RSA CONFERENCE ASIA PACIFIC 2013

Security in knowledge

THE **DROID** EXPLOITATION SAGA

ADITYA GUPTA
XYSEC

SUBHO HALDER
XYSEC

Session ID: MBS-T01

Session Classification: Intermediate

XY Security
Consultancy Services

Who Are We

- Mobile Security Researchers
- Penetration Testers & Creators of AFE
- XYSec
- Have found numerous vulnerabilities in websites such as Microsoft, Google, Facebook, Paypal, Adobe etc
- Also like finding exploits ;)

Some companies we've found vulnerabilities in



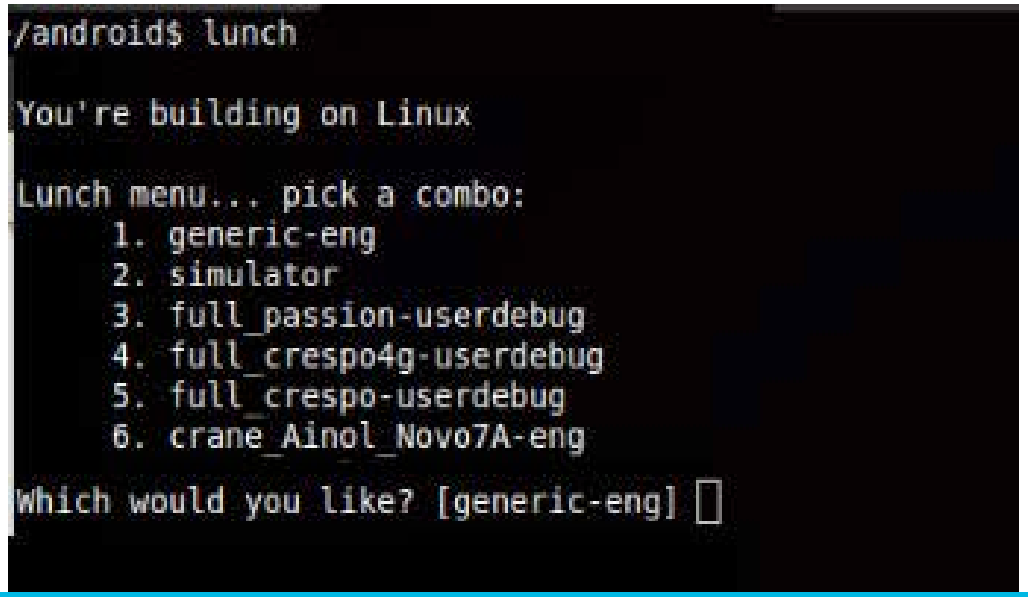


Agenda

- Android Security Overview
- Android Malwares and Recent trends
- AFE : The Android Framework for Exploitation
- Android 0-days and exploits
- App-based vulnerabilities
- BYOD

Quick Intro to Android

- Open-source platform by Google inc
- Generic builds which can be deployed in any hardware configuration



Quick Intro to Android

- Linux Kernel, Webkit Browser, Applications

```
1|shell@GT-I9100:/proc $ cat version
Linux version 2.6.38-uHD+ (build@MacBuildServer) (gcc version 4.5.2 (Ubuntu/Linaro 4.5.2-8ubuntu4) ) #55
Thu Mar 21 13:41:12 IST 2013
```

- Mostly focus on Webkit for exploit-dev

```
shell@GT-I9100:/lib $ ls -l | grep webcore
-rw-r--r-- root     root     13964197 2013-03-21 00:20 libwebcore.so
-rw-r--r-- root     root      6452924 2013-03-21 00:24 libwebcore.so-arm
```

