black hat®

MOBILE SECURITY SUMMIT
LONDON 2015

Mobile Malware Network View

Kevin McNamee : Alcatel-Lucent

JUNE 16 – 18, 2015
EXCEL LONDON | LONDON, UK
WWW.BLACKHAT.COM

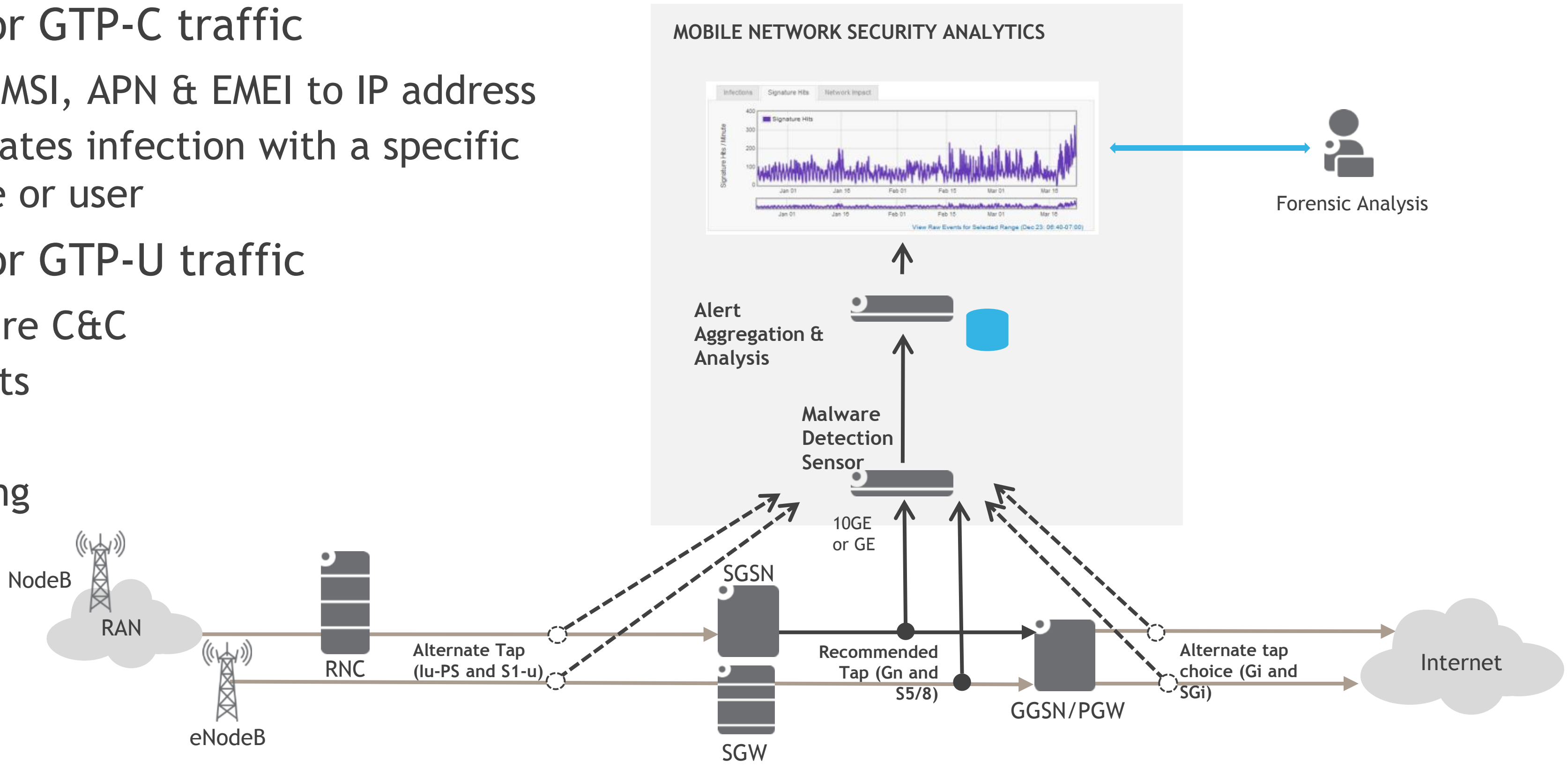
UBM

Agenda

- Introduction
- How the data is collected
- Lies, Damn Lies and Statistics
- Windows PC Malware
- Android Malware
- Network Impact
- Examples of malware
- DDOS

Monitoring the Mobile Network

- Monitor GTP-C traffic
  - Maps IMSI, APN & EMEI to IP address
  - Associates infection with a specific device or user
- Monitor GTP-U traffic
  - Malware C&C
  - Exploits
  - DDOS
  - Hacking



MOBILE NETWORK SECURITY ANALYTICS

Forensic Analysis

Alert Aggregation & Analysis

Malware Detection Sensor

10GE or GE

NodeB

RAN

eNodeB

RNC

Alternate Tap (Iu-PS and S1-u)

SGSN

SGW

Recommended Tap (Gn and S5/8)

