RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-F02

The State of End-User Security Global Data from 30,000+ Websites

Andreas Baumhof

Chief Technology Officer
ThreatMetrix Inc.
@abaumhof

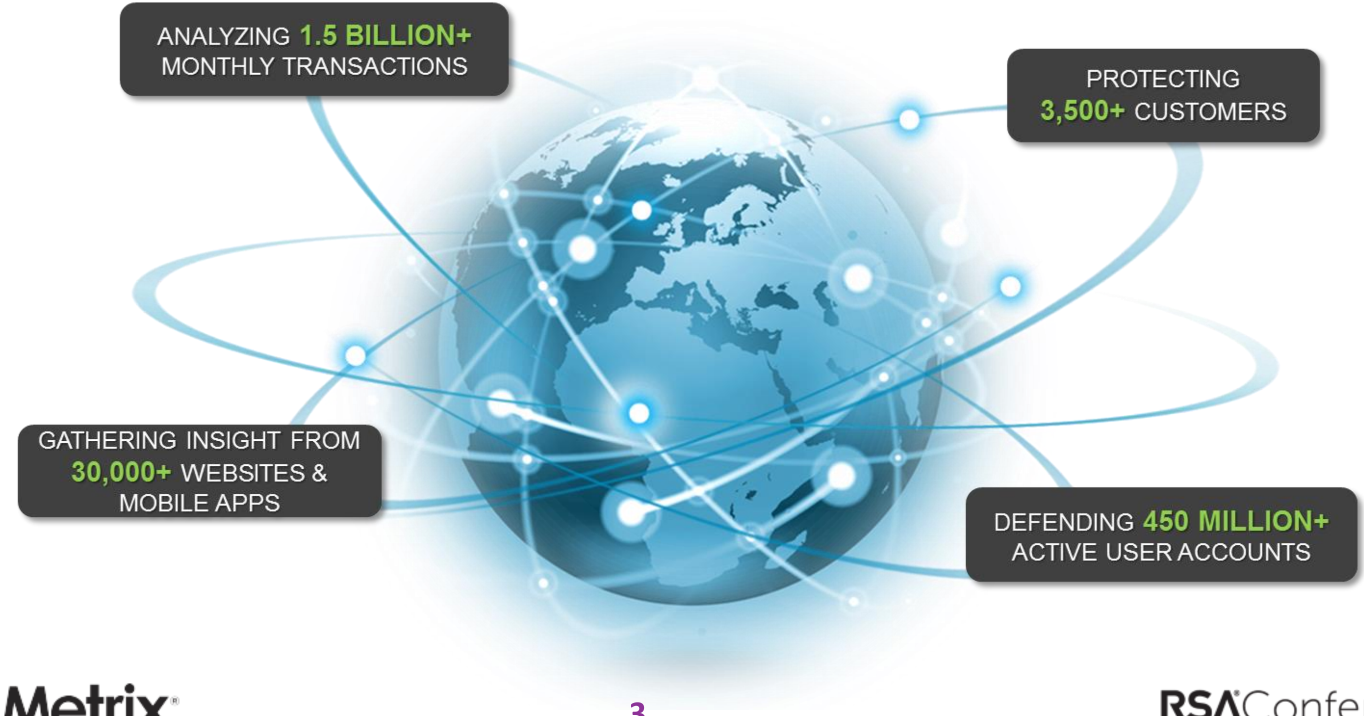
#RSAC

Goal of this talk

- Everybody talks mobile, but do we really know what’s out there? What is hype, what is myth?
- Provide detailed data that will help you
  - To differentiate theoretical attacks from reality
  - Understand the risk surface you are facing
- Enable you to make more informed decisions for your mobile strategy

ThreatMetrix Digital Identity Network

- All data presented in this talk is powered by the ThreatMetrix Digital Identity Network



ANALYZING **1.5 BILLION+** MONTHLY TRANSACTIONS

PROTECTING **3,500+** CUSTOMERS

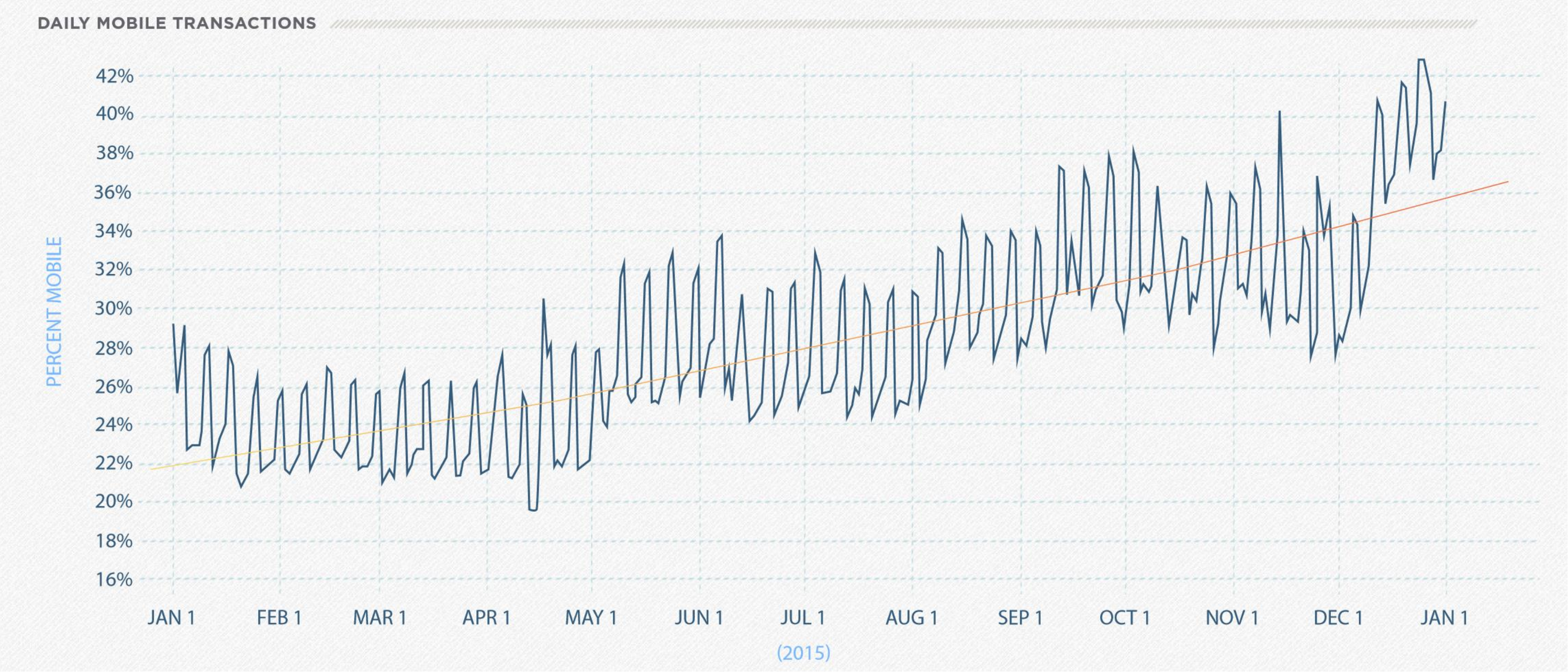
GATHERING INSIGHT FROM **30,000+** WEBSITES & MOBILE APPS

