Device Monitor for Android

Detecting botnets in mobile environment

Aleš Černivec, XLAB Research
ales.cernivec@xlab.si

Internet Security Days 2014, Brühl, Germany

XLAB d.o.o. / Pot za Brdom 100 / SI-1000 Ljubljana / Slovenia
tel. +386 1 244 77 50 / fax +386 1 244 77 70 / e-mail: info@xlab.si
www.xlab.si

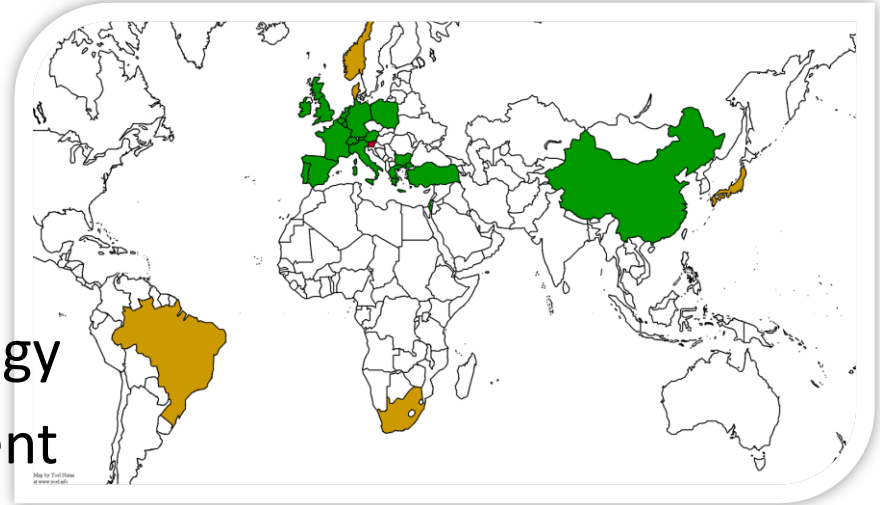
The agenda

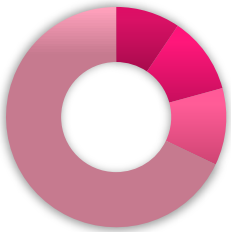
- Introduction
  - XLAB, ACDC
- Android malware
  - exploits
- Device Monitor
  - Features
  - Infrastructure
- DEMO

Introduction – about the company

XLAB

- Founded in 2001
- Strong research base
- Cloud services, cloud technology
- Mobile application development
- Application level security, best practices
- Security on mobile devices





