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

From Google I/O 2013

BadNews

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

From Technocrates.org

Motivations

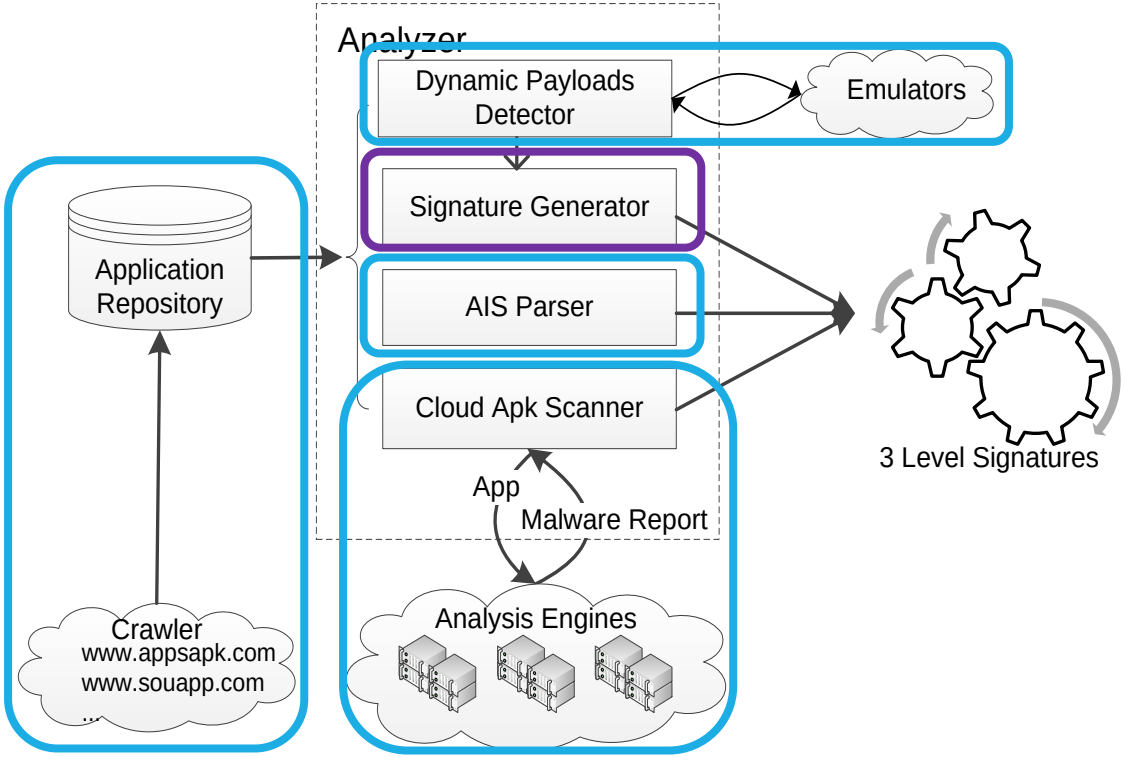
How to collect malware?

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

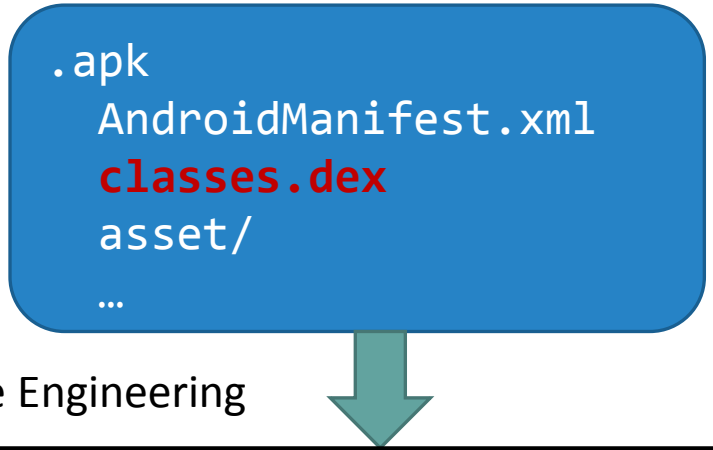
- App, classes and methods
- Defend against obfuscation
- Facilitate analysis
- Zero-day malware

Android API Calls Table

API calls with a unique ID.

