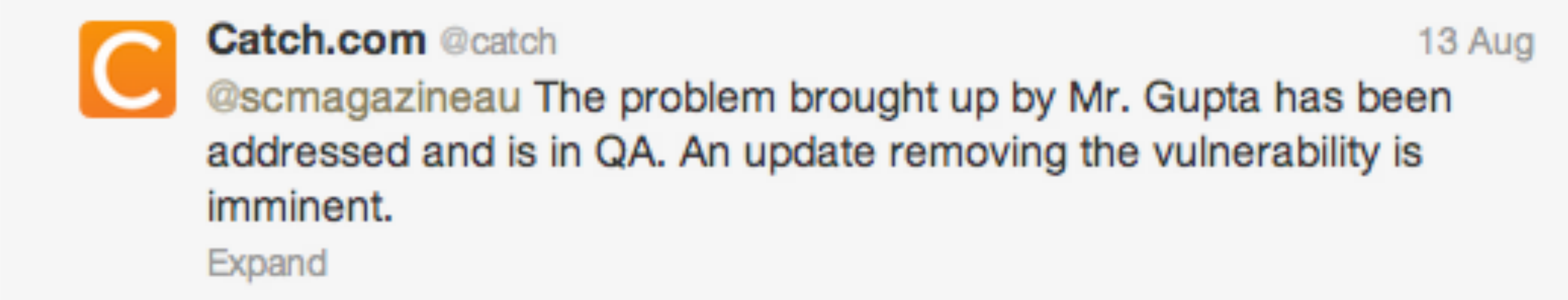
Leaking Content Providers



Researcher demos Catch Notes data-stealing hole

By Darren Pauli on Aug 13, 2012 2:47 PM
Filed under Applications

Malicious apps steal text, voice and video.

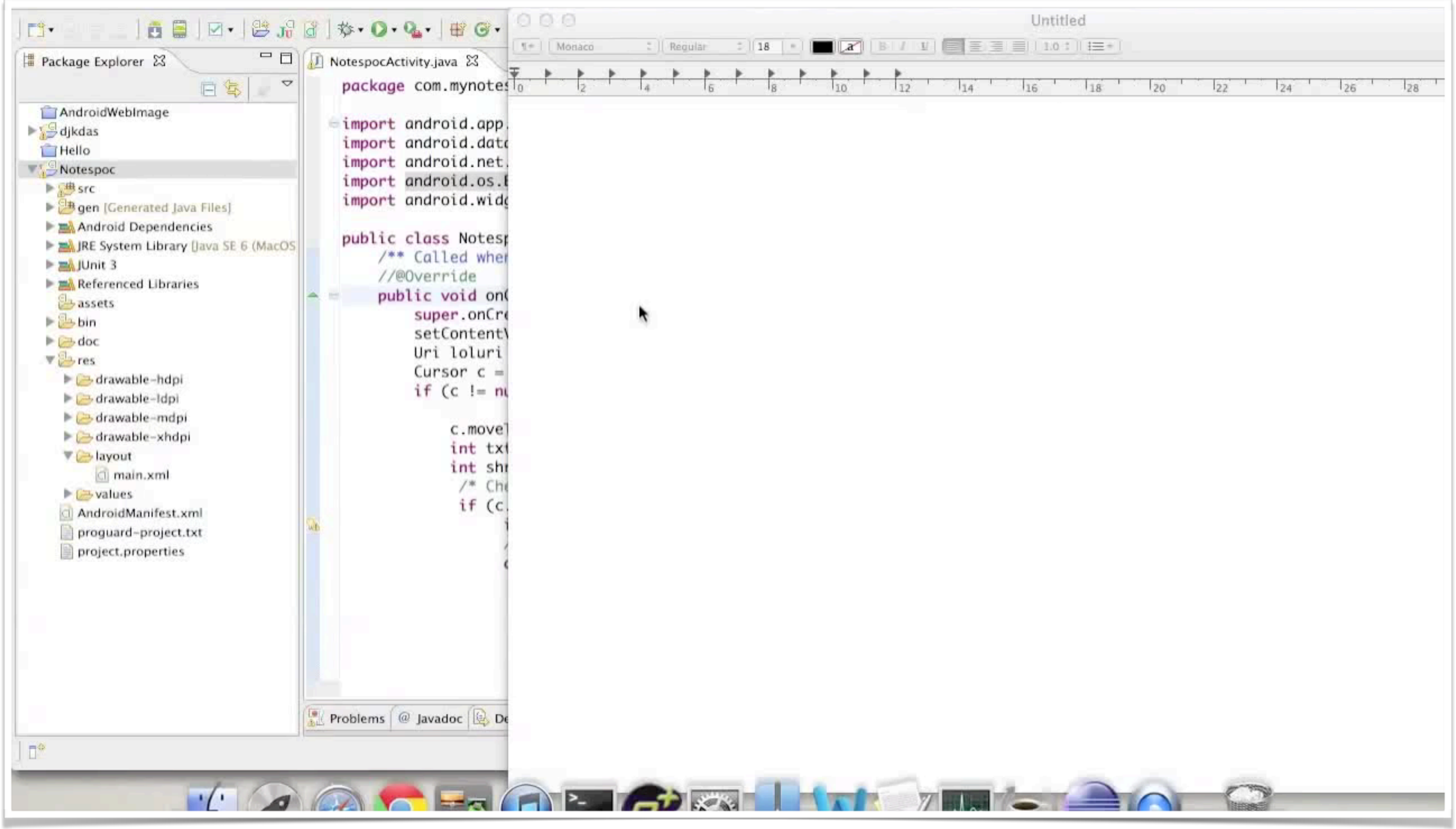


Catch.com @catch 13 Aug

@scmagazineau The problem brought up by Mr. Gupta has been addressed and is in QA. An update removing the vulnerability is imminent.

Expand

Leaking Content Providers



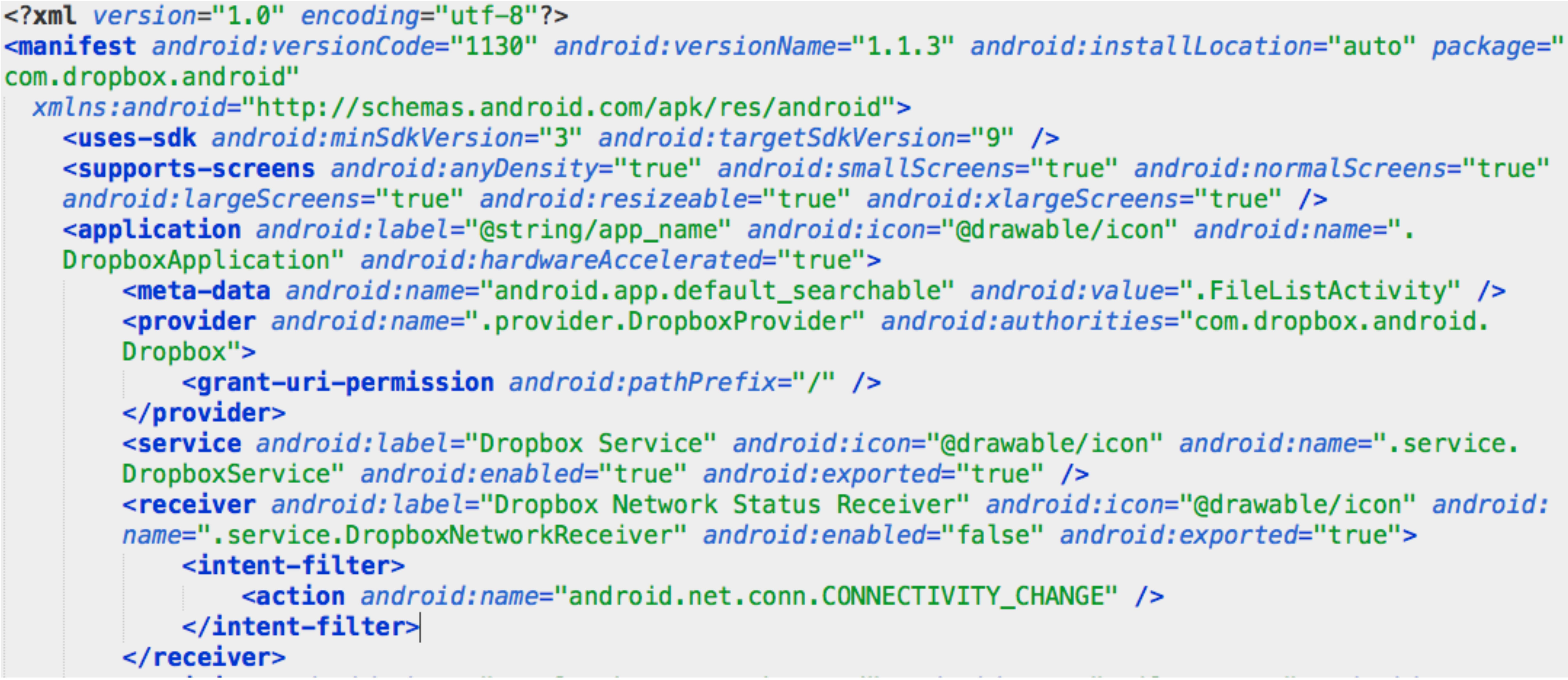
```
package com.mynotes
import android.app.
import android.data
import android.net.
import android.os.E
import android.widg

public class Notesp
    /** Called wher
    //@Override
    public void on(
        super.onCre
        setContent\
        Uri loluri
        Cursor c =
        if (c != nu

            c.moveT
            int txt
            int shr
             /* Che
             if (c.
```