PhD

MsC

Post graduate students

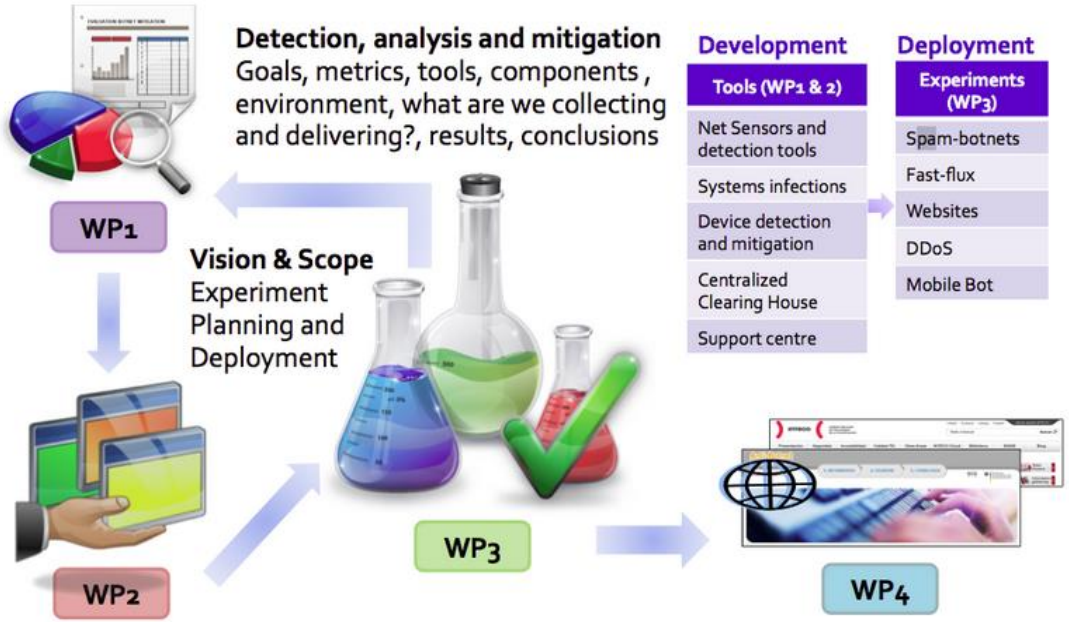
BsC

Univerza v Ljubljani

Institut "Jožef Stefan" Ljubljana, Slovenija

Advanced Cyber Defence Centre

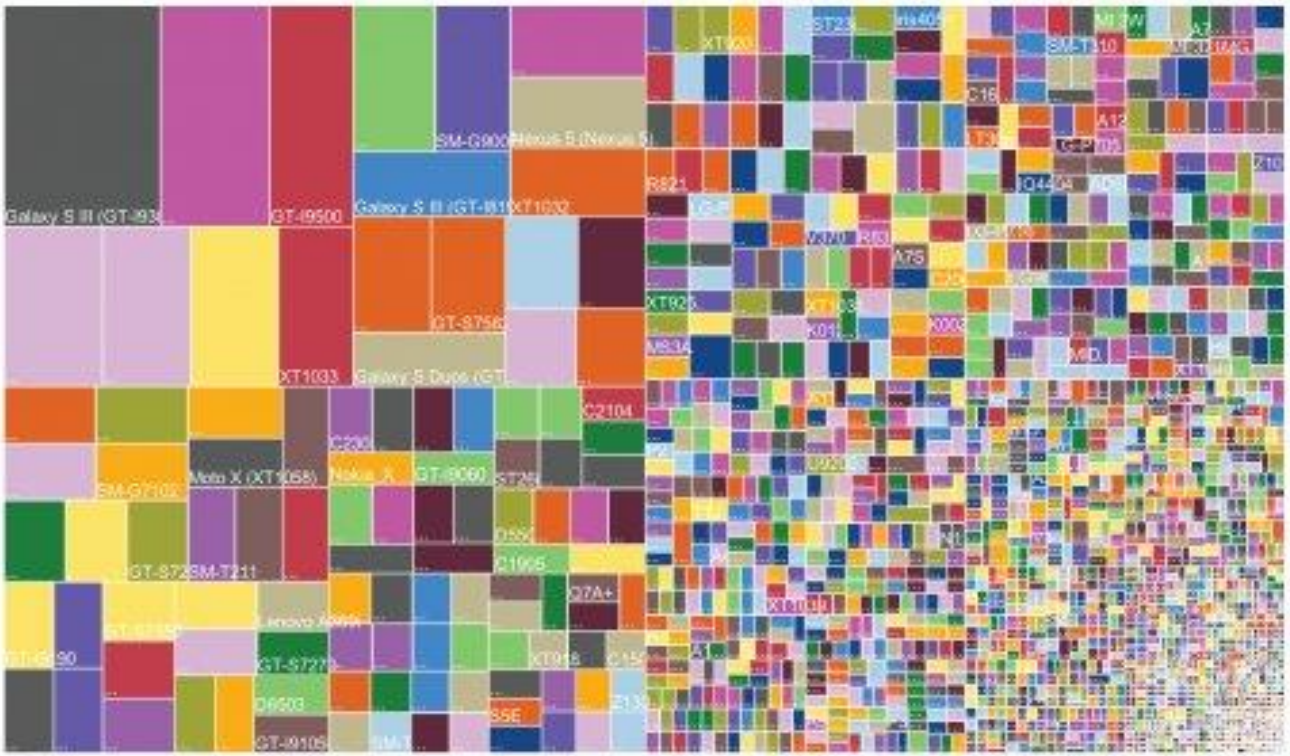
- CIP-PSP
- 28 partners
- 01/02/2013 to 31/07/2015 (30m)



