

# THE DROID EXPLOITATION SAGA



Security in  
knowledge



ADITYA GUPTA  
XYSEC

SUBHO HALDER  
XYSEC

# 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

```
/android$ lunch  
  
You're building on Linux  
  
Lunch menu... pick a combo:  
  1. generic-eng  
  2. simulator  
  3. full_passion-userdebug  
  4. full_crespo4g-userdebug  
  5. full_crespo-userdebug  
  6. crane_Ainol_Novo7A-eng  
  
which would you like? [generic-eng] 
```

# 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 Separation
- ▶ 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

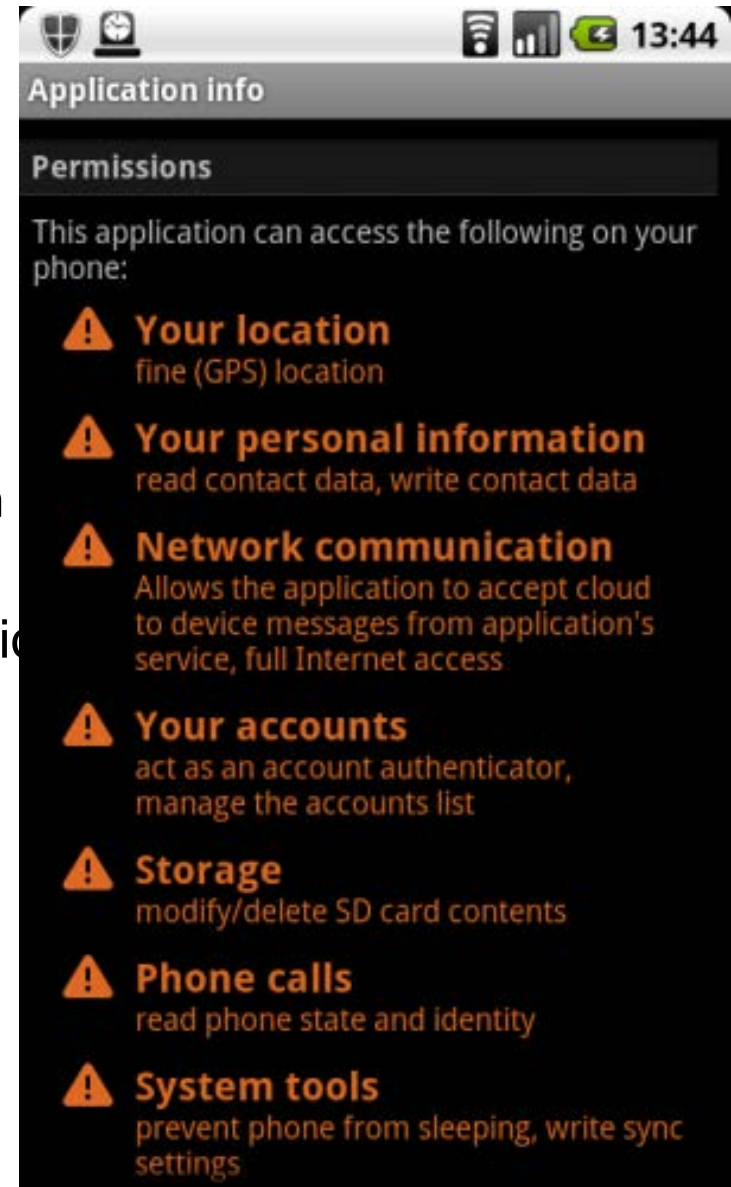
▶ DVM

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



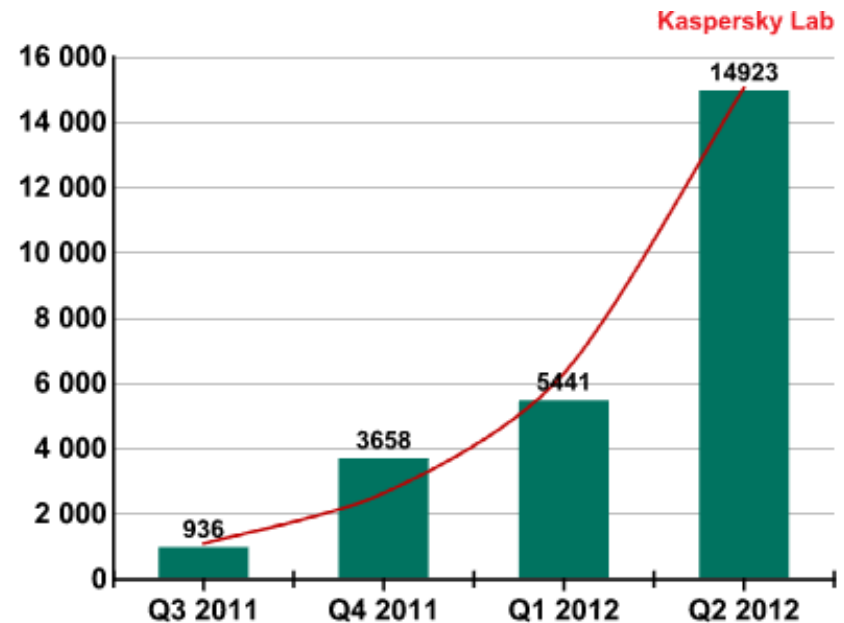
# Permission Model

- ▶ Which App would you trust :
  - ▶ An game with **INTERNET** permission
  - ▶ An game with **READ\_LOGS** permission
  - ▶ 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



SHA256: 718910c7d9ebab4d6a19b7f1be64b6ca7978920ae1c01e6e37dff30b017d7221

File name: file-4832922\_apk

Detection ratio: 30 / 46

Analysis date: 2012-12-03 18:52:50 UTC ( 1 day, 11 hours ago )



 More details

# Malwares

- ▶ Malwares can easily bypass “all” of the known anti-malwares



SHA256:	b4dc06304259198a361c180d36b5bfc85c36e4dd10b4cae06f20c3780eeddc99	
SHA1:	5ea259c8e1bad5c67c0947e671559d95177ece36	
MD5:	9e40e3b02f4e664390c7c6ab3f4022c0	
File size:	68.4 KB ( 69992 bytes )	
File name:	1-stringcrypt.apk	
File type:	Android	
Detection ratio:	4 / 46	
Analysis date:	2012-12-05 05:29:29 UTC ( 0 minutes ago )	

[Less details](#)

