Creating a kewl and simple Cheating Platform on Android

Milan Gabor & Danijel Grah

#/viris[# *]

/WhoAreWe

> Just two guys from Slovenia
> Having fun breaking stuff
> Love to play with apps

> BSidesLV, DEF CON Wall of Sheep, BalcCon, Hacktivity, GrrCON, Hackito Ergo Sum, DefCamp, Hek.si

Famous .si people

#/viris[# *]

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | ST

National Press Releases

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

Washington, D.C.
July 28, 2010

FBI National Press Office
(202) 324-3691

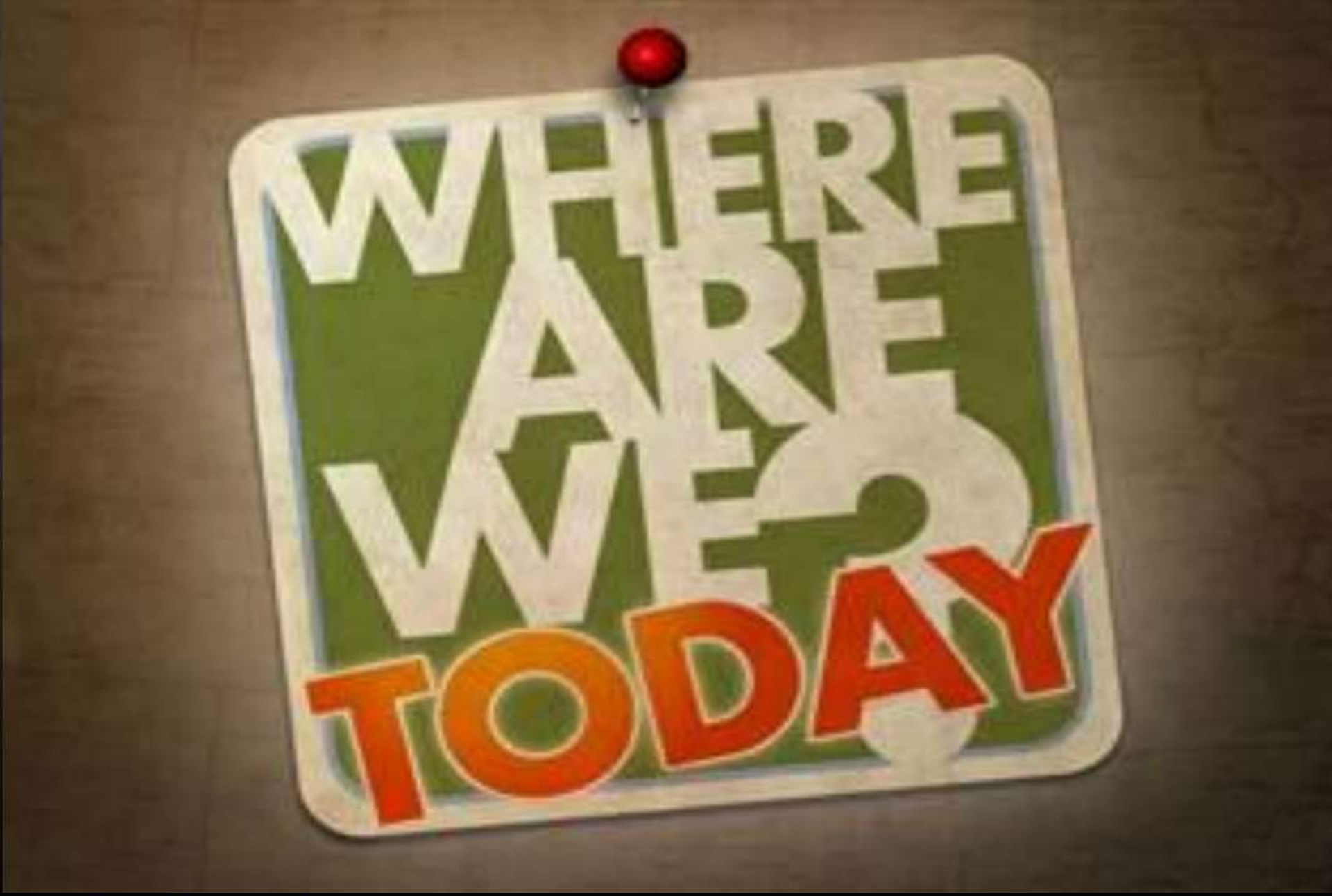
The FBI, in partnership with the Slovenian Criminal Police and the Spanish Guardia Civil, announce today significant developments in a two-year investigation of the creator and operators of the Mariposa Botnet. A botnet is a network of remote-controlled compromised computers.

The Mariposa Botnet was built with a computer virus known as "Butterfly Bot" and was used to stea 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 oth criminals, making it one of the most notorious in the world," said FBI Director Robert S. Mueller, I "These cyber intrusions, thefts, and frauds undermine the integrity of the Internet and the busines that rely on it; they also threaten the privacy and pocketbooks of all who use the Internet."

Agenda

> Android mobile apps
> Analysis (static, dynamic)
> Vaccinating APK, Android
> DEMO
> DEMO
> DEMO
> The end


WHERE ARE WE TODAY

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.

SECURITY

DoubleDirect hackers snaffle fandroid and iPhone-strokers' secrets

Windows and Linux seem immune from redirection assault

By John Leyden, 21 Nov 2014

Post a comment

Hackers are running "Man-in-the-Middle" attacks (MitM) against smartphones using a new attack technique, security researchers warn.

The so-called DoubleDirect technique enables an attacker to redirect a victim's traffic to the attacker's device. Once redirected, the attacker can steal credentials and deliver malicious payloads to the victim's mobile device that can not only quickly infect the device, but also spread throughout a corporate network," according to mobile security firm Zimperium.