Android Security Overview

- Apps run in virtual env/sandbox
- Privilege Seperation
- Each app with own UID and GID

```
radio     1520  1426  139680 0     ffffffff 00000000 S com.android.phone
app_45    1599  1426  143888 0     ffffffff 00000000 S com.bluestacks.home
app_48    1766  1426  153080 0     ffffffff 00000000 S com.google.process.gapps
app_31    1863  1426  127872 0     ffffffff 00000000 S com.bluestacks.bstfolder
system    1870  1426  130180 0     ffffffff 00000000 S com.bluestacks.BstCommandProcessor
root      2657  2     0      0     ffffffff 00000000 S kworker/0:3
app_34    3438  1426  136428 0     ffffffff 00000000 S getjar.android.client
root      4590  2     0      0     ffffffff 00000000 S kworker/0:0
app_49    4619  1426  154300 0     ffffffff 00000000 S com.android.vending
```

Android Security Overview

- ASLR
- DVM

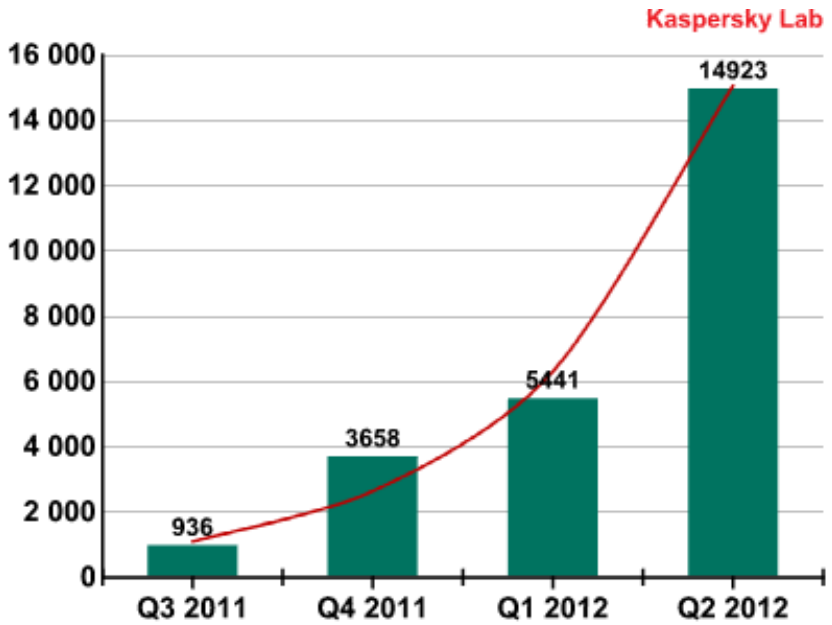
```
shell@GT-I9100:/proc/sys/kernel $ cat randomize_va_space
1
```

Permission Model

- Which App would you trust :
  - An game with **INTERNET** permission
  - An game with **READ_LOGS** permissi
  - An game with **ALL** permissions
  - A game with **NO** permissions