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

Disassembling

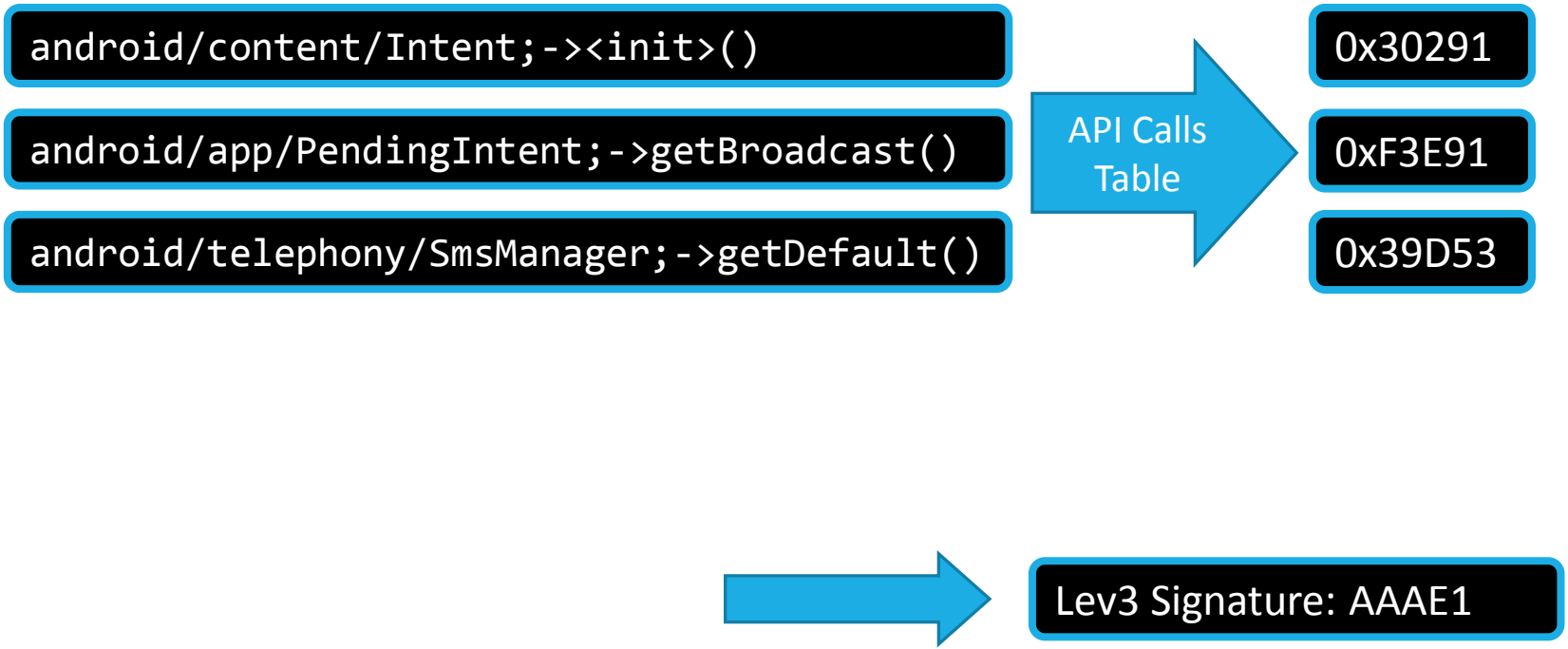



```
1  const/4 v2, 0x0
2  new-instance v3, Landroid/content/Intent;
3  const-string v5, “SENT”
4  invode-direct{v3, v4}, Landroid/content/intent;-><init>(Ljava/lang/string;)V
5  const/4 v5, 0x0
6  move-result-object v4
7  .local v4, pi:Landroid/app/PendingIntent
```

