Vaccinating Android

Milan Gabor & Danijel Grah

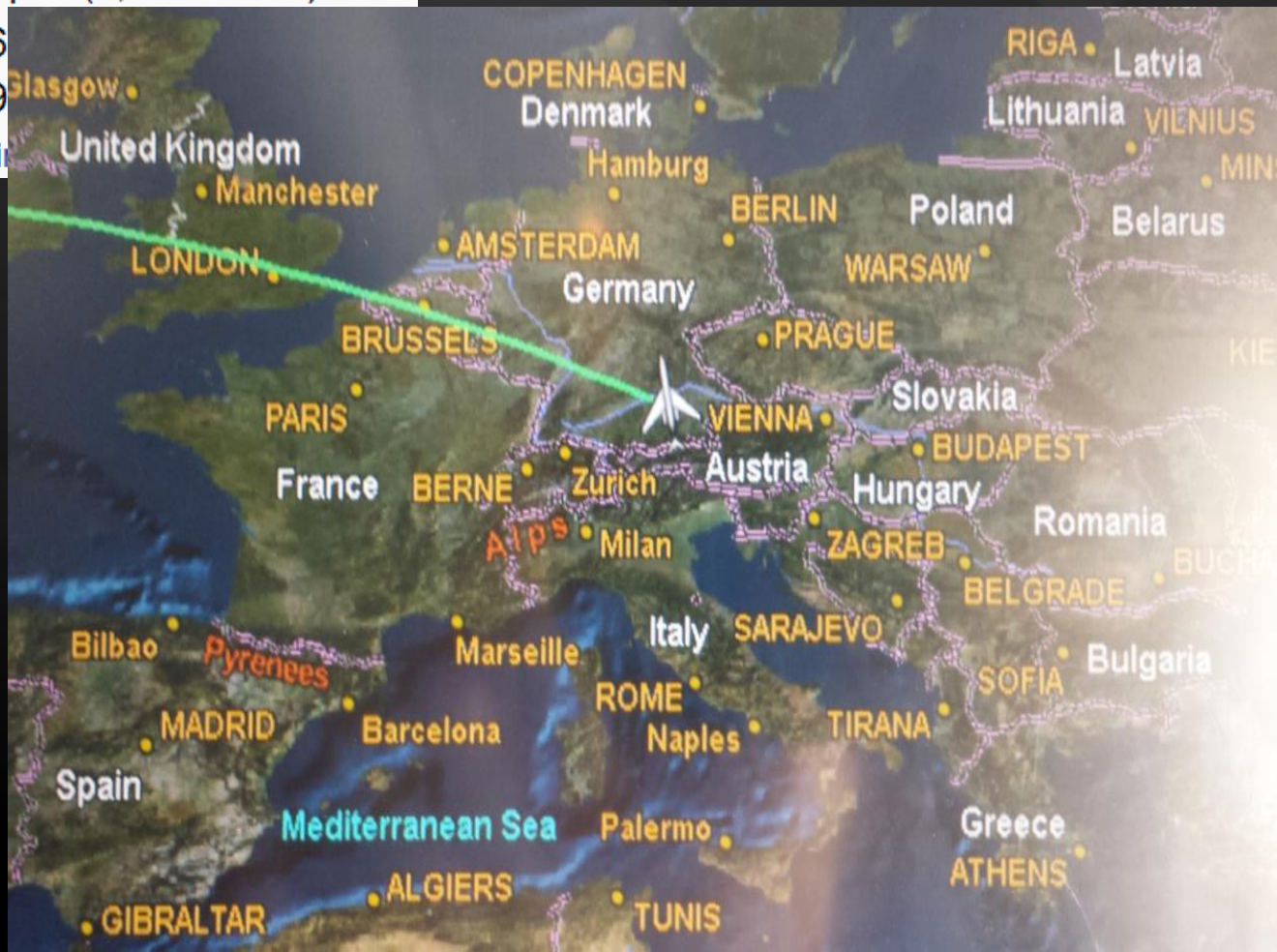
/WhoAreWe

> Just two guys from Slovenia
> Having fun breaking stuff
> Love to play with apps
> Specialized in app security

Something about sLOVEnia

Population (2010)[4]

• City	596,424
• Density	4,298.1/sq mi (1,659.5/km²)
• Urban	1,314,356
• Metro	1,951,269
	(30th most i

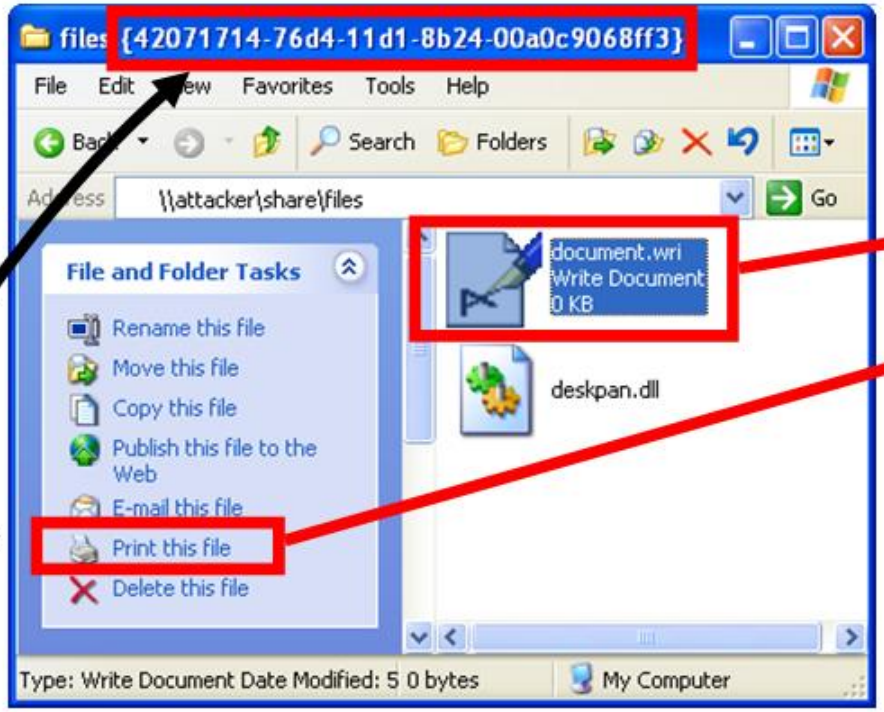


#/viris[# *]

#/viris[# *]

Windows XP & Internet Explorer 8 PoC

IEXPLORE.EXE



1st click

2nd click

CWD set

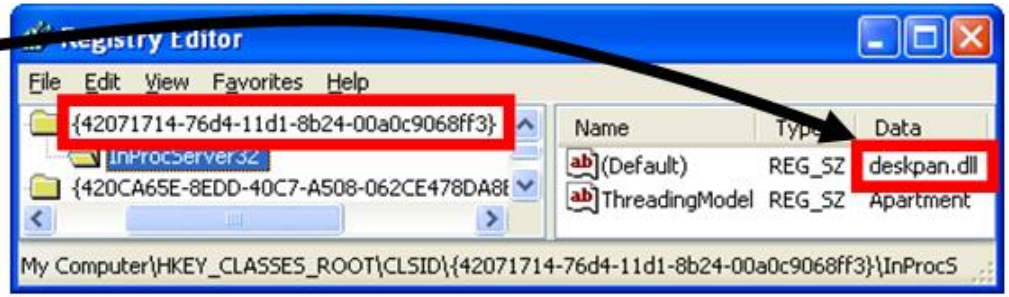
WORDPAD.EXE

CoCreateInstance(CLSID)

~~C:\Windows\System32\deskpan.dll~~

~~C:\Windows\System\deskpan.dll~~

~~C:\Windows\deskpan.dll~~



#/viris[# *]

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS

National Press Releases

Home • News • Press Room • Press Releases • FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators

Twitter Facebook (16) Share

FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators

Washington, D.C.
July 28, 2010

FBI National Press Office
(202) 324-3691

The FBI, in partnership with the Slovenian Criminal Police and the Spanish Guardia Civil, announced today significant developments in a two-year investigation of the creator and operators of the Mariposa Botnet. A botnet is a network of remote-controlled compromised computers.