http://www.acdc-project.eu/?page_id=48

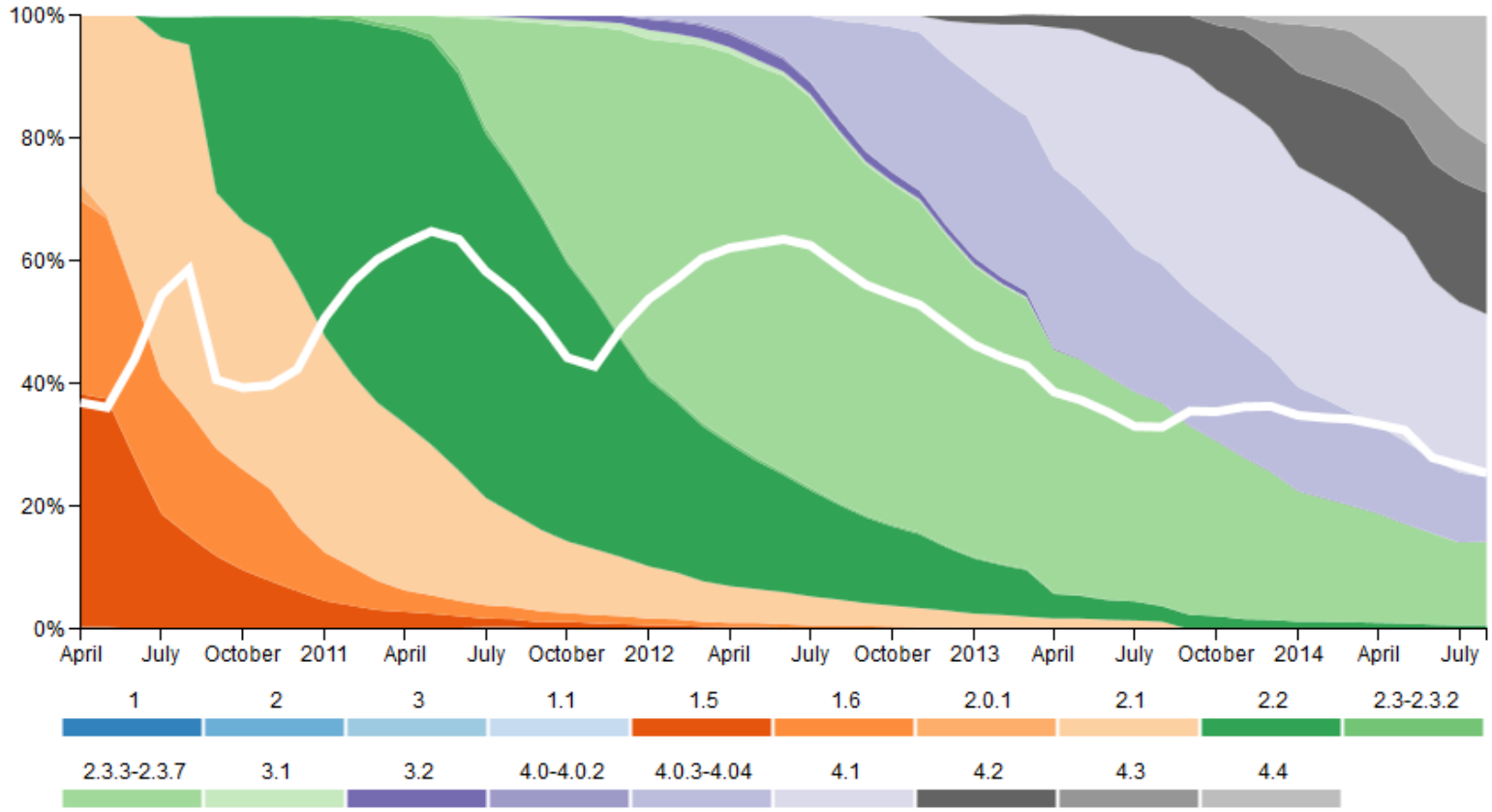
Android: malware on mobile devices?

- It exists, but...device/API fragmentation



By OpenSignal

Android API fragmentation



By OpenSignal

Mobile botnets?

Core Security
@CoreSecurity

#Botnet tactics are now targeting #mobile de
zd.net/1fGVgYq via @ZDNetCharlie @ZDNet

11:13 PM - 26 Feb 2014

5

Virus Bulletin
@virusbtn

Android malware that uses Tor for C&C communication might be 'Slempo', a vari
'Stoned Cat' botnet
blog.malwarebytes.org/mobile-2/2014/...

12:42 PM - 26 Feb 2014

Jóseph Mlodzìanowskì
@cedoxX

Mobile Botnet has been found on 23,856 A
compromised smartphones in all..... bit.ly/1iYUrwL

7:53 AM - 11 Jan 2014

1 RETWEET

David Clarke
@1DavidClarke

Follow

#mobilesecurty Large scale Android Mobile Botnet Hijacking Discovered | @scoopit ow.ly/rZtHj

9:30 PM - 22 Dec 2013

Large scale Android Mobile Botnet Hijacking Dis...

Researchers at FireEye revealed the menace today, describing MisoSMS as "one of the largest advanced mobile botnets to date" and warning that it is being utilized in more than 60 malware campaigns.

Scoop.it @scoopit

Building a mobile botnet

- Choose a device model, API version
  - 4.2
- Find weaknesses
  - Master-key, SMS hijack
- Use them to infiltrate the code
  - Drive-by-download
- Run the code „in stealth mode“
  - Commands
  - CC communication
- You could potentially control at least 20% of Android devices

Known exploits

- Master-key
  - Pretend to be A but installing the app as B
  - Repackage the application with different source
- Fake ID
  - A security hole within the OS‘ libraries
  - Internet browser‘s plugins
- SMS hijacks
  - app capable of discarding SMS messages BEFORE user gets the notification

Introduction – Device Monitor

- Mobile application - sensor
- Detection
  - Outgoing connections to malicious resources
  - Detection of SMS hijacking
- Application scanning
  - Classification based on app's permissions
  - Master-key, Fake ID
- Prevention to access known malicious resouces
  - Dedicated, corporate networks