Zimperium has detected the DoubleDirect technique in the wild in attacks against the customers of web giants including Google, Facebook, Live.com and Twitter, across 31 countries.

Hackers are also using DoubleDirect technique to gain access to victims' devices, essentially to steal usernames, emails, and passwords.

DoubleDirect creates a means to run man-in-the-middle attacks targeting smartphone and tablets users on devices running either iOS or Android. Mac OSX users are also potentially vulnerable but Windows and Linux users would appear to be immune because their operating systems don't accept ICMP redirection packets that carry malicious traffic. A blog post by Zimperium (extract below) explains the mechanism of the attack in greater depth.

DoubleDirect uses ICMP Redirect packets to modify routing tables of a

RELATED STORIES

Pay-by-bonk chip lets hackers pop all your favourite phones

Black Hat 2014 videos 'Up to two BEEELLION' mobes easily hacked by evil base stations

Researchers slurp unencrypted Viber messaging data with ease

Attack hijacks sensitive data using newer Windows features

MOST READ MOST COMMENTED

Samsung Galaxy Note 4: Spawn of Galaxy Alpha and a Note 3 unveiled

All ABOARD! Furious Facebook bus drivers join Teamsters union

Webcam hacker pervs in MASS HOME INVASION

Bang! You're dead. Who gets your email, iTunes and Facebook?

Bada-Bing! Mozilla flips Firefox to YAHOO! for search

SPOTLIGHT

Webcam hacker pervs in MASS HOME INVASION


A life of cybercrime, a caipirinha and a tan: Fraudsters love a Brazilian


UK.gov teams up with moneymen on HACK ATTACK INSURANCE

Mozilla, EFF, Cisco back free-as-in-FREE-BEER SSL cert authority


Our story


Remoting Android applications
for fun & profit
Damien Cauquil, Pierre Jaury

> YES, we can!

> We want something that works!

> We want to test mobile apps!

- > Living inside of APK
- > Changing and accesing variables
- > Executing code at runtime
- > Effectively and easy to use
- > Java based

Demo / Video

- Java code is obfuscated
- Static analysis
- Dynamical analysis
- What if…?
- Hard time


KEEP
CALM
AND
GET BACK
TO BASICS

Testing app/1

> Get the APK
> Unpack
> Decompile
> Check code
> Identify important segments

```
aramString1, String paramString2)


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


f(true);
  public void
  {
    this.m_se
    if (this.
      this.m_
  }

  public void
  {
    super.onC
```

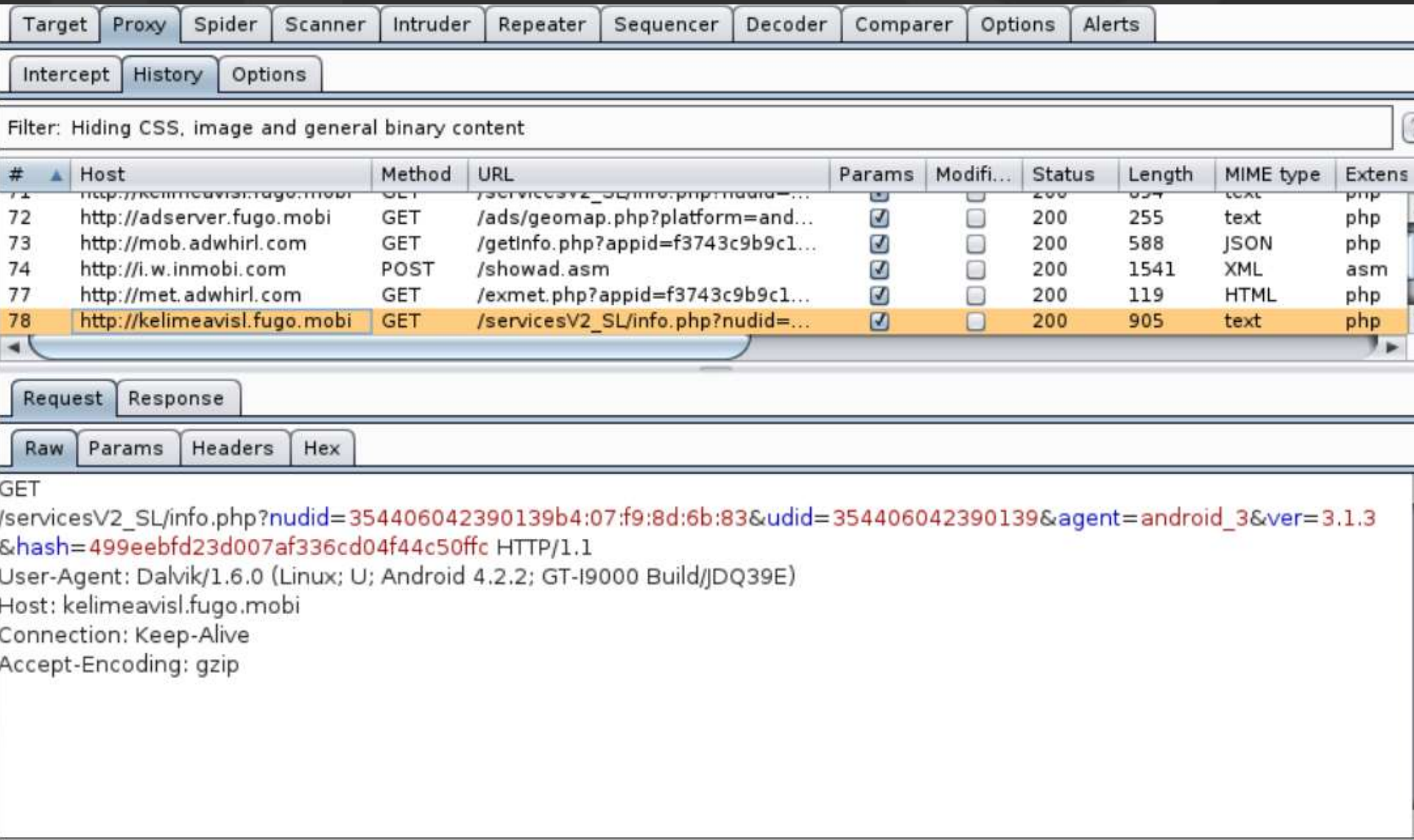
```
#/viris[
```

```
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/String
    //   18: aload_0
    //   19: getfield 26    com/ttech/turkcellsdk/util/HttpCall:httpClient  Lorg/apache/http/client/HttpClient;
    //   22: aload_2
```