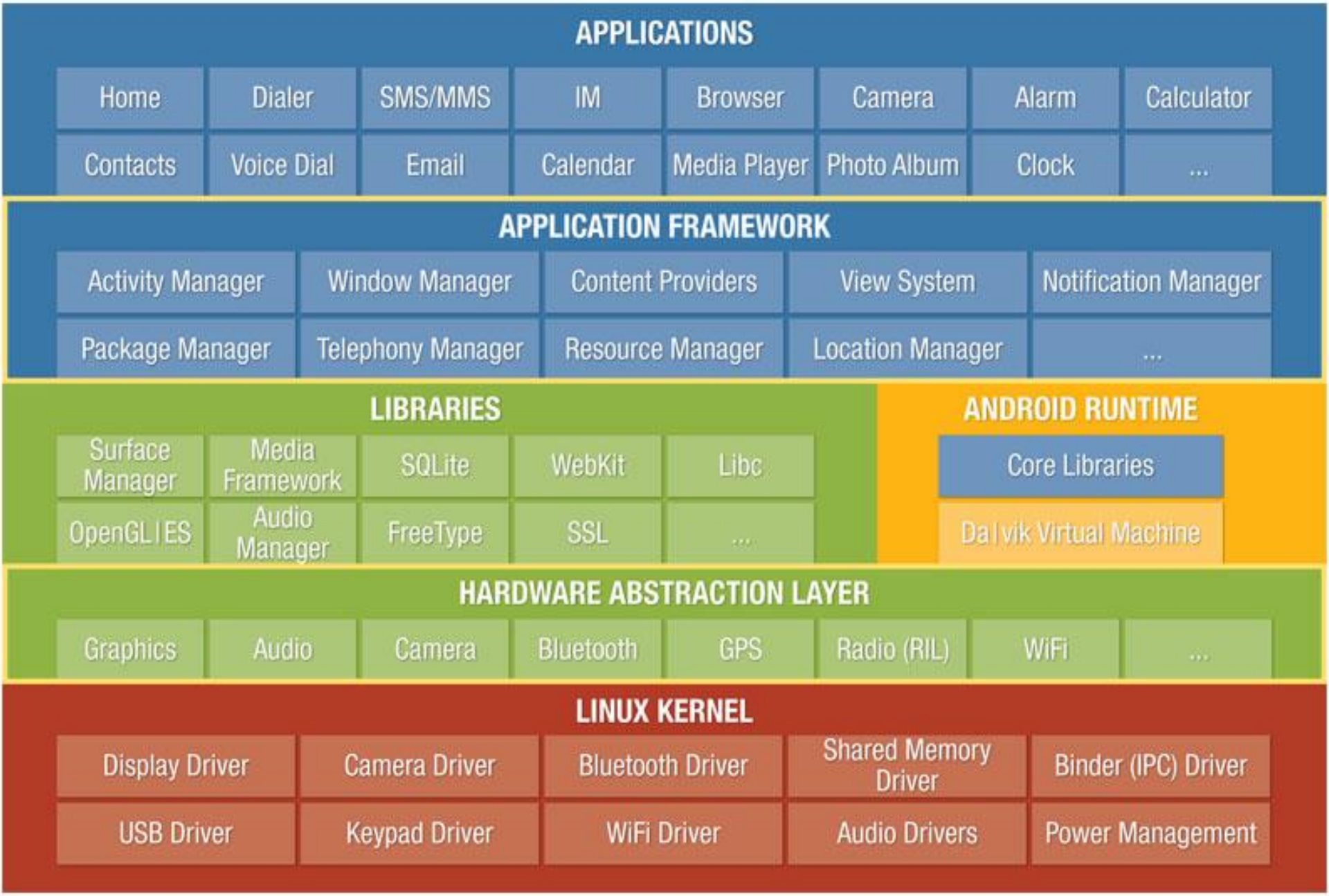
The Mariposa Botnet was built with a computer virus known as "Butterfly Bot" and was used to steal passwords for websites and financial institutions. It stole computer users' credit card and bank account information, launched denial of service attacks, and spread viruses. Industry experts estimated the Mariposa Botnet may have infected as many as 8 million to 12 million computers.

"In the last two years, the software used to create the Mariposa botnet was sold to hundreds of other criminals, making it one of the most notorious in the world," said FBI Director Robert S. Mueller, III. "These cyber intrusions, thefts, and frauds undermine the integrity of the Internet and the businesses that rely on it; they also threaten the privacy and pocketbooks of all who use the Internet."

Agenda

> Where are we today
> Short 101 APK
> Analysis (static, dynamic)
> Vaccinating APK, Android
> DEMO(s)
> The end


WHERE ARE WE TODAY


APPLICATIONS
Home
Dialer
SMS/MMS
IM
Browser
Camera
Alarm
Calculator
Contacts
Voice Dial
Email
Calendar
Media Player
Photo Album
Clock
...
APPLICATION FRAMEWORK
Activity Manager
Window Manager
Content Providers
View System
Notification Manager
Package Manager
Telephony Manager
Resource Manager
Location Manager
...
LIBRARIES
Surface Manager
Media Framework
SQLite
WebKit
Libc
OpenGL|ES
Audio Manager
FreeType
SSL
...
ANDROID RUNTIME
Core Libraries
Dalvik Virtual Machine
HARDWARE ABSTRACTION LAYER
Graphics
Audio
Camera
Bluetooth
GPS
Radio (RIL)
WiFi
...
LINUX KERNEL
Display Driver
Camera Driver
Bluetooth Driver
Shared Memory Driver
Binder (IPC) Driver
USB Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Status 2013/2014

HP research finds vulnerabilities in 9 of 10 mobile apps

Summary: *Obvious security vulnerabilities are disturbingly common in corporate mobile apps. If HP can find them, so can malicious actors.*

By Larry Seltzer for Zero Day | November 19, 2013 -- 13:15 GMT (05:15 PST)

Follow @lseltzer

Tests run by HP Fortify, the company's enterprise security arm, indicate that 90% of mobile apps have at least one security vulnerability.

The company used their Fortify On Demand for Mobile product to test the security posture of 2,107 applications published by 601 companies on the Forbes Global 2000. Only iOS apps were tested, but HP says that there is good reason to believe the same problems exist in any Android counterparts.

Overall, the problems fell into one of four categories. The analysis showed that 86% of apps that accessed potentially private data sources, such as address books or Bluetooth connections, lacked sufficient security measures to protect the data from access.

86% of apps tested lacked binary hardening protection. This refers to a group of techniques, many implemented simply with checkboxes at compile time, which protect against certain attacks, like buffer overflows, path disclosure and jailbreak detection.

Enough motivation?

The security specialists grouped the security vulnerabilities in four categories:

- 86% of mobile apps lacked of sufficient security measures to protect private data (e.g. Address books, User data).
- 86% of mobile apps tested lacked binary hardening protection, these apps have resulted vulnerable to certain attacks, including buffer overflows, jailbreak detection and path disclosure.
- 75% of mobile apps did implement data encryption for storage operations, the application stored in clear text also personal data like passwords, personal documents and chat logs.
- 18% of mobile apps transmitted data over the network without using SSL encryption, but what is also concerning is that another 18% of apps used SSL incorrectly. In both cases resulted that private data was transmitted in the clear or anyway accessible by an attacker that share same network connection, the

Kaspersky says …

98% of modern mobile threats target Android. For iOS and WP8, you can stay adequately protected with