DEFENDING **450 MILLION+** ACTIVE USER ACCOUNTS

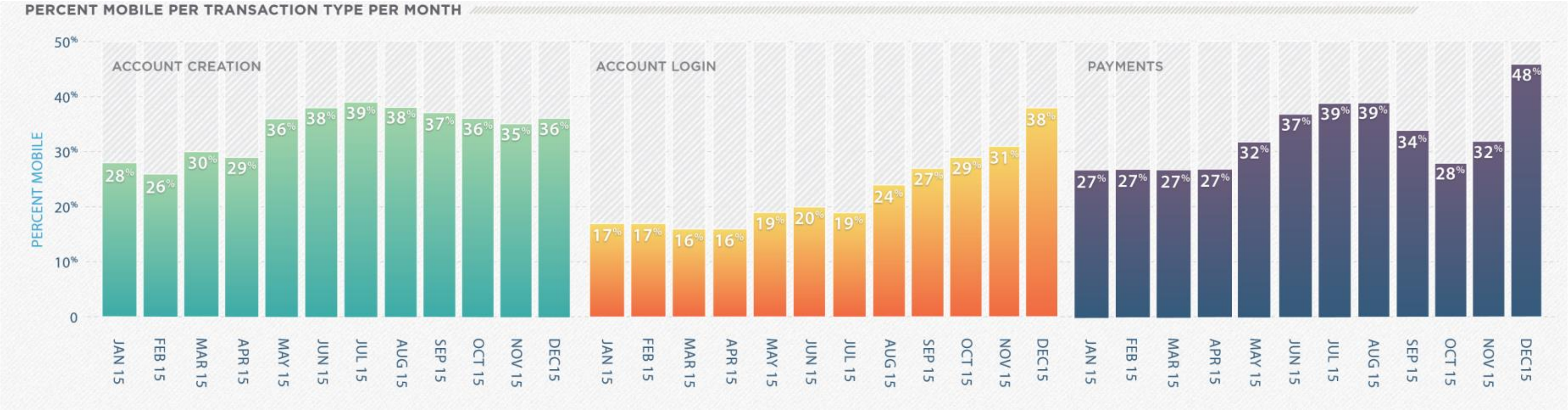
Digital Identity Network

- Consists mainly of Financial Services, Online Retailers and Social Media sites
- Main use cases are account logins (76%), payments (21%) and account creations (3%)
- Global data from every single country
- In short: It is representative data