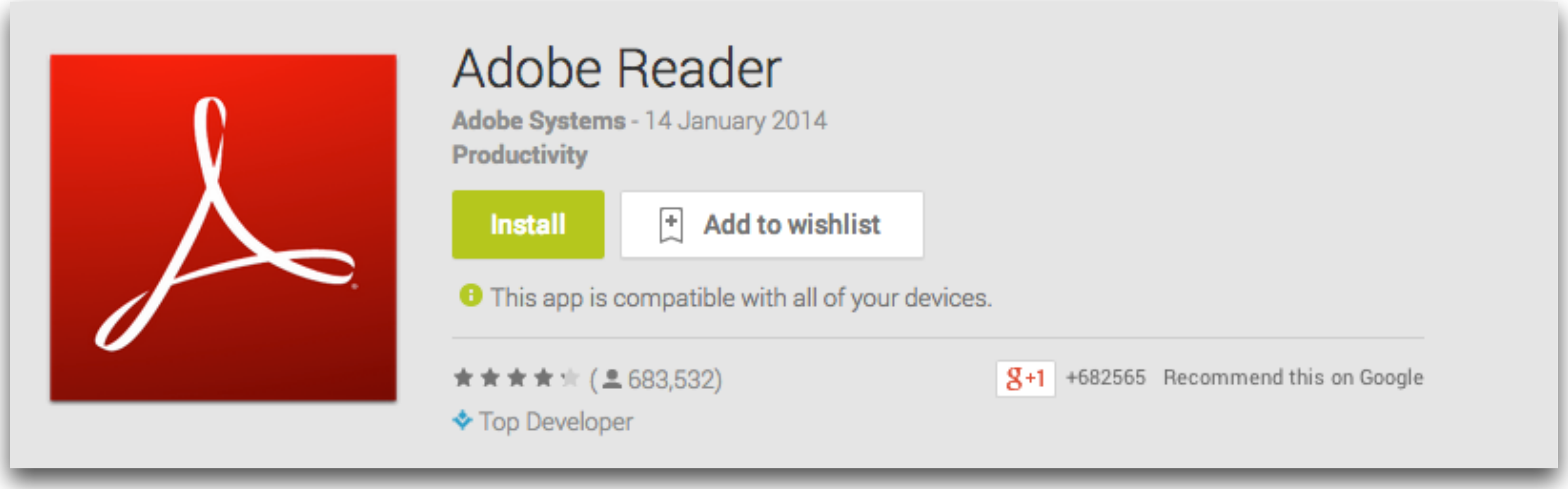
Dropbox

Dropbox



```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1130" android:versionName="1.1.3" android:installLocation="auto" package="
com.dropbox.android"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="3" android:targetSdkVersion="9" />
    <supports-screens android:anyDensity="true" android:smallScreens="true" android:normalScreens="true"
    android:largeScreens="true" android:resizeable="true" android:xlargeScreens="true" />
    <application android:label="@string/app_name" android:icon="@drawable/icon" android:name=".
    DropboxApplication" android:hardwareAccelerated="true">
        <meta-data android:name="android.app.default_searchable" android:value=".FileListActivity" />
        <provider android:name=".provider.DropboxProvider" android:authorities="com.dropbox.android.
        Dropbox">
            <grant-uri-permission android:pathPrefix="/" />
        </provider>
        <service android:label="Dropbox Service" android:icon="@drawable/icon" android:name=".service.
        DropboxService" android:enabled="true" android:exported="true" />
        <receiver android:label="Dropbox Network Status Receiver" android:icon="@drawable/icon" android:
        name=".service.DropboxNetworkReceiver" android:enabled="false" android:exported="true">
            <intent-filter>
                <action android:name="android.net.conn.CONNECTIVITY_CHANGE" />
            </intent-filter>
        </receiver>
```

Adobe Reader



Adobe Reader

Adobe Systems - 14 January 2014

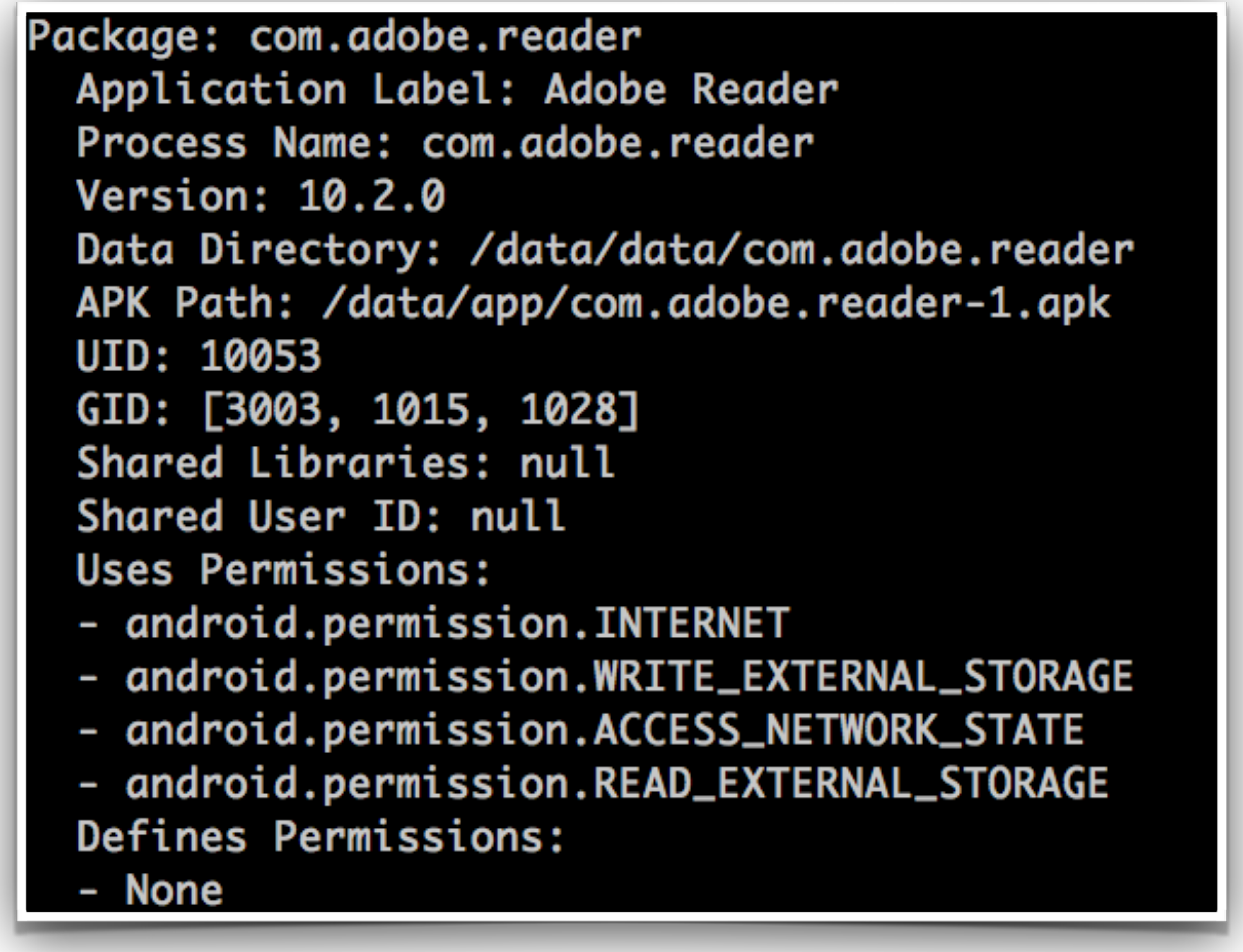
Productivity

This app is compatible with all of your devices.

★★★★☆ (683,532)