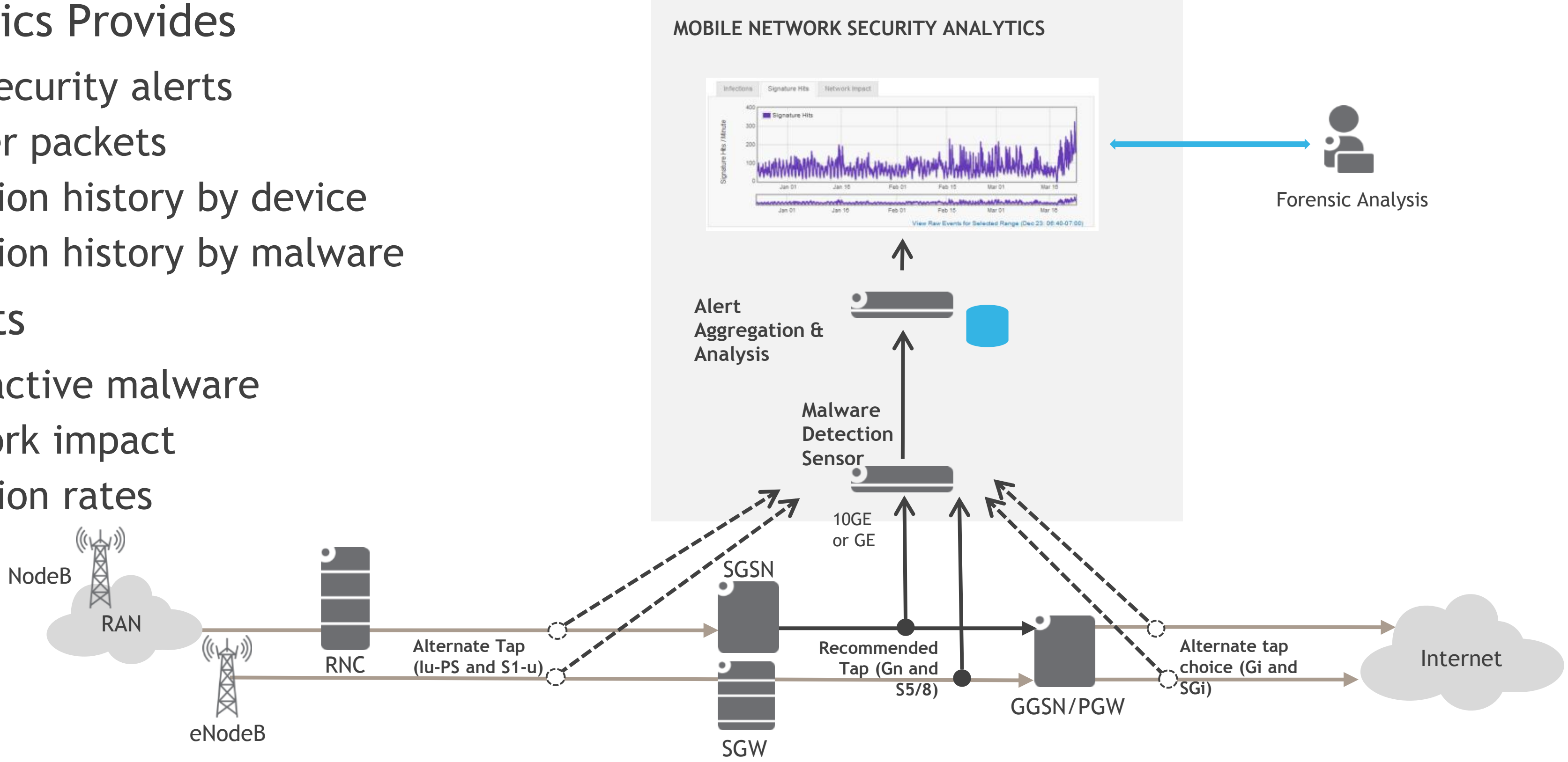
GGSN/PGW

Alternate tap choice (Gi and SGi)

Internet

Monitoring the Mobile Network

- Analytics Provides
  - Raw security alerts
  - Trigger packets
  - Infection history by device
  - Infection history by malware
- Reports
  - Most active malware
  - Network impact
  - Infection rates



MOBILE NETWORK SECURITY ANALYTICS

Forensic Analysis

Alert Aggregation & Analysis

Malware Detection Sensor

10GE or GE

NodeB

RAN

eNodeB

RNC

Alternate Tap (Iu-PS and S1-u)

SGSN

SGW

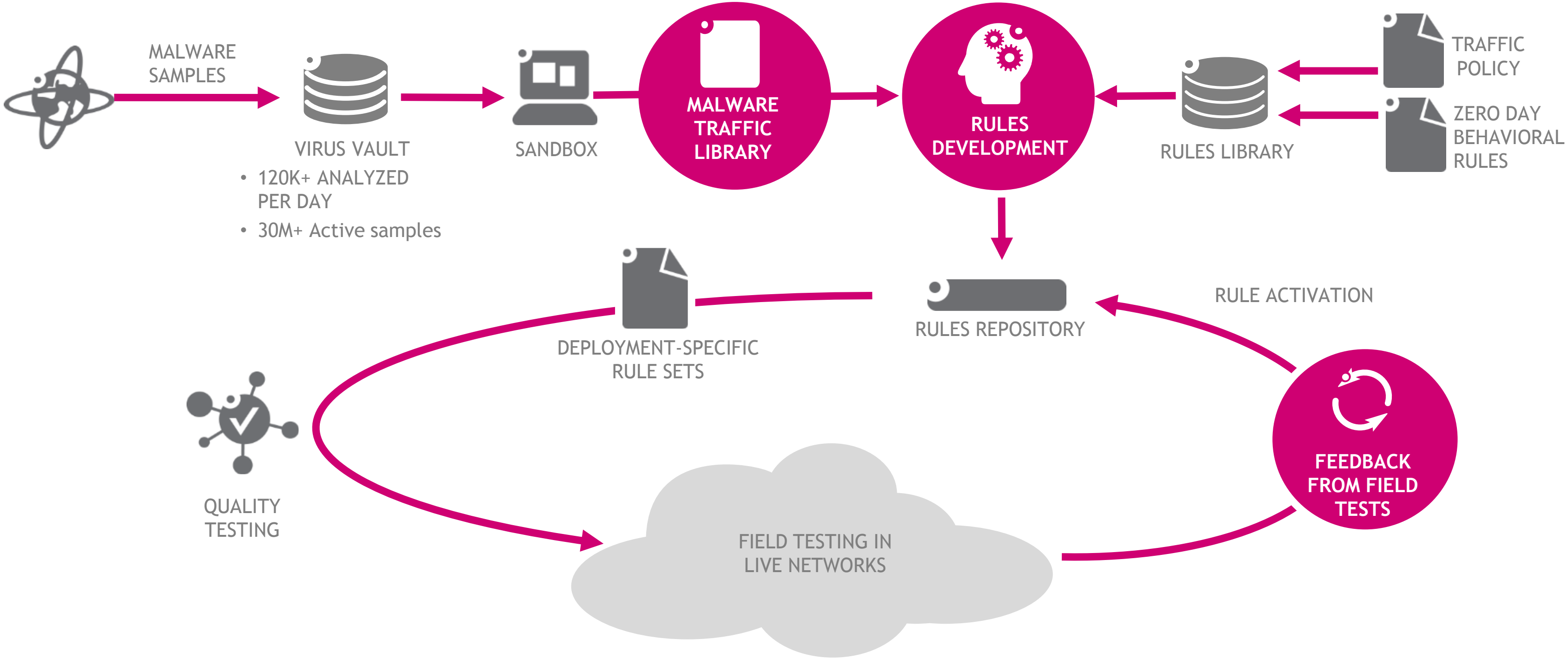
Recommended Tap (Gn and S5/8)

GGSN/PGW

Alternate tap choice (Gi and SGi)

