NDSS 2012, February 7th 2012, San Diego

NC STATE UNIVERSITY
Department of Computer Science

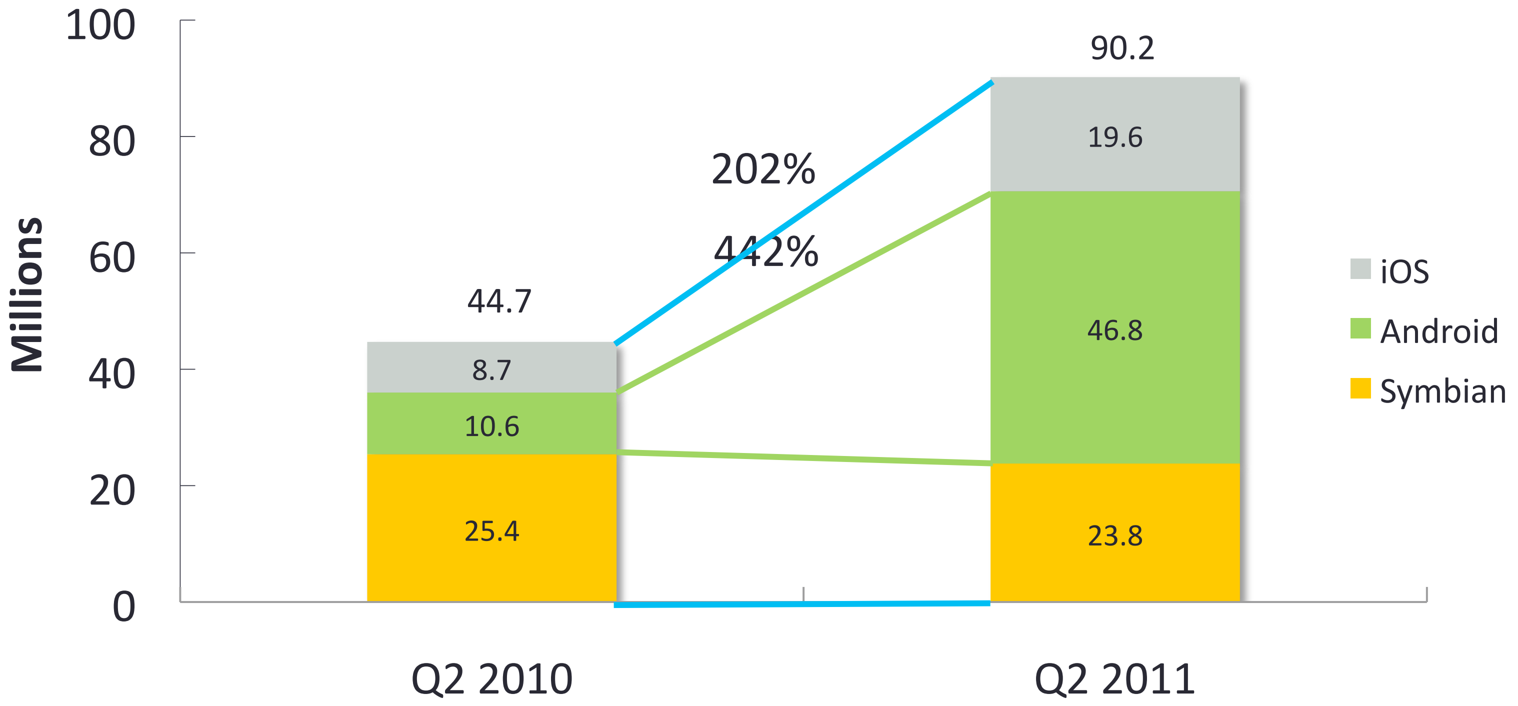
Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets

