AndroTotal

A Scalable Framework for Android Antimalware Testing

Andrea Valdi, **Federico Maggi**, **Stefano Zanero**

Politecnico di Milano, **DEIB**

fede@maggi.cc

Roadmap

1. Threats and protections
2. Limitations
3. Evaluating antimalware
4. AndroTotal
5. Status

1. Threats and protections

2. Limitations

3. Evaluating antimalware

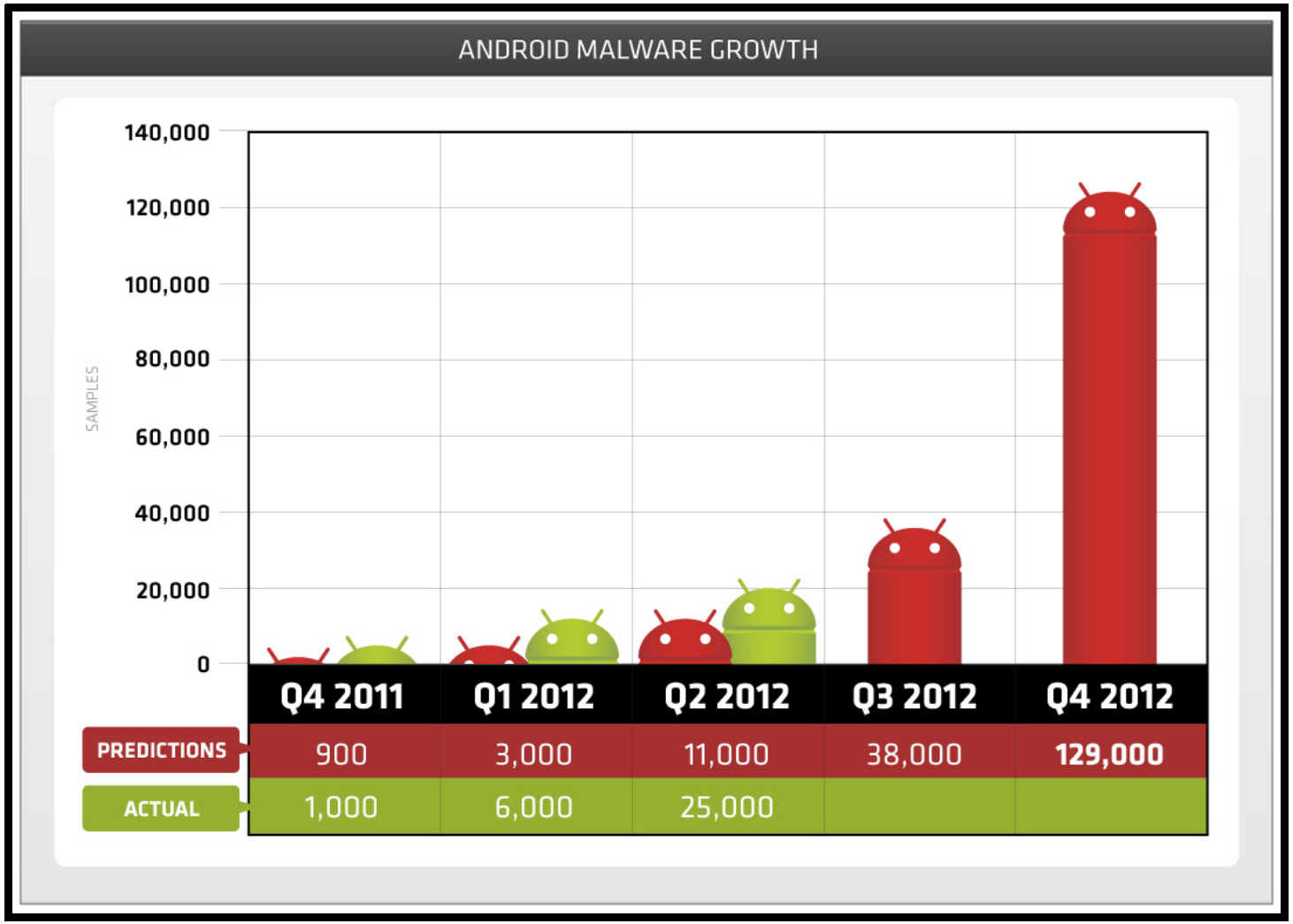
4. AndroTotal

5. Status

Android Facts

- Android is the most popular mobile platform
- Rich marketplaces stocked with apps
- Very attractive target for attackers