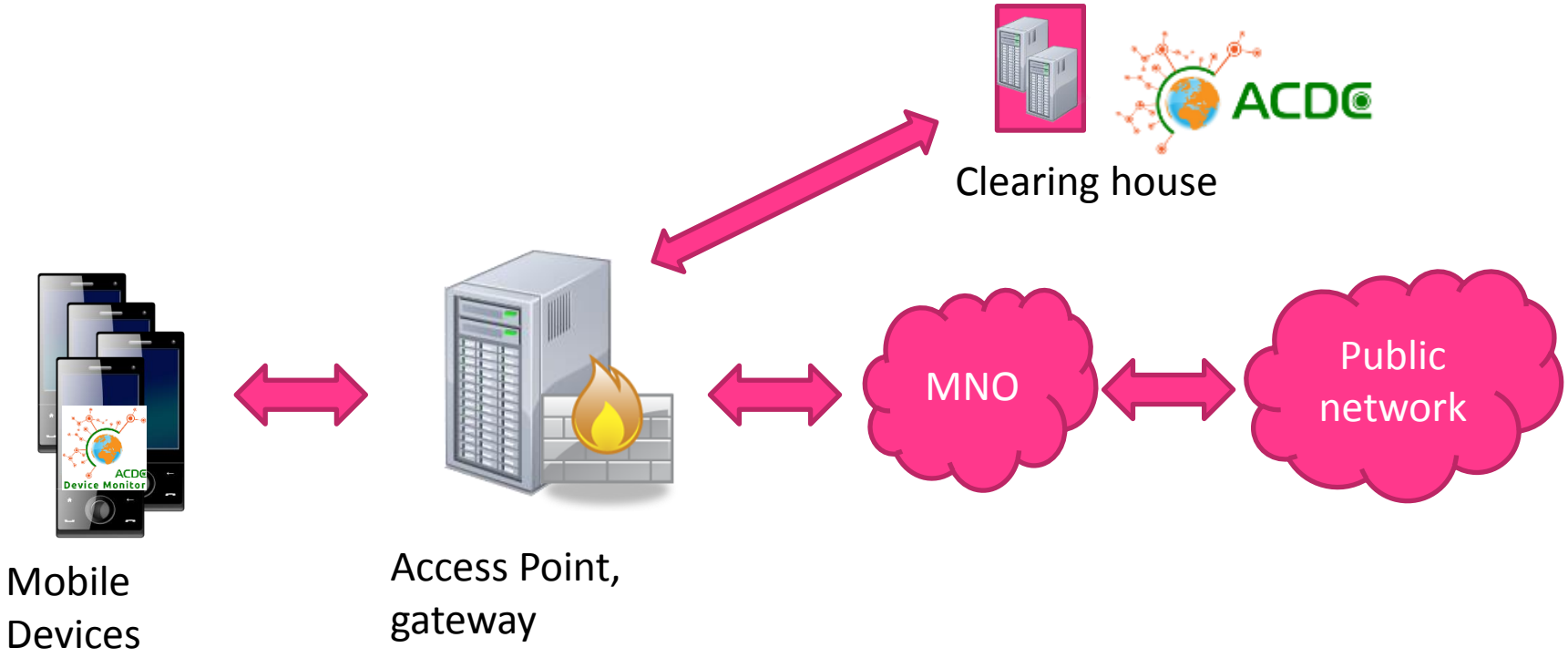
Device Monitor cont.

- Notifies the user and central server when
  - Detected malware is installed
  - Connecting to potential malicious end-points
- Dedicated infrastructure for data aggregation
- Notifies the user about suspicious events (logs)

Device Monitor features

- Network sensor on mobile device queries **GCMServer** for
  - URL status
  - list of rogue IPs which is provided by **Suricata IDS**
  - Sync detections
- On Wi-Fi networks:
  - Email clients:
    - ✓ rogue URLs can be **recognized** and **access prevented** (DEMO)
  - Other applications:
    - ✓ rogue destination IPs are **recognized** when connection is made (DEMO)
    - ✓ Connections can be dropped if so configured on the Suricata IDS
- On Mobile networks:
  - Email clients:
    - ✓ rogue URLs can be **recognized** and **access prevented** (DEMO)
  - Other applications:
    - ⊗ rogue destination IPs **cannot be recognized nor access prevented** when connection is made since mobile provider's proxy is visible as destination IP