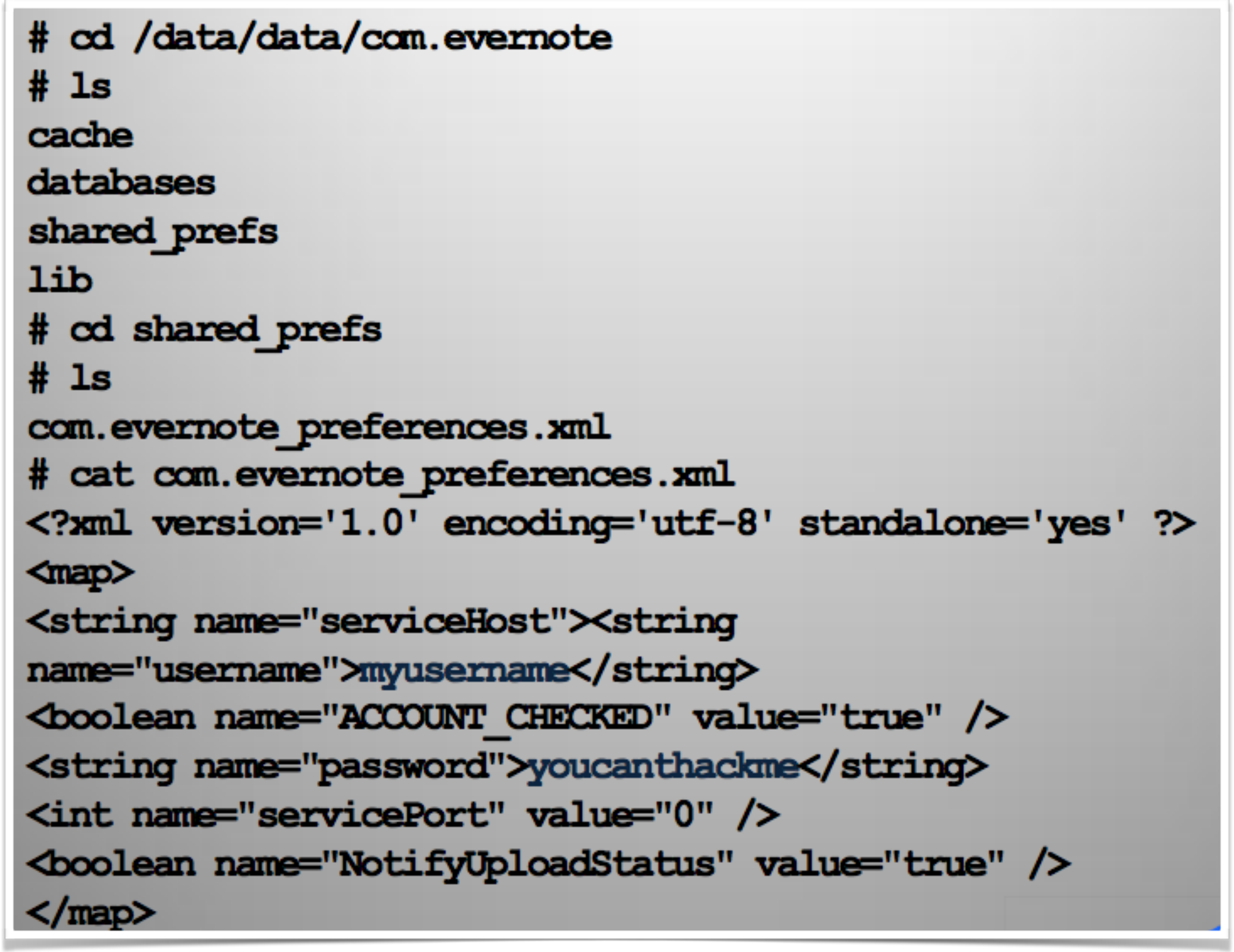
+682565 Recommend this on Google

Top Developer

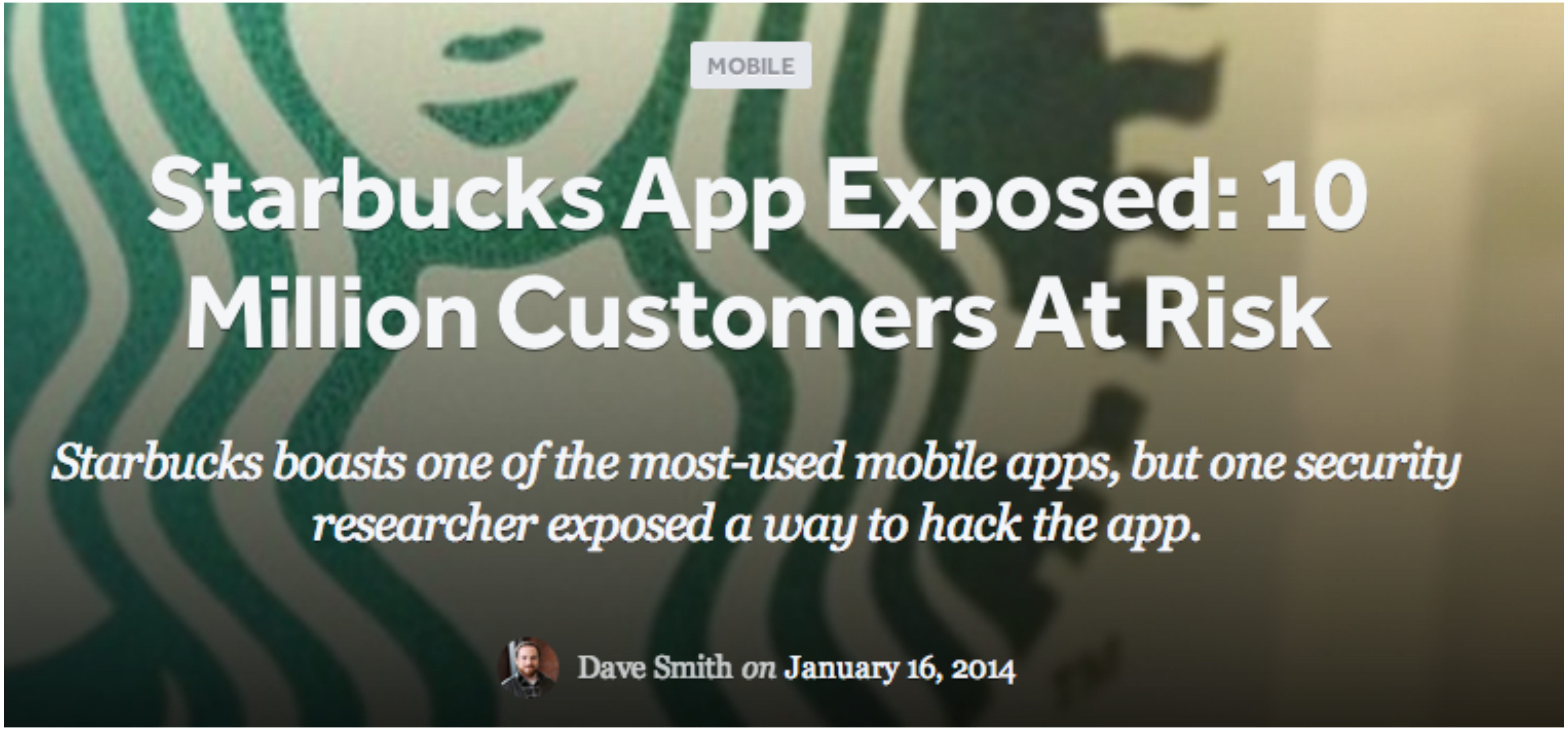


```
Package: com.adobe.reader
  Application Label: Adobe Reader
  Process Name: com.adobe.reader
  Version: 10.2.0
  Data Directory: /data/data/com.adobe.reader
  APK Path: /data/app/com.adobe.reader-1.apk
  UID: 10053
  GID: [3003, 1015, 1028]
  Shared Libraries: null
  Shared User ID: null
  Uses Permissions:
  - android.permission.INTERNET
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.READ_EXTERNAL_STORAGE
  Defines Permissions:
  - None
```

Insecure Data Storage



```
# cd /data/data/com.evernote
# ls
cache
databases
shared_prefs
lib
# cd shared_prefs
# ls
com.evernote_preferences.xml
# cat com.evernote_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="serviceHost"><string
name="username">myusername</string>
<boolean name="ACCOUNT_CHECKED" value="true" />
<string name="password">youcanthackme</string>
<int name="servicePort" value="0" />
<boolean name="NotifyUploadStatus" value="true" />
</map>
```

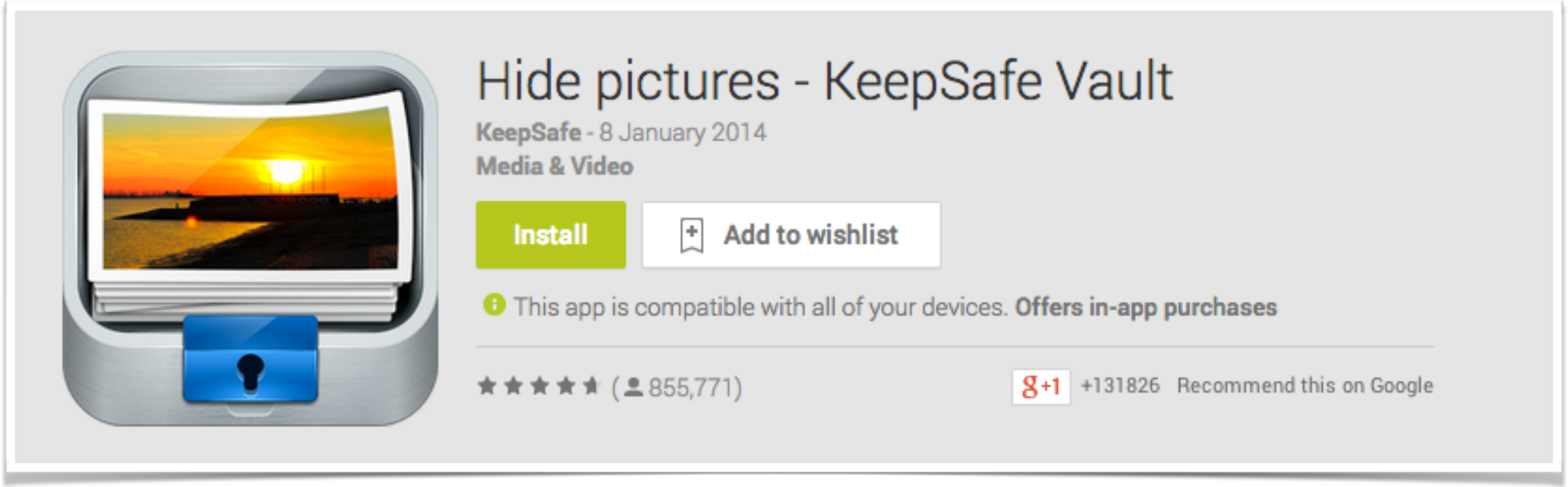


MOBILE

Starbucks App Exposed: 10 Million Customers At Risk

Starbucks boasts one of the most-used mobile apps, but one security researcher exposed a way to hack the app.