Yajin Zhou **Zhi Wang** Wu Zhou Xuxian Jiang

North Carolina State University

Motivation: Smartphones

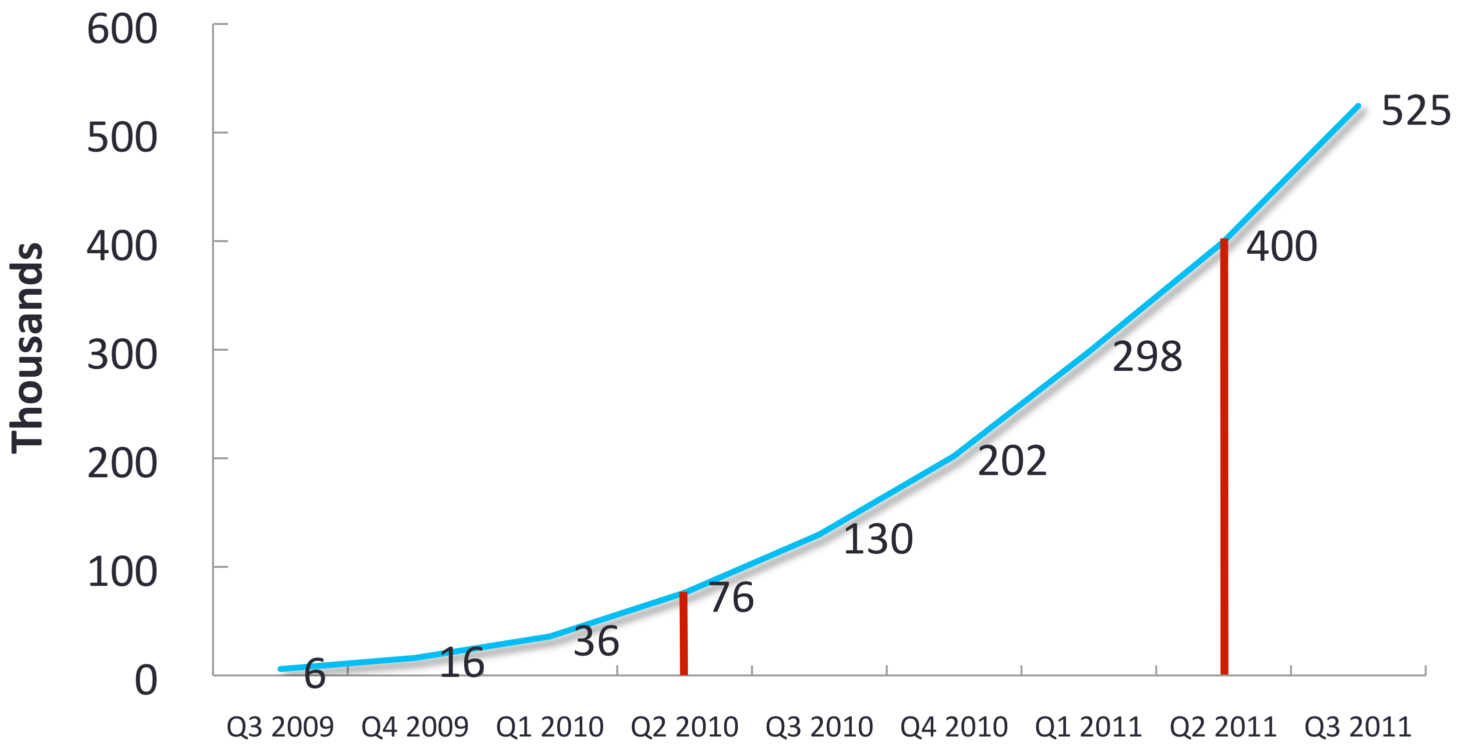
NC STATE UNIVERSITY



Worldwide Smartphone Sales [1]