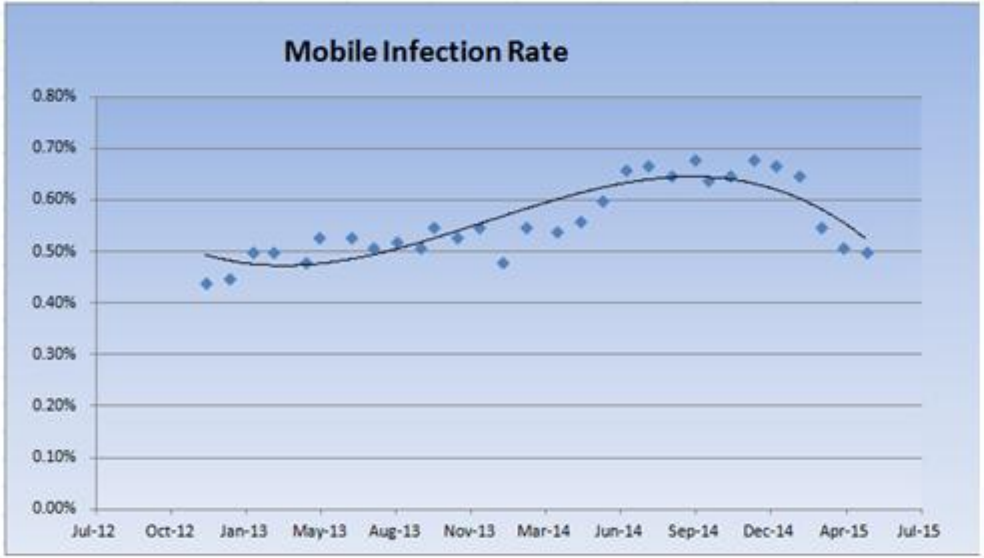
Internet

Detection Rules Development Process



- 120K+ ANALYZED PER DAY
- 30M+ Active samples

Infection Rate

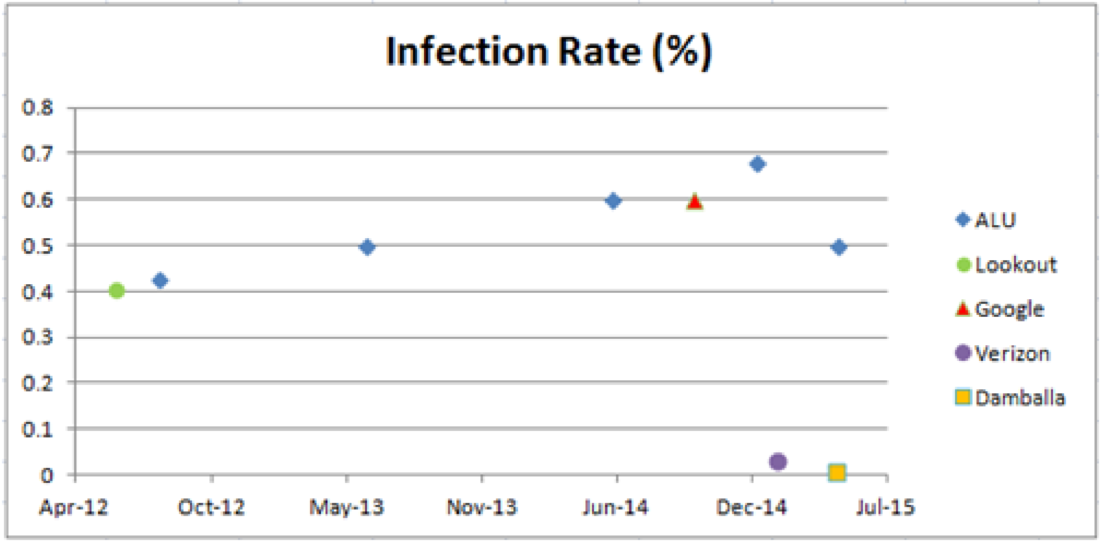


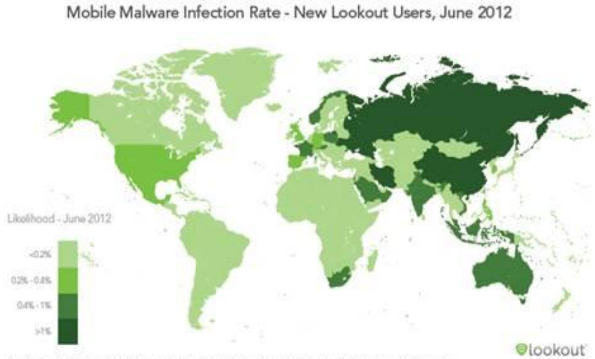
- C&C detection measures **actual infections** as seen from the network
- **Problem is growing** (by 25% in 2014)
- LTE device **5 times more likely to be infected**

However…

Estimates of Mobile Malware infection rates vary wildly

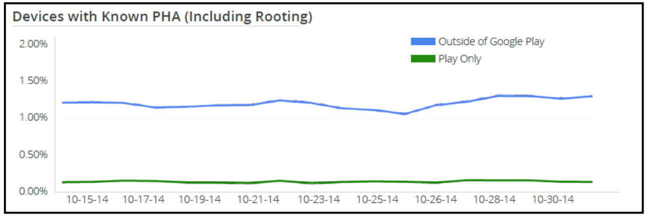
- ALU, Lookout & Google report 0.4% to 0.6%
- Verizon Breach Report quoted 0.03%
- Damballa quoted 0.0064% at RSA.





Mobile Malware Infection Rate - New Lookout Users, June 2012
Likelihood - June 2012
<0.2%
0.2%-0.4%
0.4%-1%
>1%
lookout

FIGURE 5: MOBILE MALWARE INFECTION RATE – NEW LOOKOUT USERS, JUNE 2012



Google: *"… US English devices have a PHA (potentially harmful app) installed on about 0.4% of devices, which is about 0.2% below the worldwide average."*