Dave Smith *on* January 16, 2014



Hide pictures - KeepSafe Vault

KeepSafe - 8 January 2014

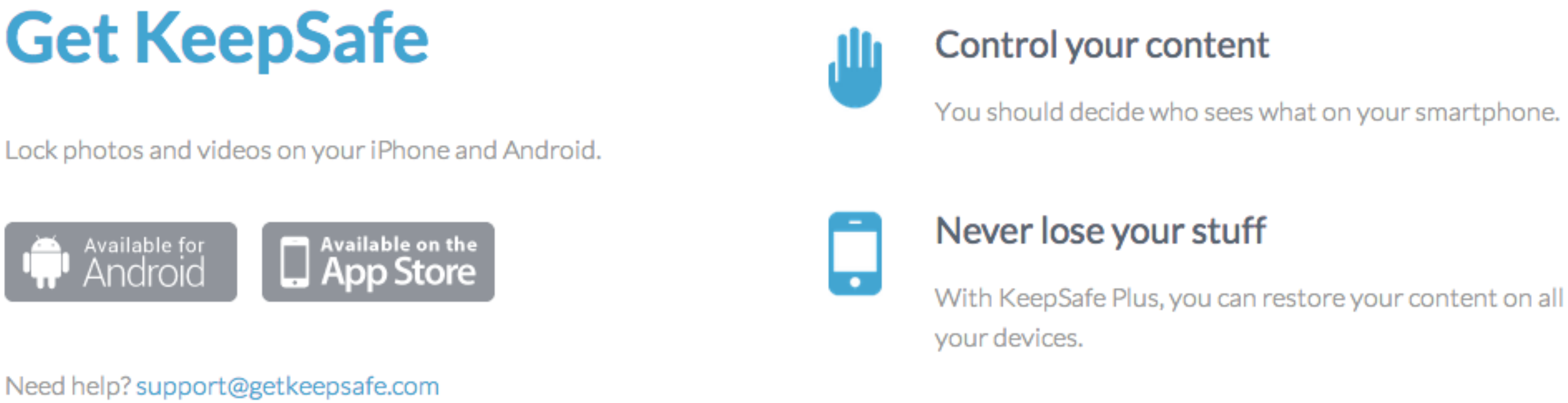
Media & Video

This app is compatible with all of your devices. **Offers in-app purchases**

★★★★★ (855,771)

+131826 Recommend this on Google

KeepSafe



Get KeepSafe

Lock photos and videos on your iPhone and Android.

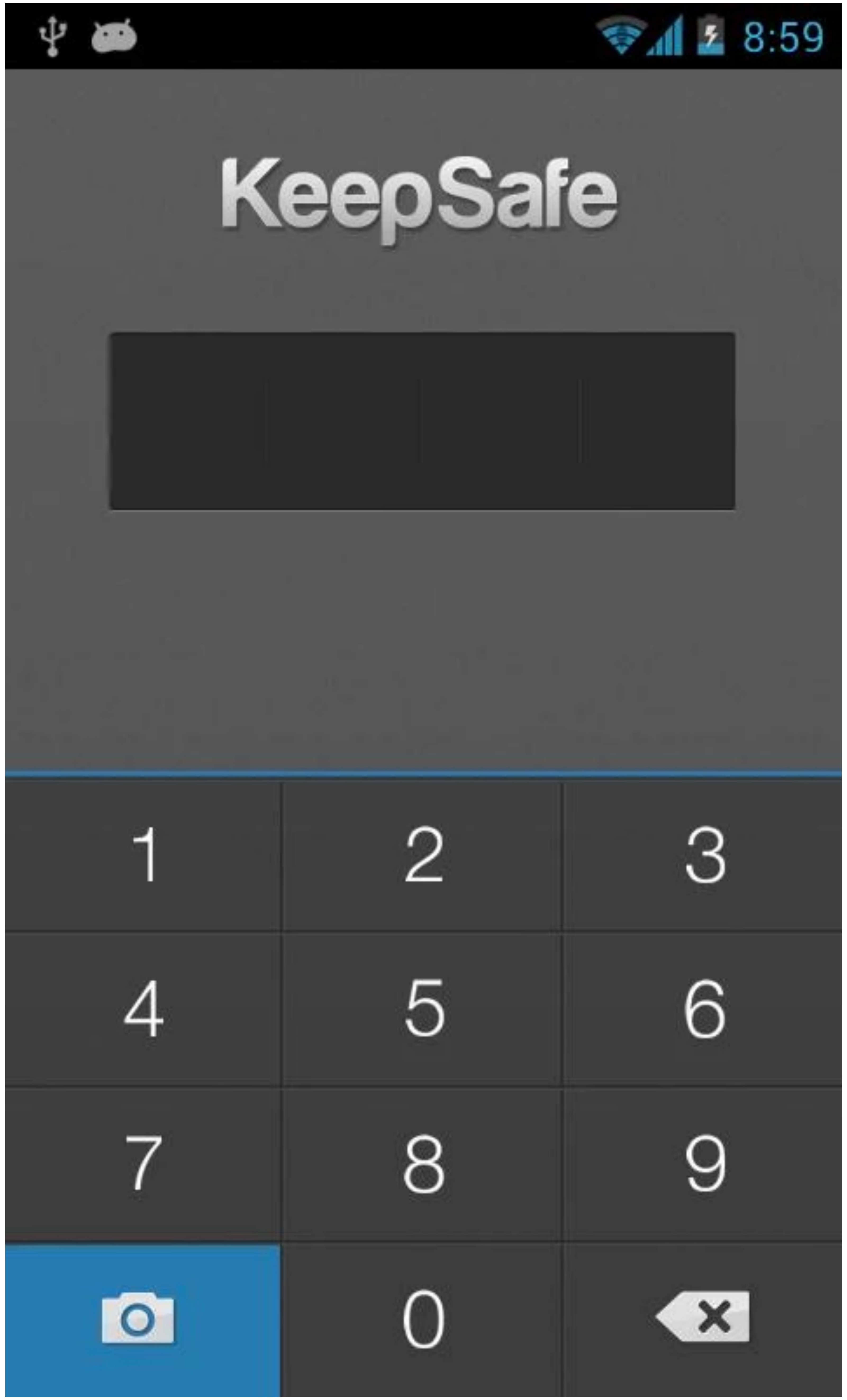
Need help? support@getkeepsafe.com

Control your content

You should decide who sees what on your smartphone.

Never lose your stuff

With KeepSafe Plus, you can restore your content on all your devices.



8:59
KeepSafe
1
2
3
4
5
6
7
8
9
0

Dynamic App Analysis

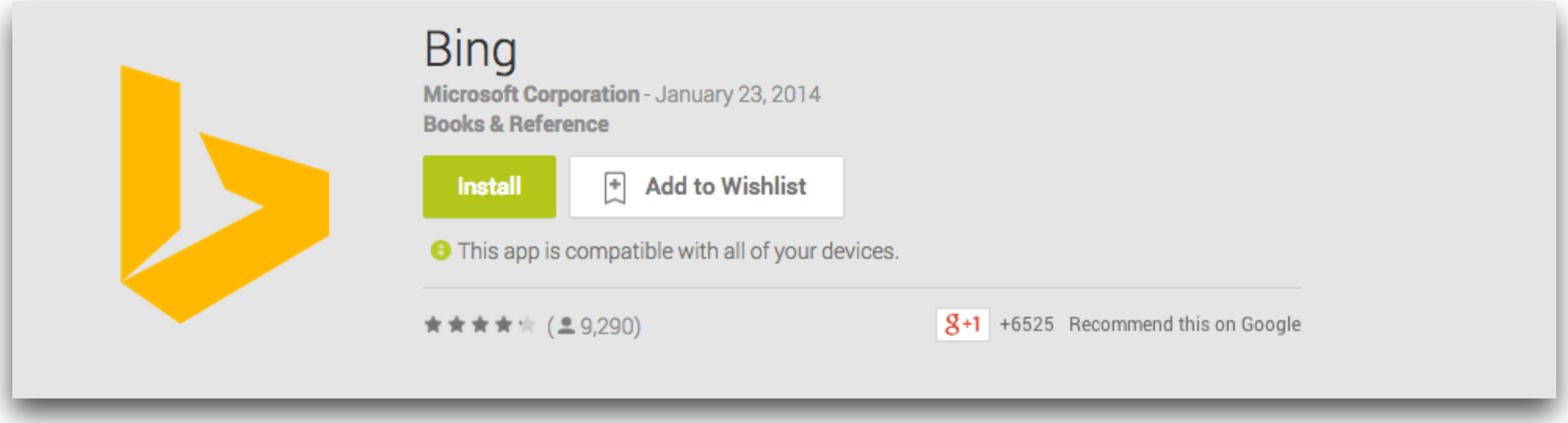
- MitmProxy / Mallory / Fiddler / Burp Suite
- Bypassing SSL Pinning (Android SSL TrustKiller)
- Data Storage Insecurities
- IPC based communications
- API Hooking - Cydia Substrate, Introspy etc
- Xposed Framework

Android Webview Vuln

- What's a Webview?
- Can the JS interact with the Java code
- What could possibly go wrong?