Infrastructure

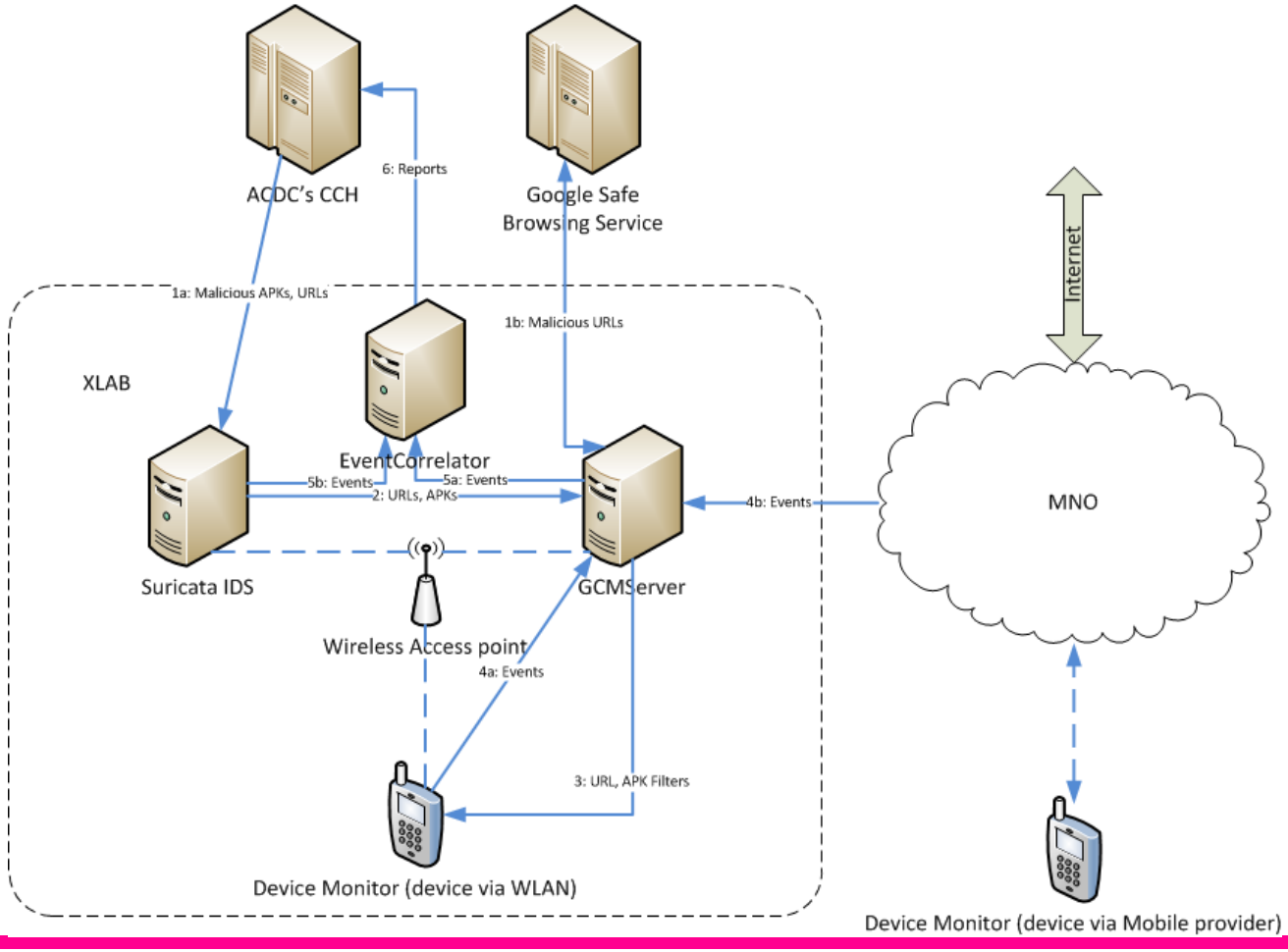


Infrastructure cont.