Source: Google Report – Android Security 2014 Year in Review

Also… Watch out for bad reporting in the press

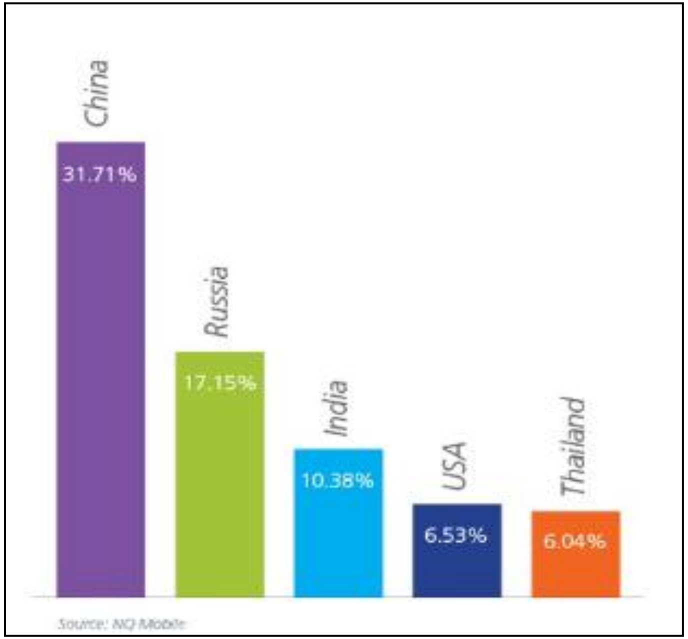
Slight change in word order makes a huge difference:

What was said:

“31.7% of infected devices are in China”

What was reported in the press:

“31.7% of devices in China are infected”

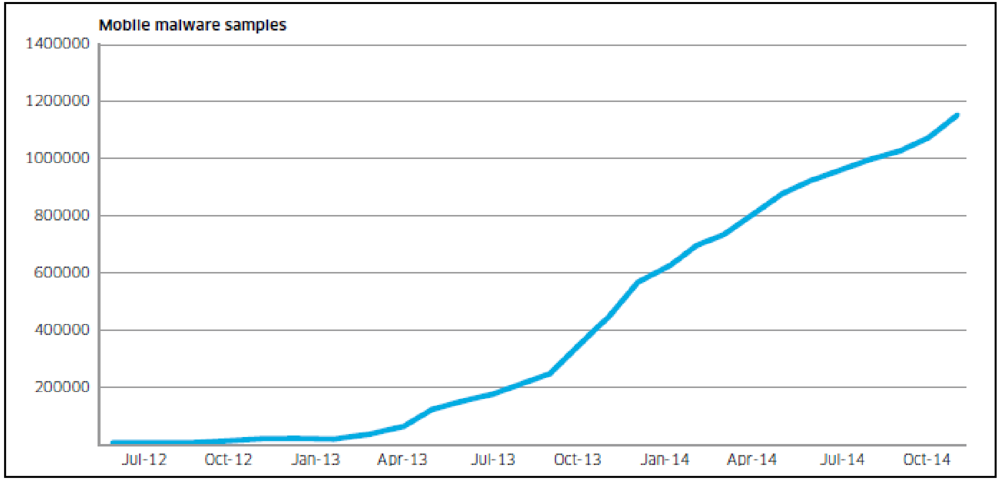


Source: NQ Mobile (2013)

See: http://www.chinaabout.net/2013-global-mobile-security-report-the-worlds-highest-mobile-virus-infection-rate-found-in-china/

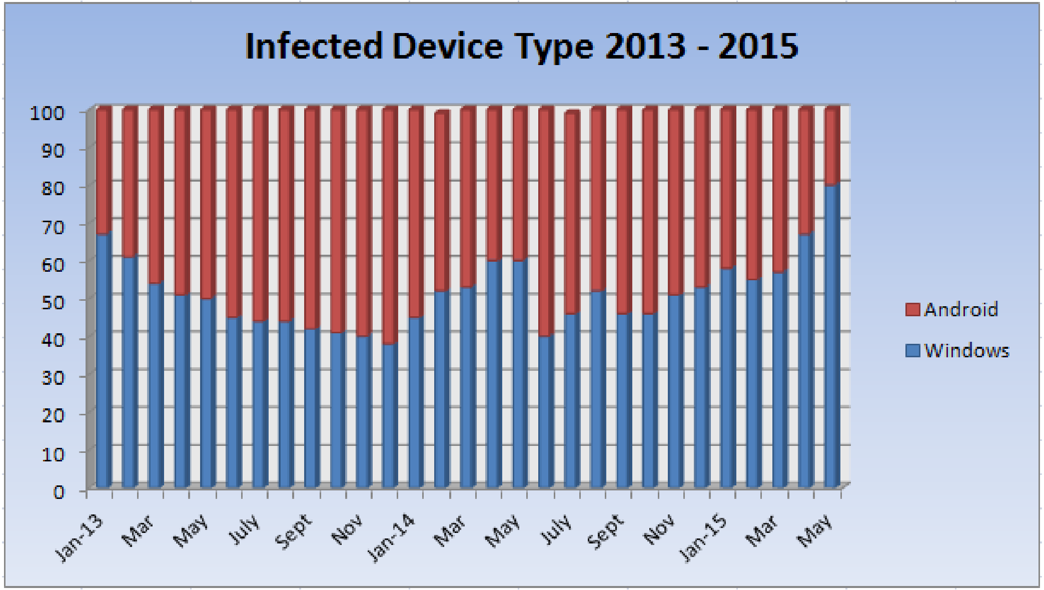
Number of Mobile malware samples grew 161% in 2014

- Samples grew by 161% in 2014
- 95% in Android space
- Download the full report on the Alcatel-Lucent website