Malicious Things that could be done with Webview

- Take over the application's Java code
- Send SMS, Make calls etc
- Install new application
- Get a reverse shell
- Modify file system or steal something from the device



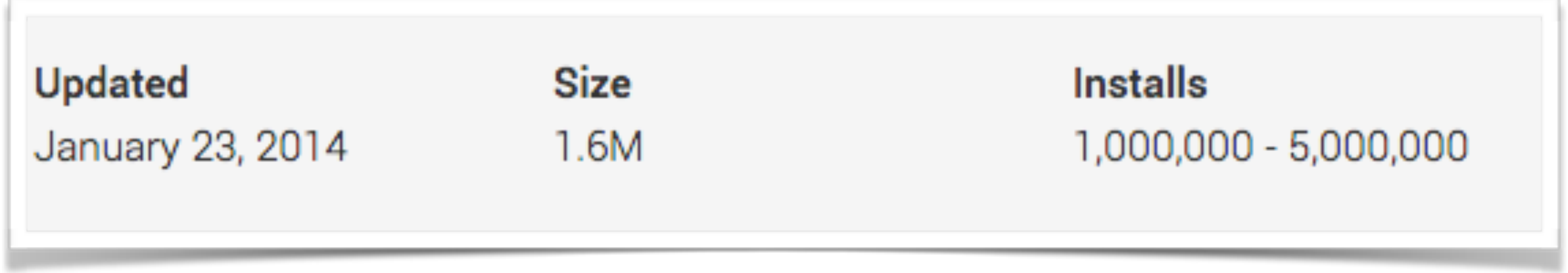
Bing

Microsoft Corporation - January 23, 2014

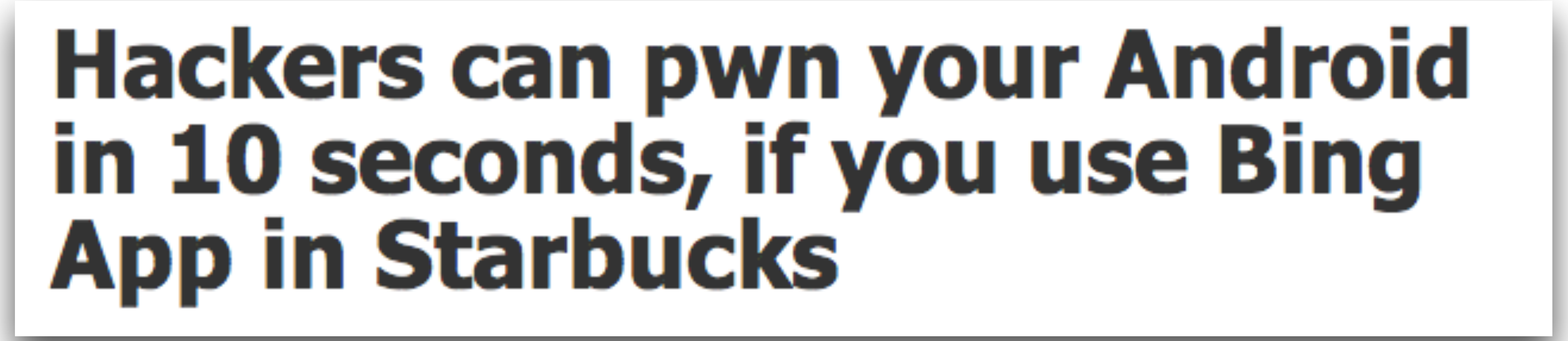
Books & Reference

This app is compatible with all of your devices.

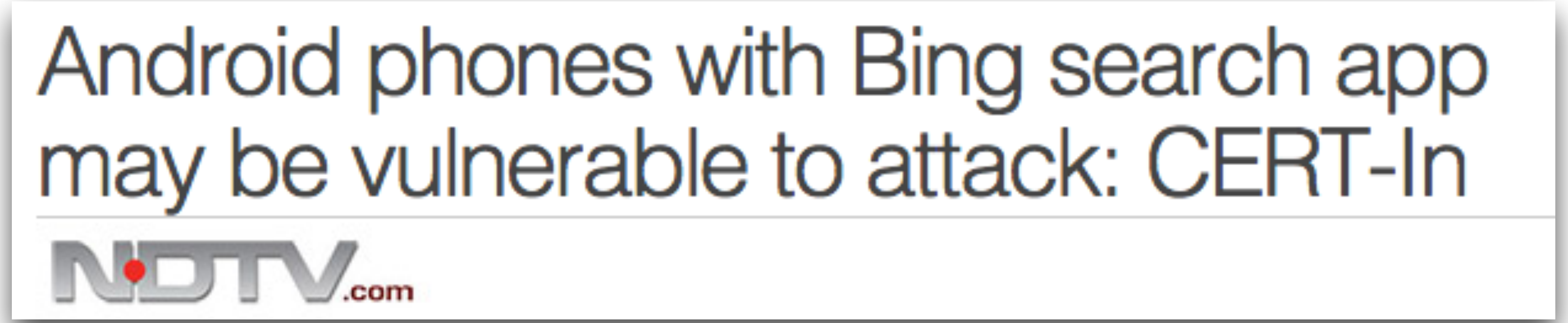
★★★★☆ (9,290)