Growth of Malicious Apps



http://blog.trendmicro.com/trendlabs-security-intelligence/byod-a-leap-of-faith-for-enterprise-users/

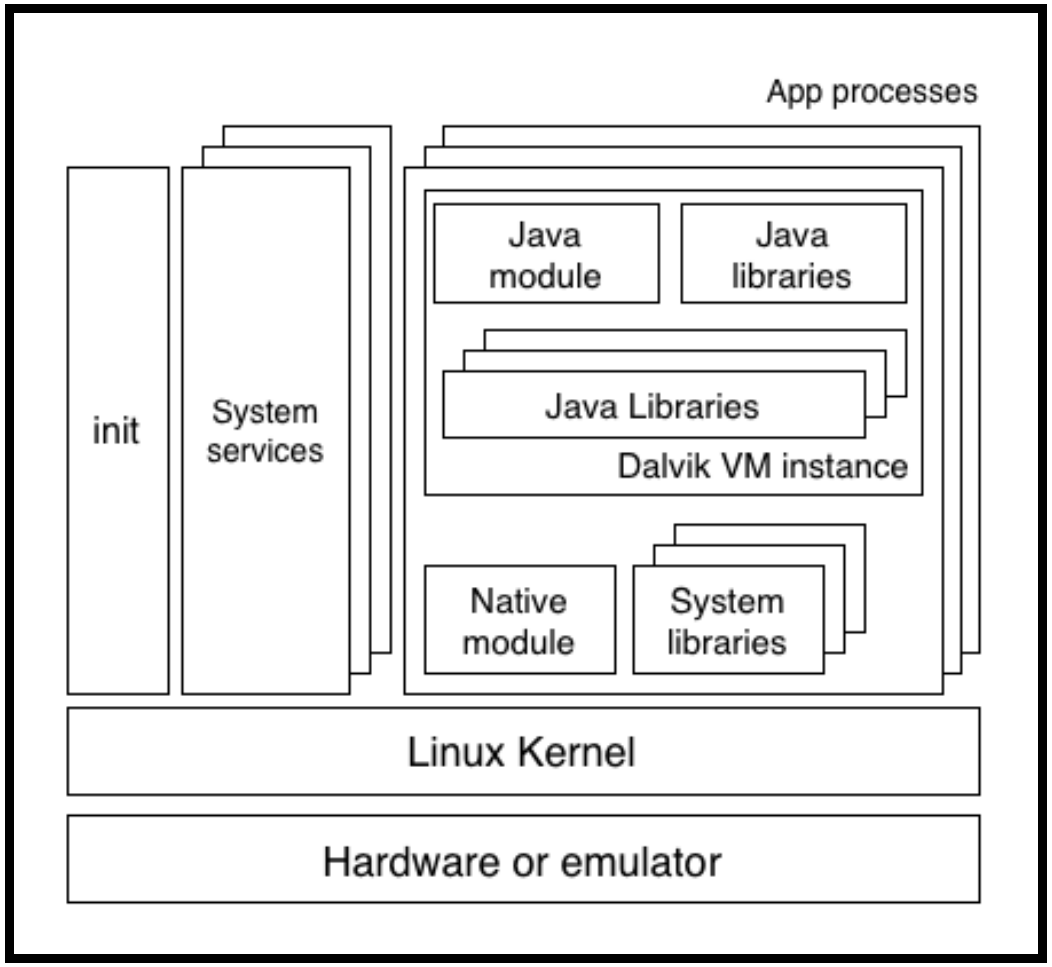
Attackers Goals

- Steal sensitive data (intercept texts or calls)
- Turn devices into bots (perform malicious actions)
- Financial gain (call or text premium numbers)

Android Security Approach

- Official apps on Google Play are vetted upon submission
- "Proprietary" JVM (Dalvik) runtime environment
- One Dalvik process per app
- Isolated processes with distinct `uid`, `gid`
- "Sensitive" operations require permissions

Android Architecture



Consequence

An app (process) cannot interfere
with another app's memory or filesystem.