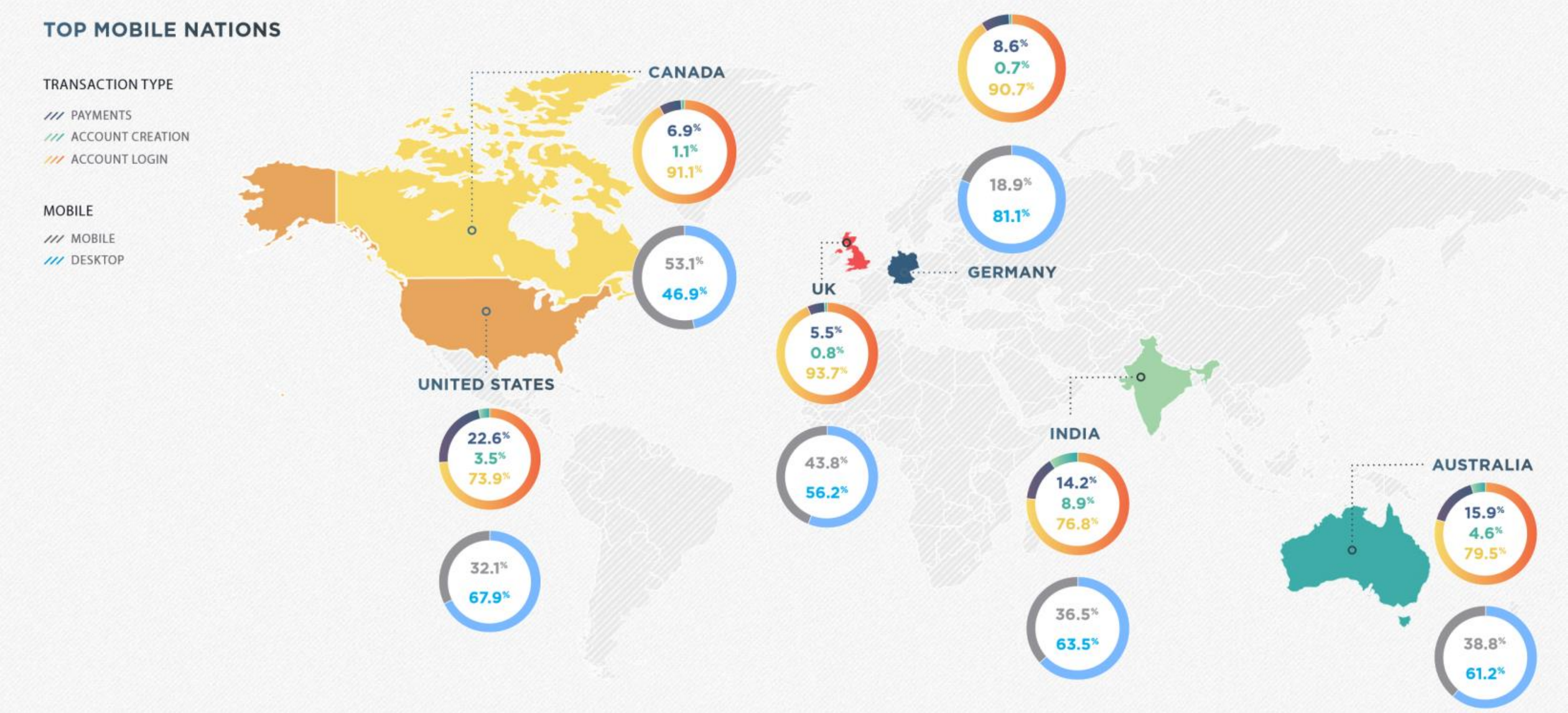
Explosion of mobile transactions



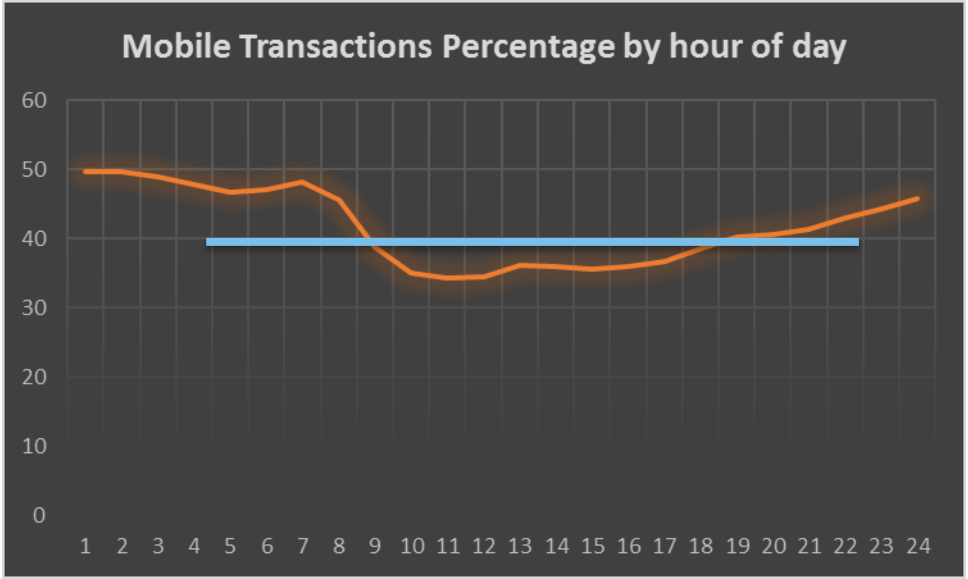
Mobile share of transactions

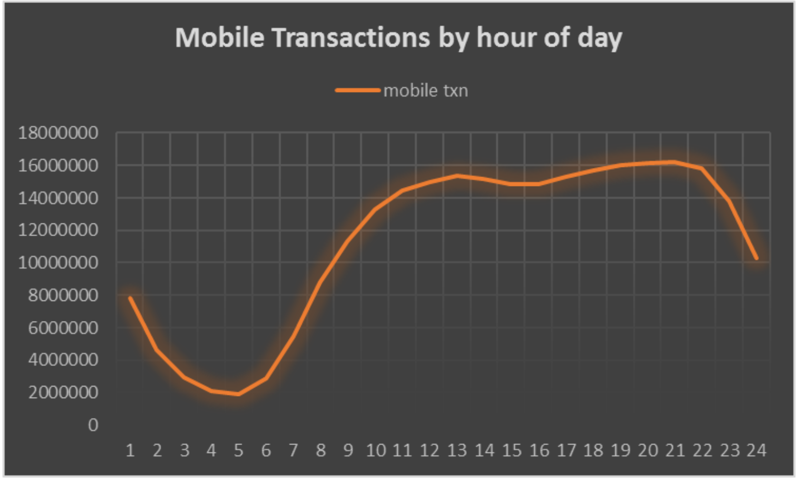


Mobile Statistics for Top Digital Nations



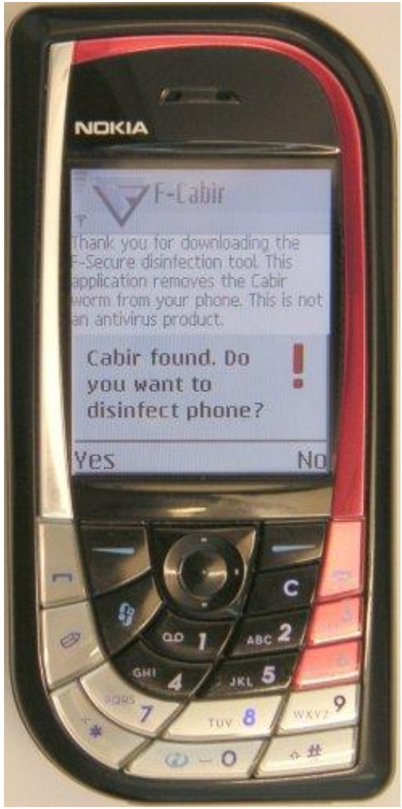
Mobile Transaction Trends - Daily





Threat view

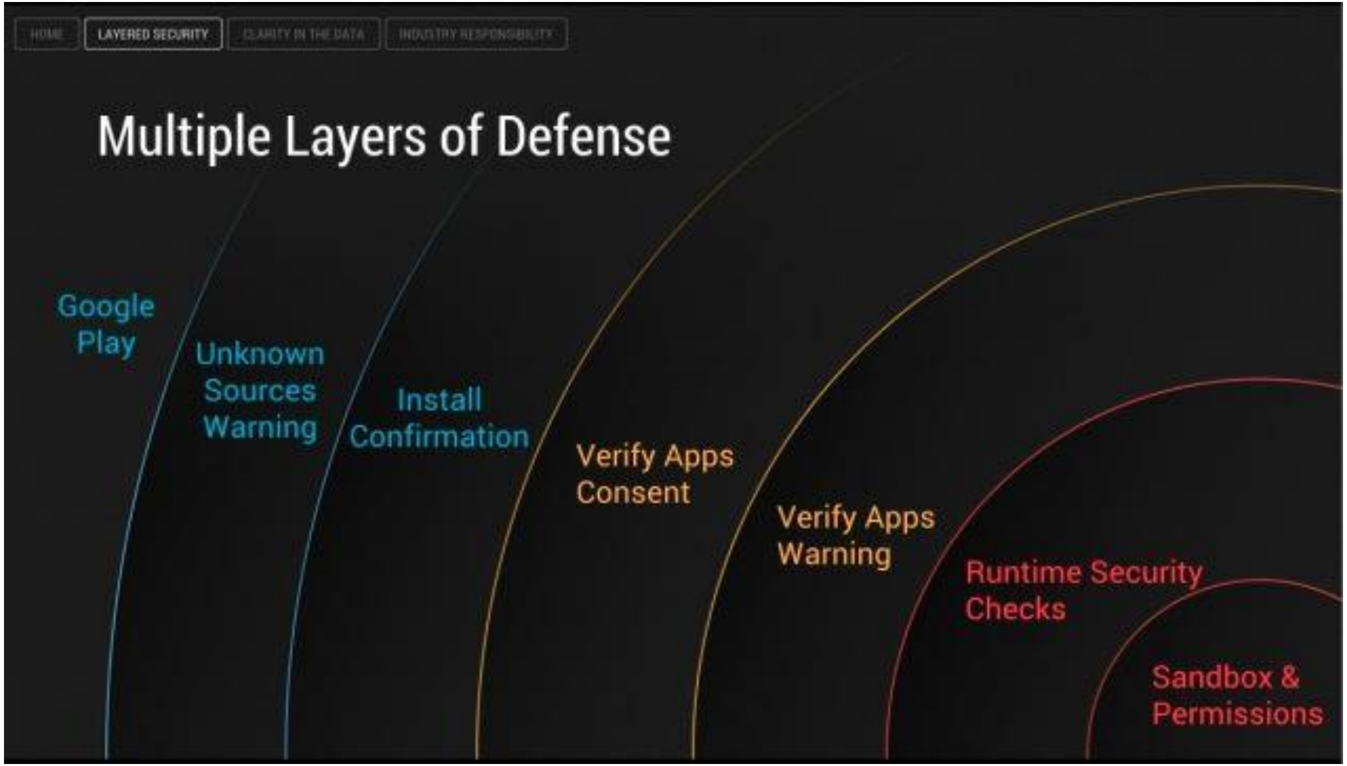
2004 – First virus for mobile (Cabir)