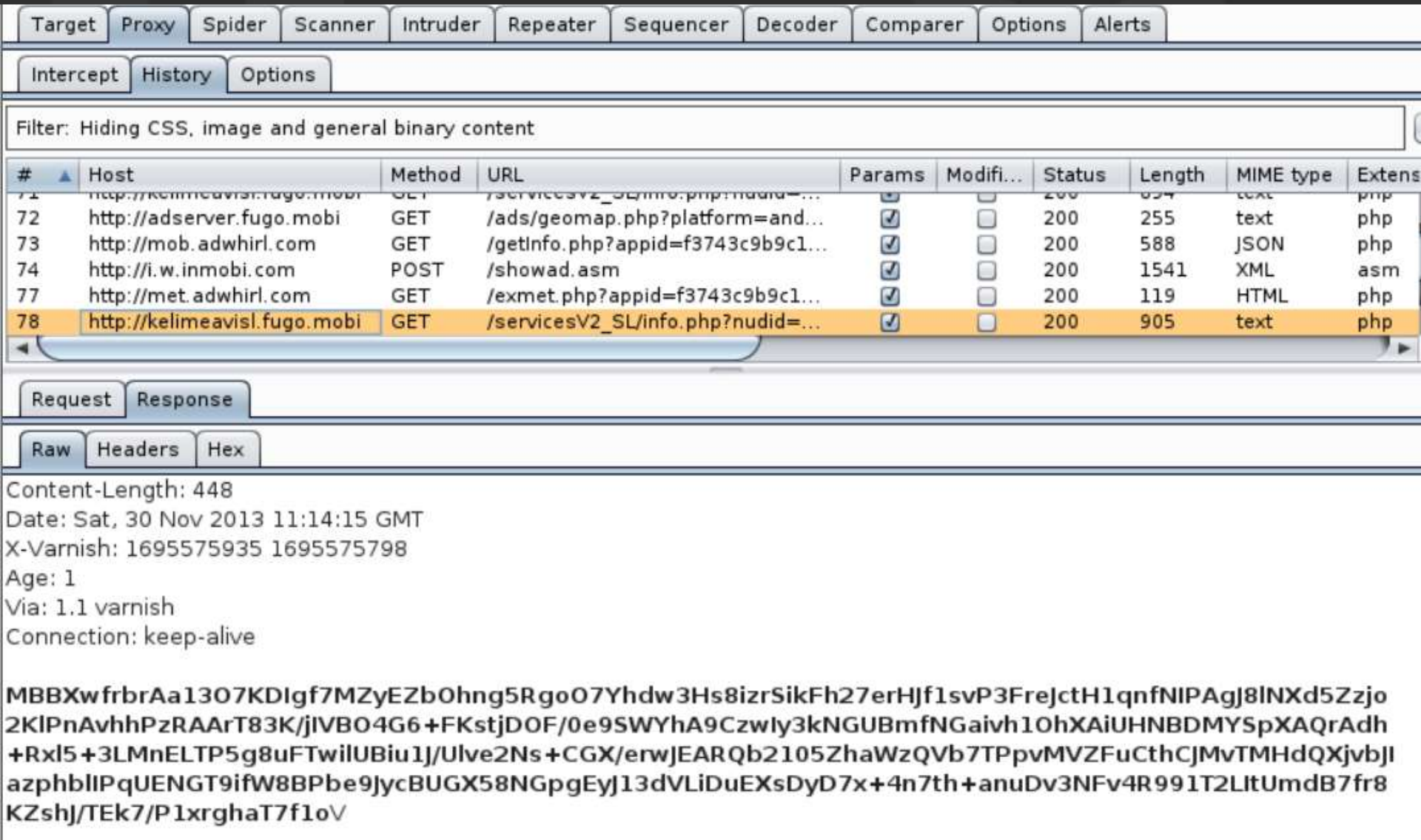
Testing app/2

- 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

Dictionary

> Dynamical analysis
> Reflection
> BeanShell
> Combination of static/dynamic

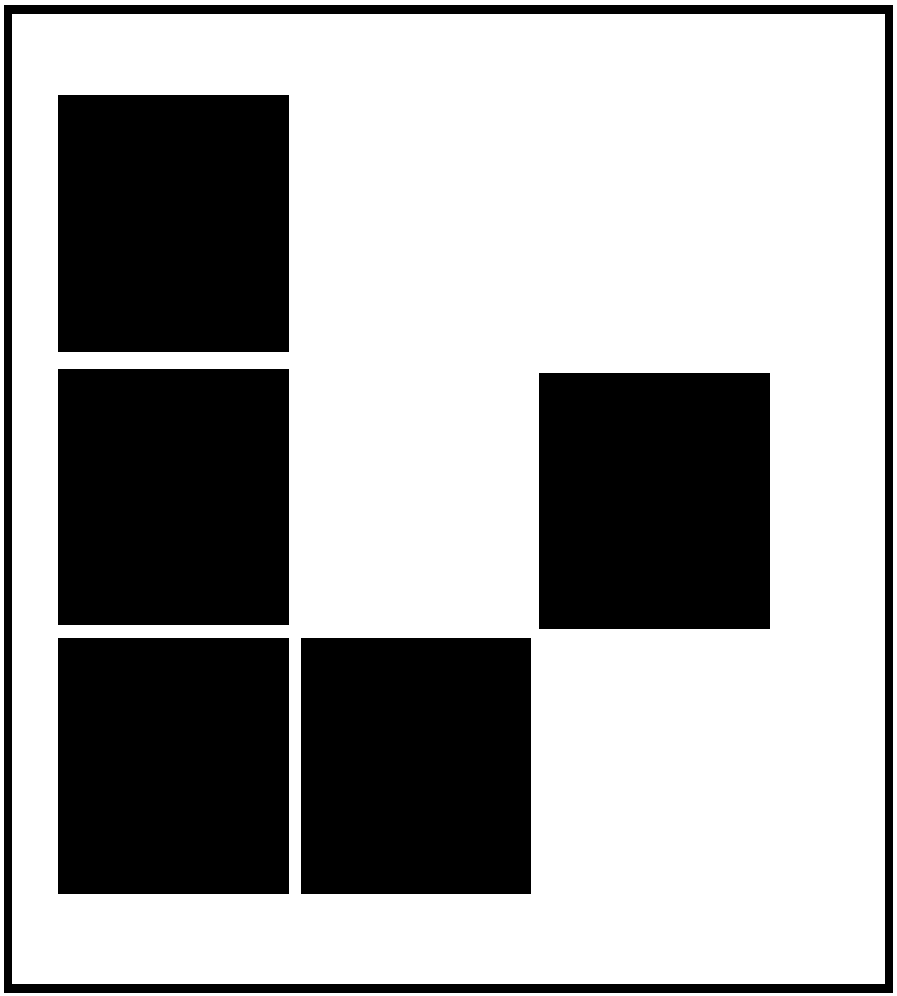