[1] Data source: gartner.com

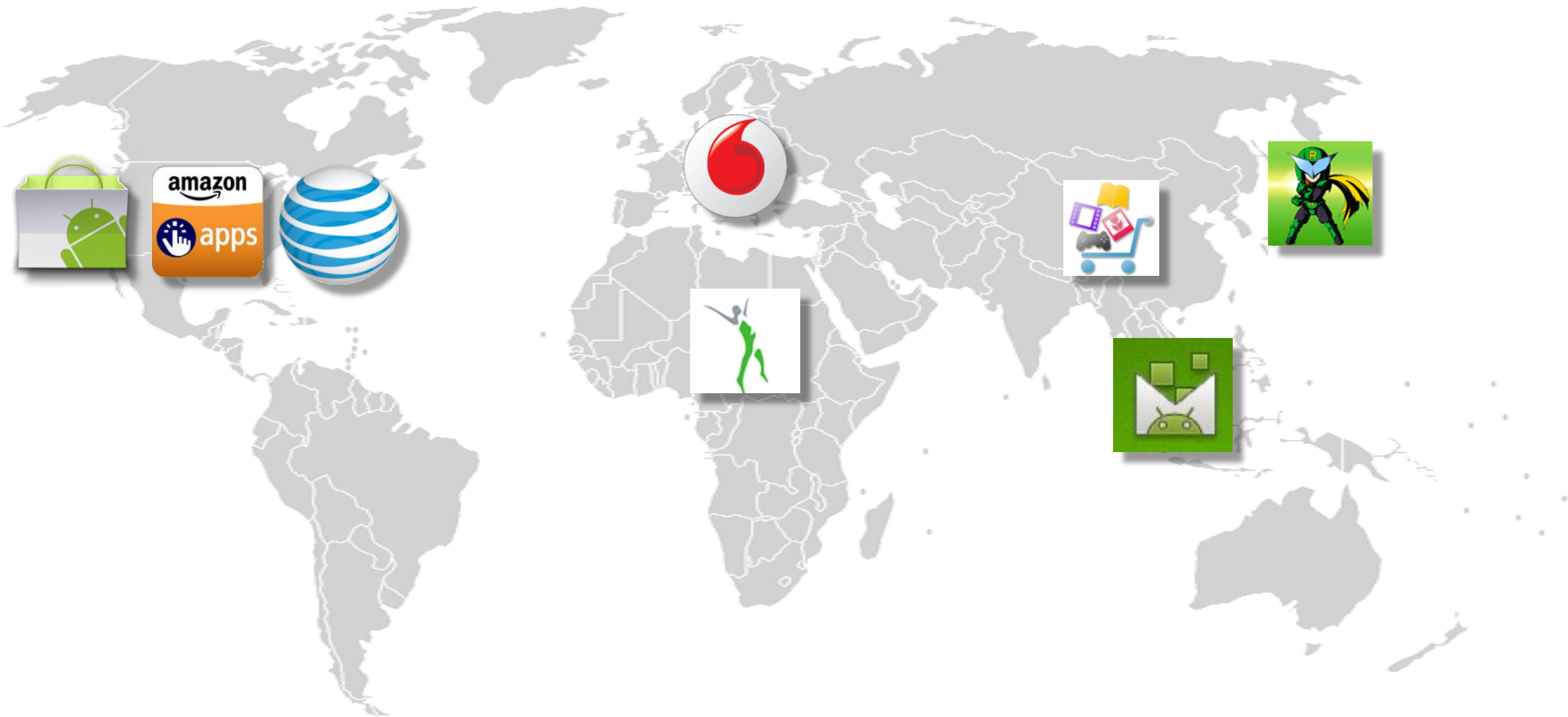
Motivation: Apps



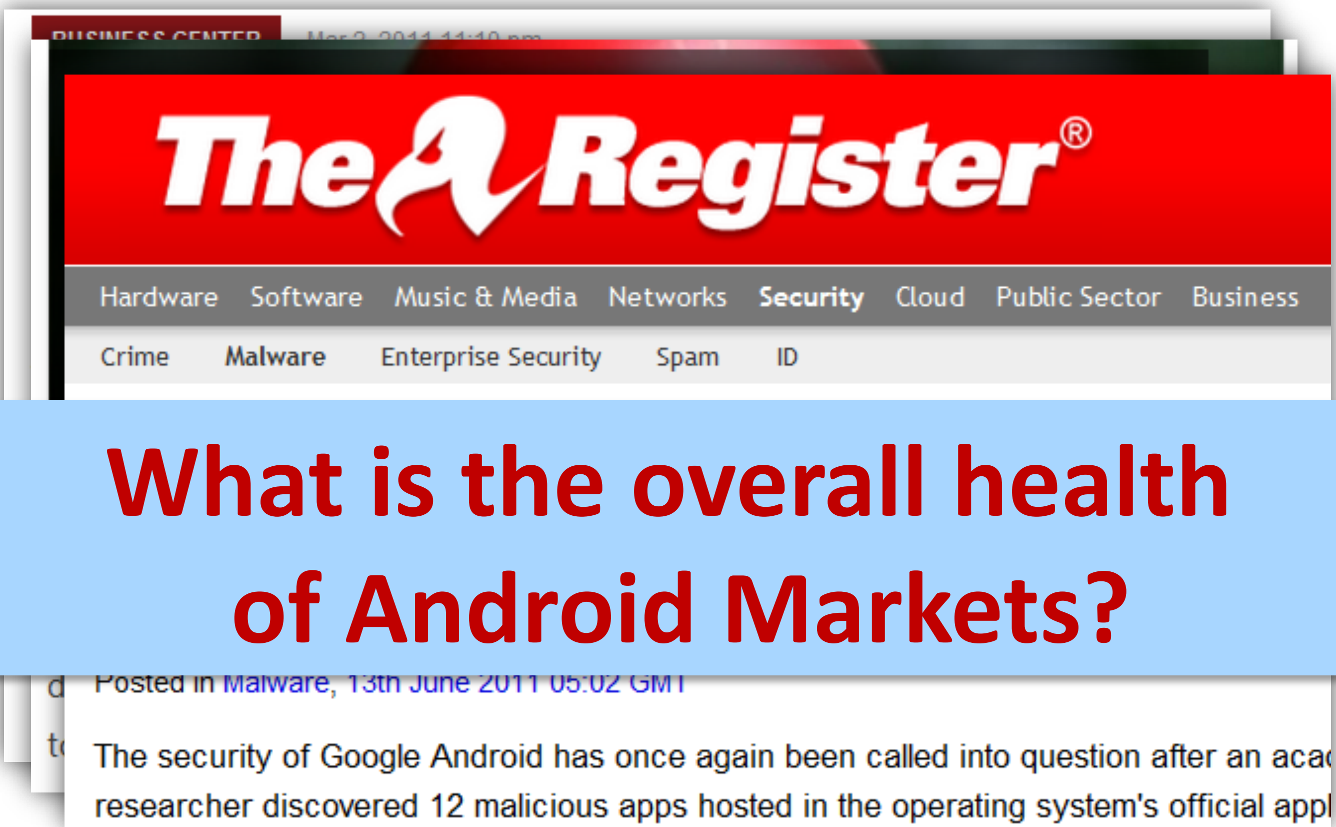
Number of Apps in Official Android Market[2]