Updated	Size	Installs
January 23, 2014	1.6M	1,000,000 - 5,000,000

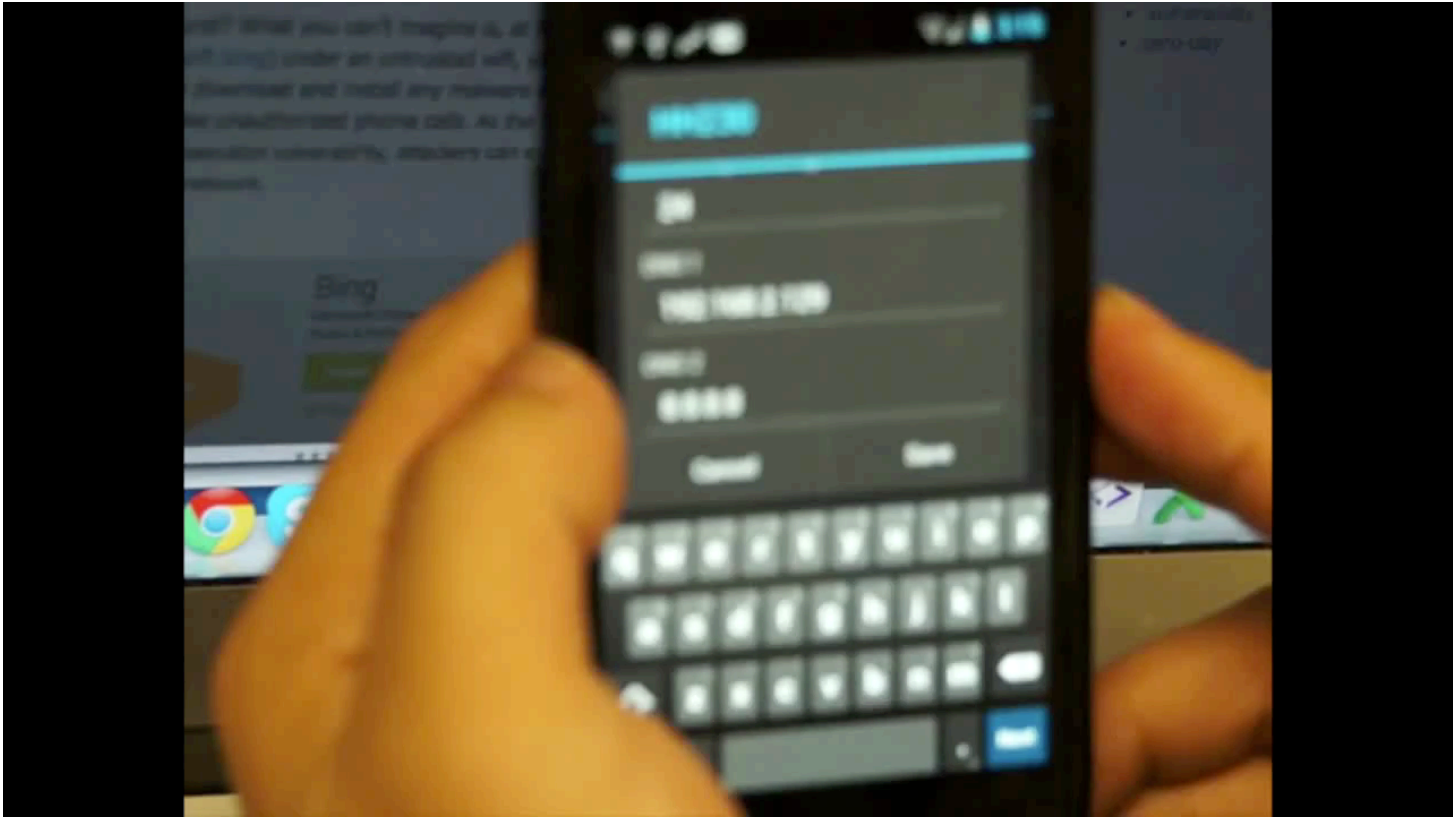


Hackers can pwn your Android in 10 seconds, if you use Bing App in Starbucks



Android phones with Bing search app may be vulnerable to attack: CERT-In

NDTV.com


Bing
Cancel
Save

Some more tools

- AndroidAuditTools
- AndroGuard
- Agnitio
- Droidbox

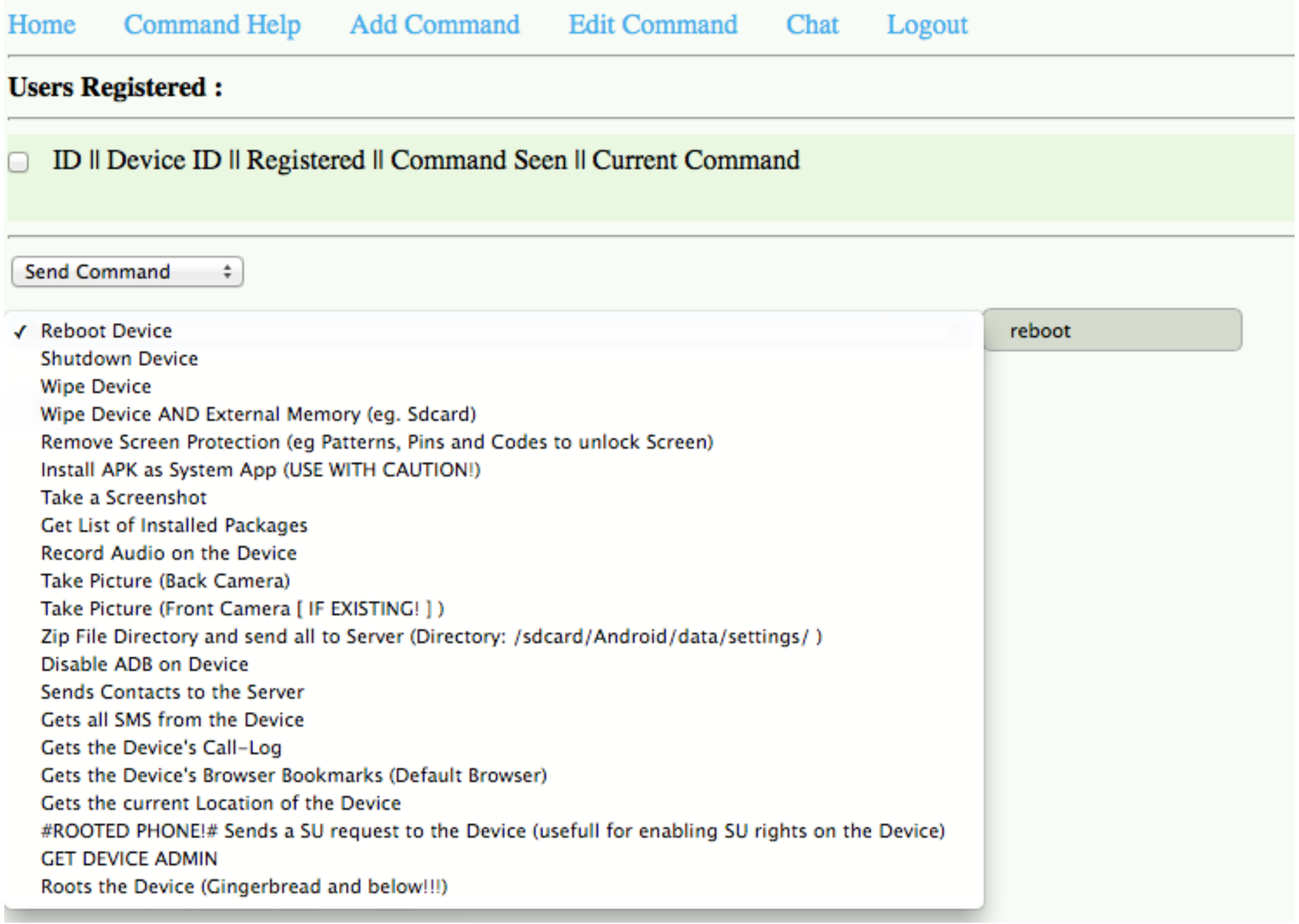
Drozer

- Great tool for Android Security Assessment
- Could be used to find content provider leakage, injection based attacks, path traversal vulns
- Free and Pro version

Android Malwares

- Android Framework for Exploitation
- Infecting legitimate apps
- Crypting and Obfuscation

Android Malwares


Home
Command Help
Add Command
Edit Command
Chat
Logout
Users Registered :
□ ID || Device ID || Registered || Command Seen || Current Command
Send Command
✓ Reboot Device
Shutdown Device
Wipe Device
Wipe Device AND External Memory (eg. Sdcard)
Remove Screen Protection (eg Patterns, Pins and Codes to unlock Screen)
Install APK as System App (USE WITH CAUTION!)
Take a Screenshot
Get List of Installed Packages
Record Audio on the Device
Take Picture (Back Camera)
Take Picture (Front Camera [IF EXISTING!])
Zip File Directory and send all to Server (Directory: /sdcard/Android/data/settings/)
Disable ADB on Device
Sends Contacts to the Server
Gets all SMS from the Device
Gets the Device's Call-Log
Gets the Device's Browser Bookmarks (Default Browser)
Gets the current Location of the Device
#ROOTED PHONE!# Sends a SU request to the Device (usefull for enabling SU rights on the Device)
GET DEVICE ADMIN
Roots the Device (Gingerbread and below!!!)
reboot

iOS Security Assessment

- iOS Security Model
- Randomized folder names
- CA unlike Android
- Objective-C

iOS Security Assessment

- Encrypted and Unencrypted Binaries
- Apps downloaded from AppStore are encrypted
- Two ways of decryption :
  - GDB : Load the app, dump, hex edit, copy, package
  - Clutch : Same stuff above, automated

iOS Tools

- Class-Dump-Z (Gives class information)
- Clutch (Convert app to unencrypted to encrypted)
- objdump and otool
- Cycript (Bridge between Javascript and Java)
- Introspy (API Hooking based on Cydia Substrate)

Auditing Apps on iOS

- Static : Class-Dump-Z + Hopper
- Dynamic : Cycript + Any Proxy

Auditing Apps on iOS

- Static : Class-Dump-Z + Hopper
- Dynamic : Cycript + Any Proxy

Cycript

- Developed by Jay Freeman (Saurik)
- Bridge between Javascript and Objective-C
- Used to do runtime manipulation in iOS apps
- ex:
  ```
  cy> UIApp.keyWindow.rootViewController.textlabel = "changed value"
  ```
- Cycript cheat sheet : http://iphonedevwiki.net/index.php/Cycript_Tricks

Bypassing app's password screen

```
UIApp.keyWindow.rootViewController->isa.messages[method-name]
= function(){return true; }
```

Getting around with Certificate Pinning

- App won't trust any other certificate than the original one
- How could be bypass it?
- Android Way of Decompiling, modifying the pin value, recompiling back
- API hooking
- Hook into the method which determines whether a certificate is true or not. Return true always.

Tools to use

- https://github.com/intrepidusgroup/trustme - gets around with SecTrustEvaluate

- iOSSSLKillSwitch - gets around with SecureTransportAPI

AppWatch

- Cloud based mobile security scanner
- For Android Apps now, iOS to be added by next month
- both Static and Dynamic analysis of the apps
- Comes along with an easy to use API
- Reports in HTML and PDF format

We scanned **Top 100 apps** in Google Play Store

with AppWatch automated scanner

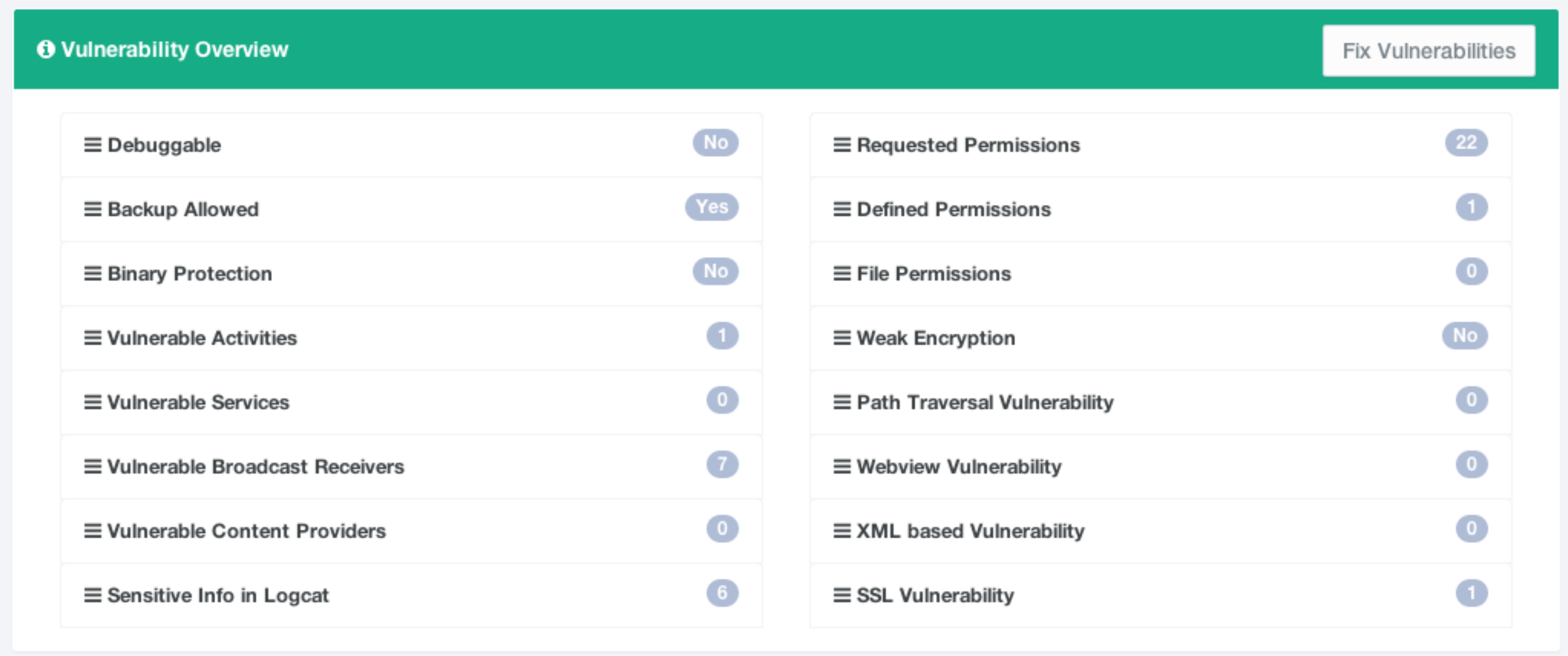
Categories

- Business
- Communication
- Education
- Entertainment
- Media & Video
- Medical
- Music & Audio
- Finance
- Shopping
- Transportation