Reflection

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

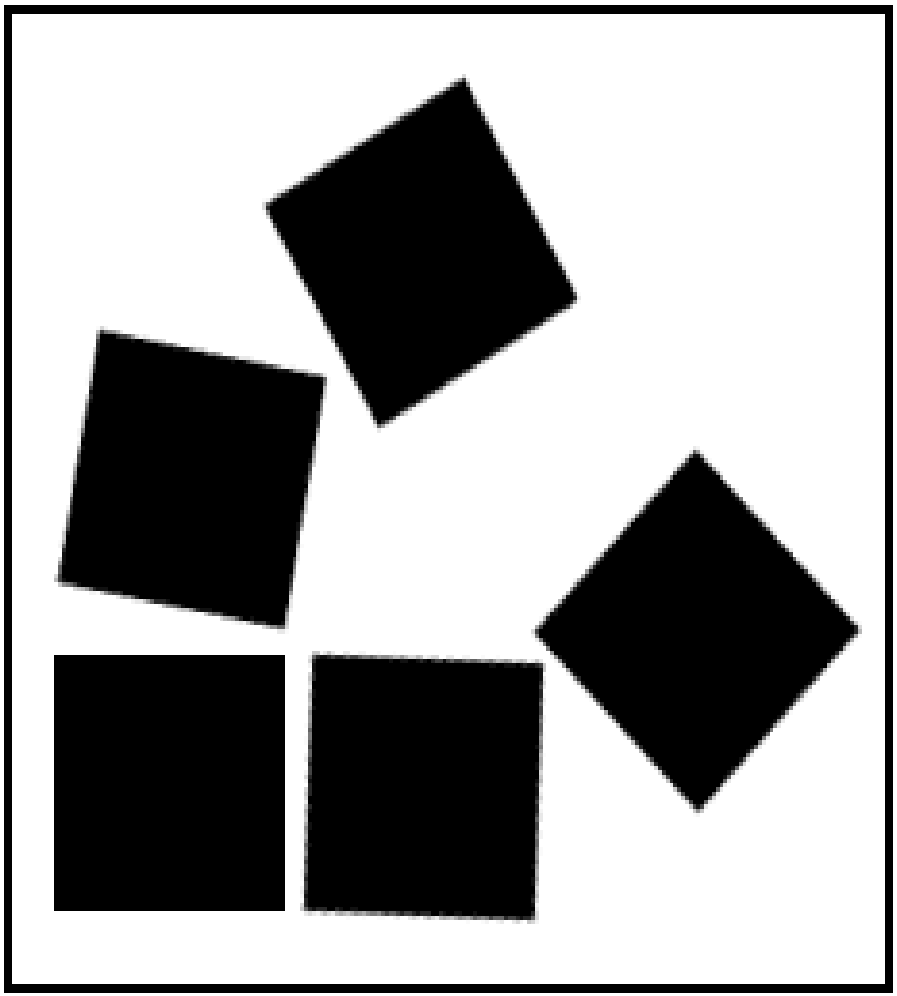
> Java looking Java

BeanShell

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

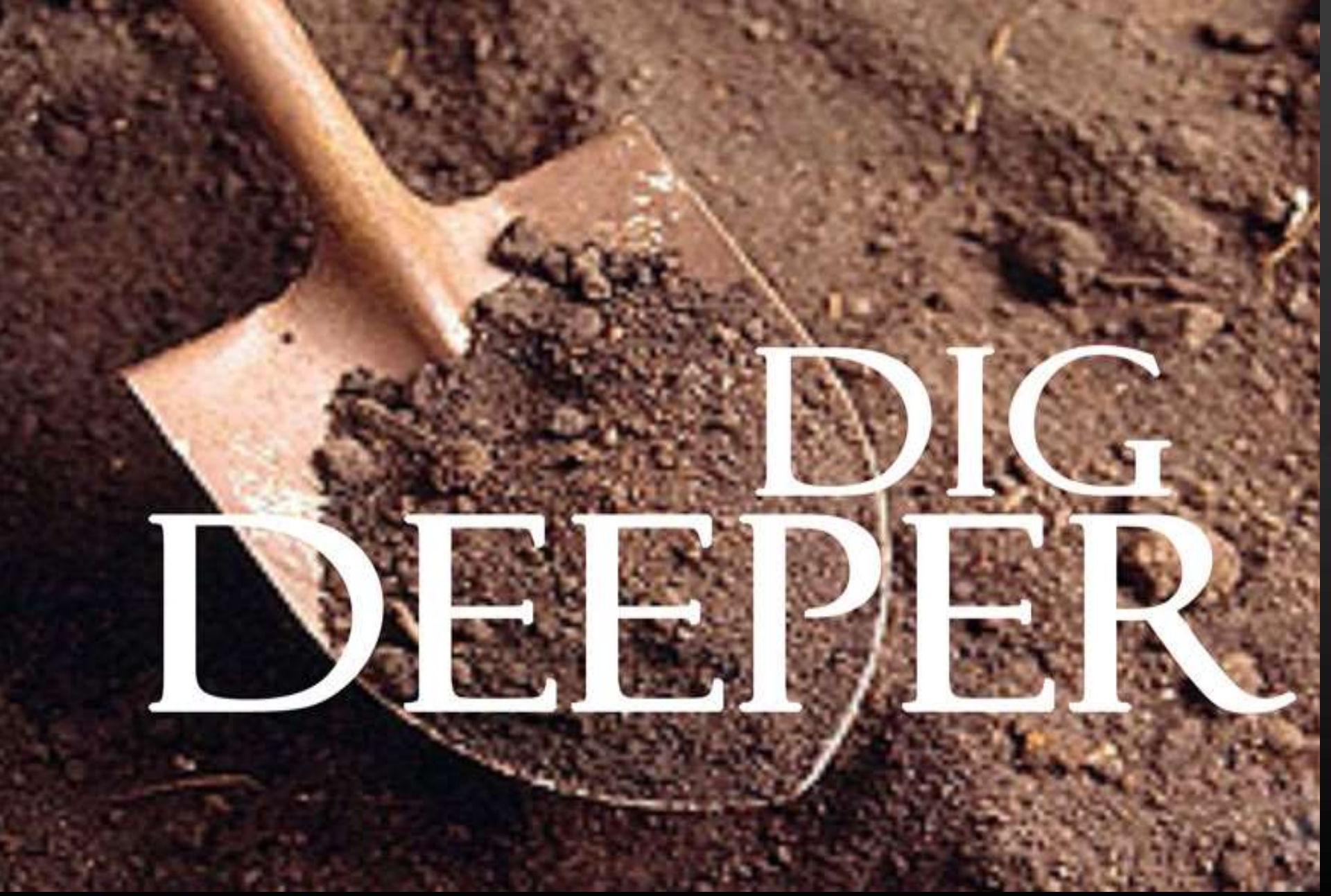