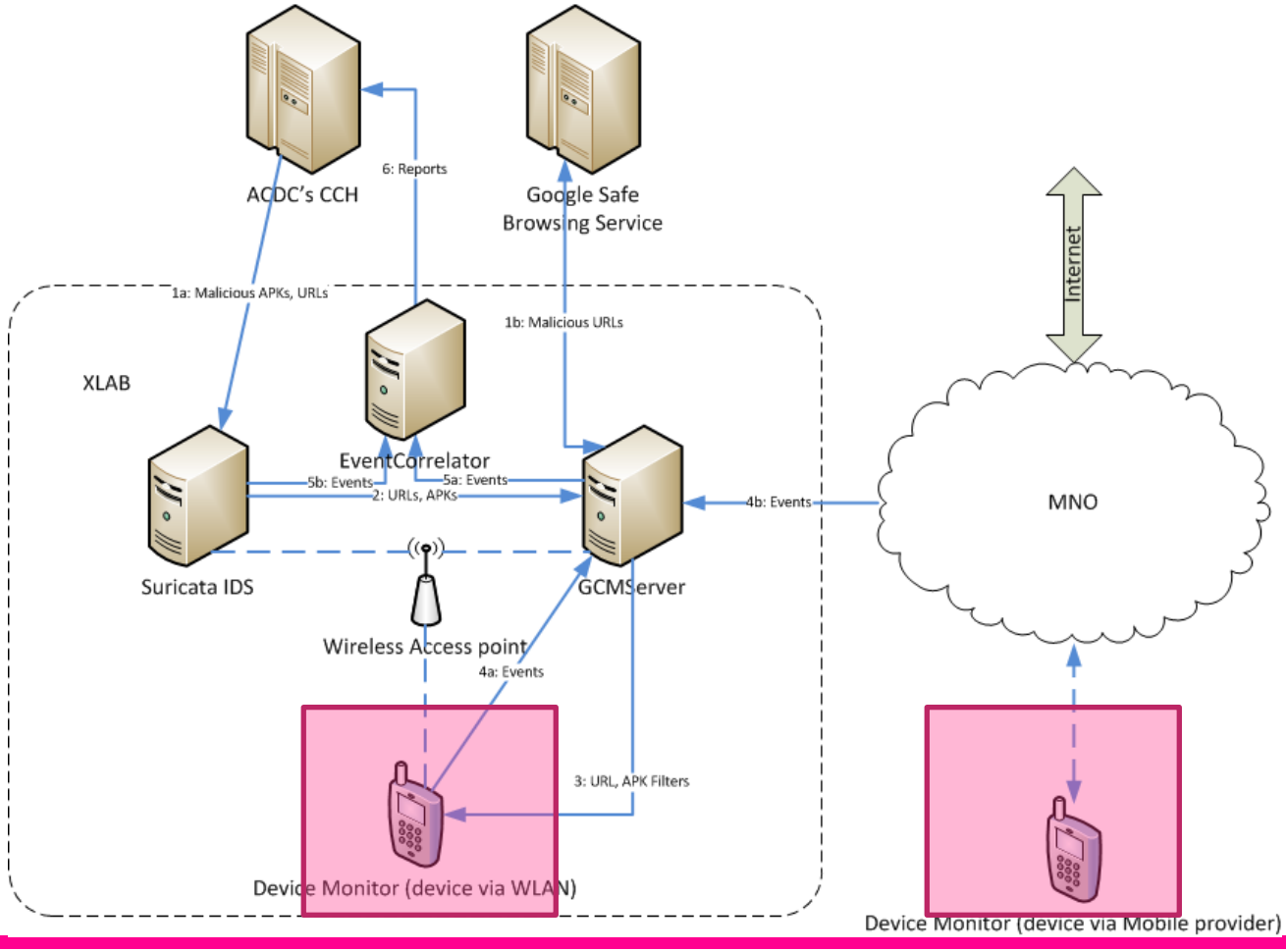
Infrastructure consists of

- Mobile agents
  - Device Monitor
- IDS
  - Suricata
- Analytics
  - EventCorrelator
- Message bus
  - GCMServer, RabbitMQ server

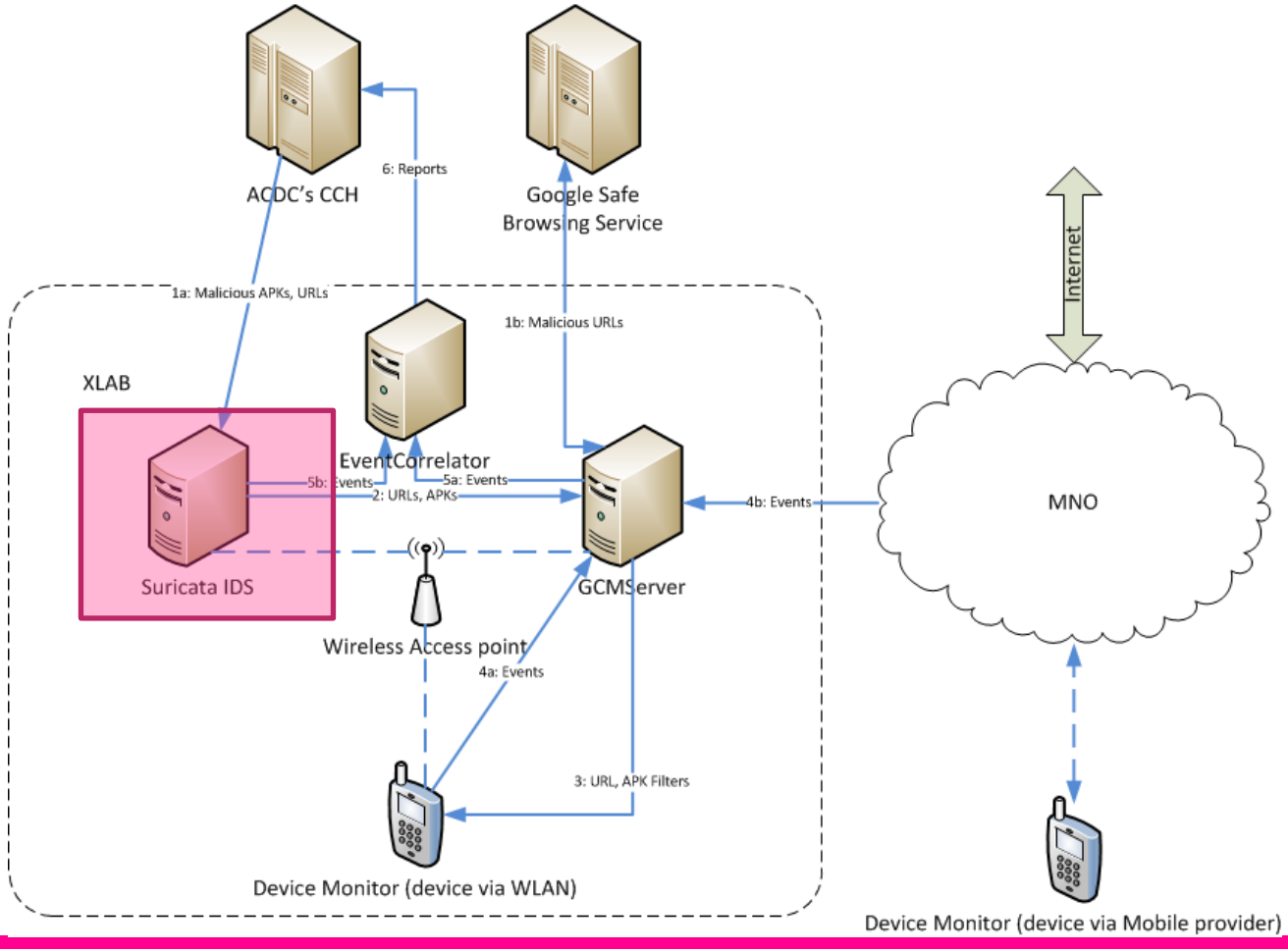
Infrastructure cont.



