

DroidAnalytics: A Signature Based Analytic System to Collect, Extract, Analyze and Associate Android Malware

Min Zheng, **Mingshen Sun**, John C.S. Lui
The Chinese University of Hong Kong

Outline

Introduction

Motivation

Architecture of DroidAnalytics

Utility & Effectiveness of Signature Based System

Analytics Capability

Zero-day Malware

Conclusion

900 MILLION 2013



BadNews

- download infected apps
- hijack
- premium SMS services
- collect privacy

Motivations

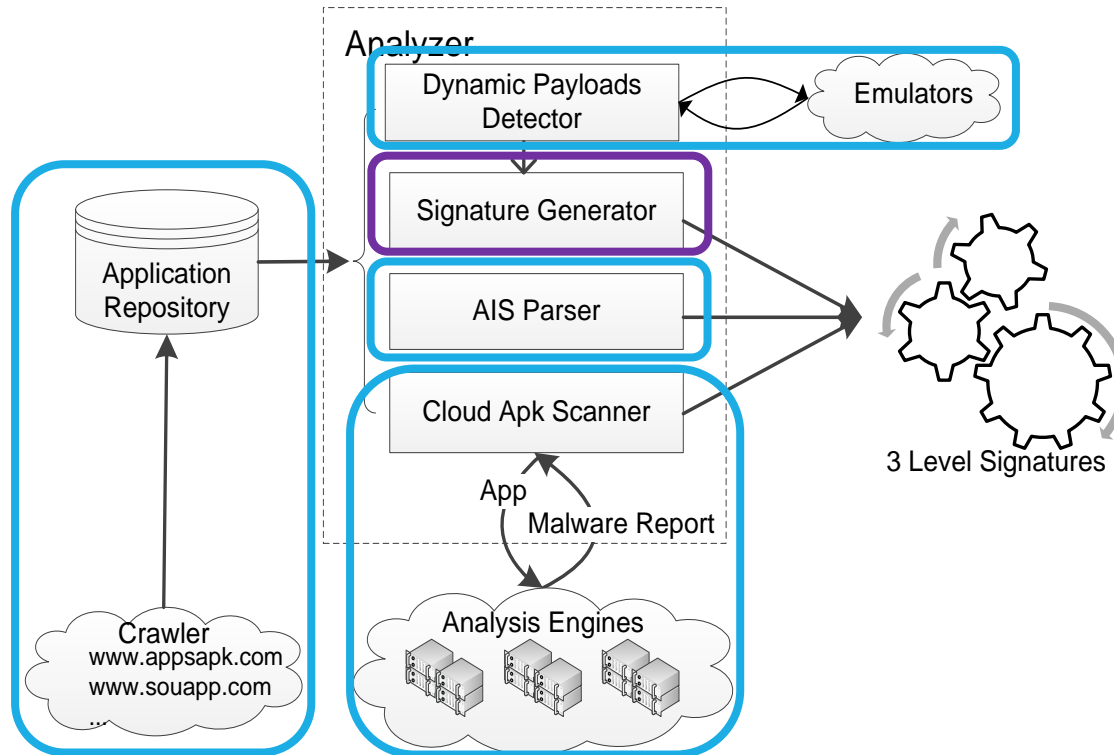
How to collect malware?

How to identify repackaged applications?

How to associate applications?

How to detect zero-day malware?

Building Blocks of DroidAnalytics



Traditional Hash vs Three-level Signature

Traditional hash

- Hackers can easily mutate a malware
- Not flexible for analysis

Three-level signature

- App, classes and methods
- Defend against obfuscation
- Facilitate analysis
- Zero-day malware

Android API Calls Table

API calls with a unique ID.

Full Path Method	Method ID
<code>android/accounts/Account;-><init></code>	<code>0x00001</code>
<code>:</code>	<code>:</code>
<code>android/content/Intent;-><init></code>	<code>0x30291</code>
<code>android/content/Intent;->toUri</code>	<code>0x30292</code>
<code>android/telephony/SmsManager;->getDefault</code>	<code>0x39D53</code>
<code>android/app/PendingIntent;->getBroadcast</code>	<code>0xF3E91</code>

Disassembling

.apk
AndroidManifest.xml
classes.dex
asset/
...