Security Vulns we identify

- Exported IPC Endpoints - Activities, Services, Broadcast Receivers
- Leaking Content Providers
- Insecure SSL Implementation
- Leaking sensitive info in network traffic
- Local Data Storage Vulnerabilities
- OWASP Mobile Top 10
- Many more uncommon ones

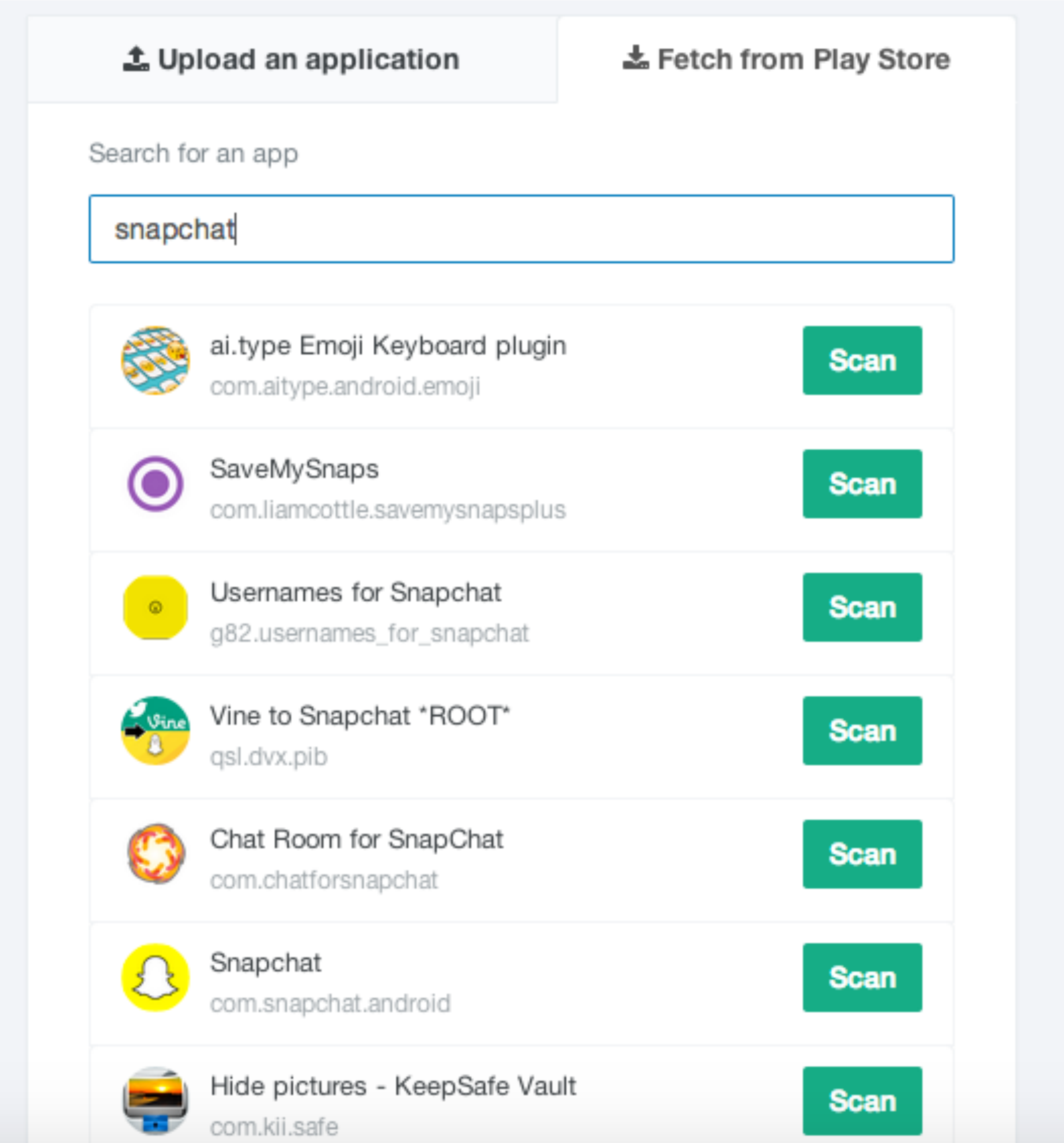
Security Vulns we identify



Vulnerability Overview

≡ Debuggable	No
≡ Backup Allowed	Yes
≡ Binary Protection	No
≡ Vulnerable Activities	1
≡ Vulnerable Services	0
≡ Vulnerable Broadcast Receivers	7
≡ Vulnerable Content Providers	0
≡ Sensitive Info in Logcat	6
≡ Requested Permissions	22
≡ Defined Permissions	1
≡ File Permissions	0
≡ Weak Encryption	No
≡ Path Traversal Vulnerability	0
≡ Webview Vulnerability	0
≡ XML based Vulnerability	0
≡ SSL Vulnerability	1

Direct Google Play App Scan



Search for an app: snapchat

ai.type Emoji Keyboard plugin
com.aitype.android.emoji

SaveMySnaps
com.liamcottle.savemysnapsplus

Usernames for Snapchat
g82.usernames_for_snapchat

Vine to Snapchat *ROOT*
qsl.dvx.pib

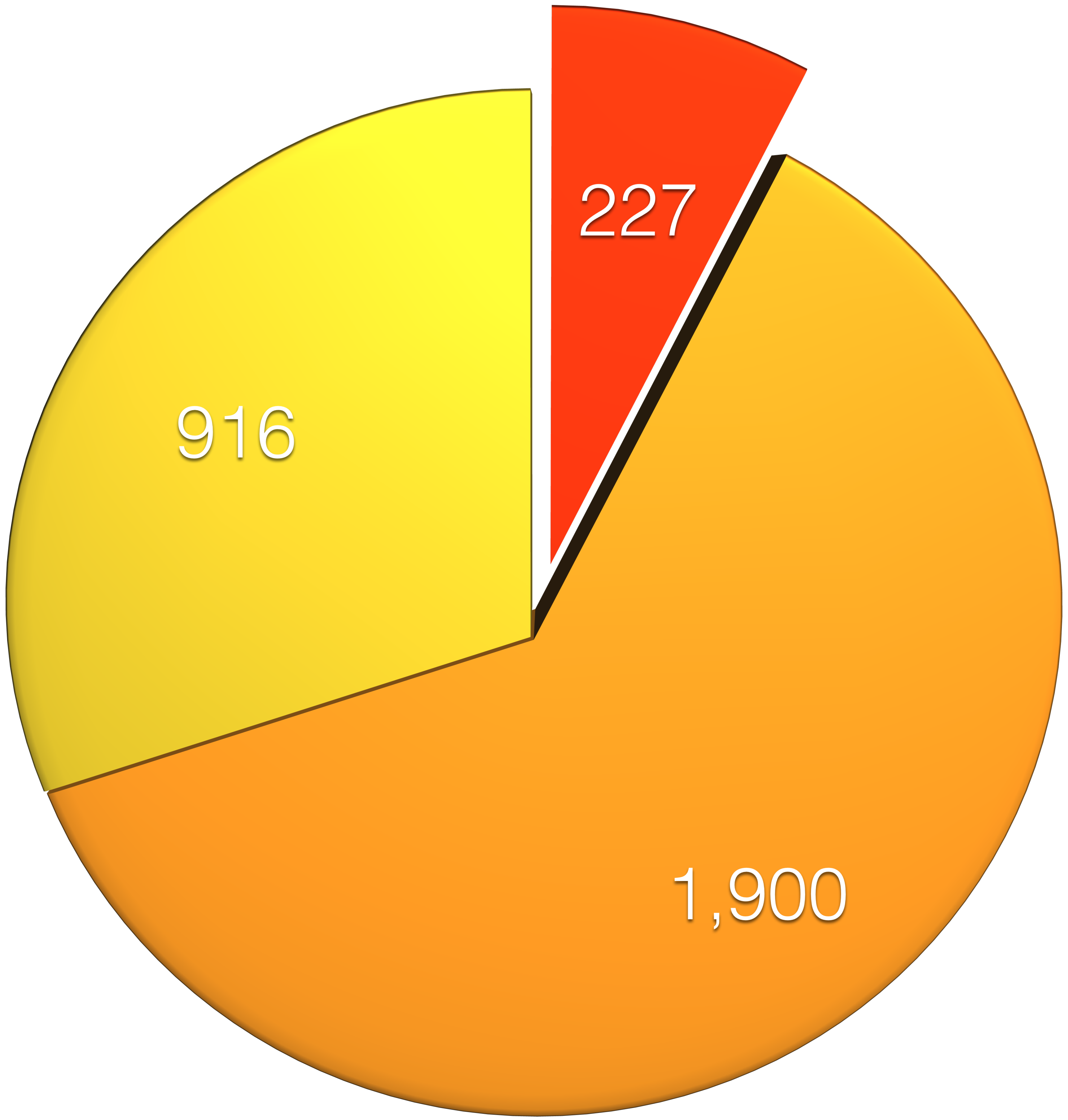
Chat Room for SnapChat
com.chatforsnapchat