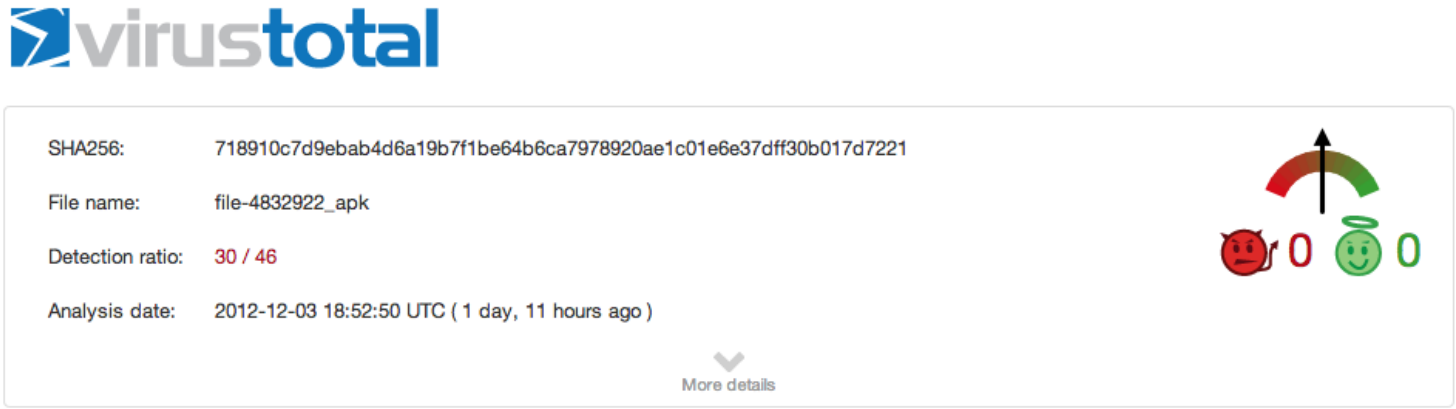
Malwares

- Android malwares rising day by day
- Getting more complicated



Malwares

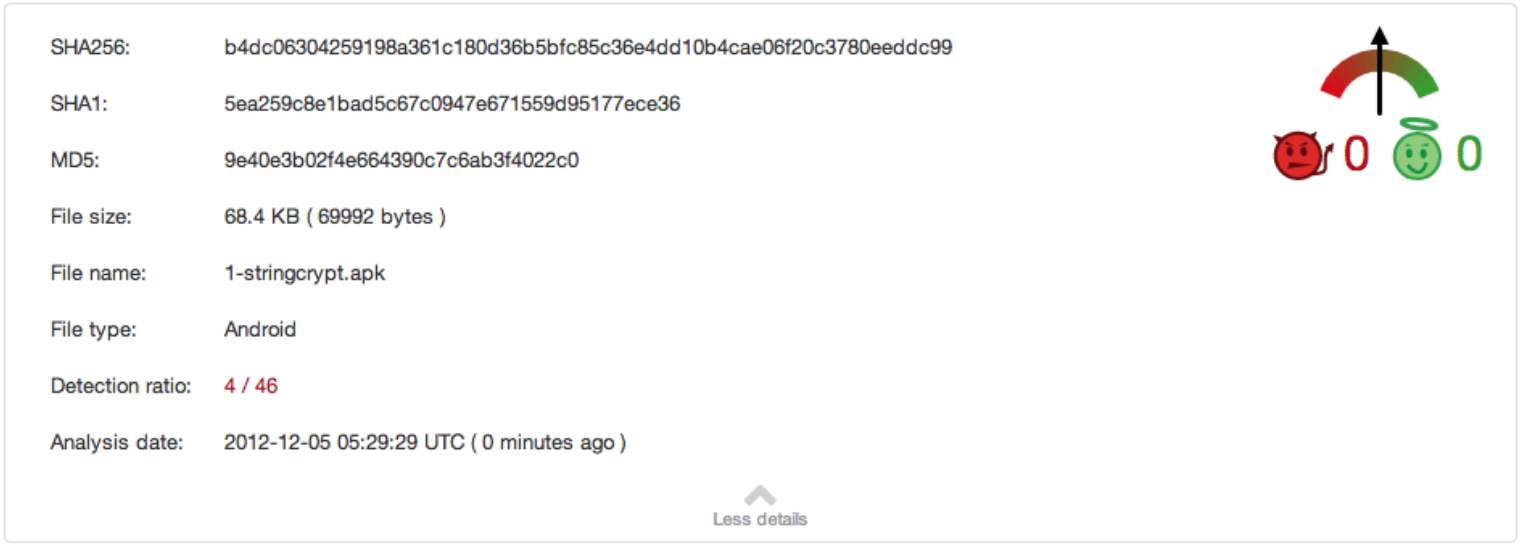
- Most of the anti-malwares are signature-based