# — 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

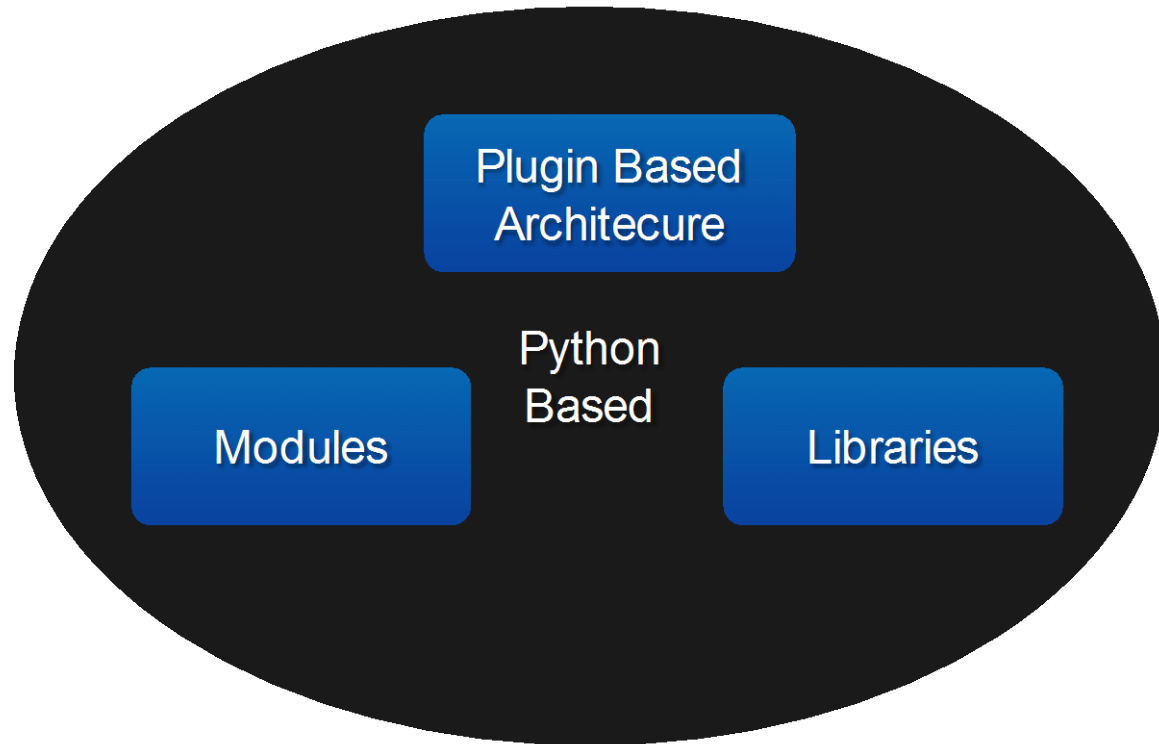
```
root@ip-10-160-33-53:/home/ec2-user
File Edit View Search Terminal Tabs Help
root@ip-10-160-33-53:/home/ec2-user x root@ip-10-160-33-53:/home/ec2-user x jono@apollo:~/bouncershell x
00 -
173.194.99.21 - - [12/May/2012 19:13:42] "POST /?v=2.2&id=9774d56d682e549c HTTP/1.1"
200 -

dr-x----- root      root      2012-05-12 11:31 config
drwxrwx--- system    cache    2012-05-12 11:31 cache
lrwxrwxrwx root      root      2012-05-12 11:31 sdcard -> /mnt/sdcard
drwxr-xr-x root      root      2012-05-12 11:31 acct
drwxrwxr-x root      system    2012-05-12 11:31 mnt
lrwxrwxrwx root      root      2012-05-12 11:31 d -> /sys/kernel/debug
lrwxrwxrwx root      root      2012-05-12 11:31 etc -> /system/etc
drwxr-xr-x root      root      2012-03-27 01:48 system
drwxr-xr-x root      root      1970-01-01 00:00 sys
drwxr-xr-x app_55534 app_55534 2012-03-06 03:25/sbin
dr-xr-xr-x root      root      1970-01-01 00:00 proc
-rwxr-x--- app_55534 app_55534 13289 2012-03-06 08:15 init.rc
-rwxr-x--- app_55534 app_55534 1681 2012-03-06 08:15 init.goldfish.rc
-rwxr-x--- app_55534 app_55534 107412 2012-03-06 08:15 init
-rw-r--r-- app_55534 app_55534 118 2012-03-06 08:15 default.prop
drwxrwx--x system    system    2012-05-12 11:36 data
drwx----- root      root      2011-09-15 00:53 root
drwxr-xr-x root      root      2012-05-12 11:32 dev
jono@bouncer $ cat /proc/cpuinfo
```