REDACTED

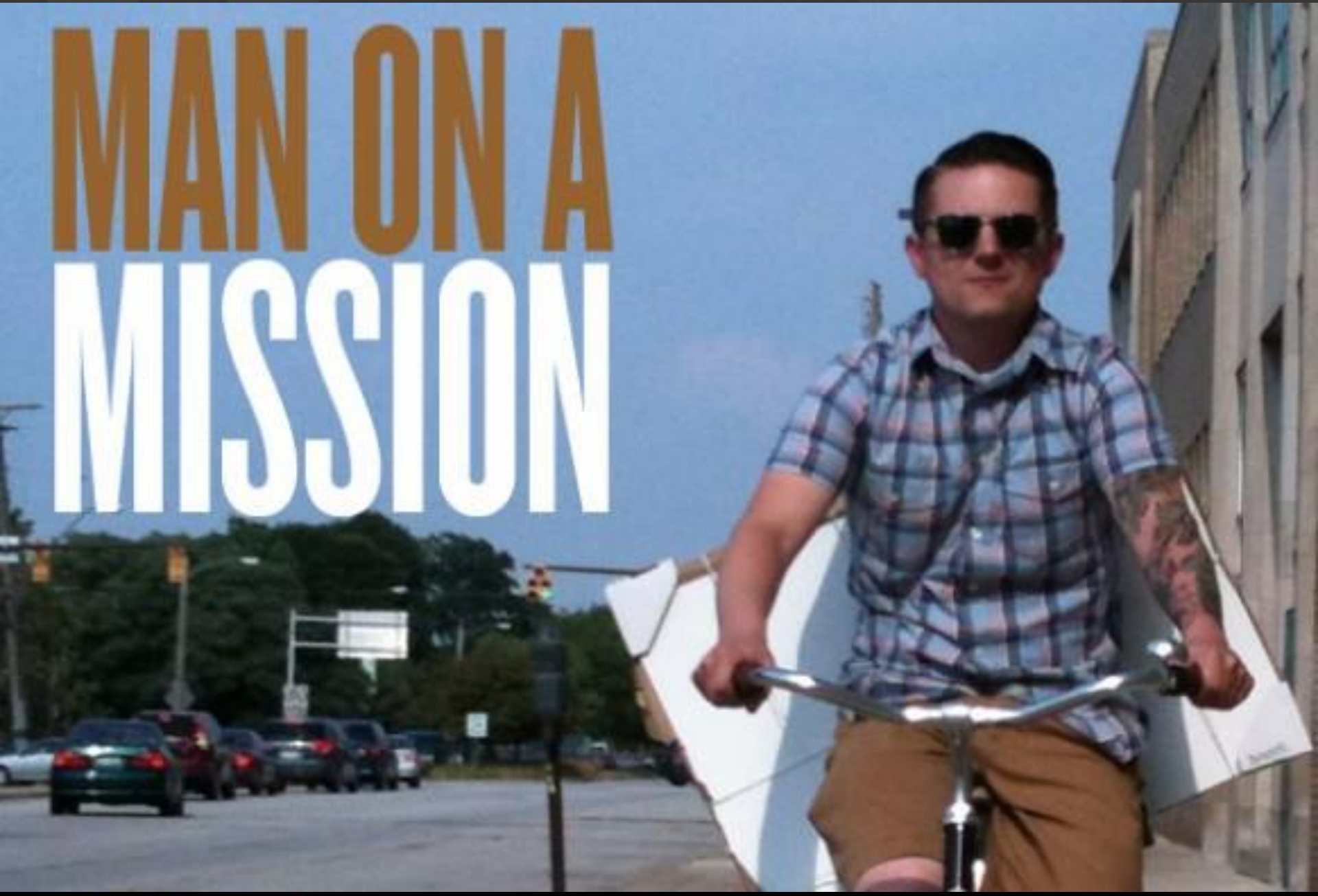
Things

- There is a (big) need for testing mobile apps
- Mobile app development feels like late 90's development
- Our experience

Why?

- Managers focused on due dates
- Developers focused on features not security
- Users don’t care about security

#/viris[ ]


MAN ON A
MISSION

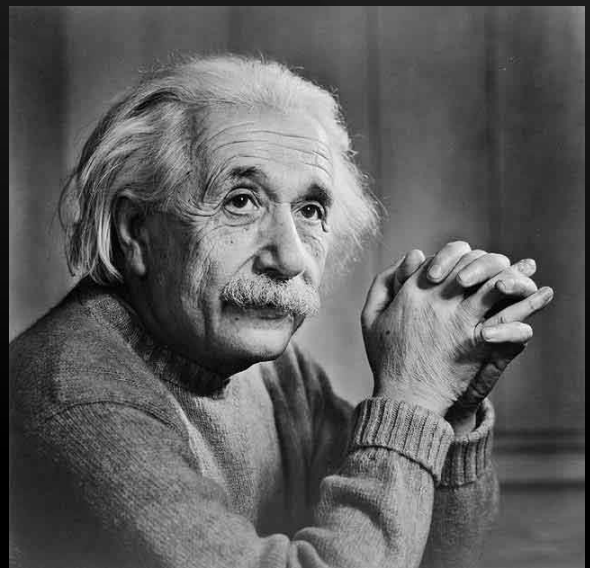
To see and feel invisible!

True vision?

I have been doing same things as other people.

I just looked them in different way.

Albert Einstein



What to check?

- Transport security
  - Plaintext Traffic
  - Improper session handling
  - Validate SSL certificates
- Compiler protection
- UIWebviews
  - Data validation
  - Analyze UIWebView implementations
- Insecure data storage
  - SQLite DB
  - File caching
  - Checking log files

What to check? (cont)

- Logging
  - Custom logs
  - Crash reports logs and files
- Binary analysis
  - Disassemble/decompile the application
  - Detect obfuscations
  - Detect anti-debugging protections
- Client side injections
- Third party libraries

#/viris[# *]

101 APK, Android

> APK? WTF?

> Get APK

> Decompile and analyze code

> Test

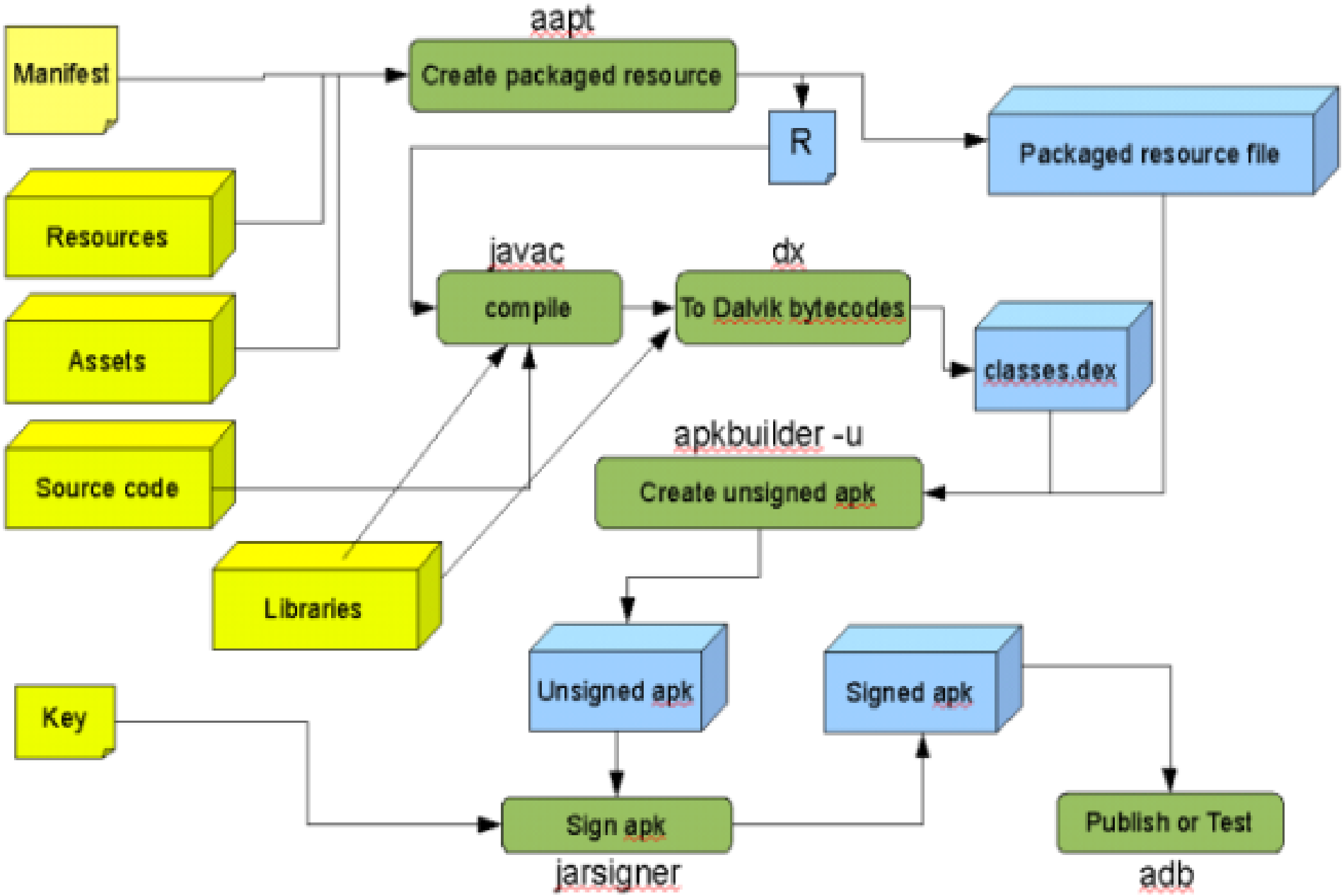
APK?