1. Threats and protections

2. Limitations

3. Evaluating antimalware

4. AndroTotal

5. Status

Antimalware Limitations

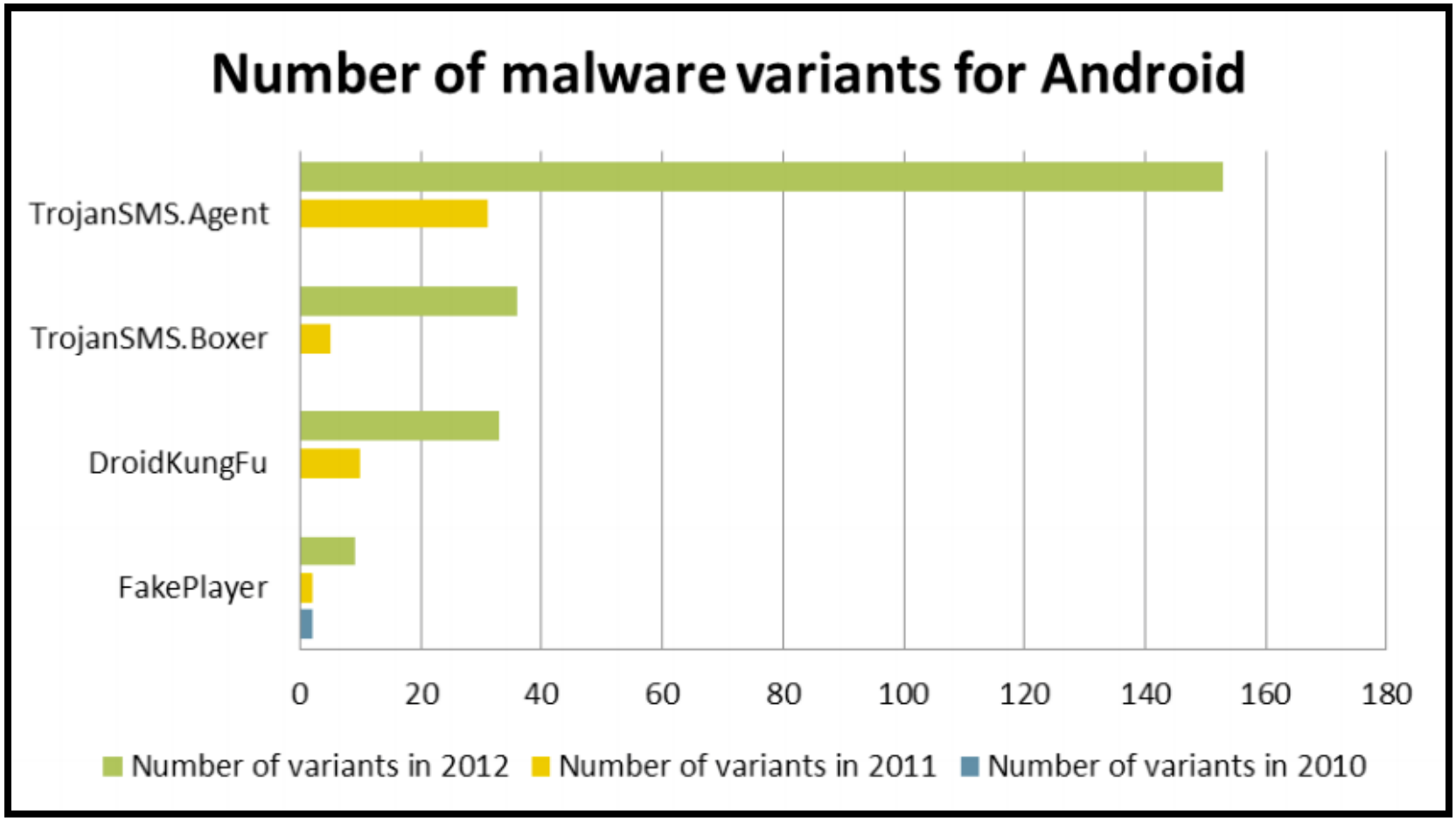
- Cannot observe running processes
- Workarounds:
  - Signature-based matching
  - Custom kernel (e.g., intercept syscalls)
  - Root the device and increase the antimalware's privileges