Static

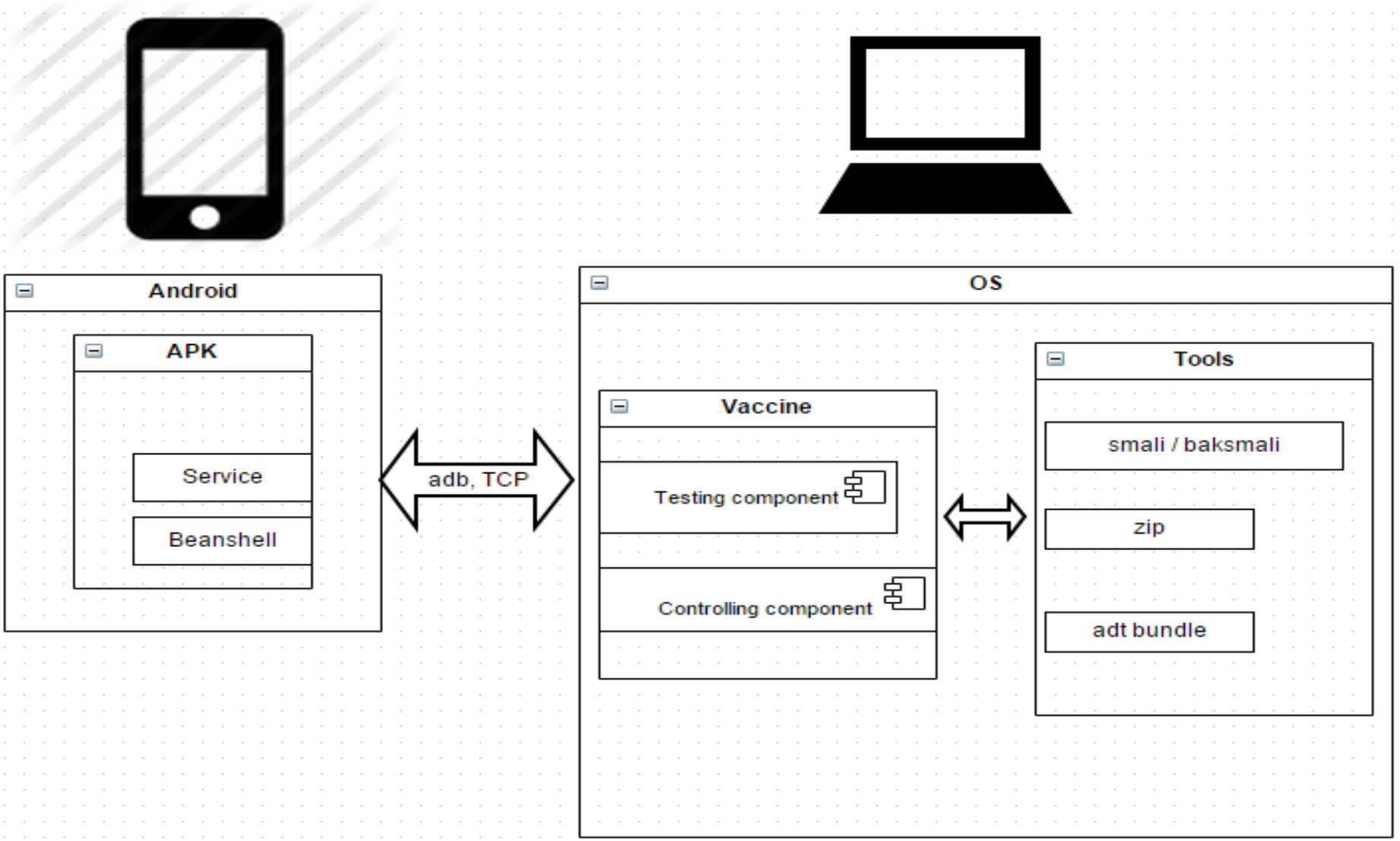


Dynamic

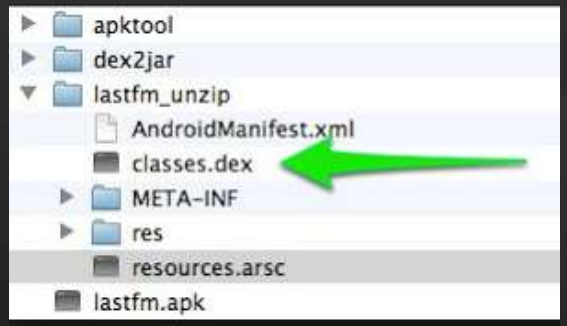

I WANT MORE!
ENDERMAN
© 2009 David Endelman


DIG
DEEPER

Vaccine

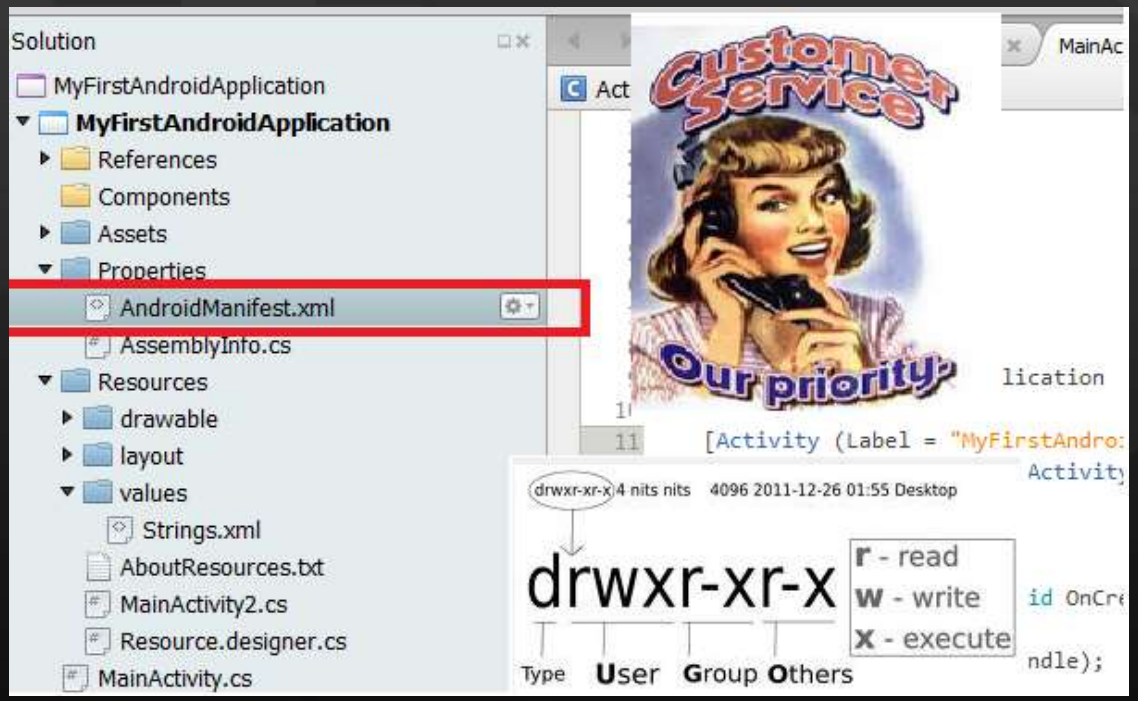

Android
APK
Service
Beanshell
adb, TCP
OS
Vaccine
Testing component
Controlling component
Tools
smali / baksmali
zip
adt bundle

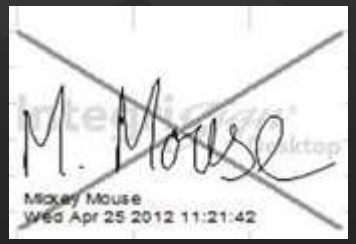
./vaccine –i game.apk

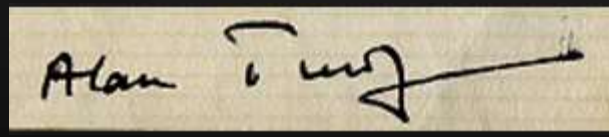


#/viris[# *]