Snapchat
com.snapchat.android

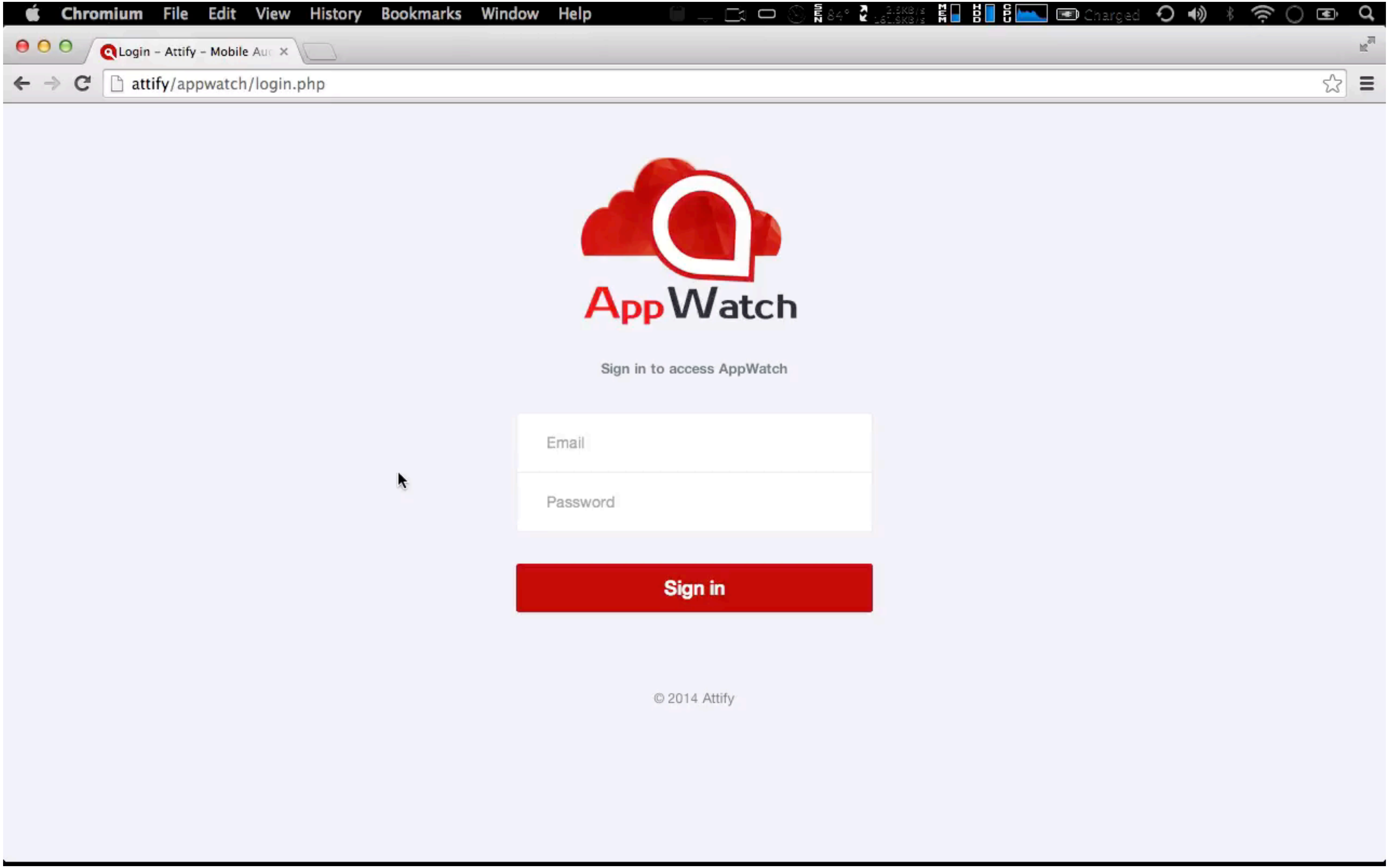
Hide pictures - KeepSafe Vault
com.kii.safe

And the Results…

Results of Top 100 Apps



AppWatch Demo



Sign in to access AppWatch

Email

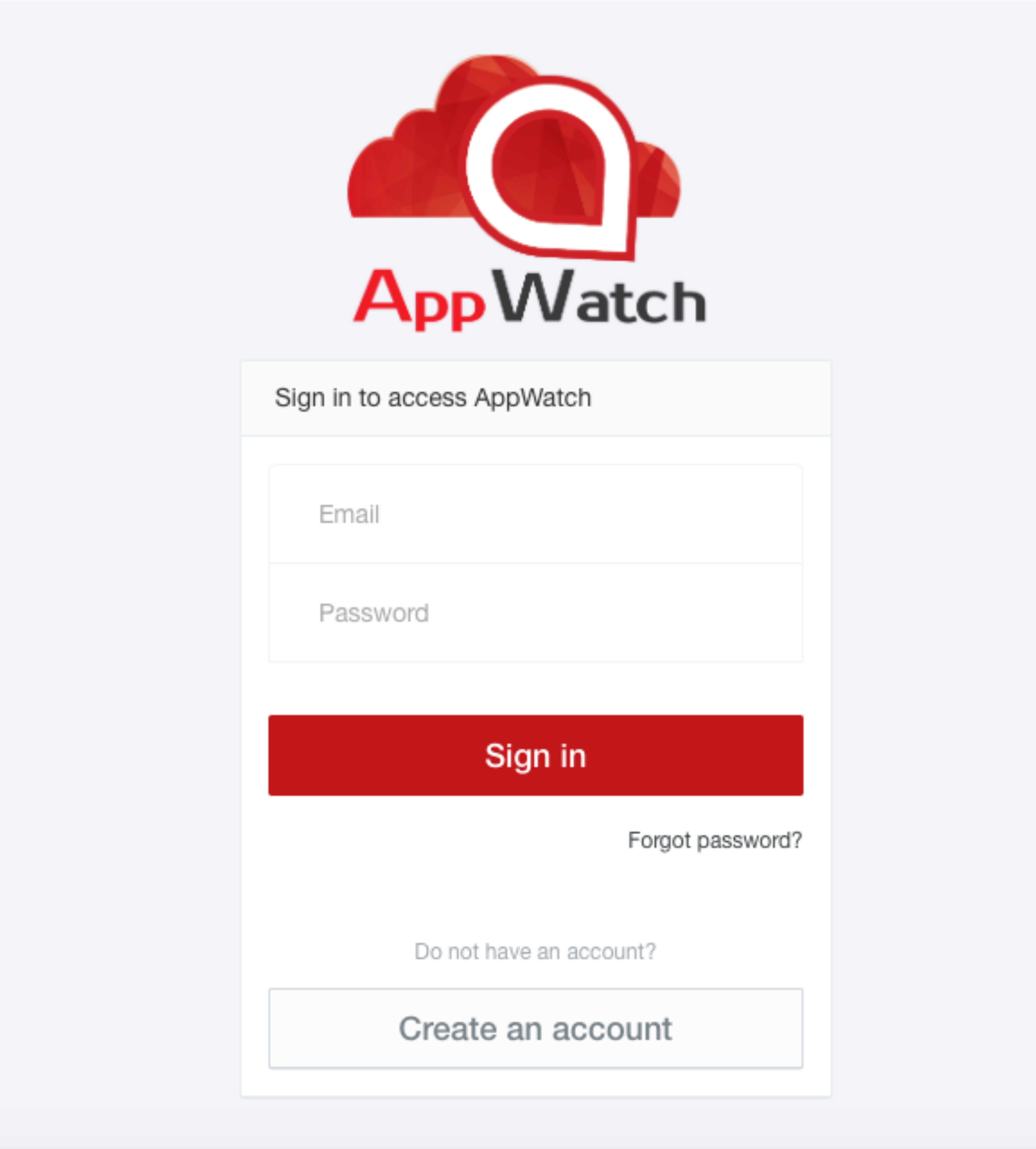
Password

© 2014 Attify

AppWatch **API** Demo

Atom
File
Edit
Selection
Find
View
Packages
Window
Help
2:03
/Volumes/Aditya/AppWatch
AppWatch
.DS_Store
AppWatch.py
AppWatch.pyc
Send Feedback
3

You can toggle the Tree View with ⌘\



Sign in to access AppWatch

Get Access to **AppWatch Community Edition**

http://attify.com/appwatch/

Get in Touch.

- Grab me after the talk
- @adi1391
- adi@attify.com
- Skype: adi0x90
- +91-9538295259