> Android application package file (**APK**) is the package file format used to distribute and install application software and middleware onto Google's Android operating system, and certain other operating systems, such as Blackberry 10 Devices with the OS version 10.2.1.

Wikipedia

Android Applications

- .apk (Android Package) format
- Nothing more than a zip
- Written exclusively in Java, with native libraries in C/C++.
- Composed of components like Activities, Services, Broadcast Receivers, etc.


aapt
Manifest
Create packaged resource
R
Packaged resource file
Resources
javac
dx
compile
To Dalvik bytecodes
classes.dex
Assets
Source code
apkbuilder -u
Create unsigned apk
Libraries
Unsigned apk
Signed apk
Key
Sign apk
Publish or Test
jarsigner
adb

Getting APK

> Copy from the phone
> Copy from the backup
> Adb pull
> http://apps.evozi.com/apk-downloader/
> Download from untrusted source ;)

Decompile

- Pull from phone.

```
adb pull /data/app(or app-private)/app1.apk
unzip app1.apk
dex2jar classes.dex
jdgui classes2jar.jar
```

or convert to smali and then analyse the code

```
adb pull /data/app/app1.apk
unzip app1.apk
java -jar baksmali.jar -o C:\pentest\app classes.dex
```

Tools used for reversing APK

> Dex2Jar

> JD-GUI

> (Back)smali

> APKTool

> http://www.decompileandroid.com/

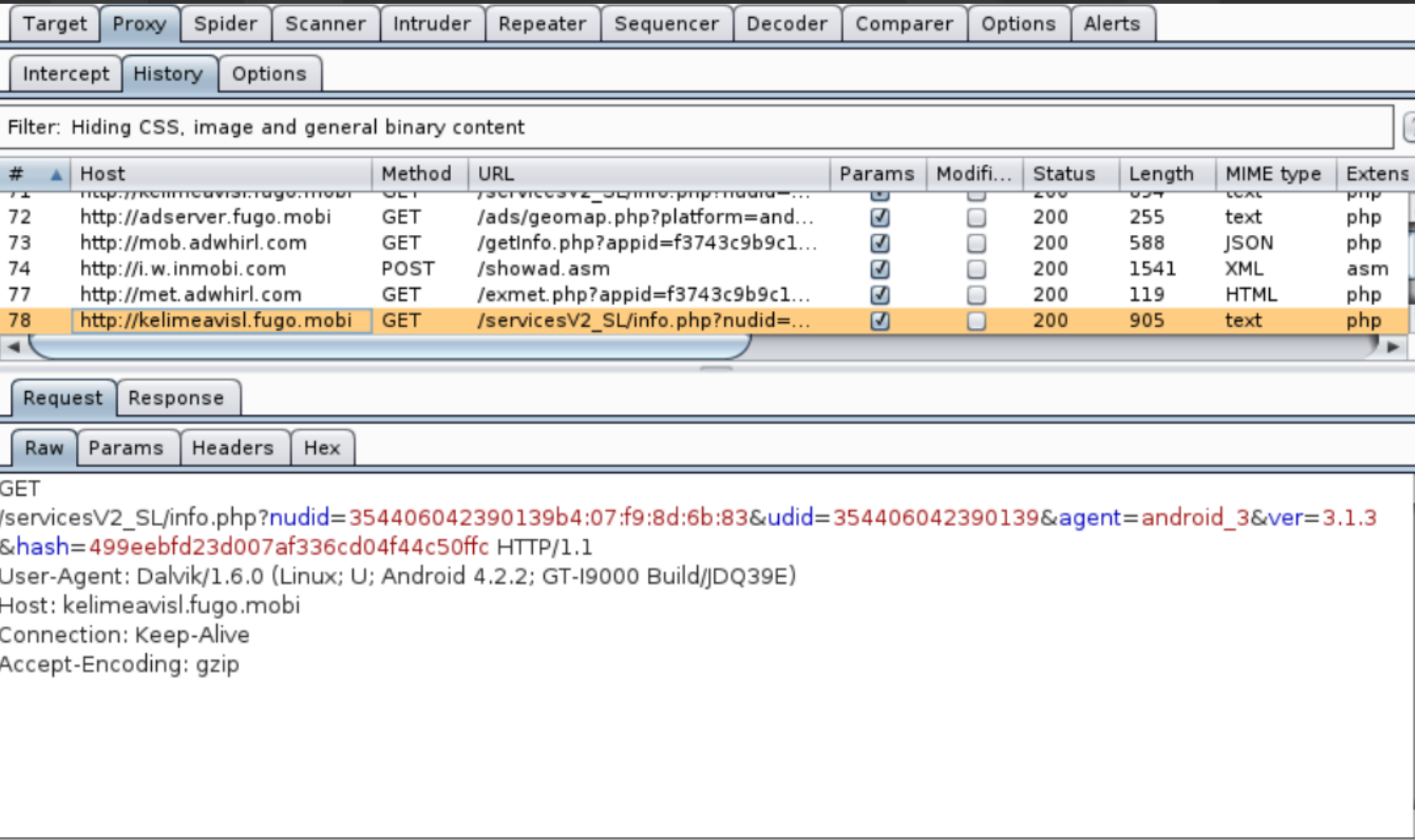
Short demo

#/viris[# *]

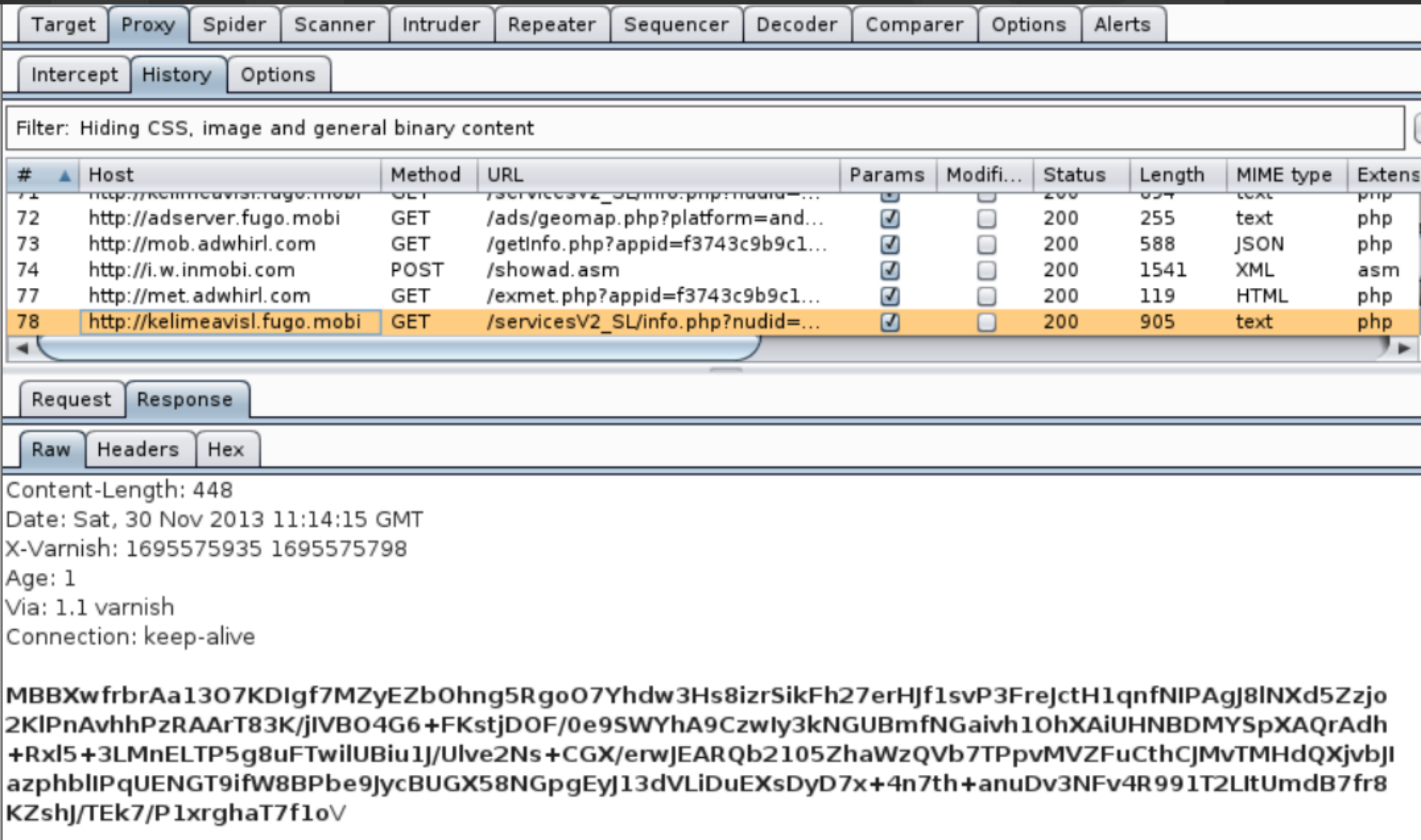
Testing app

> Start simulator with proxy
> Install app in emulator or device
> Use Wireshark, Fiddler &/|| Zap &/|| Burp to monitor network
> Run app
> See logs, dump, crashes, files