Malwares

- Malwares can easily bypass "**all**" of the known anti-malwares

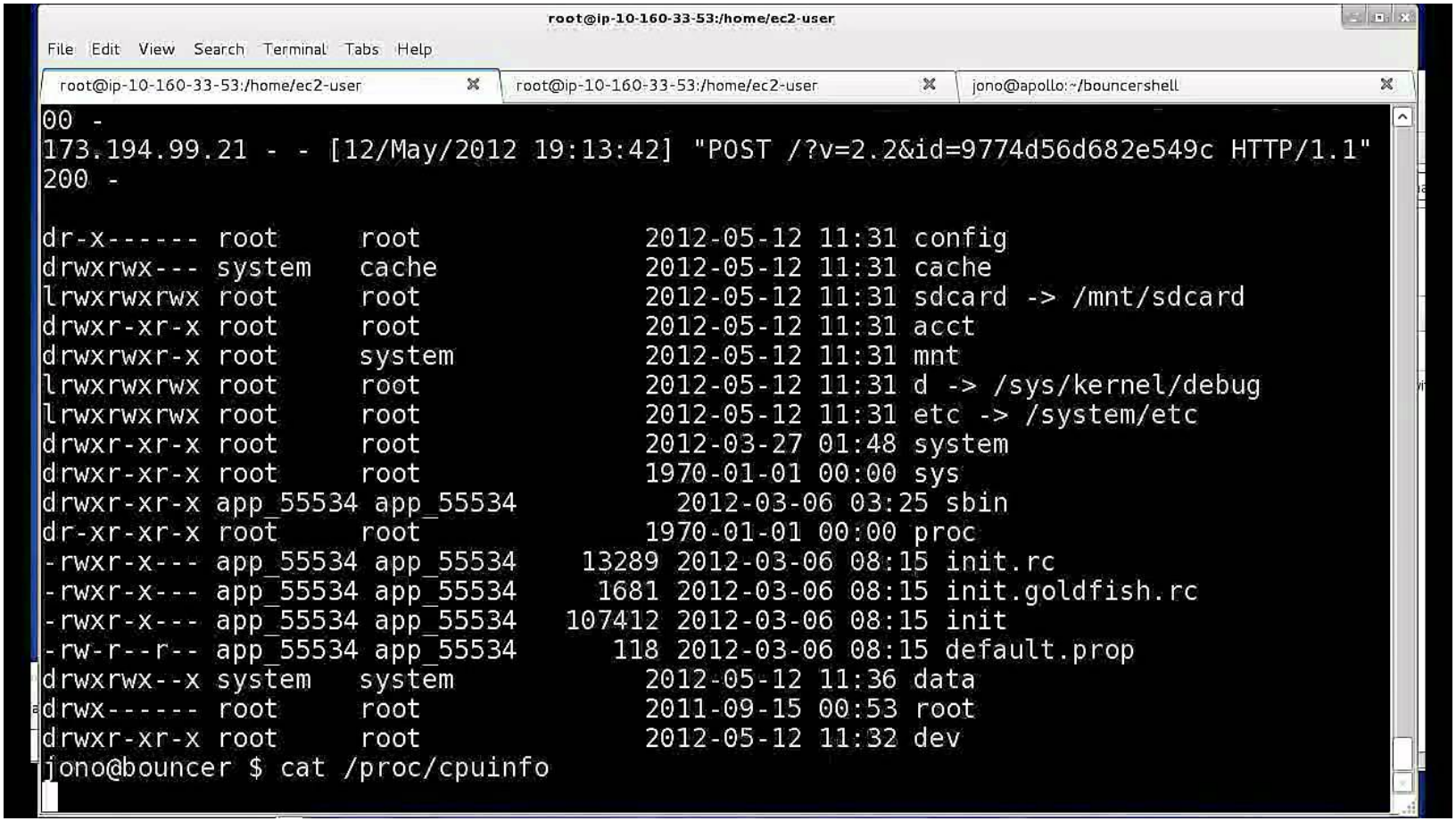
virustotal



Google Bouncer

- Virtual Environment to check if app is malicious
- Runs the app in a phone like environment for around 5 mins before publishing
- Detects most of the malwares
- Can be bypassed easily