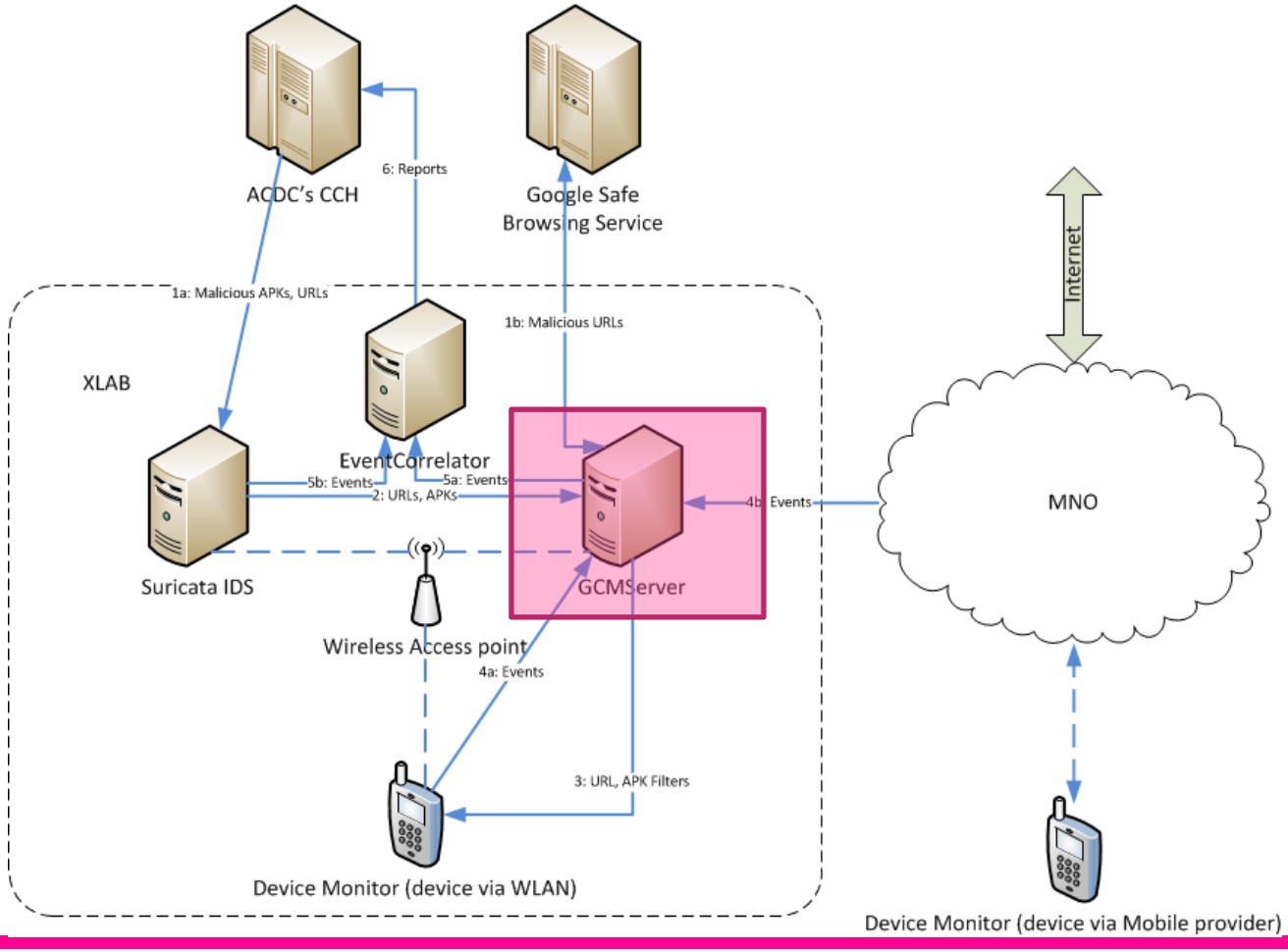
Infrastructure cont.