Request

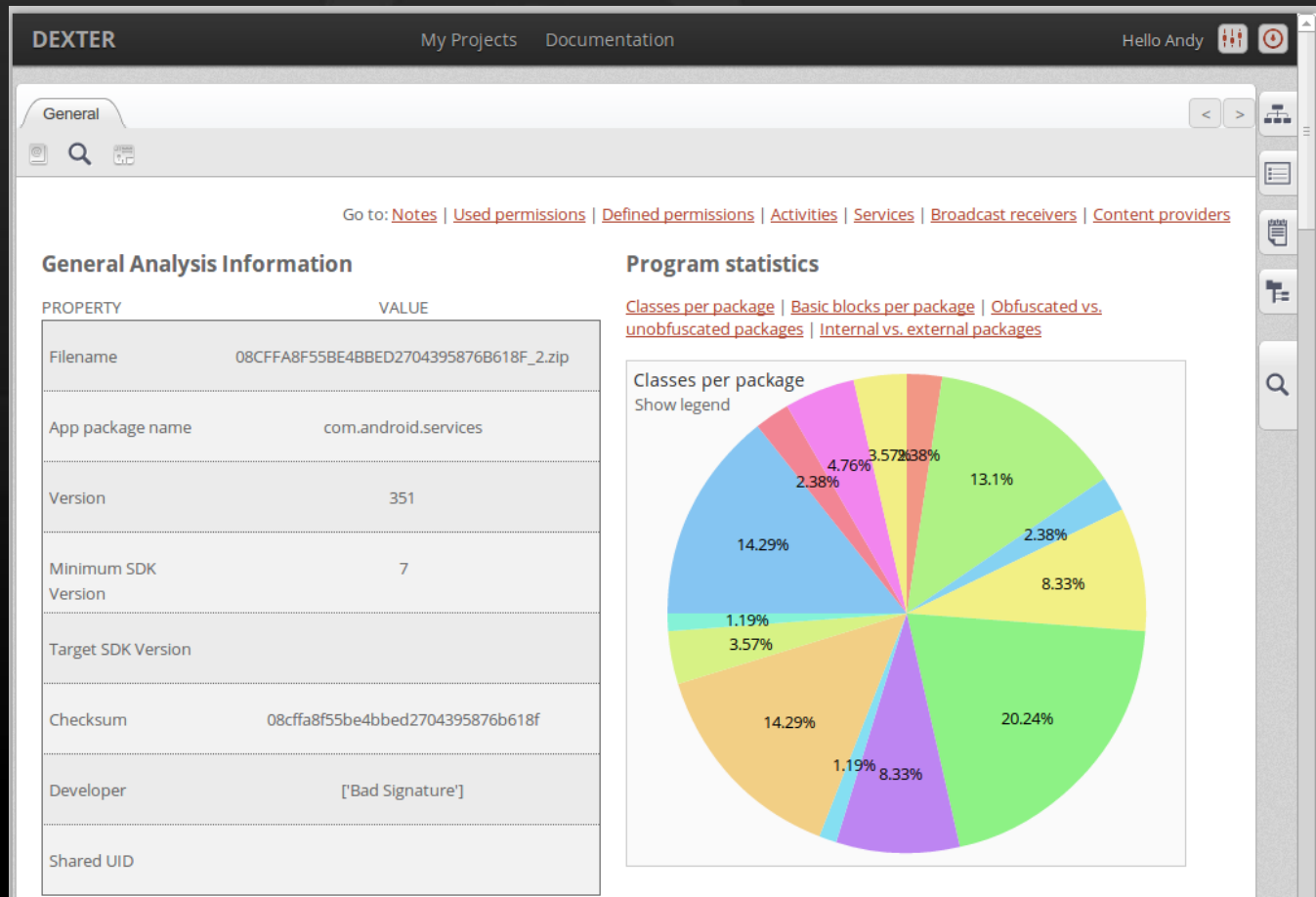

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Options
Alerts
Intercept
History
Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Modifi... Status Length MIME type Extens
72 http://adserver.fugo.mobi GET /ads/geomap.php?platform=and... 200 255 text php
73 http://mob.adwhirl.com GET /getInfo.php?appid=f3743c9b9c1... 200 588 JSON php
74 http://i.w.inmobi.com POST /showad.asm 200 1541 XML asm
77 http://met.adwhirl.com GET /exmet.php?appid=f3743c9b9c1... 200 119 HTML php
78 http://kelimeavisl.fugo.mobi GET /servicesV2_SL/info.php?nudid=... 200 905 text php
Request
Response
Raw
Params
Headers
Hex
GET
/servicesV2_SL/info.php?nudid=354406042390139b4:07:f9:8d:6b:83&udid=354406042390139&agent=android_3&ver=3.1.3
&hash=499eebfd23d007af336cd04f44c50ffc HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; GT-I9000 Build/JDQ39E)
Host: kelimeavisl.fugo.mobi
Connection: Keep-Alive
Accept-Encoding: gzip

Reply


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Options
Alerts
Intercept
History
Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Modifi... Status Length MIME type Extens
72 http://adserver.fugo.mobi GET /ads/geomap.php?platform=and... 200 255 text php
73 http://mob.adwhirl.com GET /getInfo.php?appid=f3743c9b9c1... 200 588 JSON php
74 http://i.w.inmobi.com POST /showad.asm 200 1541 XML asm
77 http://met.adwhirl.com GET /exmet.php?appid=f3743c9b9c1... 200 119 HTML php
78 http://kelimeavisl.fugo.mobi GET /servicesV2_SL/info.php?nudid=... 200 905 text php
Request
Response
Raw
Headers
Hex
Content-Length: 448
Date: Sat, 30 Nov 2013 11:14:15 GMT
X-Varnish: 1695575935 1695575798
Age: 1
Via: 1.1 varnish
Connection: keep-alive
MBBXwfrbrAa13O7KDIgf7MZyEZbOhng5RgoO7Yhdw3Hs8izrSikFh27erHJf1svP3FreJctH1qnfNIPAgJ8lNXd5Zzjo
2KlPnAvhhPzRAArT83K/jlVBO4G6+FKstjDOF/0e9SWYhA9Czwly3kNGUBmfNGaivh1OhXAiUHNBDMYSpXAQrAdh
+Rxl5+3LMnELTP5g8uFTwilUBiu1J/Ulve2Ns+CGX/erwJEARQb2105ZhaWzQVb7TPpvMVZFuCthCJMvTMHdQXjvbJI
azphblIPqUENGT9ifW8BPbe9JycBUGX58NGpgEyJ13dVLiDuEXsDyD7x+4n7th+anuDv3NFv4R991T2LItUmdB7fr8
KZshJ/TEk7/P1xrghaT7f1oV

Other tools

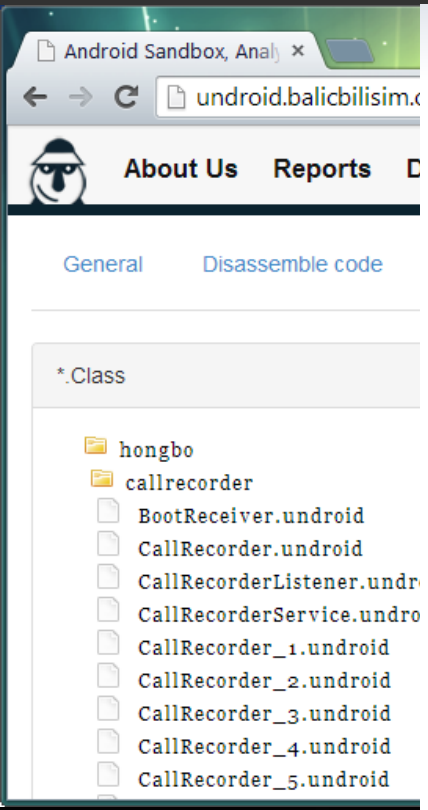
> http://dexter.dexlabs.org/



#/viris[# *]

Other tools

> http://undroid.balicbilisim.com/



Security Researcher Accidentally Crashes Google Play When Testing POC App

SHARE: SHARE SHARE TWEET

Adjust text size:

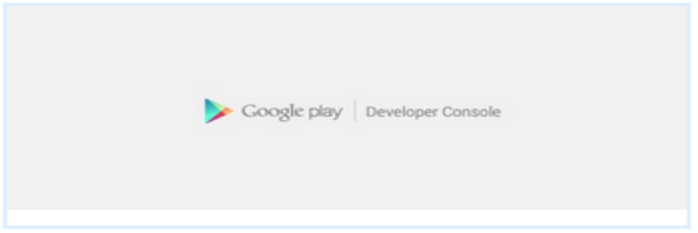
Turkish security researcher Ibrahim Balic claims to have found an Android vulnerability that could lead to memory corruption. While testing his findings, he may have crashed Google Play a couple of times.