Reverse Engineering

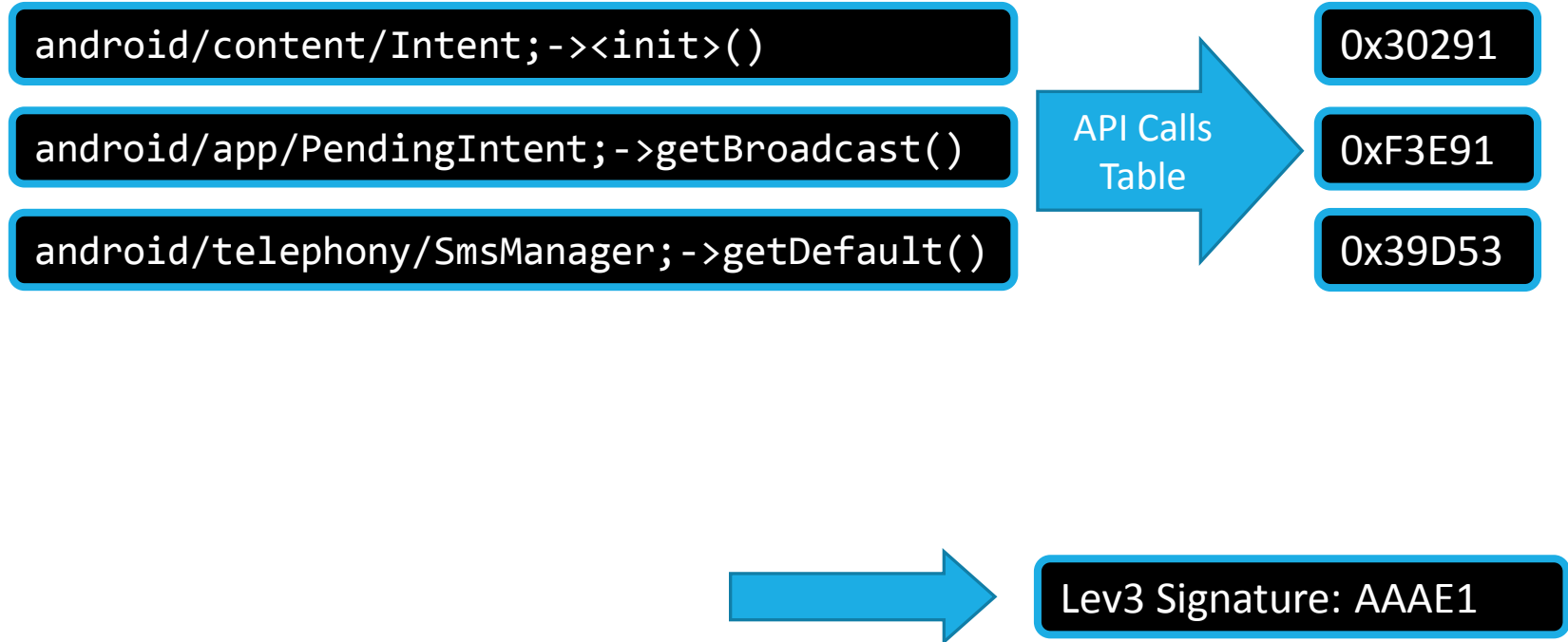


```
1  const/4 v2, 0x0
2  new-instance v3, Landroid/content/Intent;
3  const-string v5, "SENT"
4  invoke-direct{v3, v4}, Landroid/content/intent; -><init>(Ljava/lang/string;)V
5  const/4 v5, 0x0
6  move-result-object v4
7  .local v4, pi:Landroid/app/PendingIntent
```