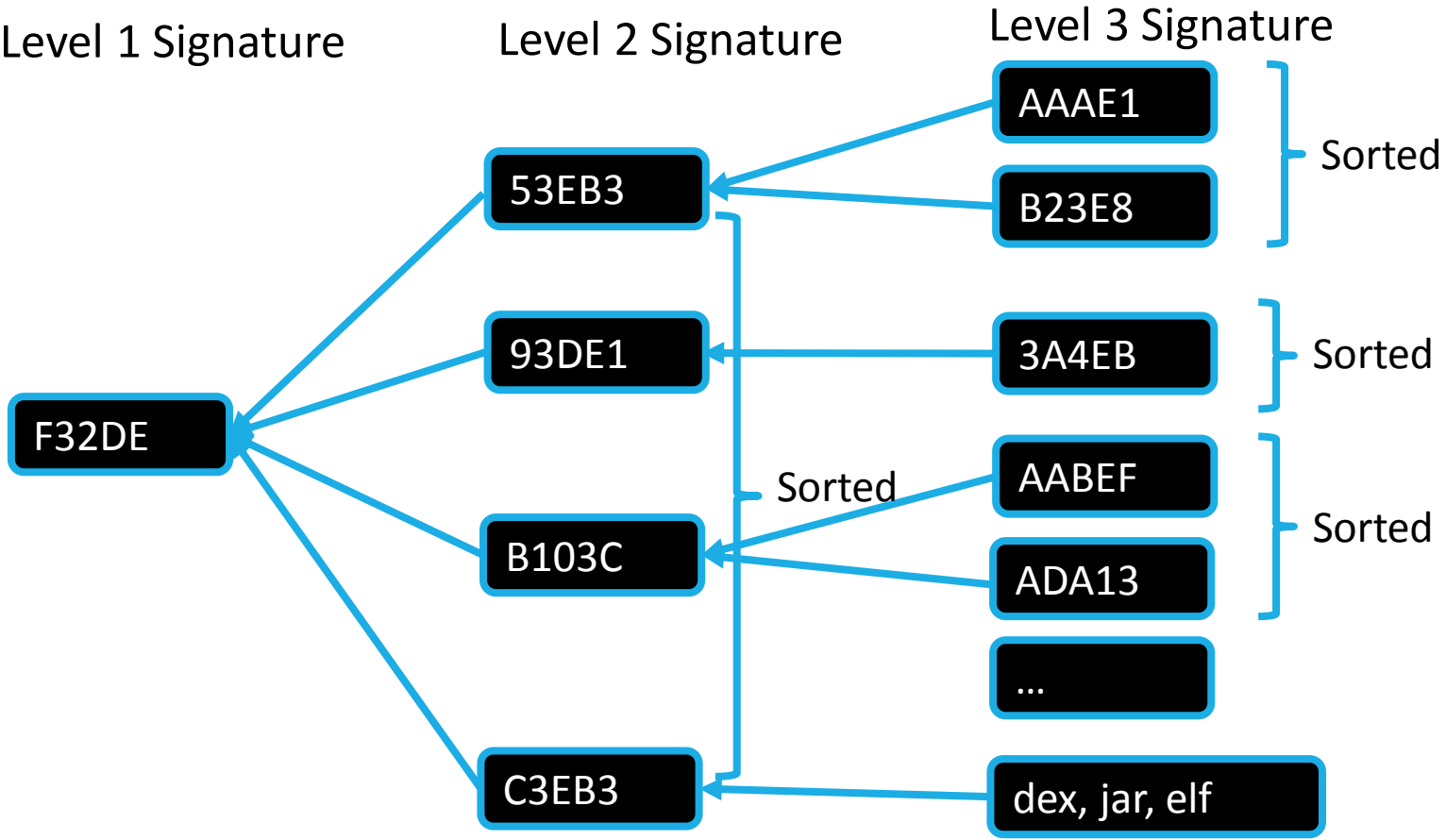
Three-level Signature – Level 3

```
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

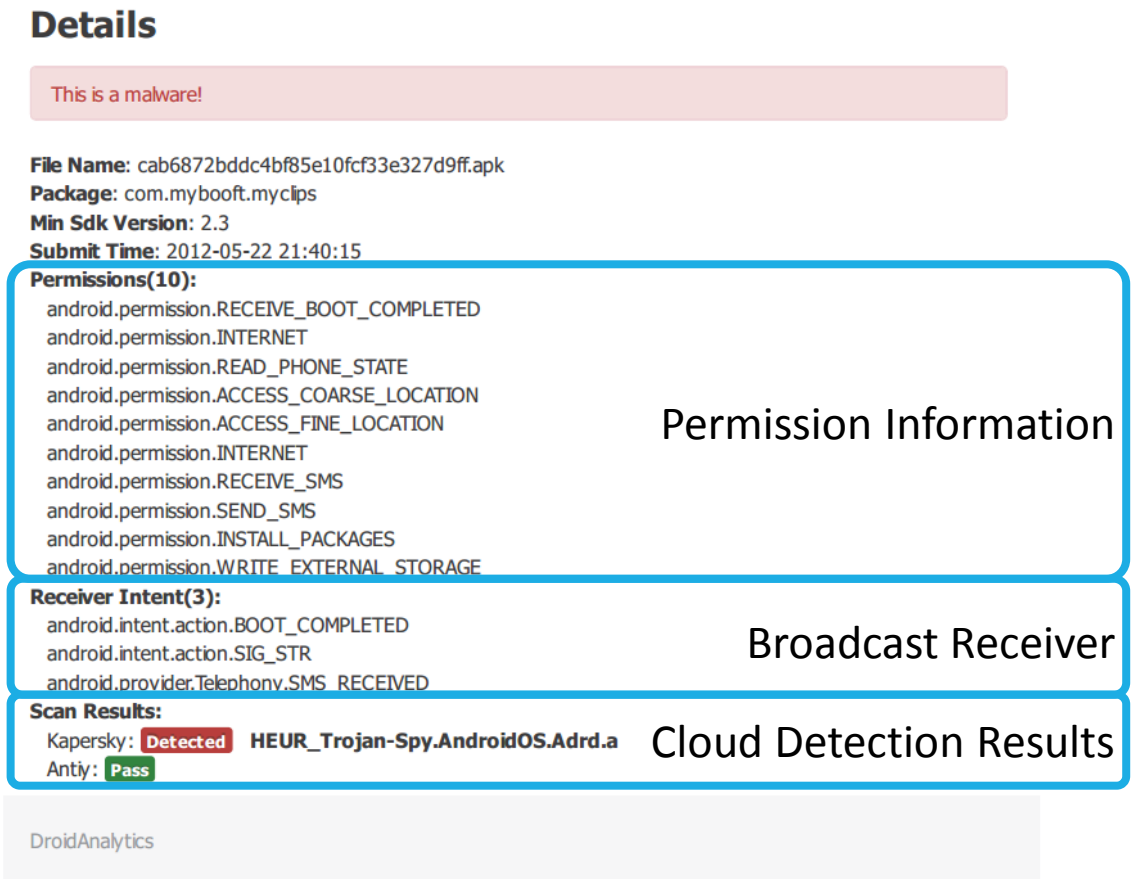
Malware Repackaging

