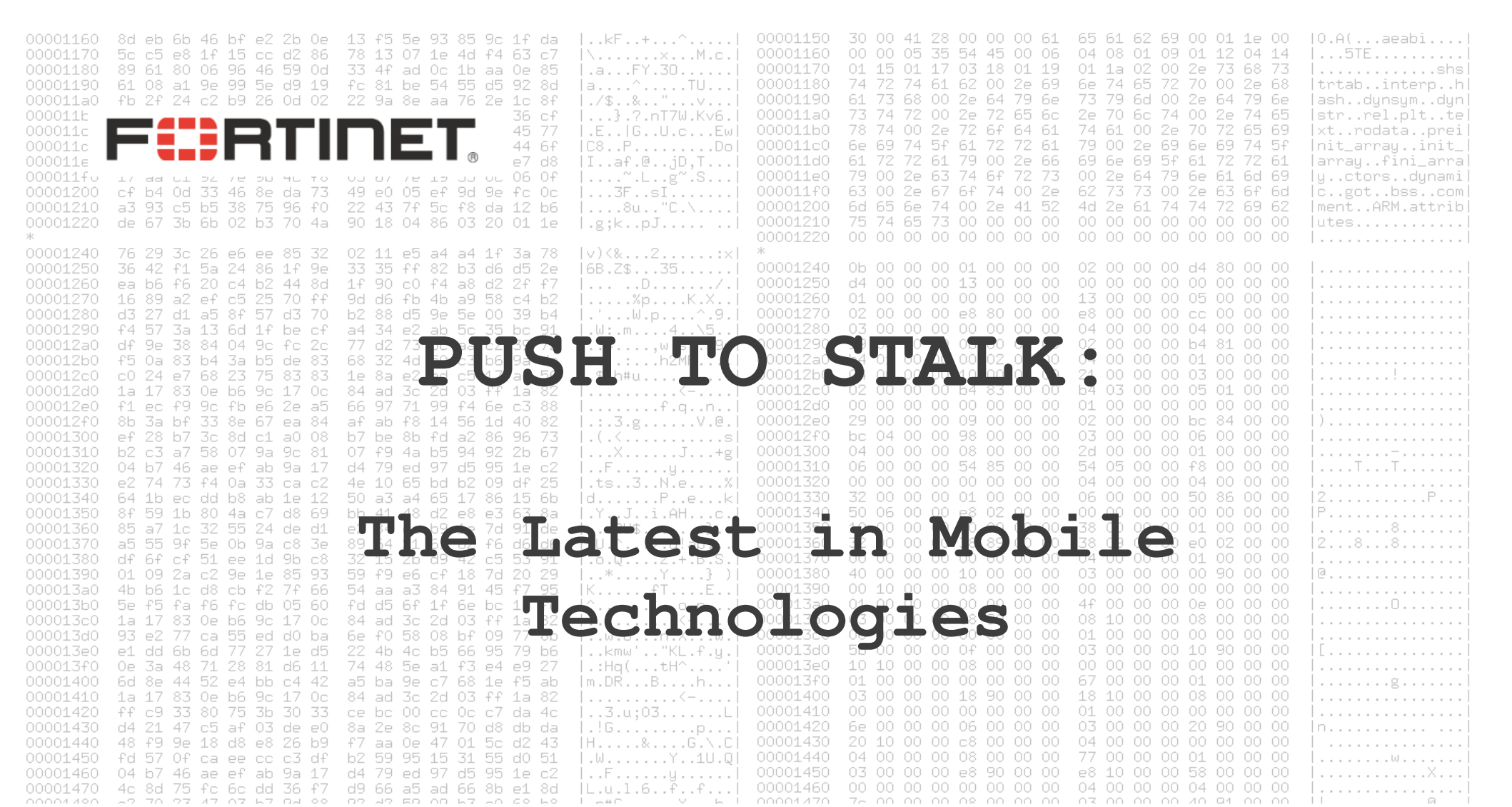


PUSH TO STALK: The Latest in Mobile Technologies

Ruchna NIGAM - AV Analyst/Researcher, Fortinet

European Forum AlpBach 2013

TODAY'S AGENDA :

- Is Mobile Malware Really an Issue?
- Evolution of Mobile Malware
- Motivations
- Attack Vectors
- Rewards
- Updates from 2013
- AndroRat Live Demo : Since Seeing is Believing