Malware Limitations

- Classic malware approaches do not apply
- Example: Memory errors cannot be exploited
- Workarounds:
  - Social engineering
  - Phishing
  - Signature evasion

Evading Signatures

repackaging, obfuscation, encryption



http://go.eset.com/us/resources/white-papers/Trends_for_2013_preview

1. Threats and protections

2. Limitations

3. Evaluating antimalware

4. AndroTotal

5. Status

Antimalware Products

- We count about 100 (free) antimalware products
- They are all based on *signature matching*
- Some provide extras if granted root privileges

How to measure their effectiveness?

1. Obtain **M** samples of known malware
2. Apply **T** transformations to each sample
3. Analyze with **P** x **V** antimalware products and versions
4. Repeat for each of the **A** Android versions

Numbers

- M = 1,000 (very conservative)
- T = 3 (obfuscation, encryption, repackaging)
- P = 100
- V = 2 (simple example)
- A = 3 (2.3, 4.1, 4.2)

1,000 x 3 x 100 x 2 x 3 = 1,800,000 tests

Lack of Automation Tools

VirusTotal.com?

- Relies on command-line, desktop-based AVs with signatures for Android
- Unclear whether the same signatures will work on the respective mobile products
- No versioning support

State of the Art

- H. Pilz, *"Building a test environment for Android anti-malware tests,"* Virus Bulletin Conference '12
  - Human oracle is needed
- M. Zheng, P. P. C. Lee, and J. C. S. Lui, *"ADAM: An Automatic and Extensible Platform to Stress Test Android Anti-Virus Systems,"* DIMVA'12
  - Focus on transformation, uses VirusTotal.com
- V. Rastogi, Y. Chen, and X. Jiang, *"DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks,"* AsiaCCS'13
  - Focus on transformation, uses custom scripts

Challenges

- Parallelization is required
- Android antimalware products are UI driven

1. Threats and protections

2. Limitations

3. Evaluating antimalware

4. AndroTotal

5. Status

- SDK for writing UI tests/scrapers
- Pluggable adapters for each antimalware
- Parametric tests (e.g., version, platform)
- Task queues with distributed workers

Characteristics

- Web frontend for humans
- JSON/REST API for machines
- Pluggable code-transformation modules
- Works on both emulators and physical devices

Scan application (advanced)

Sample File [ ] Browse

Is this sample a malware?
- ( ) Yes
- ( ) No
- ( ) I do not know

Force sample reanalysis [ ]

Are you human?

Antivirus name	Antivirus version	Android platform	Detection method	
Trend Micro, Mobile Security & Antivi	2.6.2	Android 4.1.2	On install	+
AVAST Software, avast! Mobile Security	2.0.3380	Android 4.1.2	On install	✖
AVAST Software, avast! Mobile Security	2.0.3380	Android 4.1.2	On demand	✖
AVAST Software, avast! Mobile Security	2.0.3917	Android 4.1.2	On install	✖

andrototal (beta)