# — 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

Offensive

Malware Creation

BotNet Automation

Exploit Writing

Injecting

Defensive

Content Query

App Assesment

Fuzzing

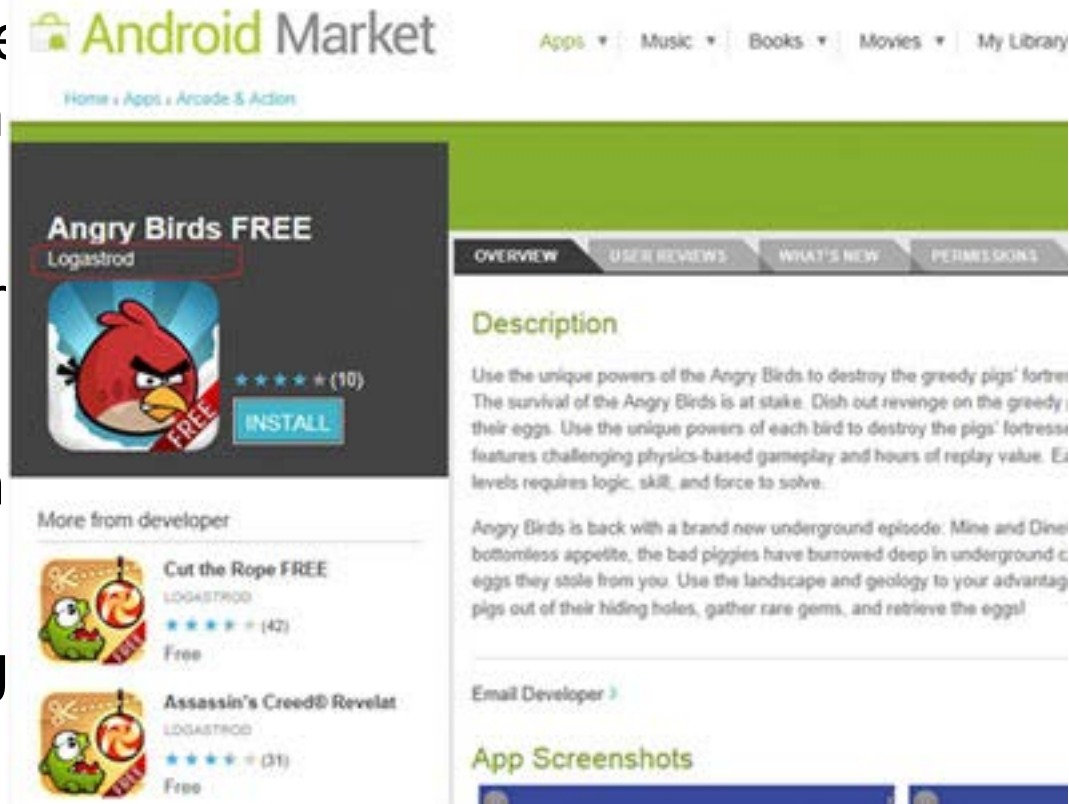
Kernel Assessment

# — Android Framework for Exploitation

Demo

# Fake legitimate apps

- ▶ Malware seen in application
- ▶ Infected Android
- ▶ Have seen
- ▶ Took Google a few cases



ps in

# Fake legitimate apps

The screenshot shows the Android Market interface for the 'Angry Birds FREE' app. The app is by Logastrod and has a 4.5-star rating from 10 reviews. The 'INSTALL' button is highlighted with a red box. The description states: 'Use the unique powers of the Angry Birds to destroy the greedy pigs' fortress. The survival of the Angry Birds is at stake. Dish out revenge on the greedy, their eggs. Use the unique powers of each bird to destroy the pigs' fortress! features challenging physics-based gameplay and hours of replay value. Each level requires logic, skill, and force to solve.' Below the description, it mentions a new underground episode: 'Mine and Dine'. The 'More from developer' section lists 'Cut the Rope FREE' (4.5 stars, 42 reviews) and 'Assassin's Creed® Revelat' (4.5 stars, 31 reviews), both by Logastrod and free. The page also has tabs for OVERVIEW, USER REVIEWS, WHAT'S NEW, and PERMISSIONS.

# — 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 3<sup>rd</sup> 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](mailto:security@xysec.com)**

Contacts us at  
[security@xysec.com](mailto:security@xysec.com)