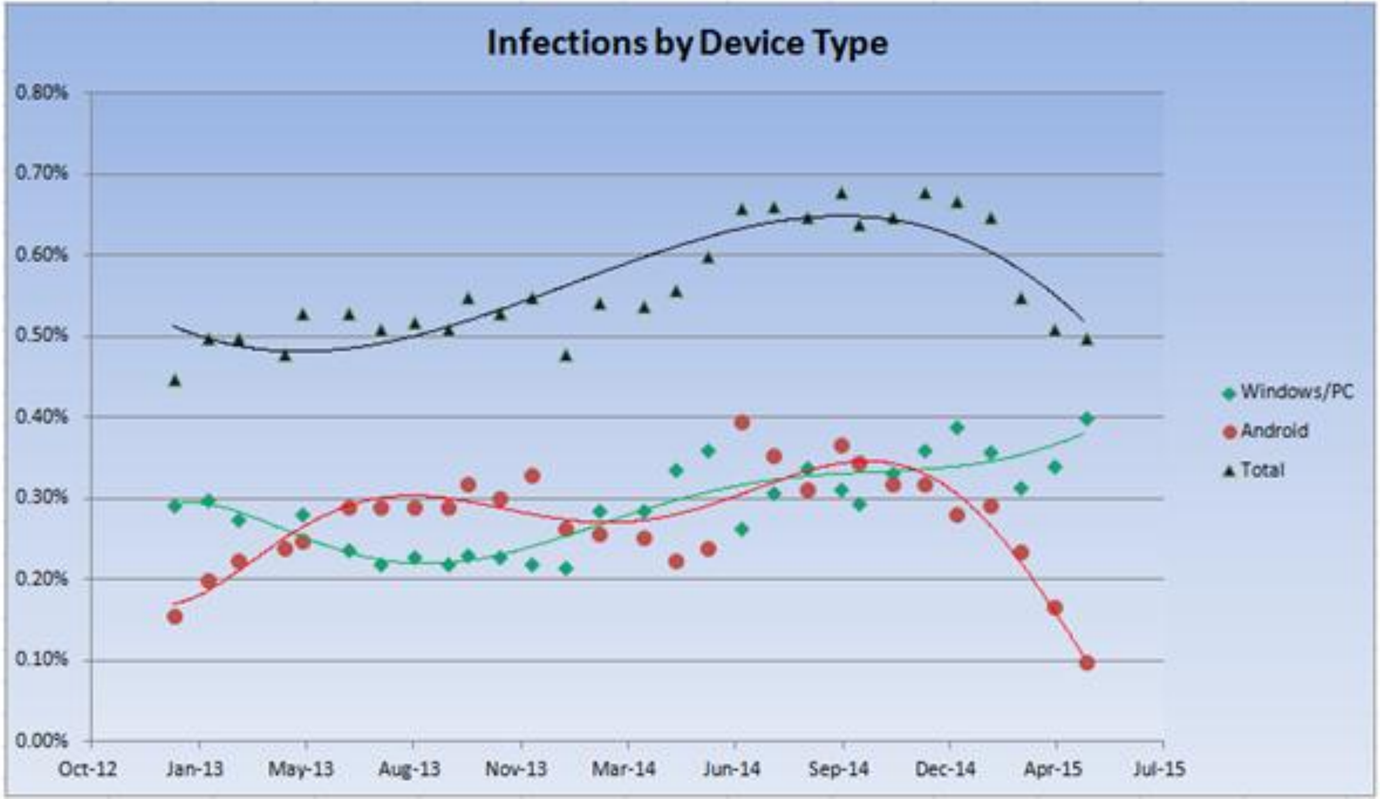
Source: Alcatel-Lucent 2014 Malware Report

Android and Windows PC are the biggest targets



- ~50% of infected devices are **Android**
- ~50% are **Windows PCs** connected to the mobile network
- <1% iPhone, Blackberry, Symbian, Windows Mobile
- Note recent reduction in Android infections

Infection Rate by Device Type



Windows Malware impacts mobile networks

- Mainstream Professional Cybercrime
- **Types**
  - Botnets, Rootkits, SPAM, Identity Theft, Banking Trojans, DDOS, Ad-Click, Bitcoin, FakeAV, Ransomware, Hacktivism, Spyware…
- **Examples**
  - Proxy bot creates 800,000 TCP sessions and consumes **3GBytes of data in 24 hr period**.
  - Roaming user draws botnet traffic from 4000 botnet peers around the world, all backhauled via his home network.
  - Bot checks in with C&C server every minute causing the radio connection to be reestablished each time.

Impact

- On the network
  - Bandwidth consumption
  - Radio signaling
  - Airtime
- Impact on user
  - Identity theft due to key loggers and password stealers
  - Financial loss due to banking trojans
  - Excessive charges due bandwidth usage
  - Extortion due to ransomware
  - Performance degradation due to consumption of computing and network resources.
  - Embarrassment from spaming and infecting friends

Android is mobile target of choice

- **Mostly trojanized apps** from 3rd party app stores or Google Play
- **Installed** by victim as a result of phishing or social engineering.
- **Types** (varies by region) : Adware, Info Stealers, Spy Phone, SMS Trojans, Banking Trojans, Fake Security Software
- **Impact** is low on the network so far but moderate to high on users

Android Malware

- Lacks Sophistication
  - C&C servers are hard coded in the source code as URL's, domain names or IP addresses.
  - The C&C protocol is not robust and can be disrupted by taking out a single server.
  - The malware make no real attempt to conceal itself or avoid detection by anti-virus software.
  - The malware makes no attempt at persistence and can be removed by a simple uninstall.

Why Android?

- **Sideloading**
  - Android apps can be download and installed from anywhere.
  - This provides the malware developer with an easy way to deliver the malware.
  - Some third part app stores specialize in pirated software with a high malware content.
- **Google Play**
  - Survey of 130k free apps in early 2014 showed 1/700 had some sort of malware content.
  - Google has greatly improved on this since then.

Why Android?

- **App Hijacking is trivial**

  1. Get the APK file for the target app
  2. Open it using “apktool d”
  3. Cut and paste the Trojan “smali” code directories into target app
  4. Edit the onCreate() function in the apps main activity to invoke the Trojan service
  5. Edit manifest to add the Trojan service and any required permissions
  6. Rebuild the app using “apktool b”
  7. Use “jarsigner” to sign the app (any key will do).
  8. Use “zipalign” to complete the process

This of course can be scripted…

Android vs Apple app security

- Signed with self signed certificates that are created by the developer.
- Available from a large number of third party app stores

- Signed with certificates issued by Apple and linked to the developer registration information.
- Only available from Apple.

Malware impacts the network and the user

Bandwidth

- SPAM
- DDOS
- Ad-Click Fraud

Signaling

- Command & Control
- Ad-Click Fraud
- Scanning

Air Time

- Command & Control
- Ad-Click Fraud
- Scanning

Customer Experience

- Identity Theft
- Financial Loss
- Excessive Charges
- Extortion
- Performance
- Embarrassment