Thank you for downloading the F-Secure disinfection tool. This application removes the Cabir worm from your phone. This is not an antivirus product.

Cabir found. Do you want to disinfect phone?

Security is not an afterthought anymore



Multiple Layers of Defense

Google Play

Unknown Sources Warning

Install Confirmation

Verify Apps Consent

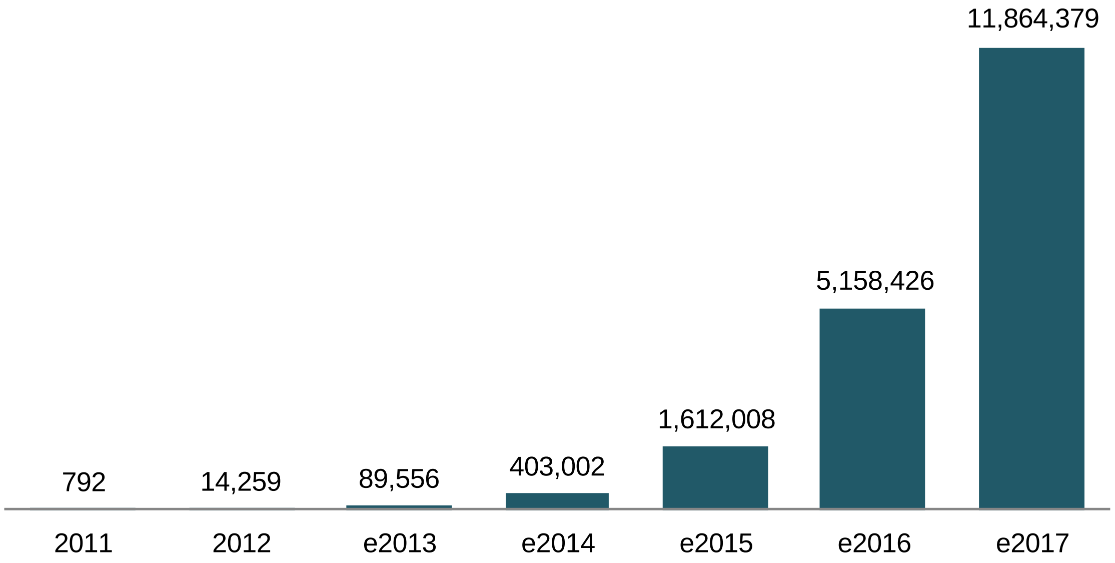
Verify Apps Warning

Runtime Security Checks

Sandbox & Permissions

So why is this skyrocketing?

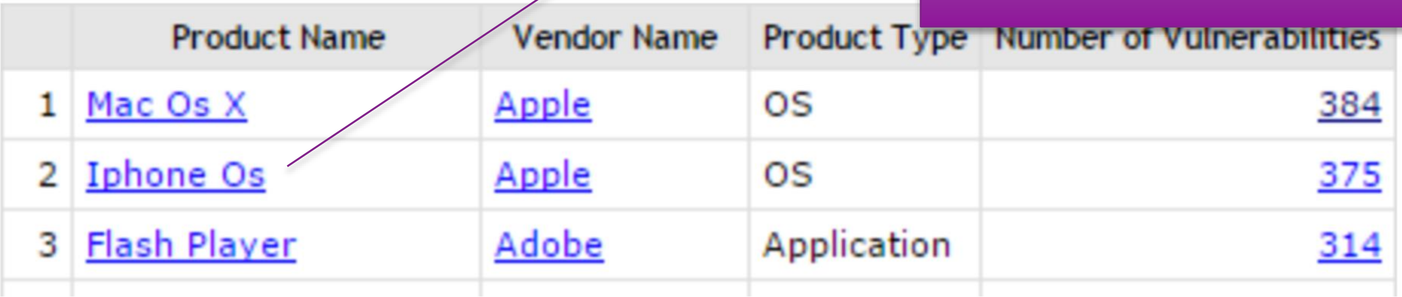
Number of Unique New Mobile Malware Strains Released Per Year



Source: McAfee Labs, Aite Group

Software with the most vulnerabilities in 2015

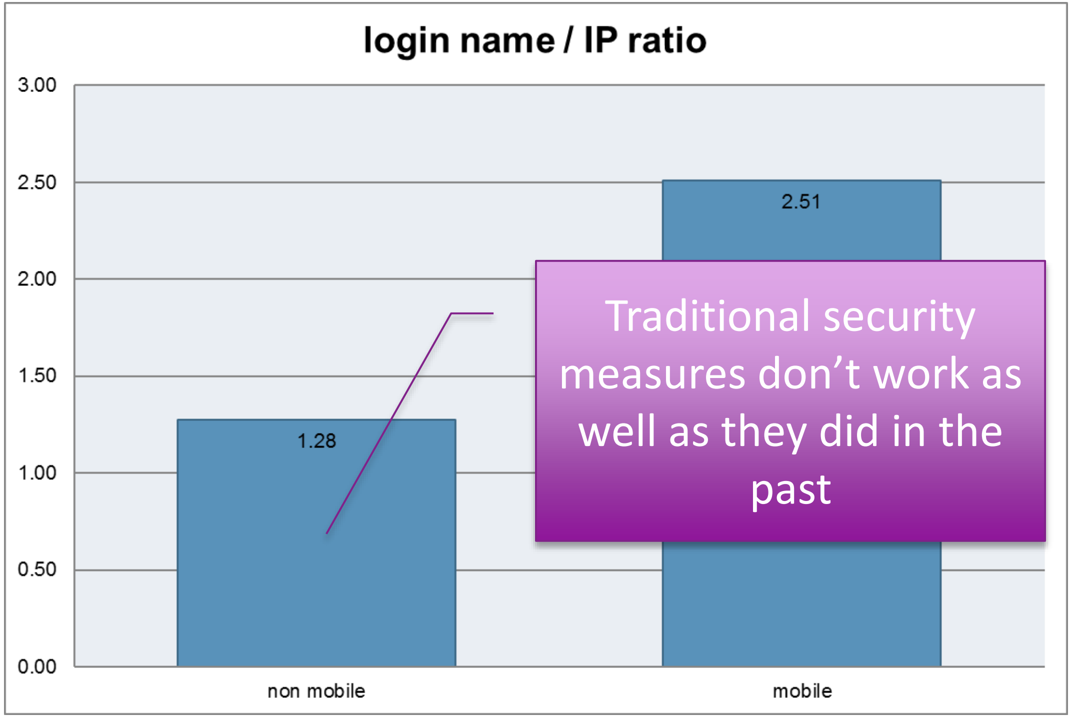
In iOS9: 4 CVE’s with Impact: *“Visiting a maliciously crafted website may lead to arbitrary code execution”*