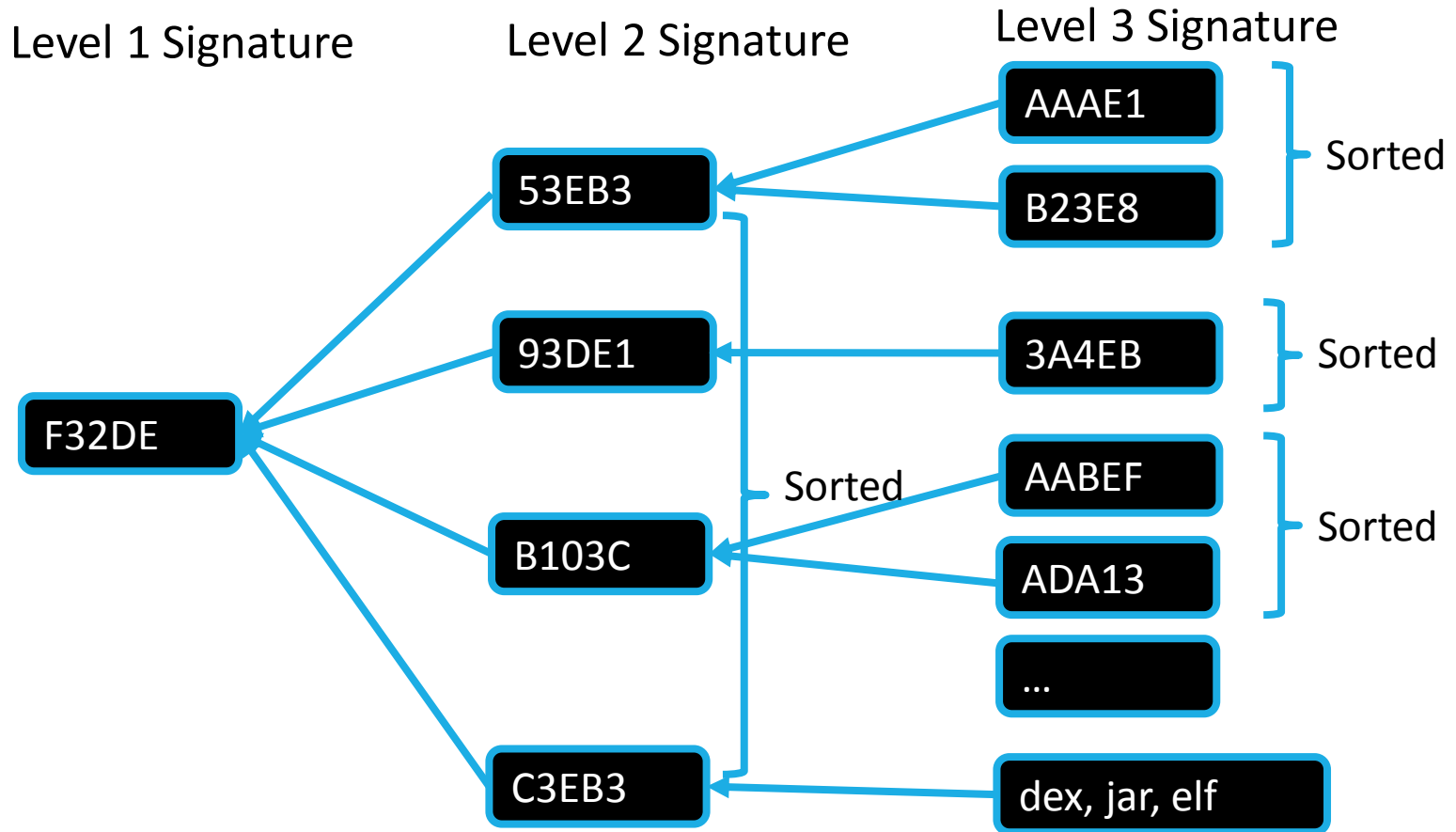
Three-level Signature – Level 3

```
1  const/4 v2, 0x0
2  new-instance v3, Landroid/content/Intent;
3  const-string v5, "SENT"
4  invoke-direct {v3, v5}, Landroid/content/Intent;-
   ><init>(Ljava/lang/String;)V
5  const/4 v5, 0x0
6  invoke-static {v1, v2, v3, v5}, Landroid/app/PendingIntent;->
   getBroadcast(Landroid/content/Context;ILandroid/content/Intent;I)
   Landroid/app/PendingIntent;
7  move-result-object v4
8  .local v4, pi:Landroid/app/PendingIntent;
9  invoke-static {}, Landroid/telephony/SmsManager;-> getDefault()\
   Landroid/telephony/SmsManager;
10 move-result-object v0
```

Three-level Signature – Level 3



Lev2 Signature and Lev1 Signature



Utility & Effectiveness of Signature Based System

Malware Repackaging

- Change hash value

Malware with Code Obfuscation

- Inject malware logic

Analytics Capability of DroidAnalytics

Details

This is a malware!