[2] Data source: androlib.com

Motivation: Markets



Motivation: Malware in Markets



Posted in Malware, 13th June 2011 05:02 GMT

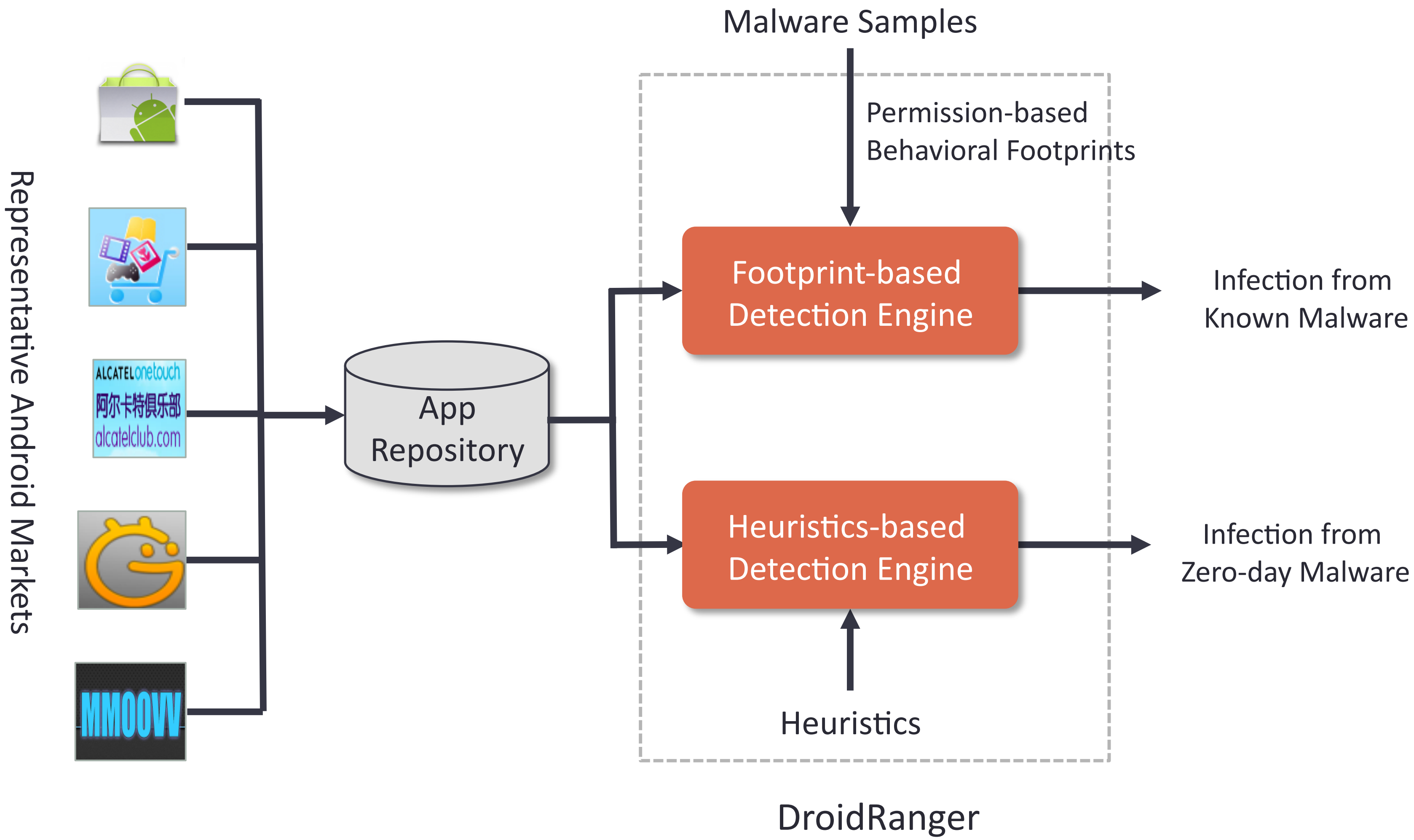
The security of Google Android has once again been called into question after an acad
researcher discovered 12 malicious apps hosted in the operating system's official appl

What is the overall health of Android Markets?

Design Goals

- Accuracy
  - Detect malware with low false positives and negatives
- Scalability
  - Scale to hundreds of thousands apps
- Efficiency
  - Process all apps in a reasonable amount of time

DroidRanger Overview


Malware Samples
Permission-based Behavioral Footprints
Representative Android Markets
ALCATEL onetouch
阿尔卡特俱乐部
alcatelclub.com
MMOOVV
App Repository
Footprint-based Detection Engine
Heuristics-based Detection Engine
Infection from Known Malware
Infection from Zero-day Malware
Heuristics
DroidRanger

Footprint-based Detection Engine

- Filter apps with essential permissions

Malware	Essential Permissions	Apps
Geinimi	INTERNET, SEND_SMS	7, 620 (4.17%)
ADRD	INTERNET, ACCESS_NETWORK_STATE RECEIVE_BOOT_COMPLETED	10, 379 (5.68%)
Pjapps	INTERNET, RECEIVE_SMS	4, 637 (2.54%)
Bgserv	INTERNET, RECEIVE_SMS, SEND_SMS	2, 880 (1.58%)
DroidDream	CHANGE_WIFI_STATE	4, 096 (2.24%)
zHash	CHANGE_WIFI_STATE	4, 096 (2.24%)
jSMSHider	INSTALL_PACKAGES	[illegible]
Zsone	RECEIVE_SMS, SEND_SMS	[illegible]

Reduced to 0.64% when considering a broadcast receiver

Footprint-based Detection Engine

- Match apps to malware behavioral footprints in multiple dimensions
  - Information in manifest file
    - ➢Declare a receiver listening to SMS_RECEIVED
  - Semantics in the byte-code
    - ➢Register a receiver listening to SMS_RECEIVED
    - ➢Call *abortBroadcast* in the receiver
    - ➢Send SMS messages to premium numbers
  - Structural layout of the app

Behavioral footprint of Zsone

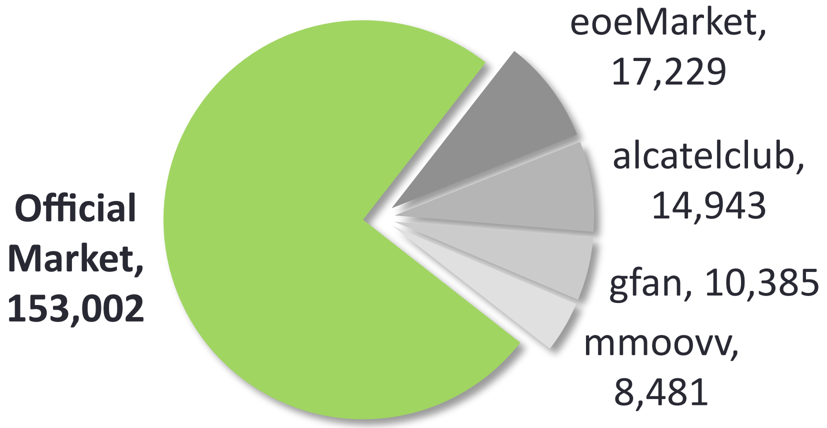
Heuristics-based Detection Engine

- Select apps with dynamic Java/native code loading
- Monitor their runtime behavior
  - Java code: permission-related framework APIs
  - Native code: system calls requiring root privileges

Evaluation: Overall

NC STATE UNIVERSITY

- Data set
  - Crawled the official & four alternative markets
  - Collected 204,040 free apps during 05/2011-06/2011
- Process time
  - Used four and half hours for all 204,040 apps