	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	384
2	Iphone Os	Apple	OS	375
3	Flash Player	Adobe	Application	314

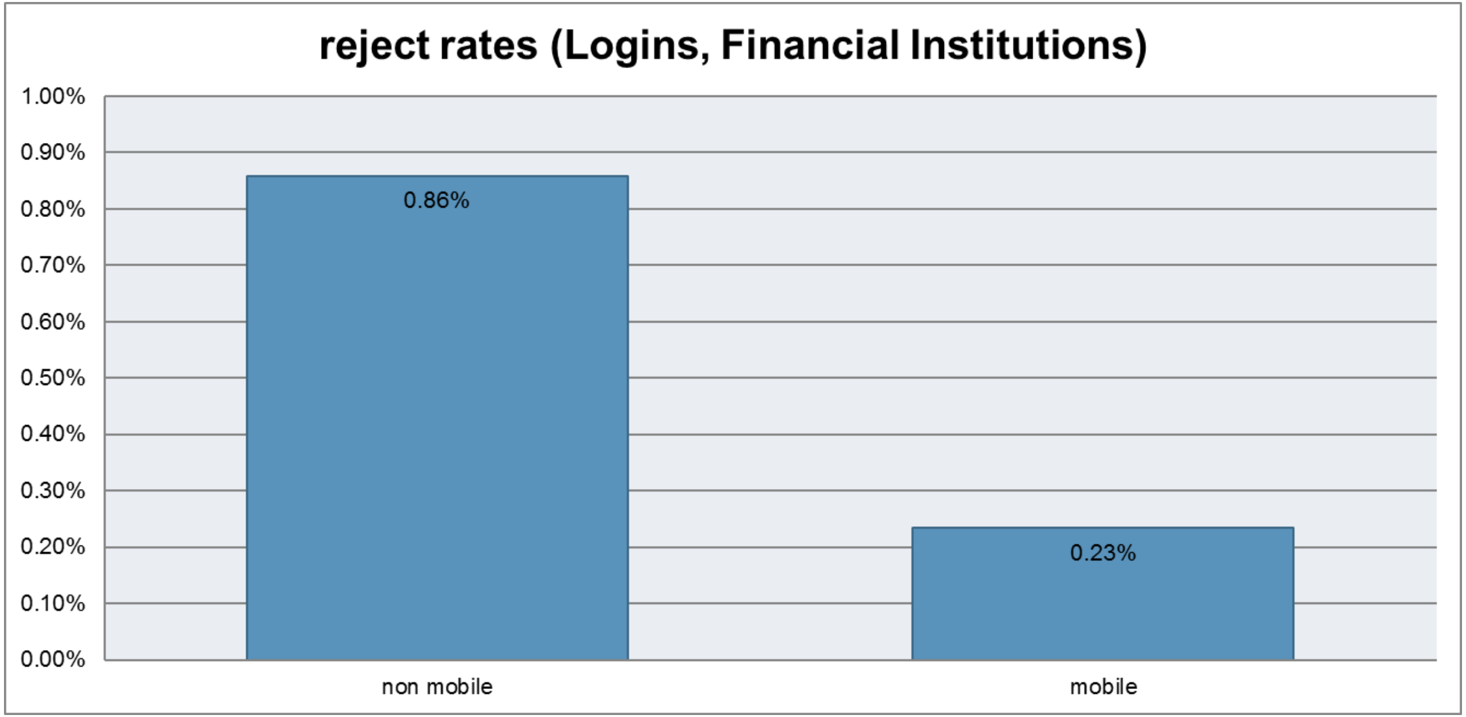
Source: http://www.cvedetails.com/

Mobile traffic is different

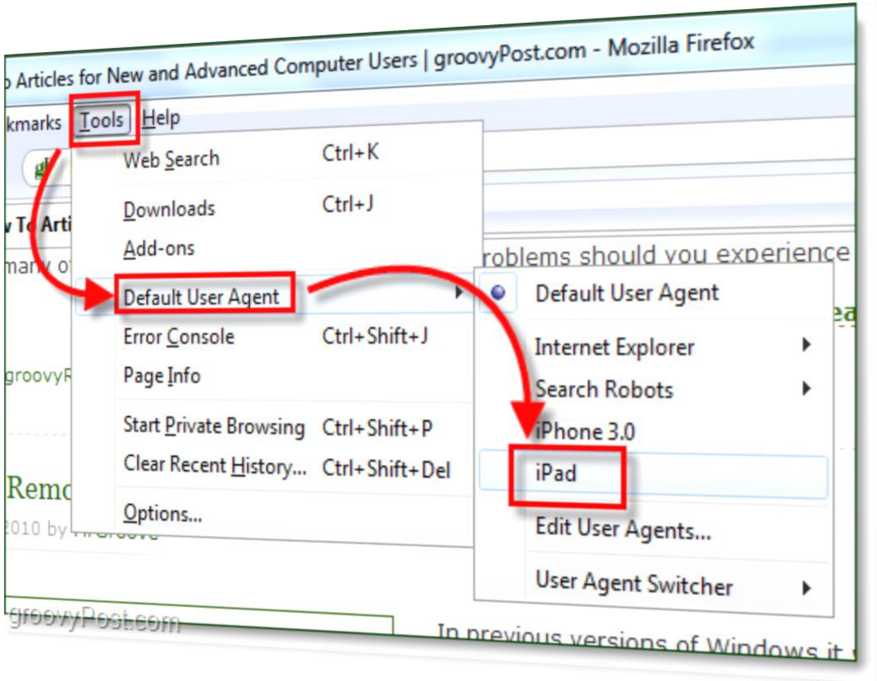


Traditional security measures don't work as well as they did in the past

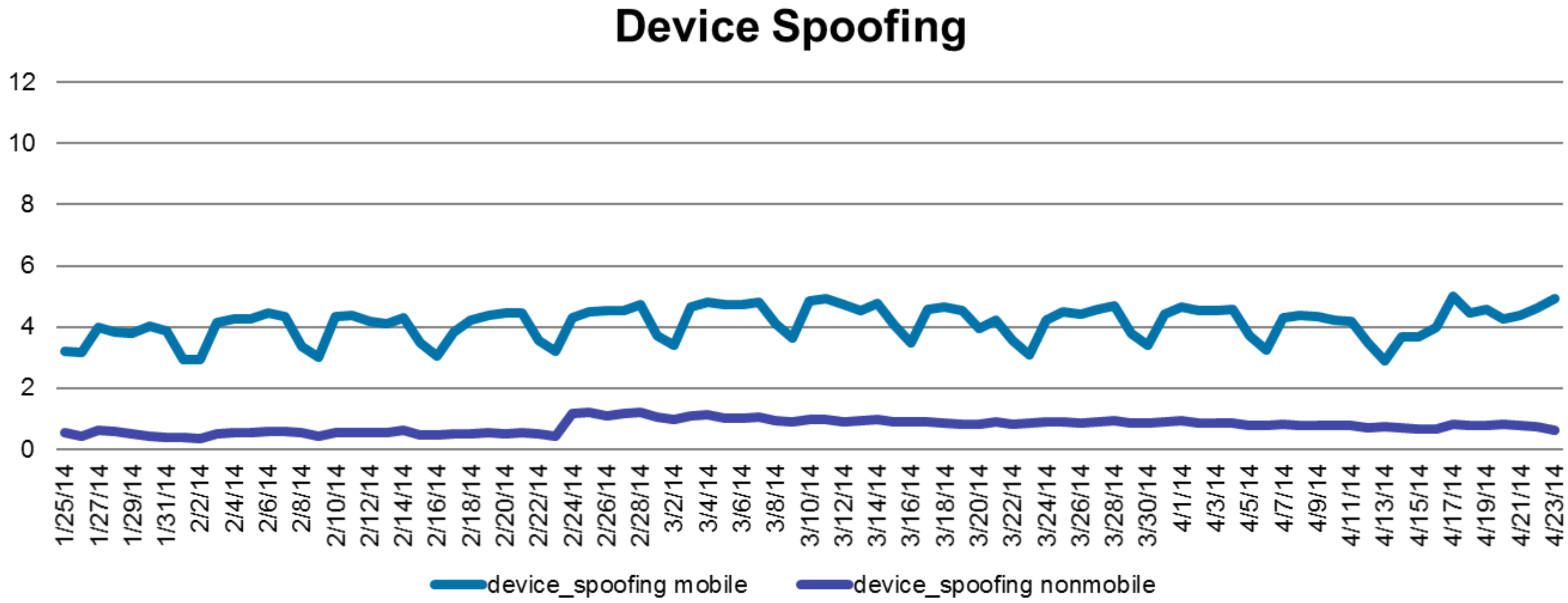
Most high risk transactions are still from the non-mobile channel



Browser spoofing is one of the most common “attacks”