Scan | Results | Admin | Logout

Sample MD5	cbdf63b2e5666799c4b74a8cd15565dd
Sample SHA-1	d9c2bc199769f8e1c817ccd23f1860f5125bdaf6
Sample SHA-256	d11de9bb4d7451ffe7e4b6bd6bab529e7411e3dbe90d468243ef87a5ed98941e
File size	959488 Bytes
First seen on	08 May 2013
Malicious labels	(Android:FakeInst-EO [PUP]). AndroidOS_FakeInst.VTD not a virus Adware.Startapp.origin.5
Package name	com.issghai.thattere
File names	com.issghai.thattere.apk
External analysis	[VirusTotal] [SandDroid]

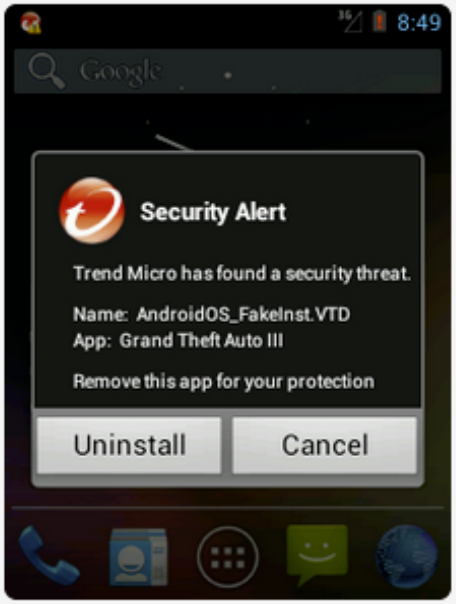
Last 10 scans performed on this sample View all »

Platform	Antivirus Name	Detected name	Date	Results
Android 4.1.2	Doctor Web, Ltd, Dr.Web Anti-virus Light (free) 7.00.3	not a virus Adware.Startapp.origin.5	08/05/13	Full report »
Android 4.1.2	Trend Micro, Mobile Security & Antivirus 2.6.2	AndroidOS_FakeInst.VTD	08/05/13	Full report »
Android 4.1.2	AVAST Software, avast! Mobile Security 2.0.3917	(Android:FakeInst-EO [PUP]).	08/05/13	Full report »
Android 4.1.2	Kaspersky Lab, Kaspersky Mobile Security Lite 9.36.28	No threat detected	08/05/13	Full report »
Android 4.1.2	NortonMobile, Norton Security & Antivirus 3.3.4.970	No threat detected	08/05/13	Full report »

Trend Micro / Mobile Security & Antivirus / 2.6.2 / 2013-05-08 17:07:23 - cbdf63b2e5666799c4b74a8cd15565dd

Mobile Security & Antivirus 2.6.2 scan for cbdf63b2e5666799c4b74a8cd15565dd

Task id	131bd4fe-3bcd-4a72-a207-683ed8eb79f1
Vendor name	Trend Micro
Antivirus name	Mobile Security & Antivirus
Engine version	2.6.2
Analysis started on	08/05/2013 at 17:05
Analysis completed on	08/05/2013 at 17:07 (took *91* seconds)
Detection method	On install
Analysis result	AndroidOS_FakeInst.VTD
Sample md5	cbdf63b2e5666799c4b74a8cd15565dd