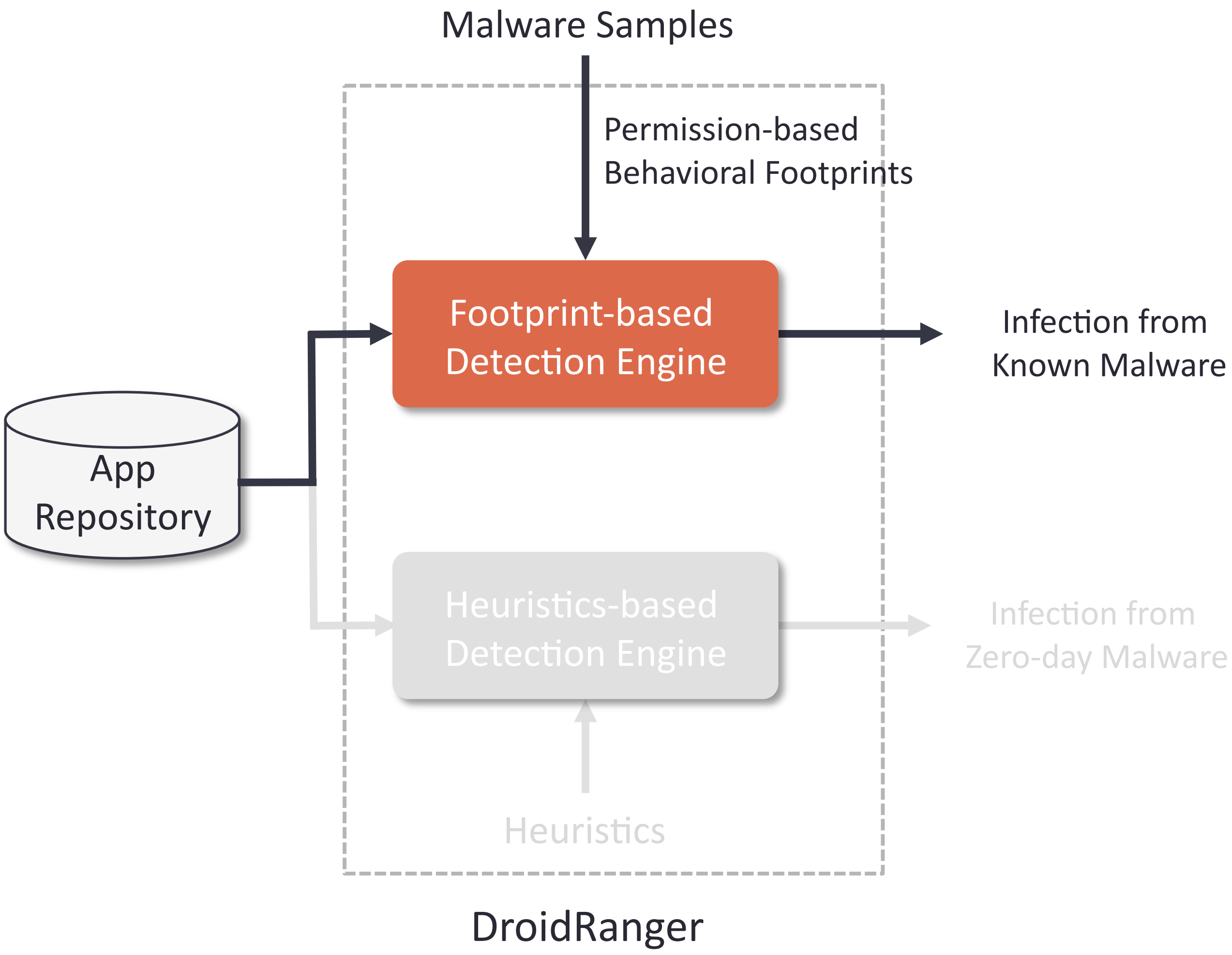


Evaluation: Overall

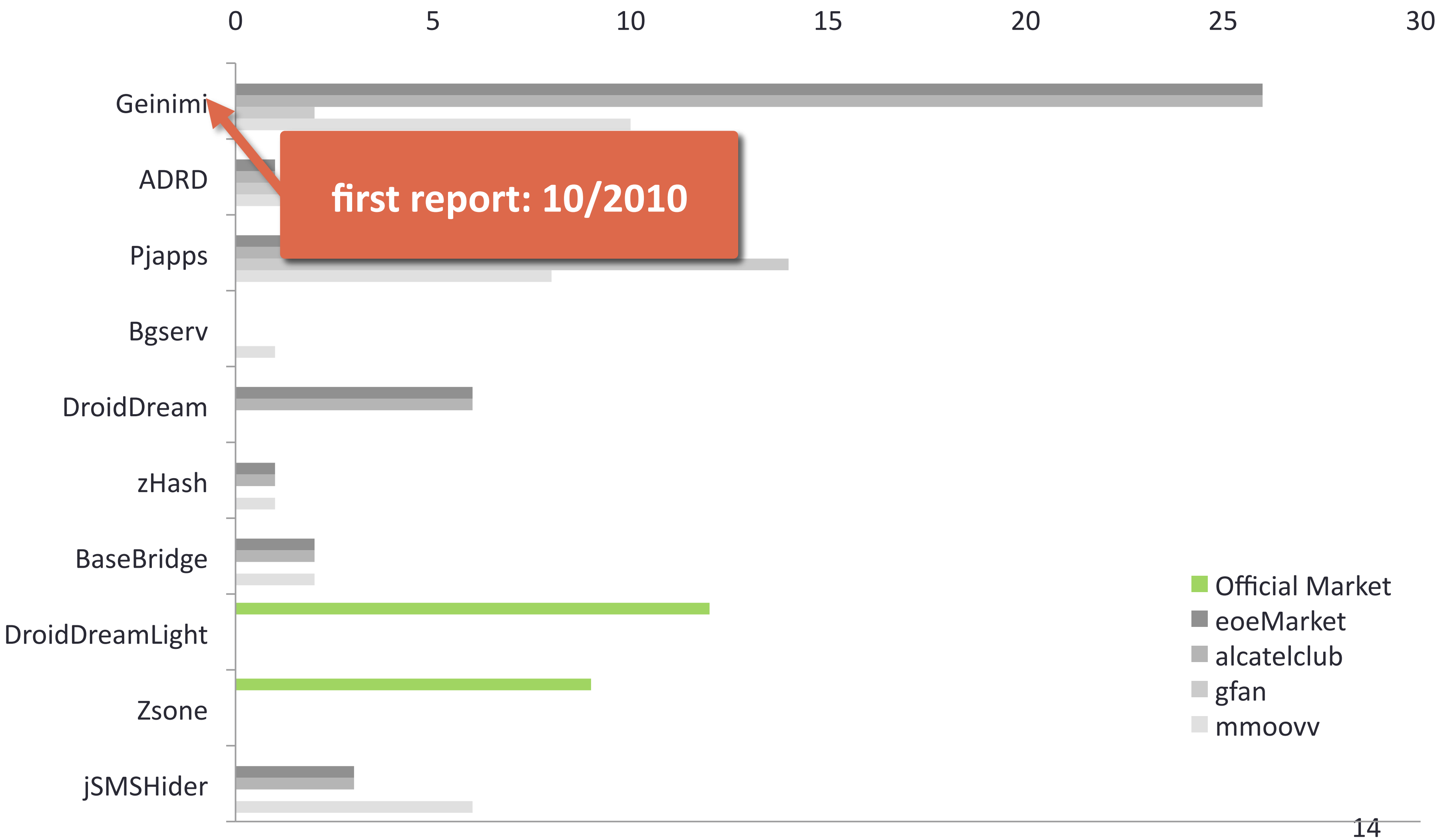
Malware	Official Market	eoeMarket	alcatelclub	gfan	mmoovv	Total
Known	21	51	48	20	31	171
Zero-day	11	9	10	1	9	40
Total	32 (**0.02%**)	60 (**0.35%**)	58 (**0.39%**)	21 (**0.20%**)	40 (**0.47%**)	211