According to the expert, Android 2.3, 4.2.2 and 4.3 are certainly affected, but he believes that all versions of the operating system are vulnerable.

He has found that executing a malformed APK file leads to a denial-of-service (DOS) condition and the device freezes. Balic wanted to test his theory against Bouncer, the Android anti-malware system developed by Google, so he uploaded a malformed APK file to Google Play.

Shortly after, he started getting errors on Google Play. In addition, during the time he performed his tests, many people reported being unable to upload applications to Google's app market.

"I think it was probably because of testing my PoC exploit on Google Play," Balic noted in a blog post.



- Google Play Developer Console crashes during te...

Static analysis

- You need to know how read Java code
- Cannot see all runtime replies
- Obfuscated, renamed?
- Identify important segments in code

Static analysis

- Apkyzer
  - » Unzip, dex2jar, jad, bash, html
- More apk‘s at once
- WebView addJavascriptInterface Remote Code Execution (September 24, 2013, https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/)
  - » grep -r -n -i --include=*.java addJavascriptInterface *
- Result.html

Side tool - apkyzer

Results for regex expression: http:|https:|file:|ftp:|pop3:

.....
Application: com.jgames.shapegame-1
.....

/root/android/apkyzer/source/com.jgames.shapegame-1/java/com/google/ads/m.java
16: public final com.google.ads.util.i.c e = new com.google.ads.util.i.c(this, "mraidBannerPath", "http://media.admob.com/mraid/v1/mraid_app_banner.js");
17: public final com.google.ads.util.i.c f = new com.google.ads.util.i.c(this, "mraidExpandedBannerPath", "http://media.admob.com/mraid/v1/mraid_app_expanded_banner.js");
18: public final com.google.ads.util.i.c g = new com.google.ads.util.i.c(this, "mraidInterstitialPath", "http://media.admob.com/mraid/v1/mraid_app_interstitial.js");
19: public final com.google.ads.util.i.c h = new com.google.ads.util.i.c(this, "badAdReportPath", "https://badad.googleplex.com/s/reportAd");

/root/android/apkyzer/source/com.jgames.shapegame-1/java/com/jgames/shapegame/HighScores.java
37: startActivity(new Intent("android.intent.action.VIEW", Uri.parse("http://imgwerx.com/games/copycat/highscores.php")));
230: httppost = new HttpPost("http://www.imgwerx.com/games/copycat/submit_score.php");

/root/android/apkyzer/source/com.jgames.shapegame-1/java/com/jgames/shapegame/Info.java
48: startActivity(new Intent("android.intent.action.VIEW", Uri.parse("http://imgwerx.com/")));
84: private final String webUri = "http://imgwerx.com/";

```
amString1, String paramString2)


ML("http://my-own-gamme.com/api/save.php?t=" + paramString1 + "&u=" + paramString2);
);
lueOf(false);


true);
```


```java
public class HttpCall
{
  private static String SECURITY_TOKEN = "AE94DFKMADF4U94MNSDF324SF3ADASCAR4GASDFF94";
  private CookieStore cookieStore = new BasicCookieStore();
  private HttpClient httpClient = new DefaultHttpClient();
  private HttpContext localContext = new BasicHttpContext();

  public HttpCall()
  {
    this.localContext.setAttribute("http.cookie-store", this.cookieStore);
  }

  // ERROR //
  public String call(String paramString)
  {
    // Byte code:
    //   0: new 52   org/apache/http/client/methods/HttpPost
    //   3: dup
    //   4: aload_1
    //   5: invokespecial 55   org/apache/http/client/methods/HttpPost:<init>  (Ljava/lang/String;)V
    //   8: astore_2
    //   9: aload_2
    //   10: ldc 57
    //   12: getstatic 18   com/ttech/turkcellsdk/util/HttpCall:SECURITY_TOKEN Ljava/lang/String;
    //   15: invokevirtual 61  org/apache/http/client/methods/HttpPost:setHeader   (Ljava/lang/String;Ljava/lang/S
    //   18: aload_0
```

Dynamical analysis

- Monitoring/changing traffic with proxy
- Debugging
- Reflection

Reflection

> "Reflection" is a language's ability to inspect and dynamically call classes, methods, attributes, etc. at runtime.

BeanShell

- Java Interpreter
- Scripting Language
- Small
- Embeddable / Extensible
- A natural scripting language for Java

Debugging vs Reflection

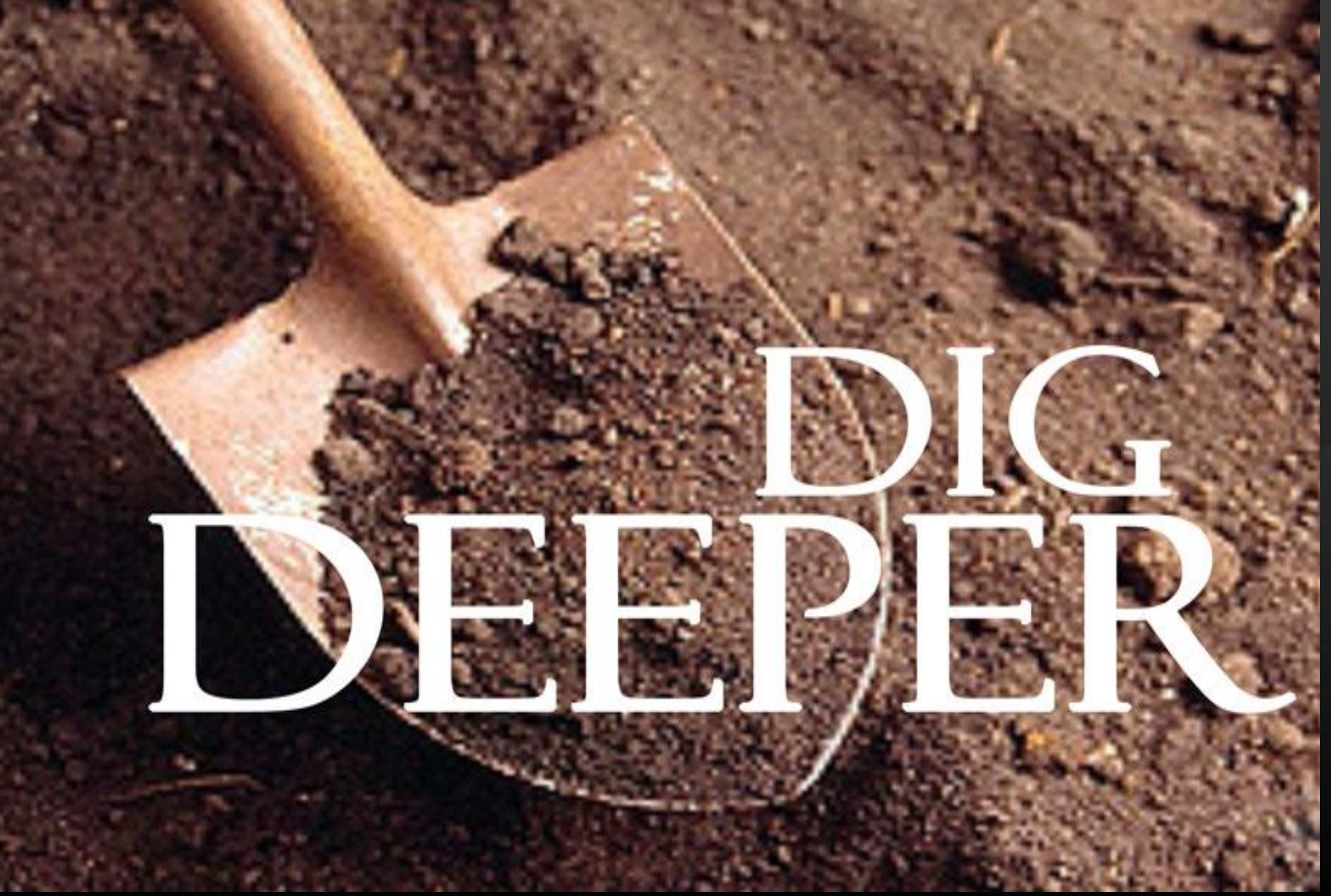
- Higher level view
- Better idea how application works
- Java like access to objects, methods, variables
- Interaction with application