Logcat dump (download)

```
99.  I/tmms-vsapi-jni(  674): VSReadVirusPattern OK. Action successful.
100. I/tmms-vsapi-jni(  674): OK. VSSetProcessAllFileInArcFlag. oldValue = ret = 0.
101. I/tmms-vsapi-jni(  674): OK. VSSetExpandLiteFlag. oldValue = ret = 1.
102. I/tmms-vsapi-jni(  674): OK. VSSetProcessAllFileFlag. oldValue = ret = 0.
103. I/tmms-vsapi-jni(  674): OK. VSSetCleanZipFlag. oldValue = ret = 0.
104. I/tmms-vsapi-jni(  674): OK. VSSetCleanBackupFlag. oldValue = ret = 0.
105. I/tmms-vsapi-jni(  674): VSGetDetectableVirusNumber virus in patter num = 3283
106. I/tmms-vsapi-jni(  674): filename = /data/data/com.trendmicro.tmmspersonal/Library/pattern/msvpnaos.457
107. I/tmms-vsapi-jni(  674): InternalVer = 145700, PtnVer = 457.
108. D/PrepareVSAPI4RTScan(  674): before tmmsAntiMalwareJni4RTScan.init()!
109. I/tmms-vsapi-jni(  674): VSInit OK!
110. D/PrepareVSAPI4RTScan(  674): after tmmsAntiMalwareJni4RTScan.init()!
111. I/tmms-vsapi-jni(  674): in vsSetPatternPath, vc = 711579352
112. I/tmms-vsapi-jni(  674): Current pattern path is : /etc/iscan
113. I/tmms-vsapi-jni(  674): Pattern path is set to : /data/data/com.trendmicro.tmmspersonal/Library/pattern
114. I/tmms-vsapi-jni(  674): Pattern file(s) successfully deleted.
115. I/tmms-vsapi-jni(  674): in vsLoadPattern, vc = 711579352, sharedVC = 708085592, scanType =
116. I/tmms-vsapi-jni(  674): vsLoadPattern patternPath = /data/data/com.trendmicro.tmmspersonal/Library/pattern.
```

Writing tests ~~is~~ was tedious

We have abstracted away the low level details, so that we can focus on the important things: *extracting the results*.

Test Recipe (on-install detection)

```
#andrototal-adapters/ComZonerAndroidAntivirus.py
class TestSuite(base.BaseTestSuite):
  def on_install_detection(self, sample_path):
    self.pilot.install_package(sample_path)

    if self.pilot.wait_for_activity(
        "com.zoner.android.antivirus_common.ActScanResults", 10):

      result = self.pilot.get_view_by_id("scaninfected_row_virus")
    else:
      result = False
```

Test Recipe (on-demand detection)

```
#...
def on_demand_detection(self, sample_path):
  self.pilot.install_package(sample_path)
  self.pilot.start_activity("com.zoner.android.antivirus", ".ActMain")
  self.pilot.wait_for_activity("com.zoner.android.antivirus.ActMain")

  self.pilot.tap_on_coordinates(120, 130)
  self.pilot.wait_for_activity("com.zoner.android.antivirus.ActMalware")

  # start scan
  self.pilot.tap_on_coordinates(120, 80)
  self.pilot.wait_for_activity(
    "com.zoner.android.antivirus_common.ActScanResults")

  self.pilot.refre dsh()
# ...
```