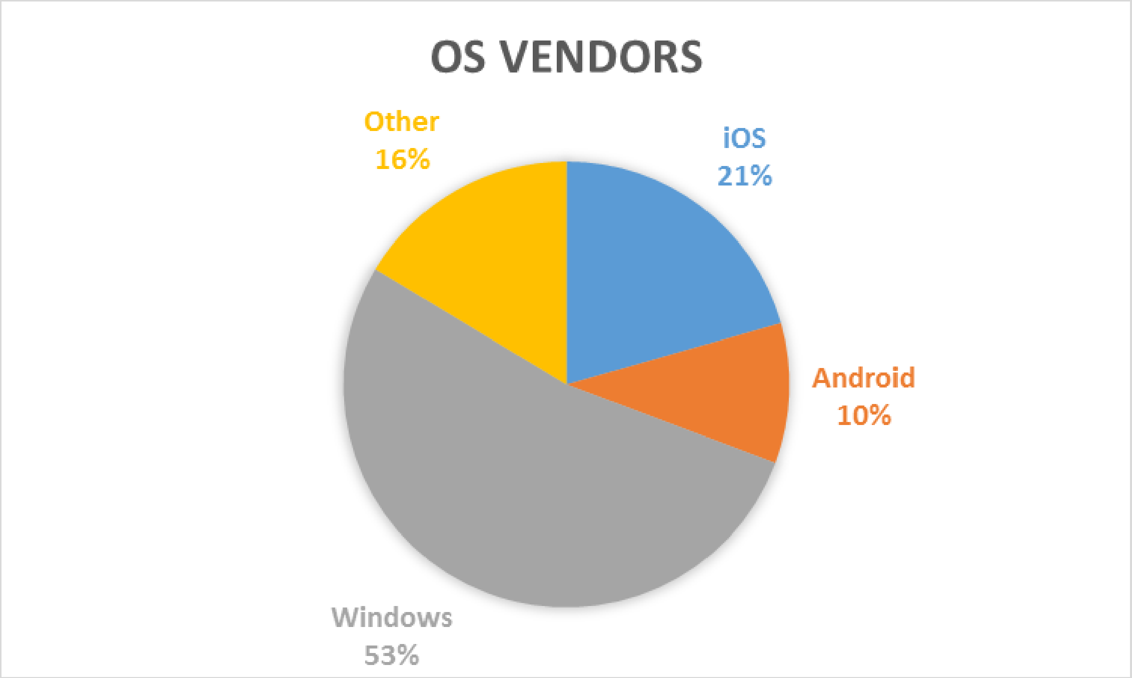

Articles for New and Advanced Computer Users | groovyPost.com - Mozilla Firefox
kmarks
Tools
Help
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Default User Agent
Error Console Ctrl+Shift+J
Page Info
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Options...
Default User Agent
Internet Explorer
Search Robots
iPhone 3.0
iPad
Edit User Agents...
User Agent Switcher
roblems should you experience
groovyPost.com
In previous versions of Windows it