Top 20 Android Malware

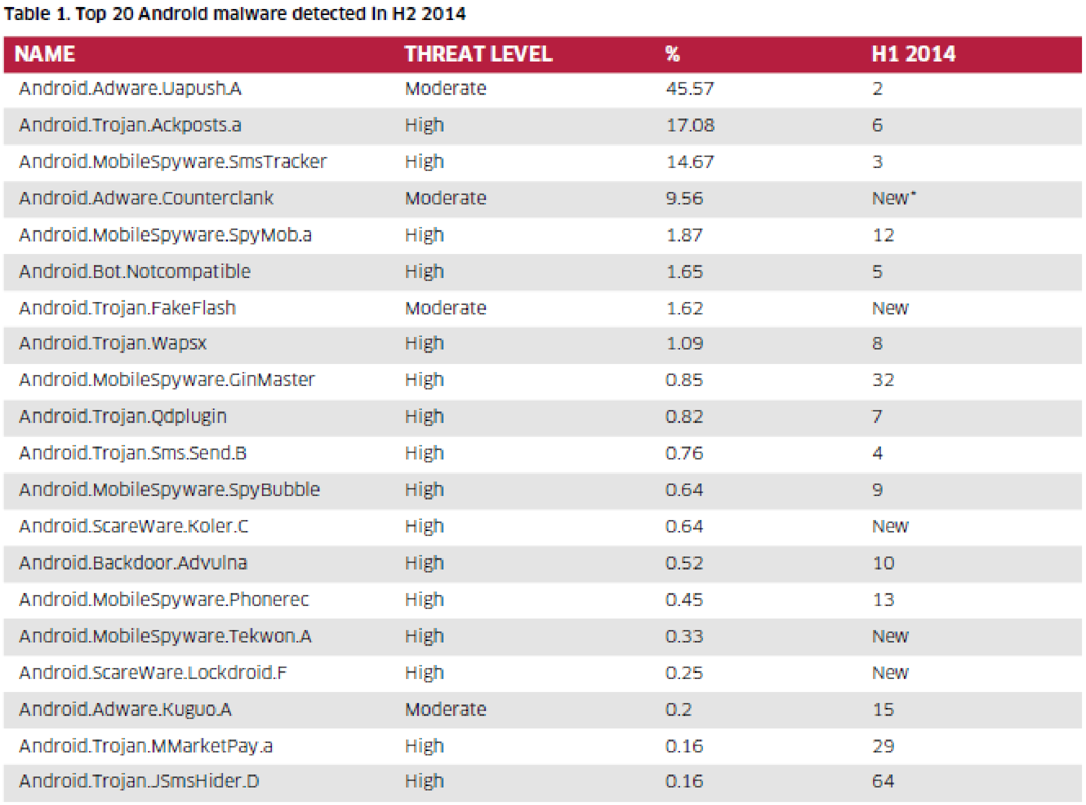
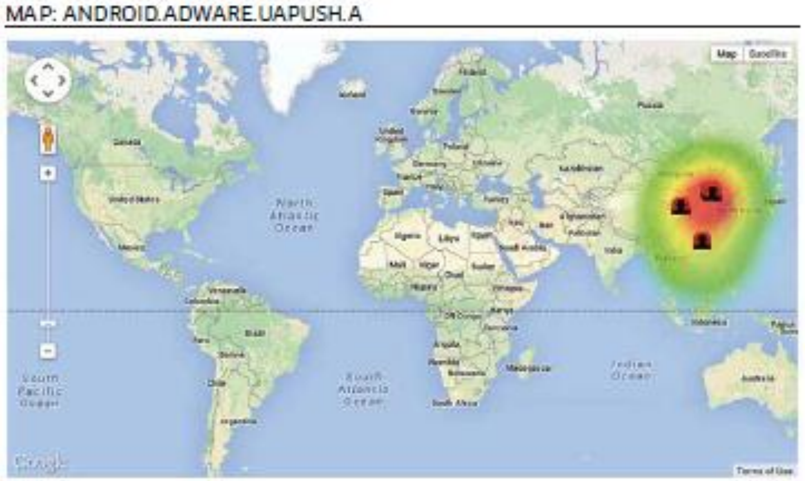


Table 1. Top 20 Android malware detected in H2 2014

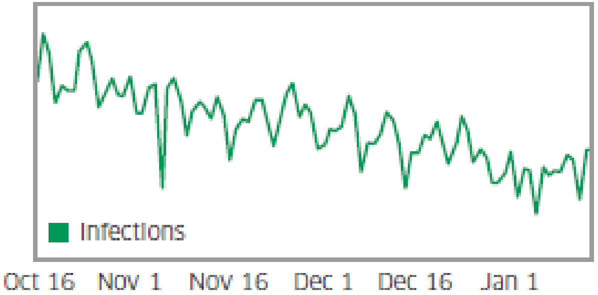
NAME	THREAT LEVEL	%	H1 2014
Android.Adware.Uapush.A	Moderate	45.57	2
Android.Trojan.Ackposts.a	High	17.08	6
Android.MobileSpyware.SmsTracker	High	14.67	3
Android.Adware.Counterclank	Moderate	9.56	New*
Android.MobileSpyware.SpyMob.a	High	1.87	12
Android.Bot.Notcompatible	High	1.65	5
Android.Trojan.FakeFlash	Moderate	1.62	New
Android.Trojan.Wapsx	High	1.09	8
Android.MobileSpyware.GinMaster	High	0.85	32
Android.Trojan.Qdplugin	High	0.82	7
Android.Trojan.Sms.Send.B	High	0.76	4
Android.MobileSpyware.SpyBubble	High	0.64	9
Android.ScareWare.Koler.C	High	0.64	New
Android.Backdoor.Advulna	High	0.52	10
Android.MobileSpyware.Phonerec	High	0.45	13
Android.MobileSpyware.Tekwon.A	High	0.33	New
Android.ScareWare.Lockdroid.F	High	0.25	New
Android.Adware.Kuguo.A	Moderate	0.2	15
Android.Trojan.MMarketPay.a	High	0.16	29
Android.Trojan.JSmsHider.D	High	0.16	64

UAPUSH

- **Uapush.A** is an Android adware Trojan with a moderate threat level
- Sends IMSI, IMEI, contact information, bookmarks and call history to a C&C server in China
- It also may send Short Message Service (SMS) messages without the user’s consent.
- Activity on this decreased steadily since the first half of the year.



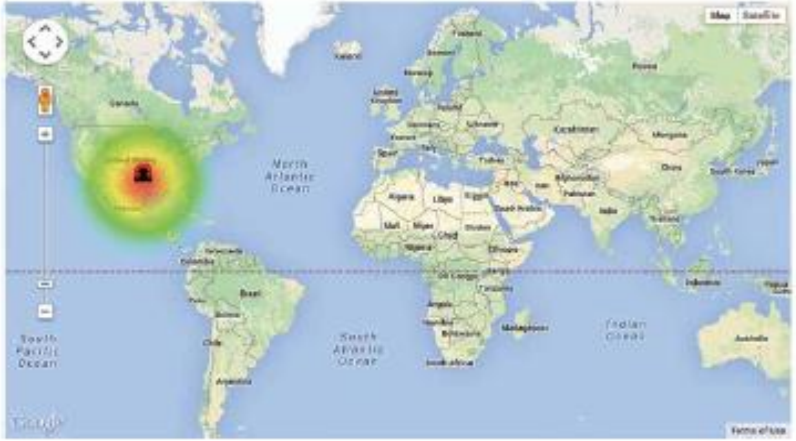
MAP: ANDROID.ADWARE.UAPUSH.A

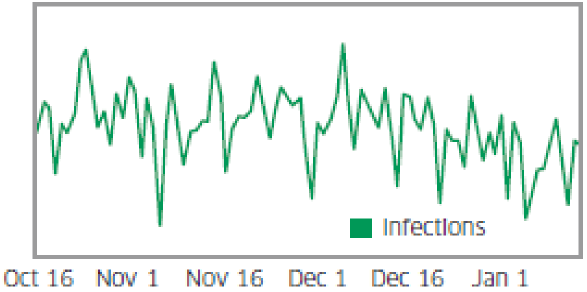


SMSTRACKER

- **SMSTracker** is an Android spyphone app that provides a complete remote phone tracking and monitoring system for Android phones.
- It allows the attacker to remotely track and monitor all SMS, Multimedia Messaging Service (MMS), text messages, voice calls, GPS locations and browser history.
- This is also known as Android.Monitor.Gizmo.A.