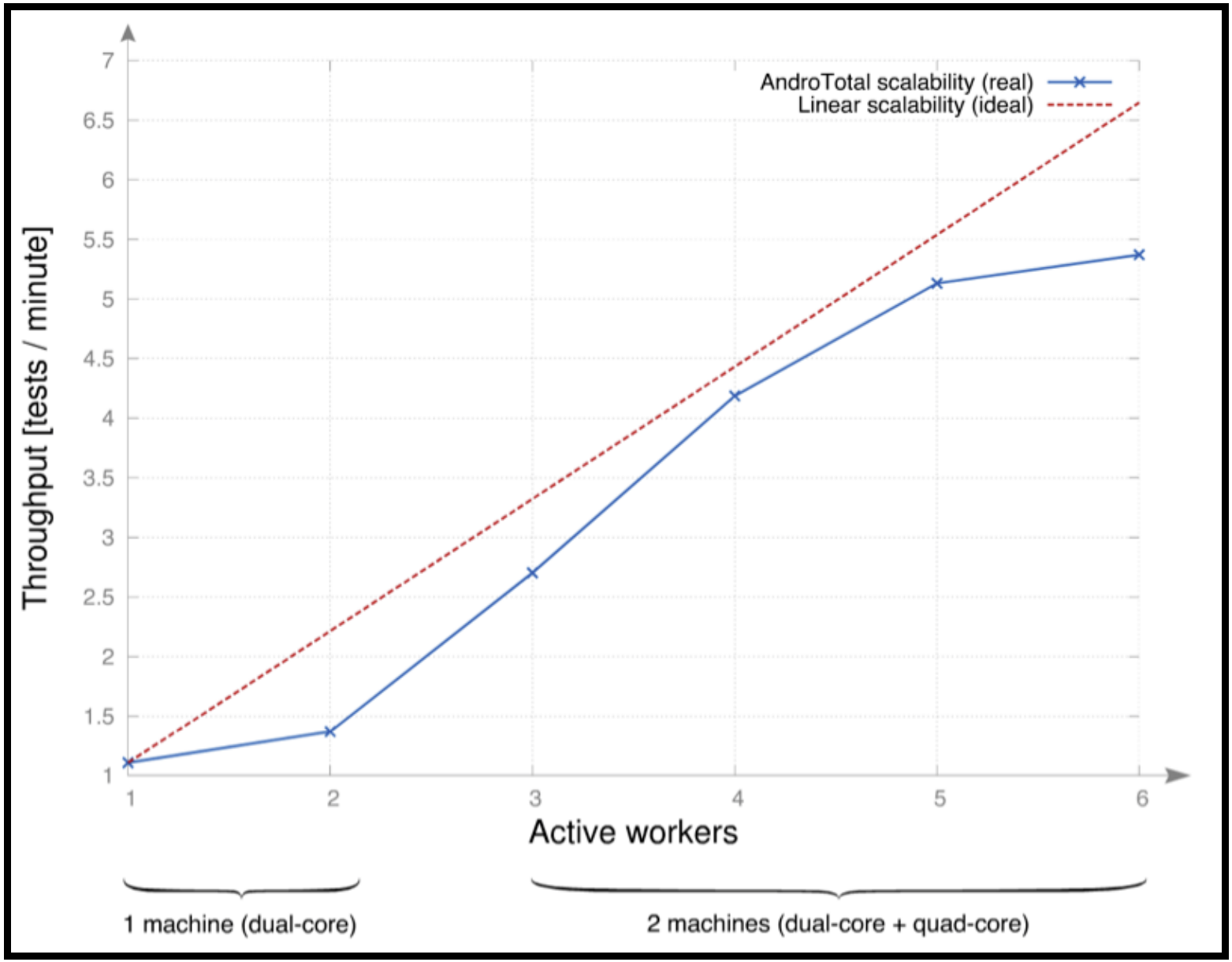
Workflow

1. Retrieve a suspicious APK
2. Choose parameters
   - Android version(s)
   - List of antimalware product and versions
3. Pull clean image(s) from repository
4. Instantiate one test per combination of
   - Android version
   - Product version
5. Enqueue test instances

Architecture

- Web frontend
- Repository of clean Android images
- Asynchronous task dispatcher
- Distributed workers