Total infected apps detected by DroidRanger

Evaluation: Footprint-based Detection Engine

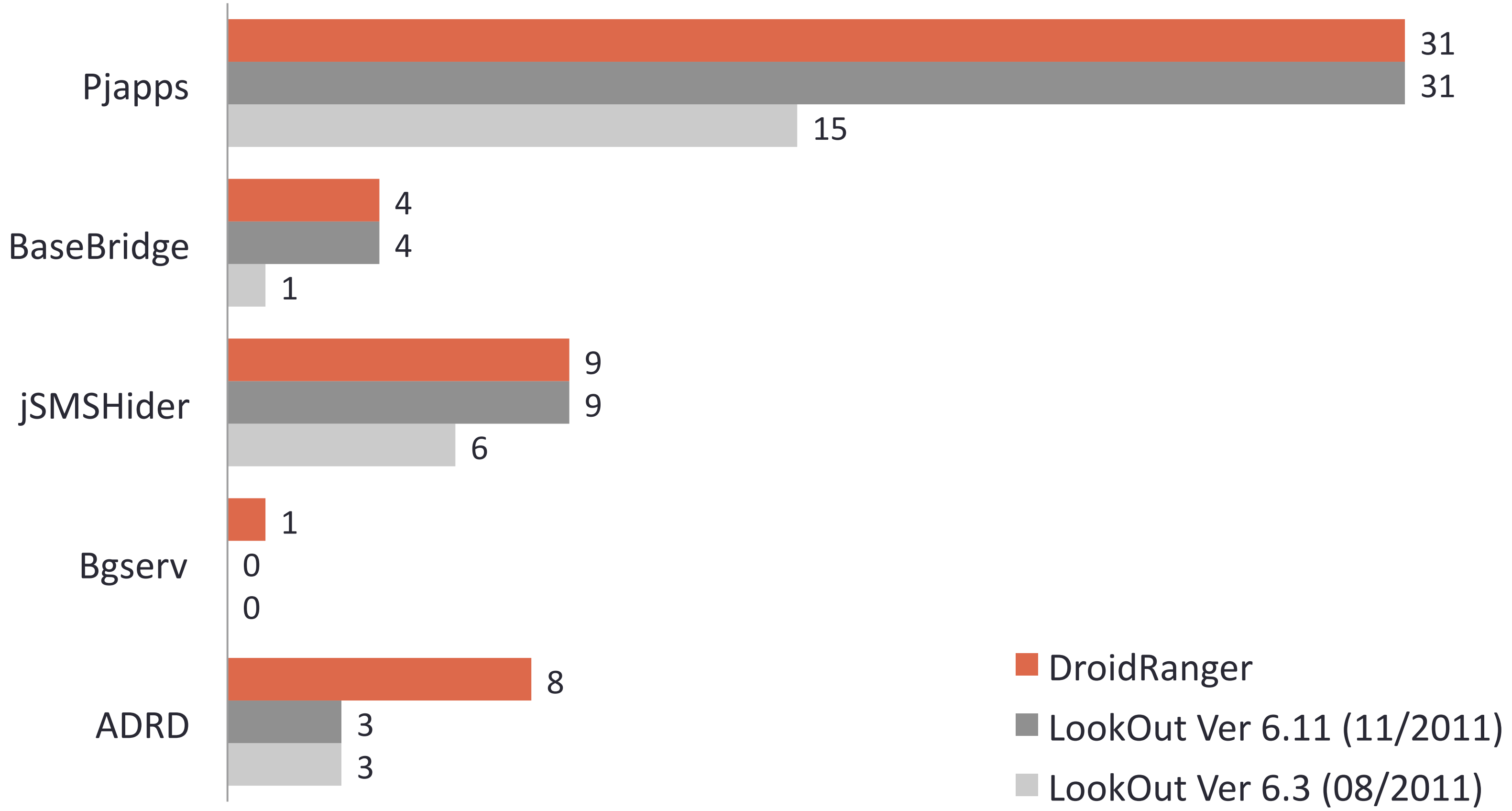


Evaluation: Infected Apps



first report: 10/2010

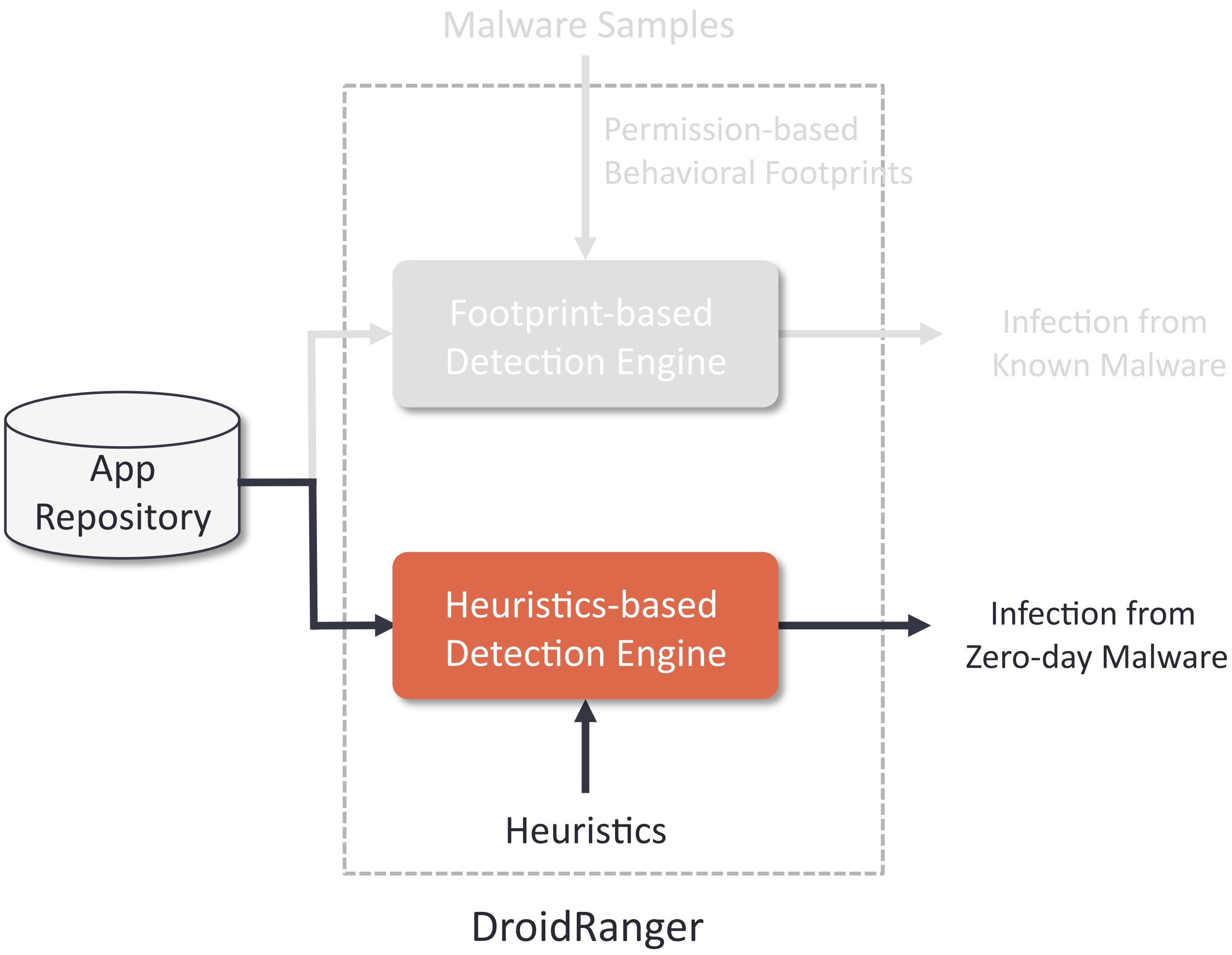
Evaluation: Accuracy



Evaluation: Accuracy

- 24 samples in 10 known families from *contagio*
- DroidRanger detected 23 samples (96%)
  - Missed a payload of DroidDream, not the malware itself
  - Found one mis-categorized sample for ADRD