Browser spoofing is significantly higher on mobile than on non-mobile



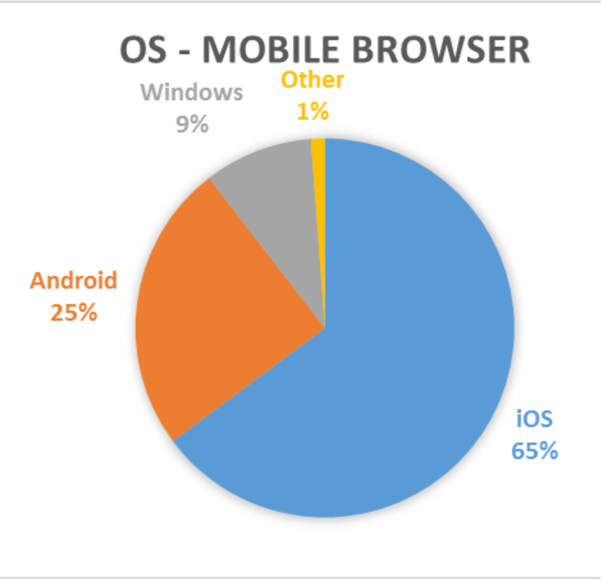
Detailed statistics

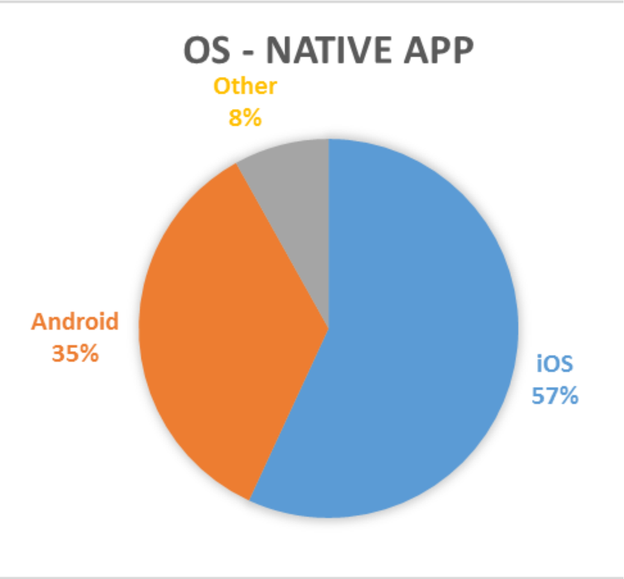
Mobile and Non-mobile OS is converging



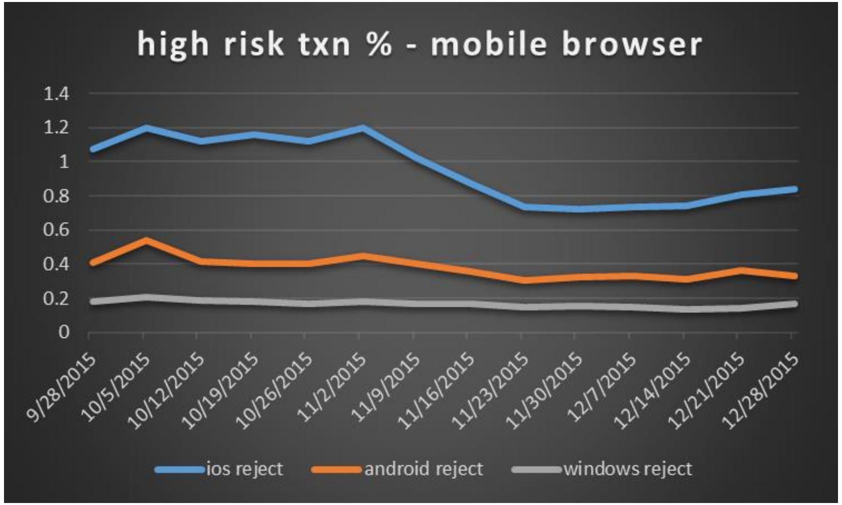
Data is for **all** transactions, not just mobile transactions