MAP: ANDROID.TROJAN.SMSTRACKER

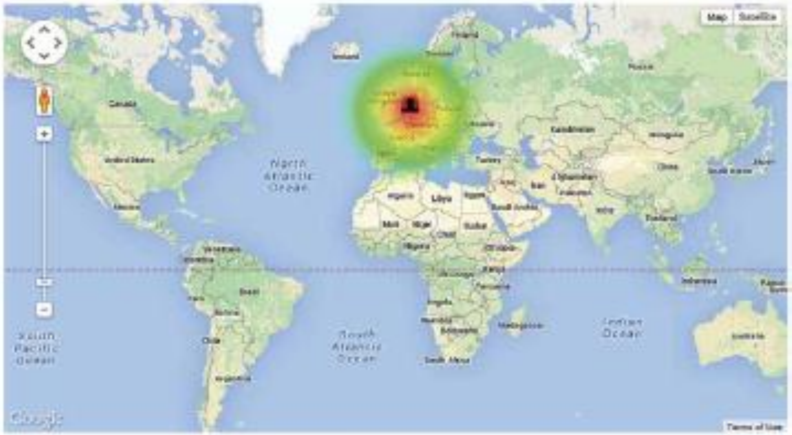


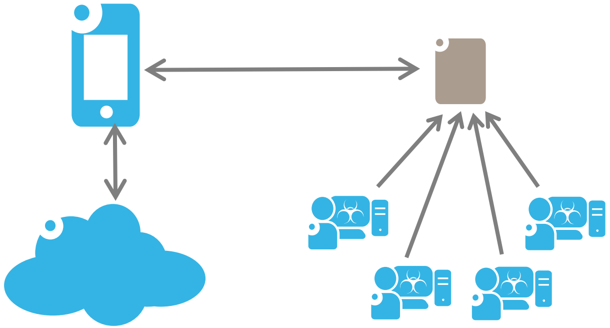


NOTCOMPATIBLE

- Web Proxy Bot ported from Windows to Android environment.
- Uses same C&C as Windows version.
- Allows remote miscreants to anonymously browse the web through the victim's phone.
- Consumes lots of bandwidth
- 165MB in two hours over 300K TCP sessions
- Infection rate is currently only 0.03%
- In a network of 1M users that's 600GB per day

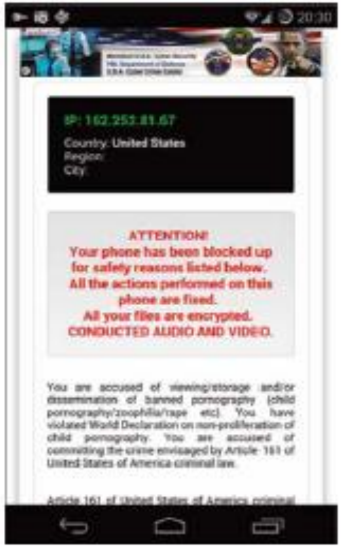
MAP: ANDROID.BOT.NOTCOMPATIBLE





KOLER

- Koler is an Android scareware Trojan that claims it has encrypted all the data on your phone and demands a ransom to restore the data.



IP: 162.253.81.67

Country: United States
Region:
City:

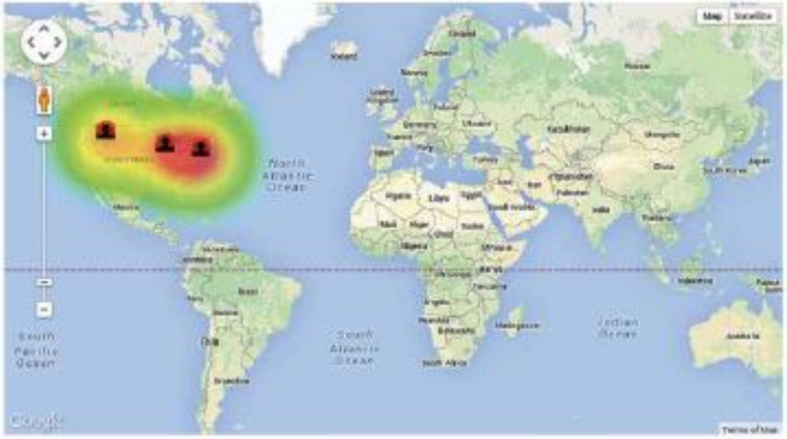
ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

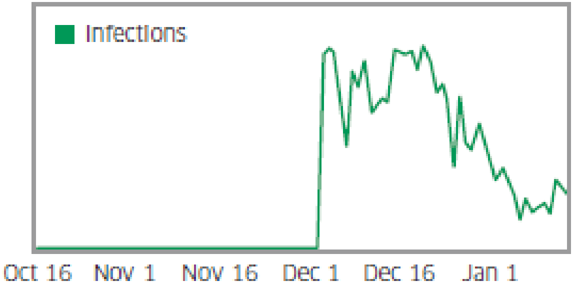
You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal

The victims are usually visitors to Internet-based pornographic sites, who are duped into downloading and installing a “premium access video player.” The malware “lock-screen” is customized depending on the location of the phone. The screen image is from a United States based phone.