Evaluation: Heuristics-based Detection Engine



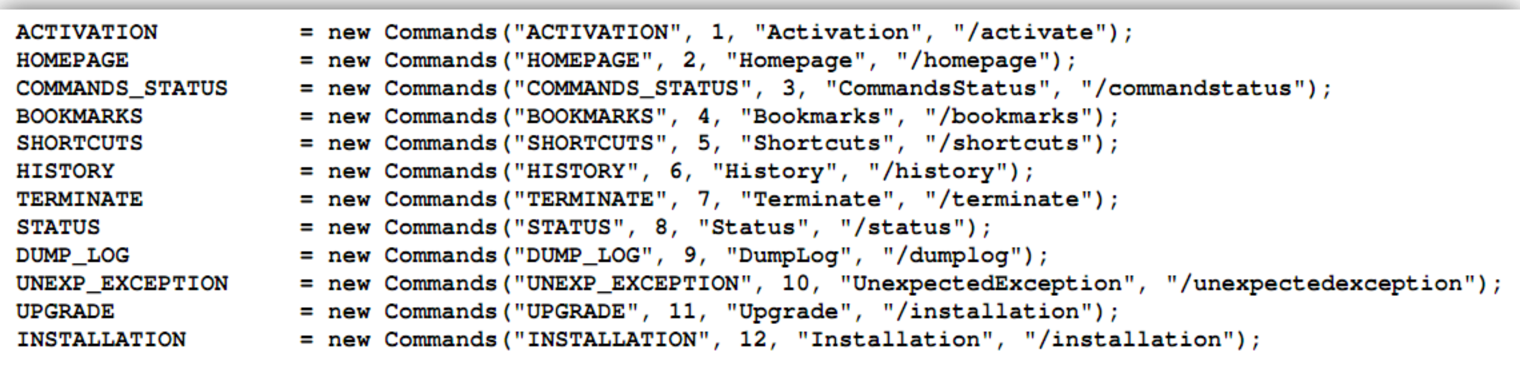
Evaluation: Infected Apps

- Detected two zero-day malware using heuristics
  - Plankton: dynamic loading of Java code
  - DroidKungFu: dynamic loading of native code
- Detected 40 samples using behavioral footprints
  - 11 samples from the official Android Market
  - 29 samples from alternative Android Markets

Evaluation: Malware Behaviors

NC STATE UNIVERSITY

- Plankton
  - Uploads a list of permissions before downloading a payload
  - Contains a bot-like command & control channel
- D



```
ACTIVATION          = new Commands("ACTIVATION", 1, "Activation", "/activate");
HOMEPAGE            = new Commands("HOMEPAGE", 2, "Homepage", "/homepage");
COMMANDS_STATUS     = new Commands("COMMANDS_STATUS", 3, "CommandsStatus", "/commandstatus");
BOOKMARKS           = new Commands("BOOKMARKS", 4, "Bookmarks", "/bookmarks");
SHORTCUTS           = new Commands("SHORTCUTS", 5, "Shortcuts", "/shortcuts");
HISTORY             = new Commands("HISTORY", 6, "History", "/history");
TERMINATE           = new Commands("TERMINATE", 7, "Terminate", "/terminate");
STATUS              = new Commands("STATUS", 8, "Status", "/status");
DUMP_LOG            = new Commands("DUMP_LOG", 9, "DumpLog", "/dumplog");
UNEXP_EXCEPTION     = new Commands("UNEXP_EXCEPTION", 10, "UnexpectedException", "/unexpectedexception");
UPGRADE             = new Commands("UPGRADE", 11, "Upgrade", "/installation");
INSTALLATION        = new Commands("INSTALLATION", 12, "Installation", "/installation");
```

Discussion

- Need more comprehensive heuristics
  - Background sending of unauthorized SMS messages?
  - Bot-like behavior controlled by SMS messages?
- A call for rigorous vetting processes
  - A large number of users can be infected
  - Malware remains in alternative markets for a long time
  - Zero-day malware exists in Android Markets

Related Work

- Smartphone platform security
  - TaintDroid (Enck et al., OSDI 10), PiOS (Egele et al., NDSS 11), Stowaway (Felt et al., CCS 11), Cells (Andrus et al., SOSP 11), AppFence (Hornyack et al., CCS 11), Quire (Dietz et al., USENIX Security 11), A Study of Android Application Security (Enck et al., USENIX Security 11), TISSA (Zhou et al., TRUST 11), Woodpecker (Grace et al., NDSS 12) …
- Malware detection on mobile devices
  - pBMDS (Xie et al., WiSec 10), VirusMeter (Liu et al., RAID 09), Crowdroid (Burguera et al., CCS-SPSM 11) …
- Other systematic security study
  - HoneyMonkey (Wang et al., NDSS 06), Systematic Web Spyware Study (Moshchuk et al., NDSS 06), All Your iFRAMEs Point to Us (Provos et al., USENIX Security 08) …

Conclusion

- DroidRanger is a system to systematically study the overall health of existing Android Markets

Malware	Official Market	eoeMarket	alcatelclub	gfan	mmoovv	Total
Known	21	51	48	20	31	171
Zero-day	11	9	10	1	9	40
Total	32 (0.02%)	60 (0.35%)	58 (0.39%)	21 (0.20%)	40 (0.47%)	211

Thank You!

Evaluation: Known Malware Samples

- 20 samples from 10 malware families

Malware	First Report	Summary
Geinimi	10/2010	Trojan with bot-like capability
ADRD	02/2011	Trojan with bot-like capability
Pjapps	02/2011	Trojan with bot-like capability
Bgserv	03/2011	Trojan with bot-like capability
DroidDream	03/2011	Root exploit with Exploid, Rageagainstthecage
zHash	03/2011	Root exploit with Exploid
BaseBridge	05/2011	Root exploit with Rageagainstthecage
DroidDreamLight	05/2011	Trojan with information stealing capability
Zsone	05/2011	Trojan that sends premium-rate SMS
jSMSHider	06/2011	Trojan that target third-party firmware