Features

- Access all variables
- Change values of variables
- Call methods
- Use variables and scripts
- Use full BeanShell
- Write Java code

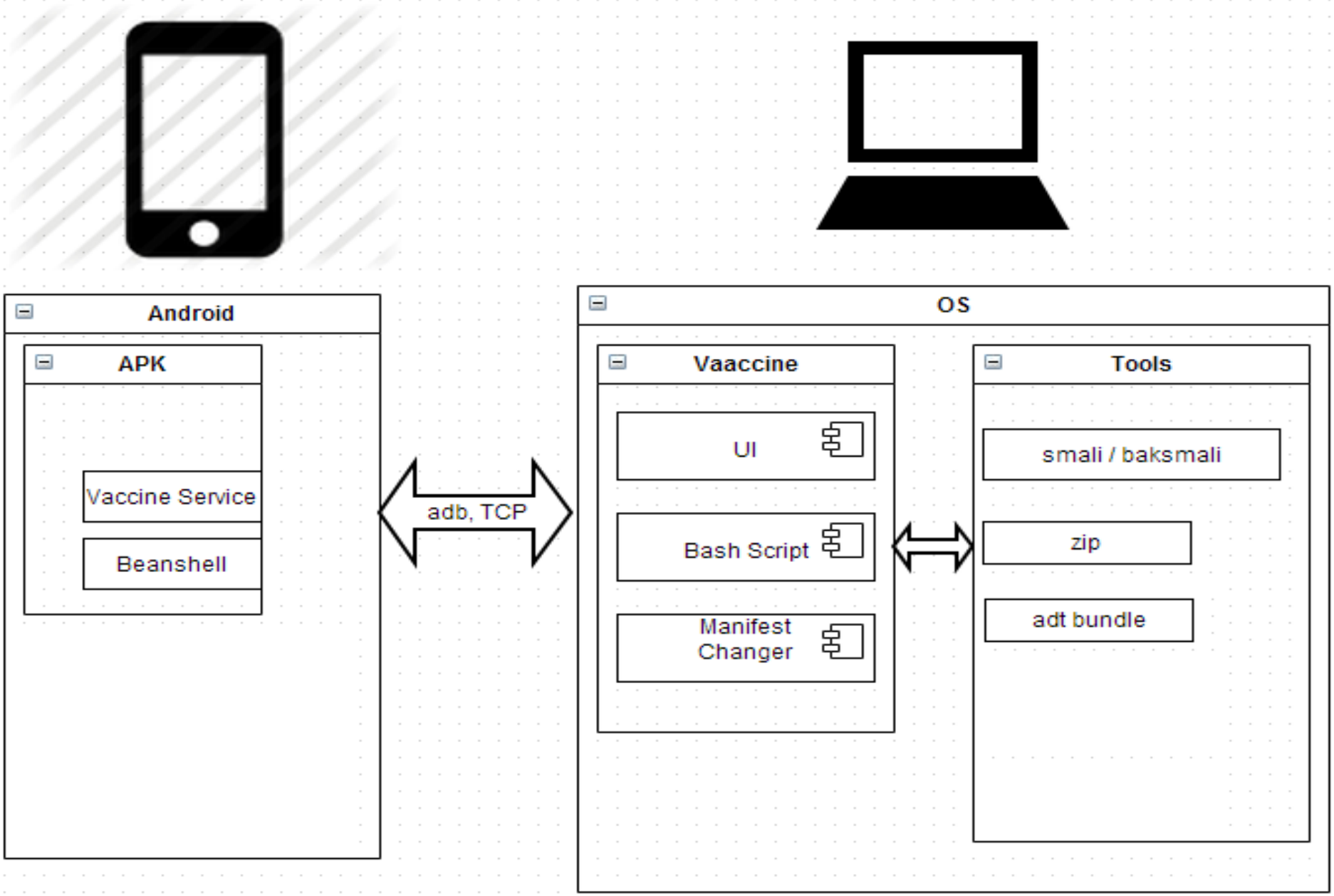
What do we see..

- Authentication PINs system logs in debug builds
- Session identifiers and credentials cached in WebView
- Inappropriate data stored in local SQLite databases
- Internal IP’s
- Hardcoded usernames, passwords, leftovers


DIG
DEEPER

Vaccine

- Repackaging if injecting in APK
- Service injection
- Injecting Beanshell
- Connection and Dynamical analysis


Android
APK
Vaccine Service
Beanshell
adb, TCP
OS
Vaaccine
UI
Bash Script
Manifest
Changer
Tools
smali / baksmali
zip
adt bundle

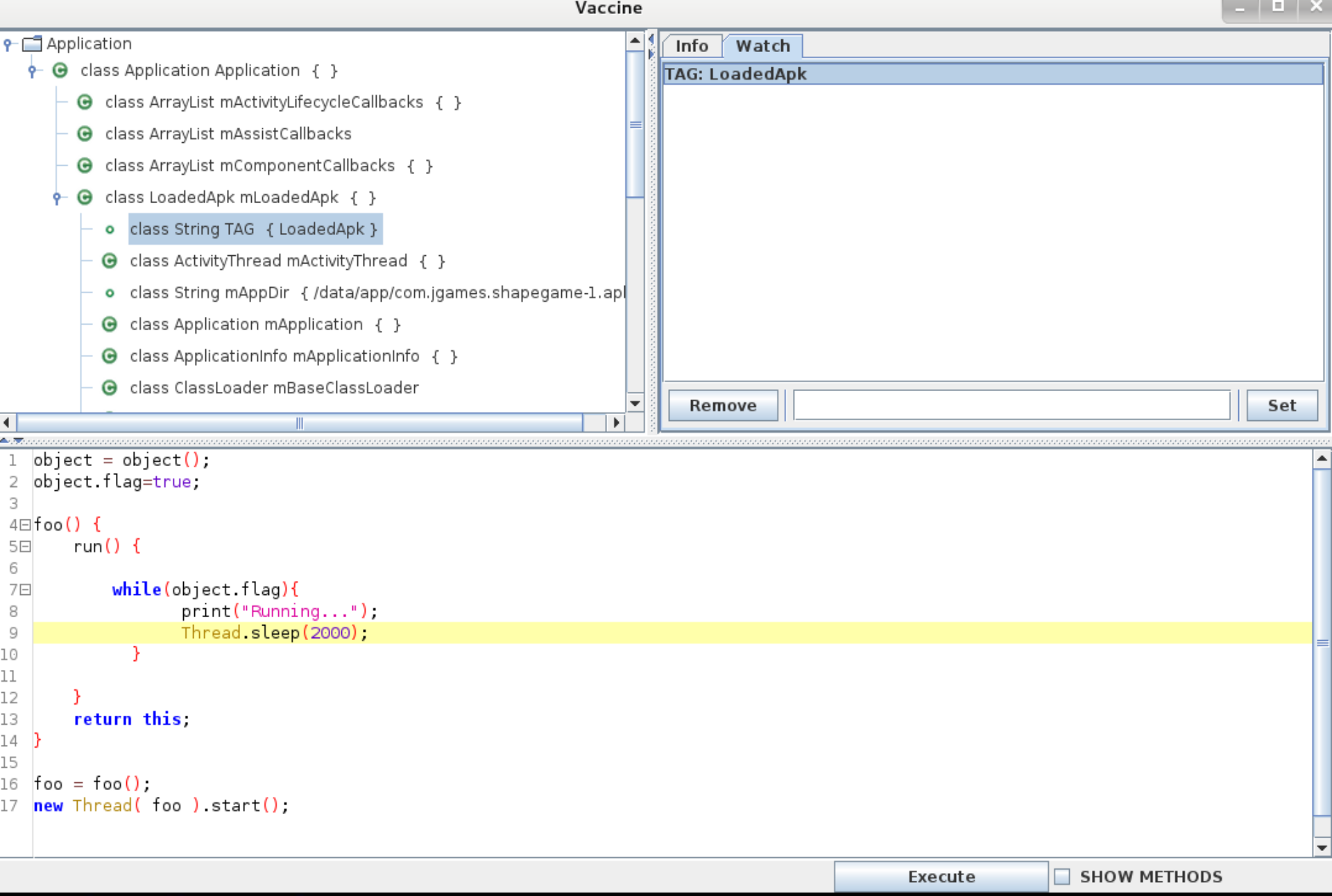
Vaccine (bash)script

> Preparing the APK

- » Copy APK
- » Unzip
- » Baksmali classes.dex – smali source code
- » Adding smali source of service
- » Smaling source – classes.dex
- » Changing AndoidManifest.xml
- » Replacement of classes.dex and AndroidManifest.xml
- » Removing signature
- » Signing
- » Installing the mobile application
- » Starting the service
- » Connecting and showing UI

Vaccine

- Accessing objects and fields
- Executing methods
- Using objects, varibales in java source and beanshell scripts
- ...