MAP: ANDROID.SCAREWARE.KOLER.C

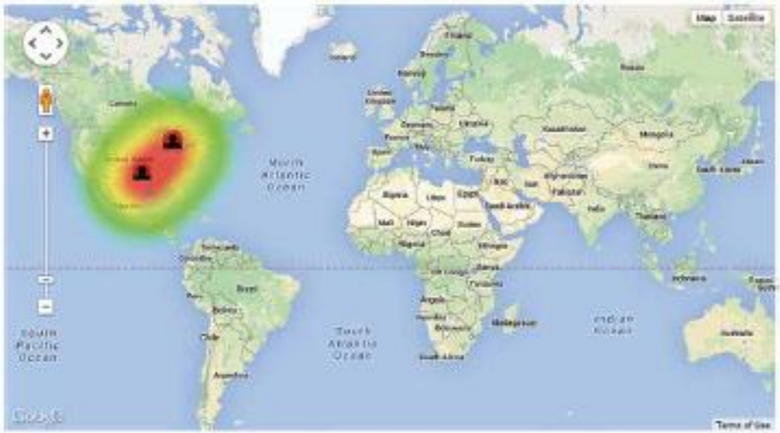


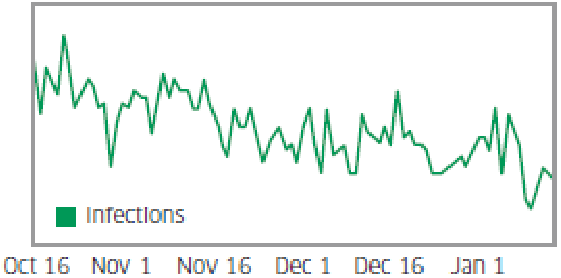


FAKEFLASH

- FakeFlash is a scam application distributed under the name “Install Flash Player 11.”
- It charges money for downloading and installing the Adobe Flash Player.

MAP: ANDROID.TROJAN.FAKEFLASH





Mobile Spyware

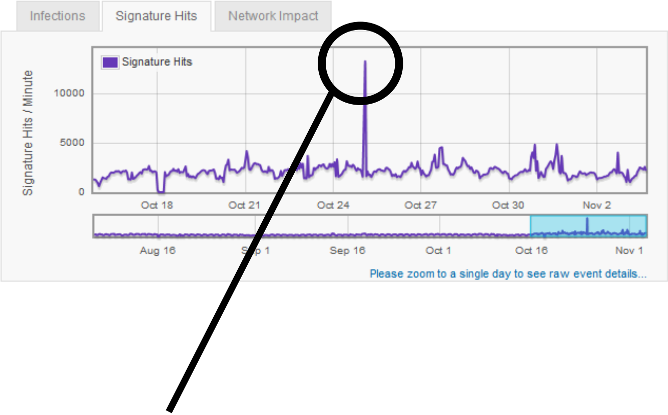
- Mobile spyware is definitely on the increase. Six of the mobile malware in the 2014 top 20 list are mobile spyware.
- These are apps that are used to spy on the phone's owner.
- They track the phone's location, monitor ingoing and outgoing calls and text messages, monitor email and track the victim's web browsing.
- Used by individuals, private investigators and in cyber espionage.

Official Site
SPYPHONE®
The World Leader in Spy Phone Software
for Monitoring your Android Cell Phone.
Turn your Android into a Family Monitoring Tool
GPS Tracking On Cell Phone Location
View Incoming/Outgoing Calls
View Incoming/Outgoing Text Messages
View Websites Visited on Phone
100% Free Product
Finally we as parents are getting tools to combat the ever increasing threats that come with an age of free flowing information.
-Joyce M
Mother
Get the App Now
Free Download

iNTERCEPTOR
SPYPHONE
SOFTWARE
Receive both incoming and outgoing text messages
Dial in and listen to surrounding vicinity
Text notification when the target phone is switched on
Time and date stamping
Text notification when the target phone receives call
Text notification shows number calling in
Text notifications when the target phone dials
Text notification shows number being called
iNTERCEPTOR
SPYPHONE
SOFTWARE

Impact of Scanning

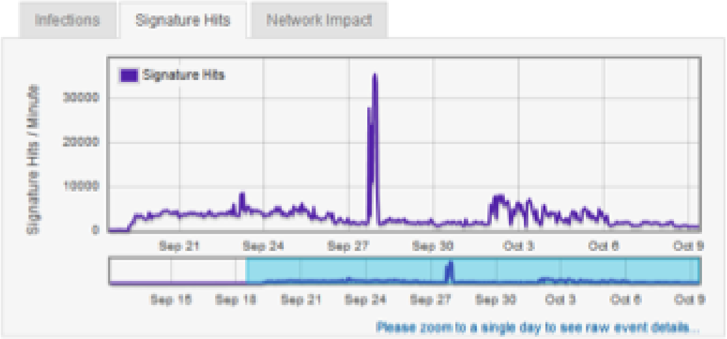
- Cyber-criminals and security researchers often scan the Internet for vulnerable devices.
- In mobile networks these scans can cause excessive radio paging and signaling as large numbers of idle devices must be reconnected to the network to respond to the scan.
- Not a problem if the mobile subnets are NATed



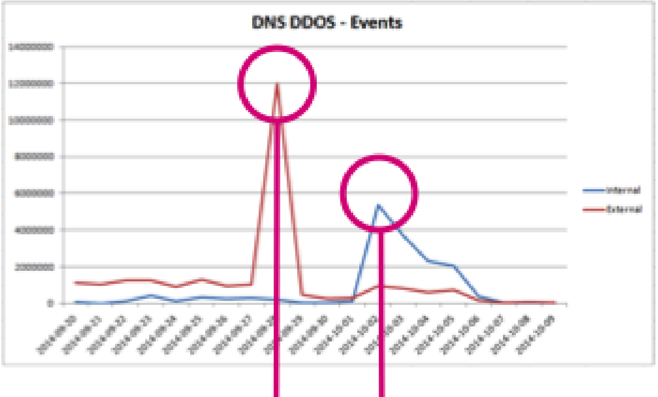
Network Scan

DNS Amplification DDOS Attack in Mobile Network

- Mobile Wifi devices have been used in DNS DDOS amplification attacks
- Device configuration problem caused some devices to provide an internet facing recursive DNS service
- This attack is very similar to the Spark DDoS attack on Sept 8-9th 2014 in New-Zealand, where the mobile and fixed data services were down due to 138 compromised devices



Please zoom to a single day to see raw event details...



~12M EXTERNAL EVENTS

~5.5M INTERNAL EVENTS

Conclusion

- **Mobile Malware**
  - Currently lacks sophistication
  - Has relatively low infection rates (0.1%)
  - Greenfield opportunities include:
    - Spyphone (Tracking family, Private Investigators, Cyber Espionage)
    - SMS Trojans
- **Things to watch for**
  - Botnets move to mobile devices for SMS & Voice SPAM
  - More sophisticated C&C, persistence & stealth
  - DDOS against SMS and Voice
  - Hactivism goes mobile
  - Internet of Things gets hit

Questions ?