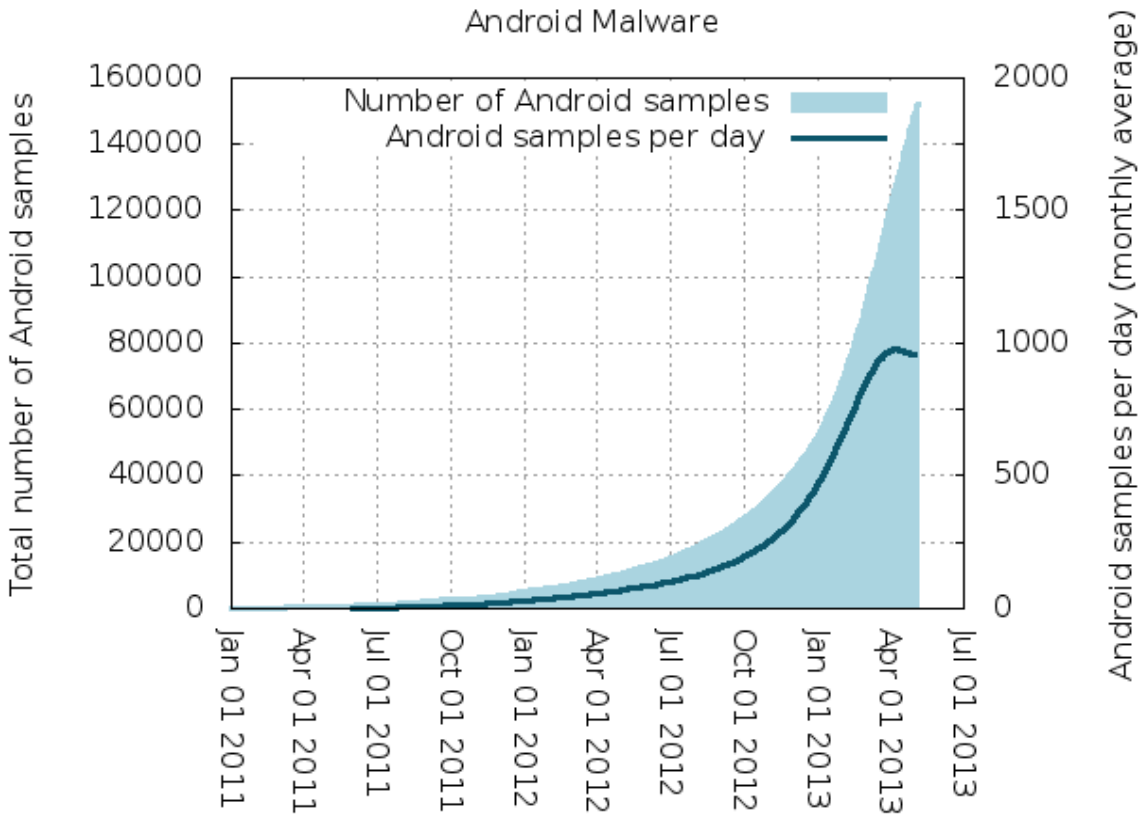
Ques: Is Mobile Malware Really an Issue?

- Answer : Yes!
- Not just an excuse to make presentations, supported with concrete statistics.
  - 15,000 signatures for mobile devices
  - ~98% of total mobile malware is for Android devices
  - Top 5 Mobile Malware on monthly Virus Watch List

    http://www.fortiguard.com/antivirus/

Evolution of Mobile Malware

- **2004–2010:**
  Symbian OS
- **2009:**
  First iPhone malware discovered
- **Post 2010:**
  Steep rise in Android malware



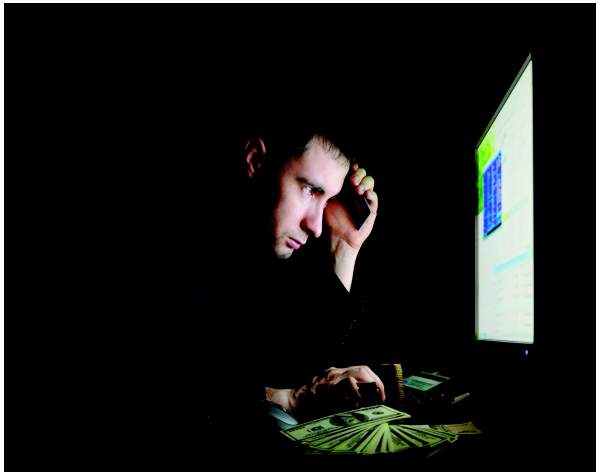
Over 150,000 Android malware @ 1,000 samples per day

Why Android?

- **Widespread** : Windows of the mobile world
- **79% Market Share** in Q2 2013
- **Several 'App Stores'** : Possibility to bypass Android Market Verification
- **SIMPLICITY** of programming : Boon that comes at a heavy price

Motivations:
The Advantages of Attacking a Mobile Phone

- **SMARTphones** – An attacker's dream come true
  - Stays with victim at most times
  - Permanently connected to the internet (in most cases)
- **Perfect Spying Device**
  - Camera
  - Microphone
  - GPS
  - Emails
  - Social Networks
  - SMS messages



Attack Vectors:

How do I get a victim to install my application?

- **Trojans** : Nothing as it seems
  - Banking Application
  - Popular Games
  - **Fake Anti-Virus**
  - Wallpaper Applications
- **Links** on websites that download packages
  Victim still needs to install
- **NEW! Targeted Attack** : Android package as attachment to an email

REWARDS !