Scalability



1. Threats and protections

2. Limitations

3. Evaluating antimalware

4. AndroTotal

5. Status

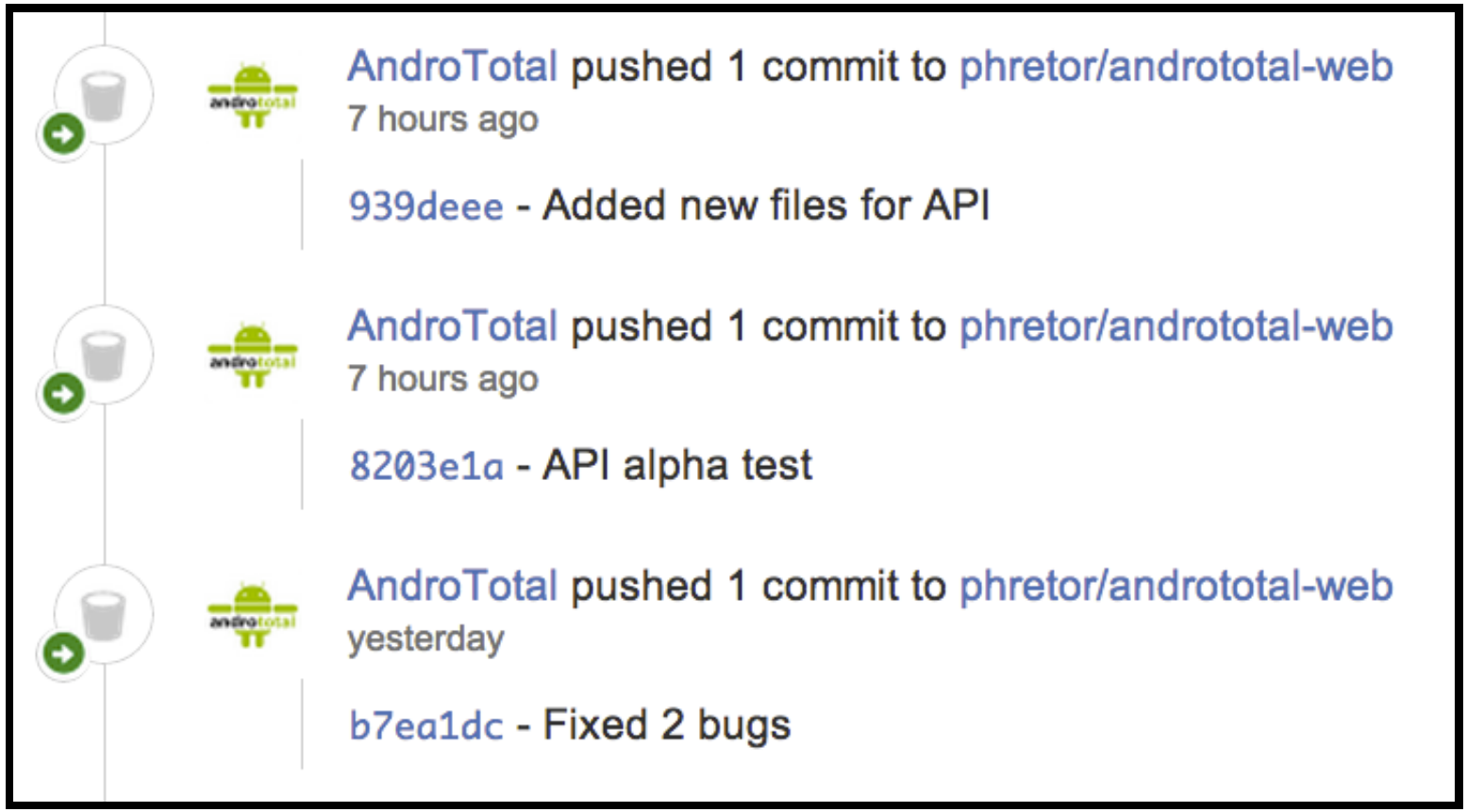
Numbers

- 455 users subscribed in less than a month
- 13 antimalware vendors supported (not all public)
- 16 products overall (not all public)
- 1,465 distinct samples submitted so far

Future Work

- Write a paper :)
- Compare labels and detection results with VirusTotal.com
- Incorporate code-mutation modules
- Add more cores and scale
- ~~Finish the API (only sample sharing is supported as of now)~~
- Deploy on ARM boards and monitor power consumption

7 hours ago...


AndroTotal pushed 1 commit to phretor/andrototal-web
7 hours ago
939deee - Added new files for API
AndroTotal pushed 1 commit to phretor/andrototal-web
7 hours ago
8203e1a - API alpha test
AndroTotal pushed 1 commit to phretor/andrototal-web
yesterday
b7ea1dc - Fixed 2 bugs

Other Ongoing Work on Android Malware Analysis

- PLASMA - Android framework instrumented for malware dynamic analysis
- PuppetDroid - increasing code coverage of "corner cases" in dynamic analysis through semi-automatic UI stimulation
- MoBucket (Mobile Malware Bucket) - consolidated dataset of mobile malware

Thank you!

Questions?

Try it now at **andrototal.org**!

fede@maggi.cc

Extra Slides

Android Popularity