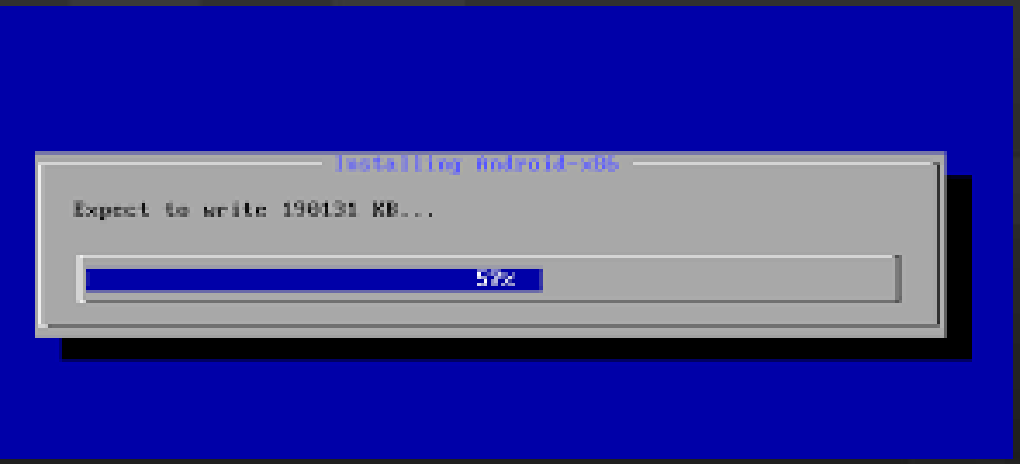
./vaccine –i game.apk

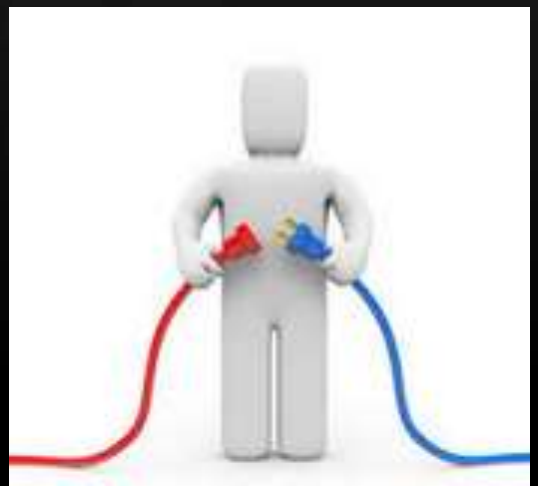






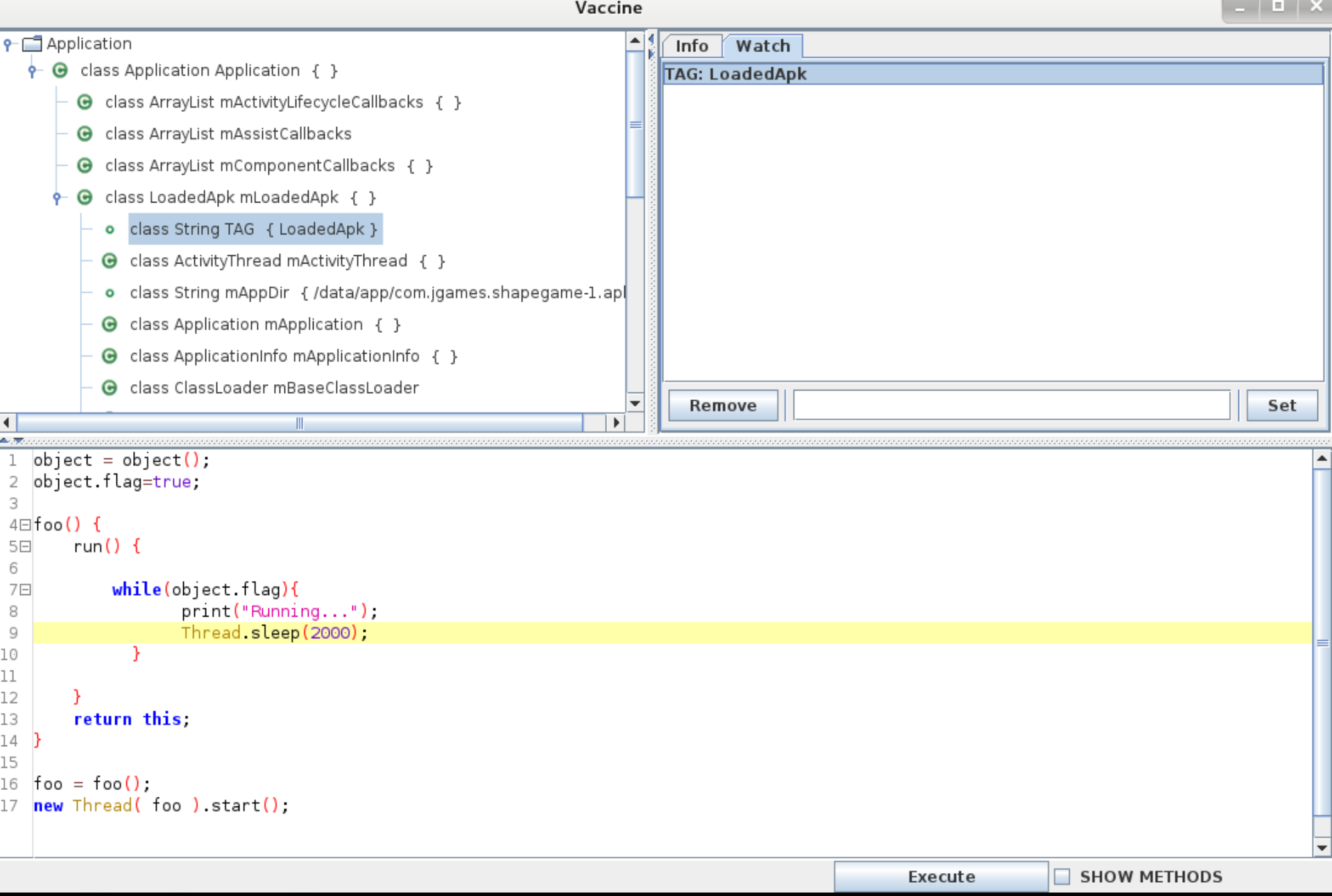
./vaccine –i game.apk





#/viris[ ]

DeepSec 2014


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

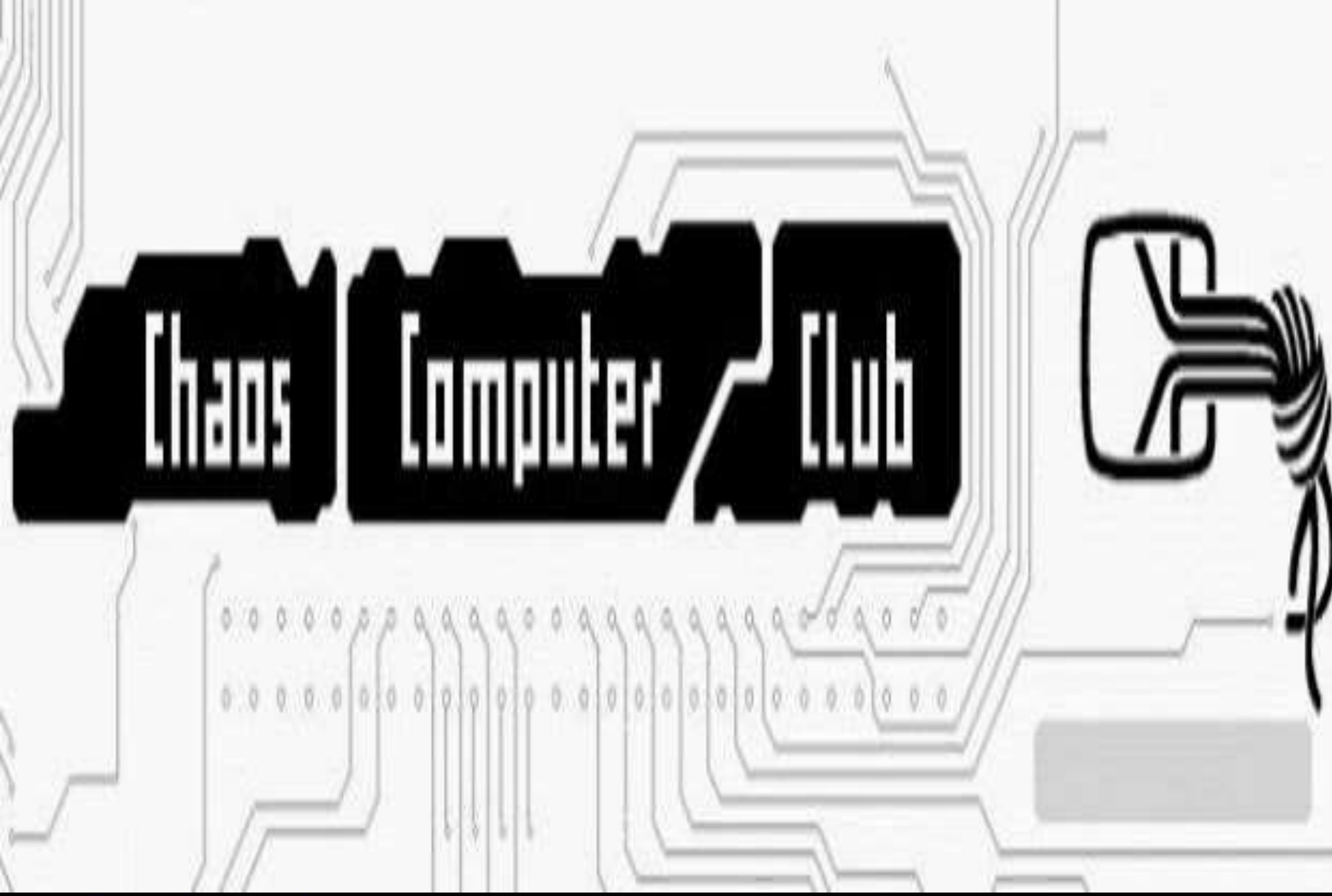
Disclaimer

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/

Demo(s)

```
./vaccine -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

Dictionary

- > ADBI, DDI
- > Zygote
- > Shared libraries
- > Hooking
- > JNI and native functions

Injecting vaccine at runtime

- Little hacking provided Collin's examples
- Prepared shared library with DDI framework
- Using hijack from ADBI framework to „hijack“ Zygote
- When Zygote specializes the shared libary is loaded into target proces and executed
- Shared library contains native code that „replaces“ (hooks) android.app.Activity onStart method
- Native methods loads classes from /data/dalvi-cache/vaclasses.dex (Vaccine service, Beanshell)
- Native method gives execution over to original method
- Connect and 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)


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)

> SIMPLE and Ultimate cheating platform

Final thoughts

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

www.github.com/viris

@MilanGabor

@alm8i