- **MONETARY**
  - **SIMPLE**
    - **Premium SMS messages**
    - Eg : Android/FakeMart – 17,000 victims in France, losses of ~500,000 euros
  - **ADVANCED**
    - **mTAN Stealing**
    - Eg : Zitmo, Spitmo
    - Used with PC malware – **Zeus**, **SpyEye**
    - Authorize bank transfers of thousands of euros
- **DATA STEALING**

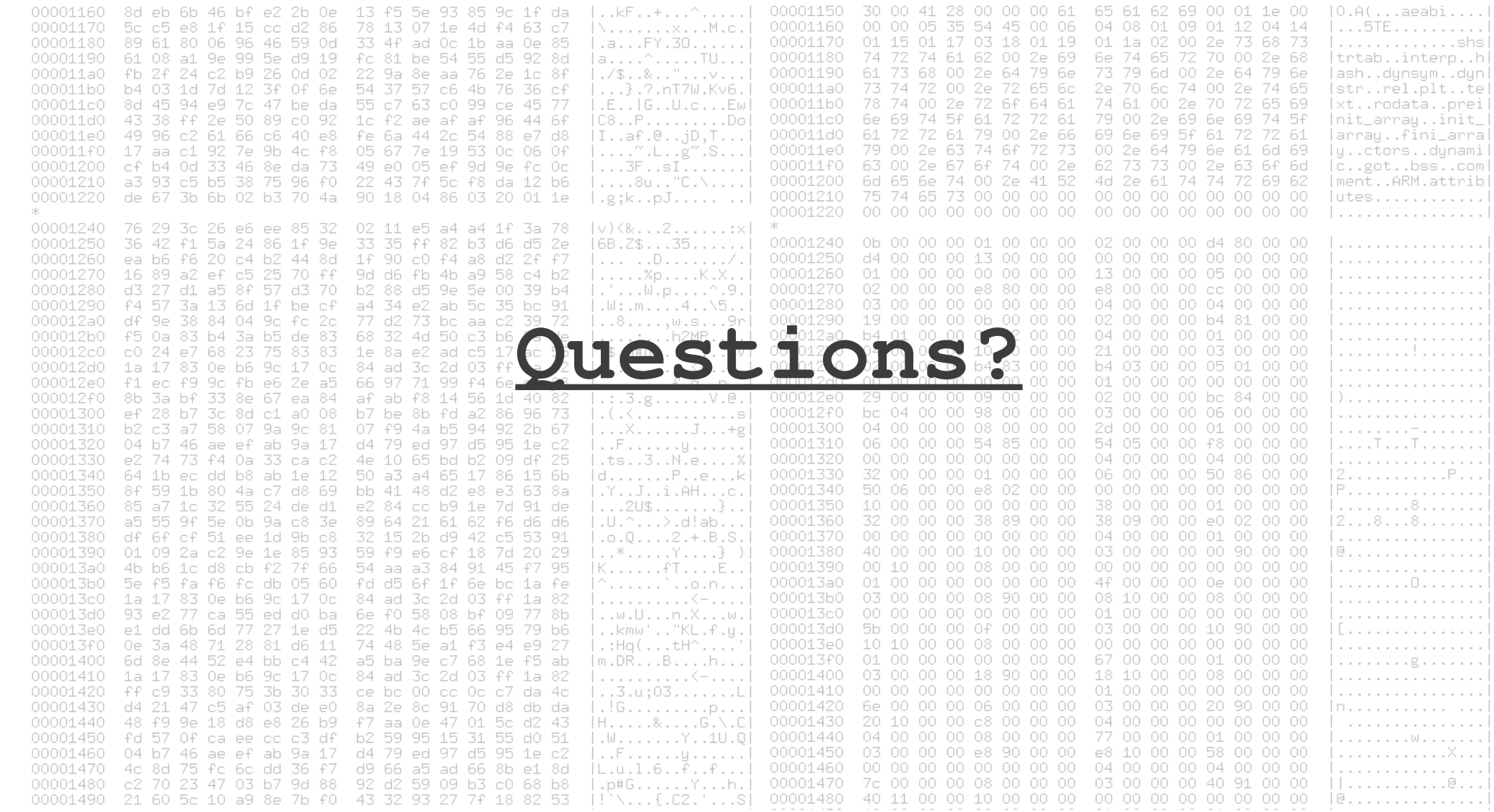
Updates from 2013

- **FEBRUARY > First PC infector : Android/Claco.A!tr**
- **MARCH > First Targeted Attack : Android/Chuli.A!tr.spy**
  - Sent to Tibetan activists as email attachment
  - Sends SMS, Contact and Location information from infected phone to the attacker
- **APRIL > Android/BadNews.A!tr.dldr**
  - Botnet
  - Infected around **9 million** devices
- **JULY > First Ransomware : Android/FakeDefend.A!tr**
  - Poses as an Anti-Virus application
  - Renders phone useless
  - Victim's Credit Card Details sent to attacker in Plain Text
  - **Fraud ransomware** – Phone not restored even after payment

AndroRat Live Demo:

Since Seeing is Believing

http://www.youtube.com/watch?v=aVx8ntyr-yk


Questions?

Thank you!

Contact:

rnigam[at]fortinet[dot]com

http://blog.fortinet.com

Twitter : @FortiGuardLabs