- Change hash value

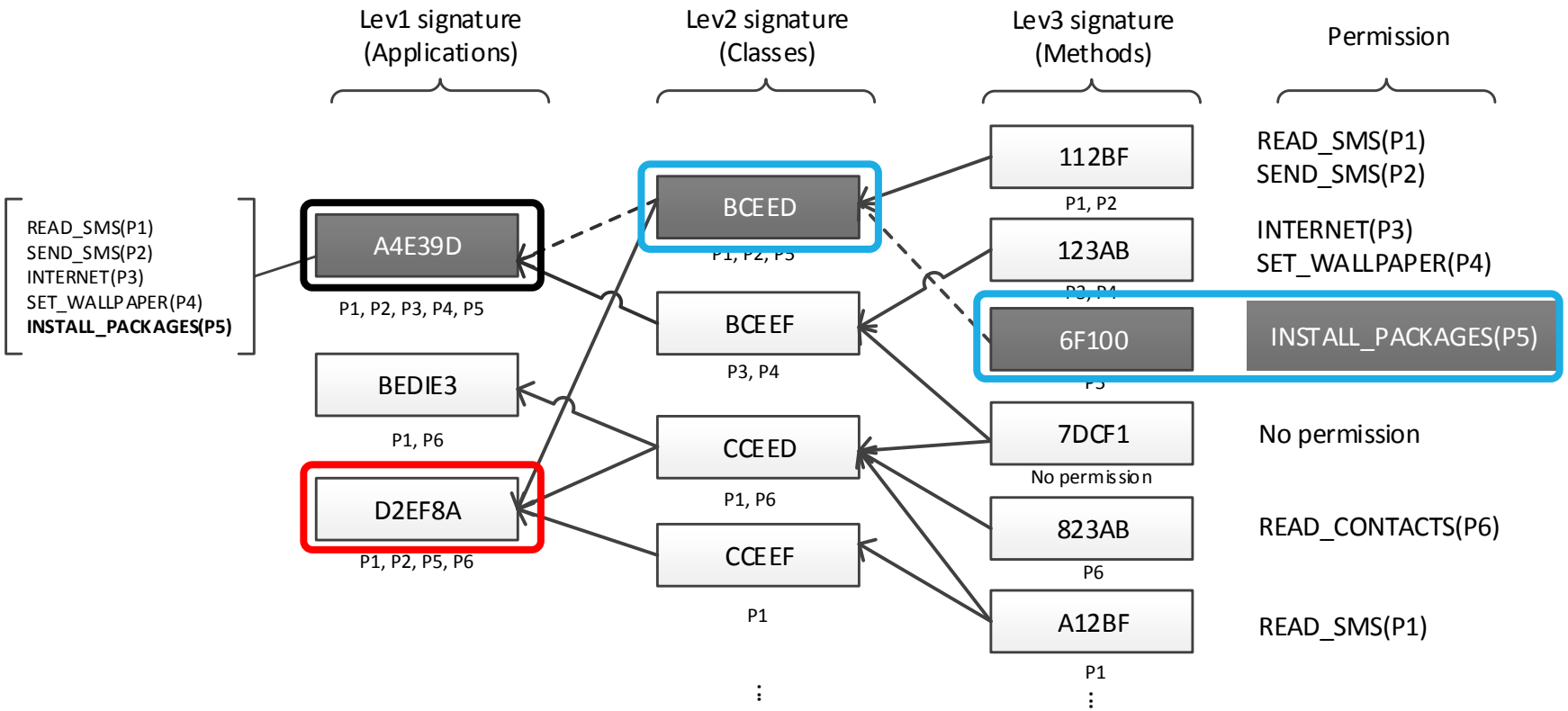
Malware with Code Obfuscation

- Inject malware logic

Analytics Capability of DroidAnalytics



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!