Vaccine
Application
class Application Application { }
class ArrayList mActivityLifecycleCallbacks { }
class ArrayList mAssistCallbacks
class ArrayList mComponentCallbacks { }
class LoadedApk mLoadedApk { }
class String TAG { LoadedApk }
class ActivityThread mActivityThread { }
class String mAppDir { /data/app/com.jgames.shapegame-1.apl
class Application mApplication { }
class ApplicationInfo mApplicationInfo { }
class ClassLoader mBaseClassLoader
Info
Watch
TAG: LoadedApk
Remove
Set
1 object = object();
2 object.flag=true;
3
4 foo() {
5 run() {
6
7 while(object.flag){
8 print("Running...");
9 Thread.sleep(2000);
10 }
11
12 }
13 return this;
14 }
15
16 foo = foo();
17 new Thread(foo).start();
Execute
SHOW METHODS

Demo(s)

```
./vaccine.sh -i android.apk -p 8888
```

Disclaimer

This presentation was created for educational purposes. We will not take any responsibility for any action you cause using the information shown in this presentation. Please do not contact us with blackhat type hacking requests. Thanks!

Original taken from: http://www.lo0.ro/

KEEP CALM

WHAT

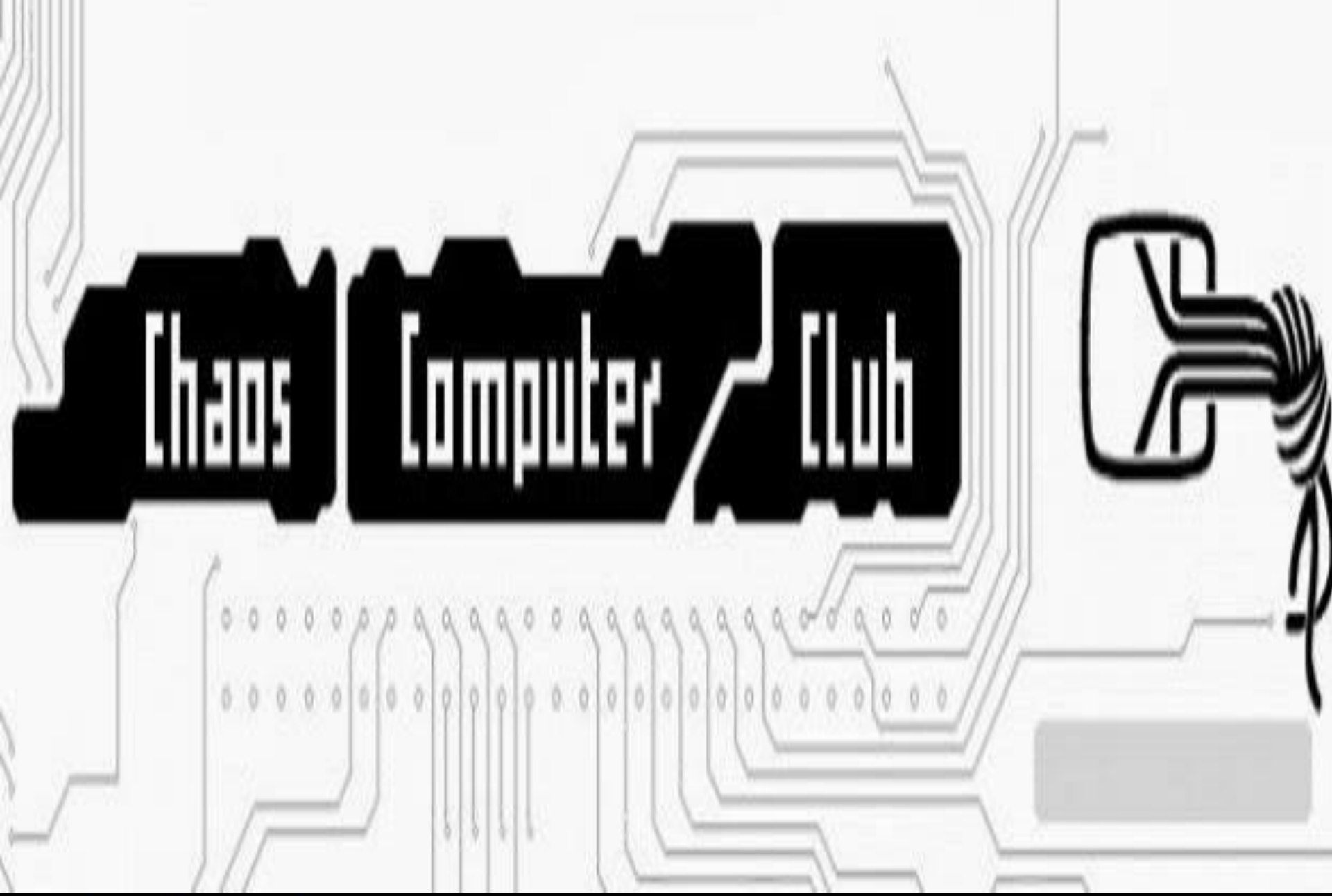
HAPPENS IN

VEGAS STAYS

IN VEGAS

Demo(s)

```
./vaccine.sh -i android.apk -p 8888
```


Chaos Computer Club

Northeastern University
Systems Security Lab

Android DDI: Dynamic Dalvik Instrumentation

30th Chaos Communication Congress
Hamburg, Dec. 29th, 2013

Collin Mulliner
collin[at]mulliner.org twitter: @collinrm

Injecting vaccine at runtime

- Little hacking provided Collin's examples
- Instead of changing APK, we "hijack" running process (in our case zygote)
- Inject shared library into process
- Hook android.app.Activity onStart method
- Injects Vaccine service and additional BeanShell classes when app is started
- Use vaccine as before

Demo

> Is it possible to inject Vaccine into Google apps at runtime?

Pros/cons APK Android

- APK
  - No need for rooted phone
  - Untrusted sources
  - Download, modify, upload
- Android
  - No need for APK modification
  - Rooted phone
  - Injecting shared libs (more skills needed)


#/viris[# *]


CHALLENGES
AHEAD
dreamstime.com

Possible usage

- Not only for Android
- Reflection is still NOT dead
- Tested with Oracle Foms
- Have idea to use it with other Java apps/applets (Minecraft maybe)

Other possibilities

- Many apks:
  - » gmail, dropbox, playstore, games...
  - » Messaging, settings, browser...
- Getting Phone instance
- Using phone as framework(Quick SMS)
- Sending class 0 SMS
- Extending by writing BeanShell scripts
- Testing, fuzzing
- **Ultimate cheating platform**

Final thoughts

- One script, small GUI tool (never be finished)
- Help testers, researchers (hackers, cheaters)
- Open for suggestions, improvements, comments

Some tips

- Know your platform (this means read at least 1 more book different than iOS/Android in 10 minutes)
- Know how things are made off
- Know where things are stored (save, conf, cache, logs)
- Experience/mileage helps a lot


Welcome to
CLARK COUNTY + McCARRAN INTERNATIONAL AIRPORT
LAS VEGAS
Baggage Claim
Ground Transportation
Ticketing
A B C & E Gates

#/viris[! # Q *]


Questions?

www.github.com/viris

@MilanGabor

@alm8i