File Name: cab6872bddc4bf85e10fcf33e327d9ff.apk

Package: com.mybooft.myclips

Min Sdk Version: 2.3

Submit Time: 2012-05-22 21:40:15

Permissions(10):

android.permission.RECEIVE_BOOT_COMPLETED
android.permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.INTERNET
android.permission.RECEIVE_SMS
android.permission.SEND_SMS
android.permission.INSTALL_PACKAGES
android.permission.WRITE_EXTERNAL_STORAGE

Permission Information

Receiver Intent(3):

android.intent.action.BOOT_COMPLETED
android.intent.action.SIG_STR
android.provider.Telephony.SMS_RECEIVED

Broadcast Receiver

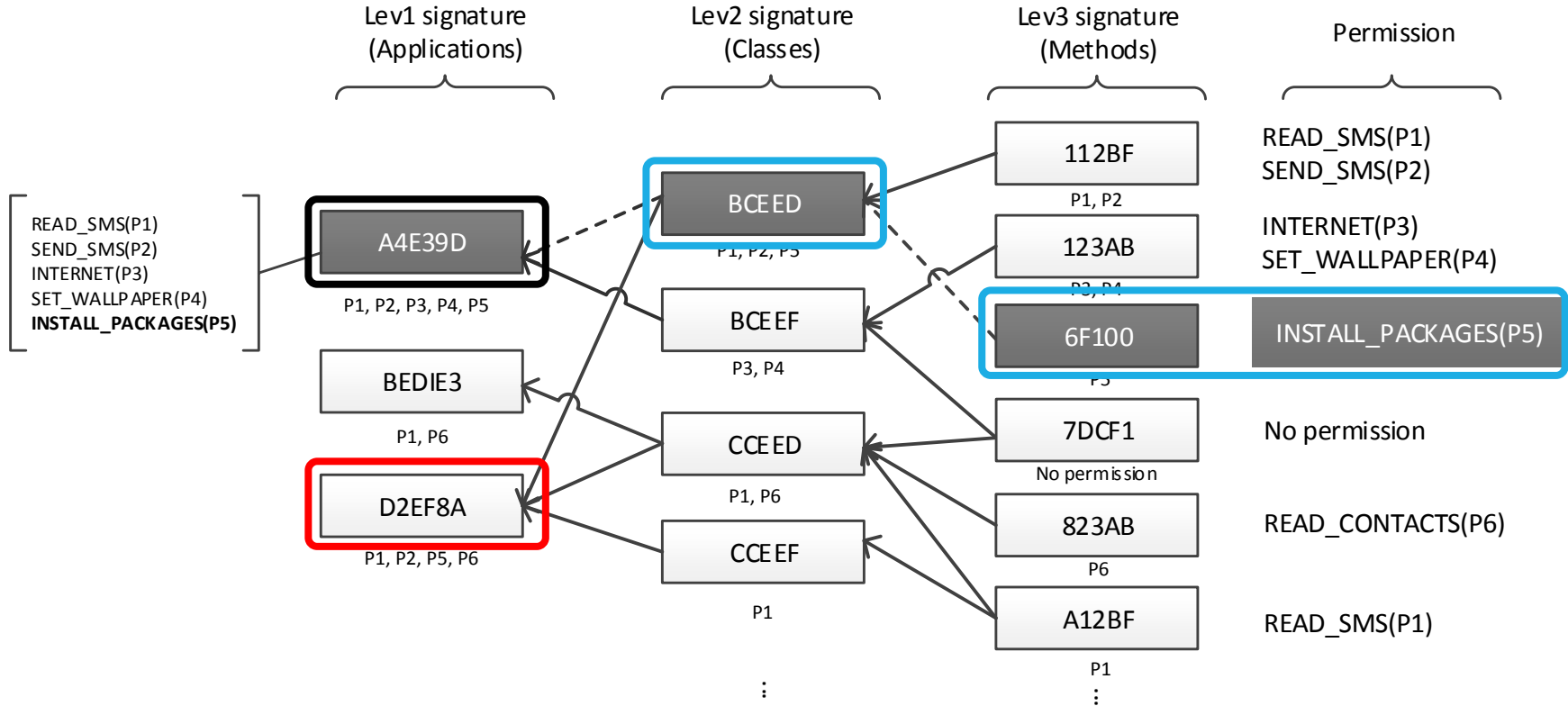
Scan Results:

Kaspersky: **Detected** HEUR_Trojan-Spy.AndroidOS.Adrd.a
Antiy: **Pass**

Cloud Detection Results

DroidAnalytics

Class Association



Zero-day Malware Detection

Similarity score

Clustering algorithm

- White list
- Combining clusters with the largest similarity score
- Suspicious cluster

327 zero-day malware

Conclusion

150,368 Android applications

2,475 malware

Three-level signature

Common analytics and class association

327 zero-day malware

Thank you!