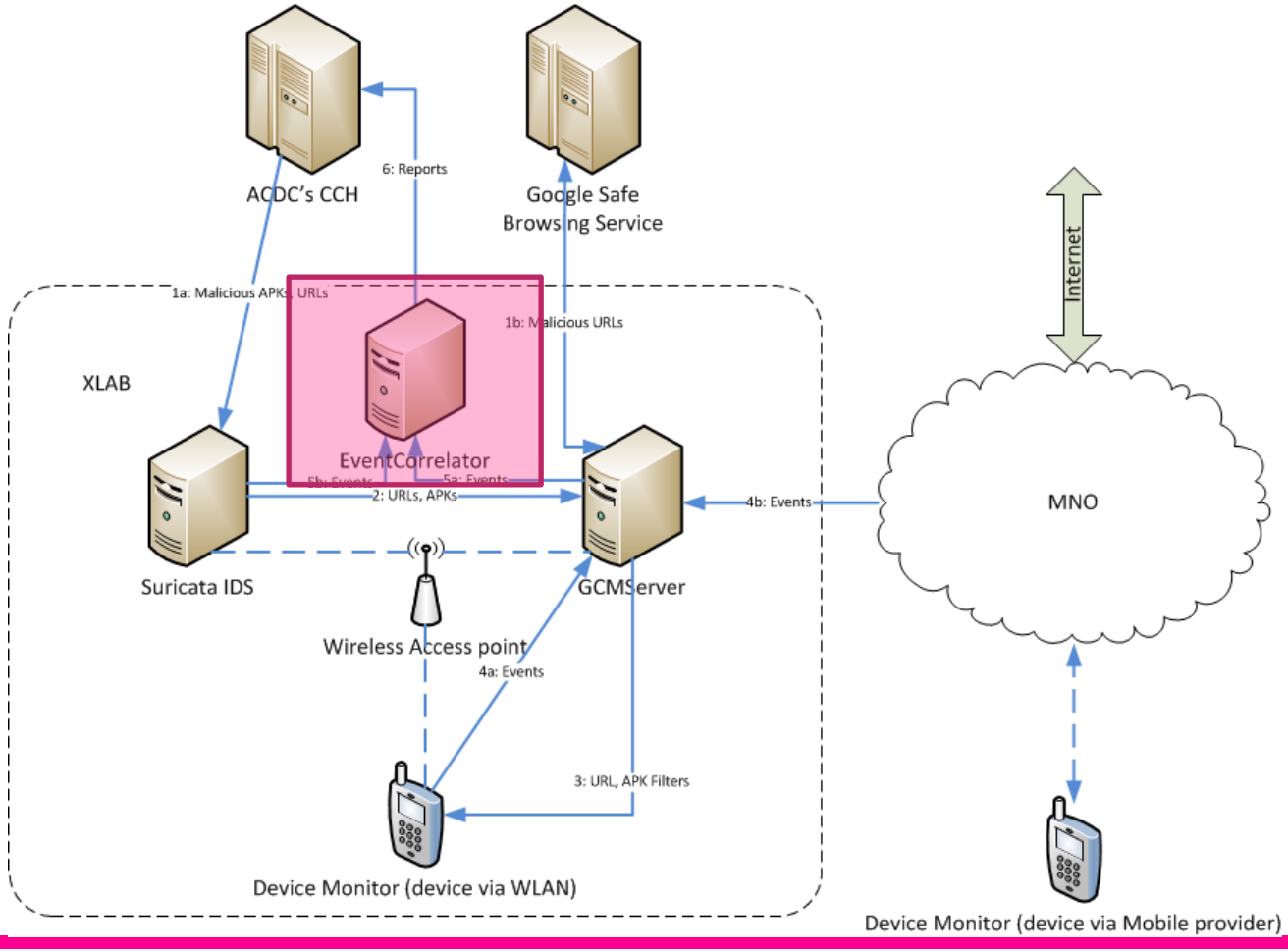
Infrastructure cont.



Infrastructure cont.



Infrastructure cont.



Device Monitor features recap

What can be detected within MNOs or dedicated network (AP) with Device Monitor?

	App classification	SMS hijack	Master-key	Fake ID	UrlBrowse	Suspicious connection	Prevention to access
MNO							
Wireless AP							

Available on Google Play Store

- https://play.google.com/store/apps/details?id=eu.acdc.xlab.devicemonitor


PRESENTATION'S OVER
Device Monitor
• URLCheck
• Suspicious connections
• SMS hijack
• Master Key and Fake ID exploits
IT'S DEMO TIME!
memegenerator.net

Thanks!

Questions?

Acknowledgements

Advanced Cyber Defence Center