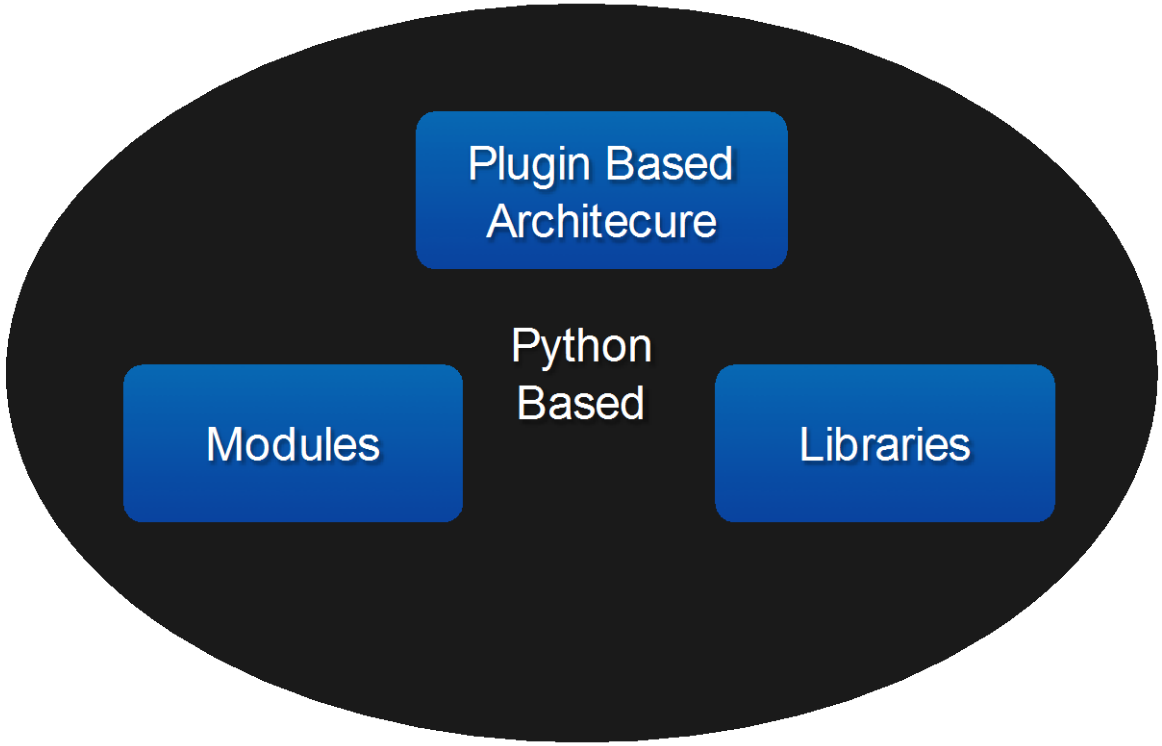
Google Bouncer



Analyzing malwares

- Decompile an app -> Analyze the code
- Apktool, dex2jar, Jd-GUI, Androguard, IDA Pro
- Droidbox, Mobile-sandbox, dexter labs, Taintdroid
- Grep + regex with the smali codes

Android Framework for Exploitation



Android Framework for Exploitation

Android Framework for Exploitation

Demo

Fake legitimate apps

- Malware se
  application
- Infected Ar
- Have seen
- Took Goog ps in few cases

Fake legitimate apps

Fake legitimate apps

App vulnerabilities

- Apps could contain a lot of vulnerabilities
- Leaking content providers
- Insecure storage / data transmission
- SQLi/LFI
- Other issues

Using AFE to find vulns

Demo

Android 0-days

- How to find 0-days on Android
- Webkit FTW!
- ASLR makes things tough
- Tough but not impossible
- Contact us ;)

BYOD

- BYOD : Next-gen issue
- Enterprises need to be careful
- If a malware gets on a phone, it could jump on the enterprise’s wifi network
- We provide solutions for BYOD

Conclusion

- Be safe
- Don’t download apps from 3rd party markets
- Turn USB debugging OFF
- Anti-virus vendors -> Switch to dynamic analysis
- Focus on BYOD security
- Use AFE (personal/enterprise) to protect apps
- We also conduct trainings on Advanced Mobile Hands-on Security/Exploitation for both Android and iOS
- Questions – **security@xysec.com**

RSA CONFERENCE ASIA PACIFIC 2013

Contacts us at

security@xysec.com

XY Security
Consultancy Services