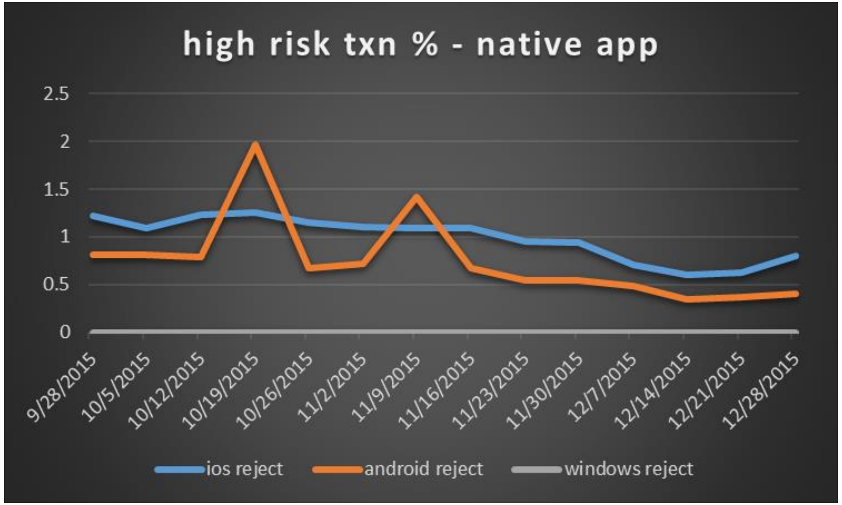
iOS is leading the charge



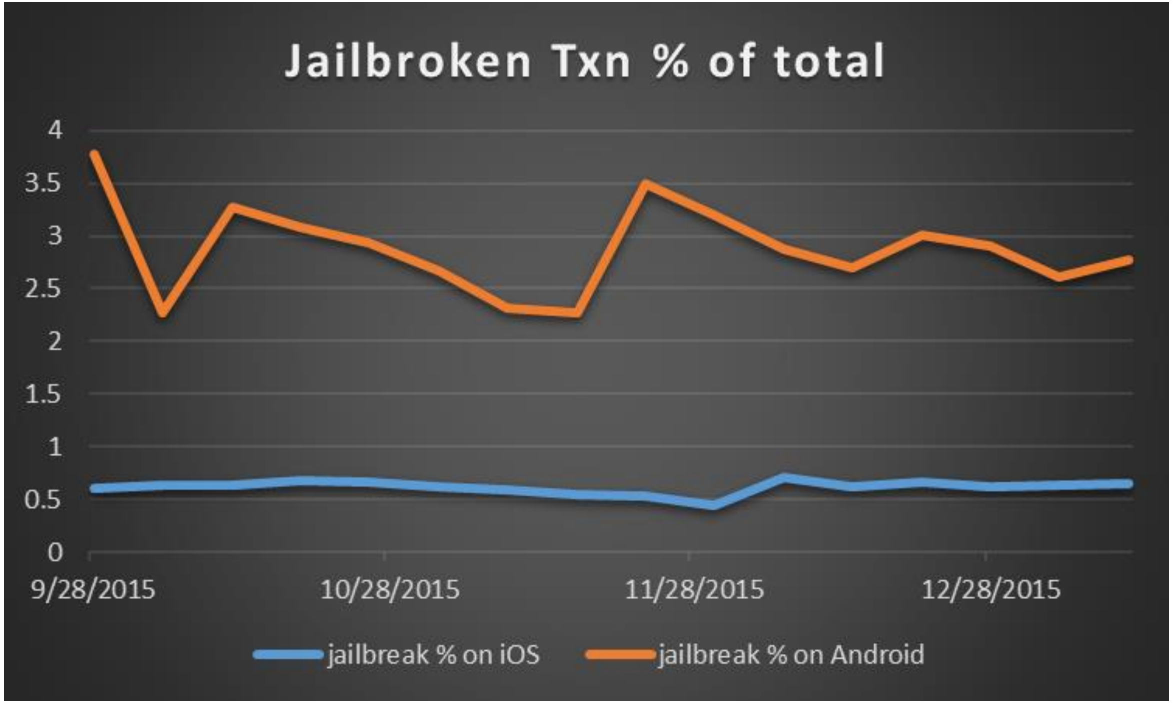


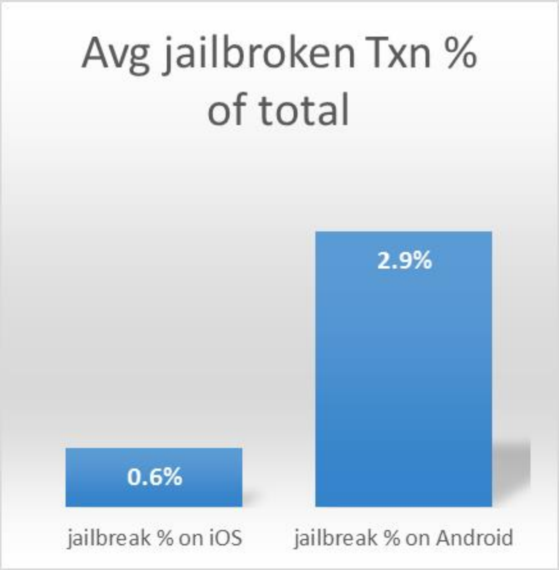
Reversed picture if we look at the high risk transactions





Jailbroken devices

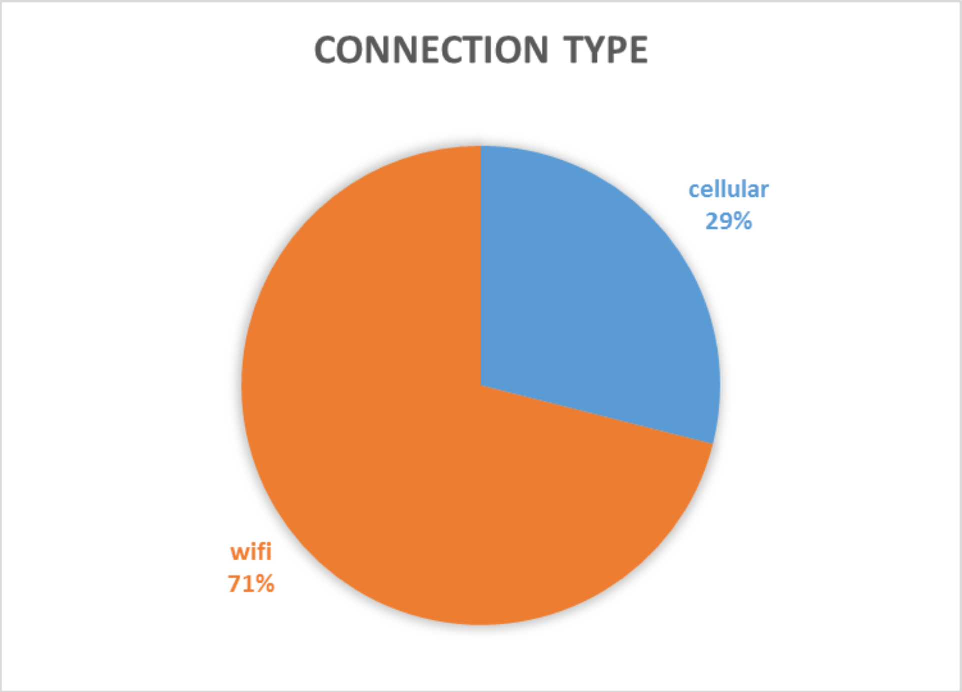




Jailbreak detection methods

- Most common identifier for Jailbreak
  - file:///private/var/lib/cydia
  - file:///private/var/stash
  - file:///private/var/lib/apt
- Beware though
  - You would miss 65% of jailbroken detections if you “just” focus on these

How are people connecting?

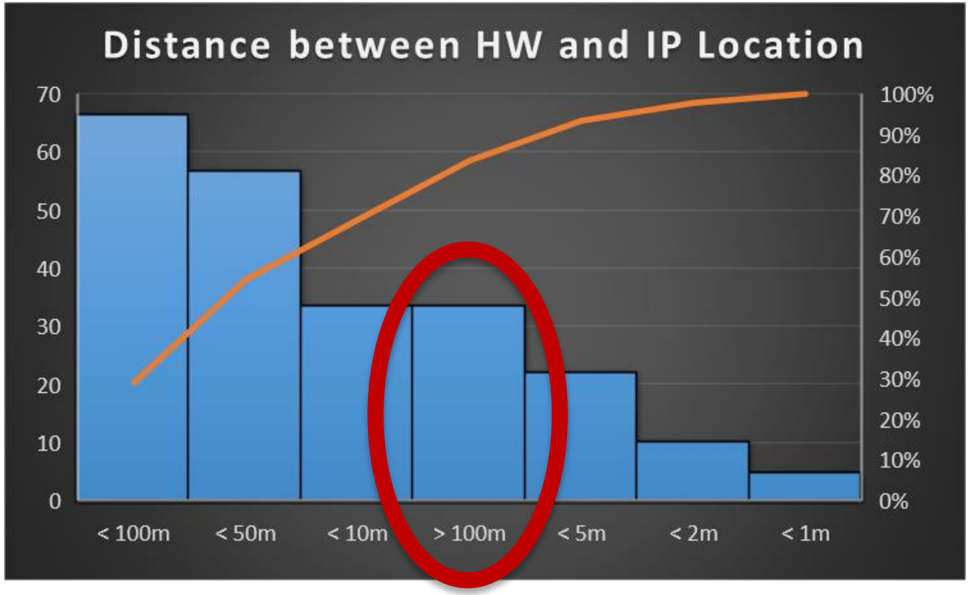


Location is important

- On a native mobile device, location can be obtained in many ways
  - GPS
  - IP (True IP, DNS IP, …)
  - Signal strength

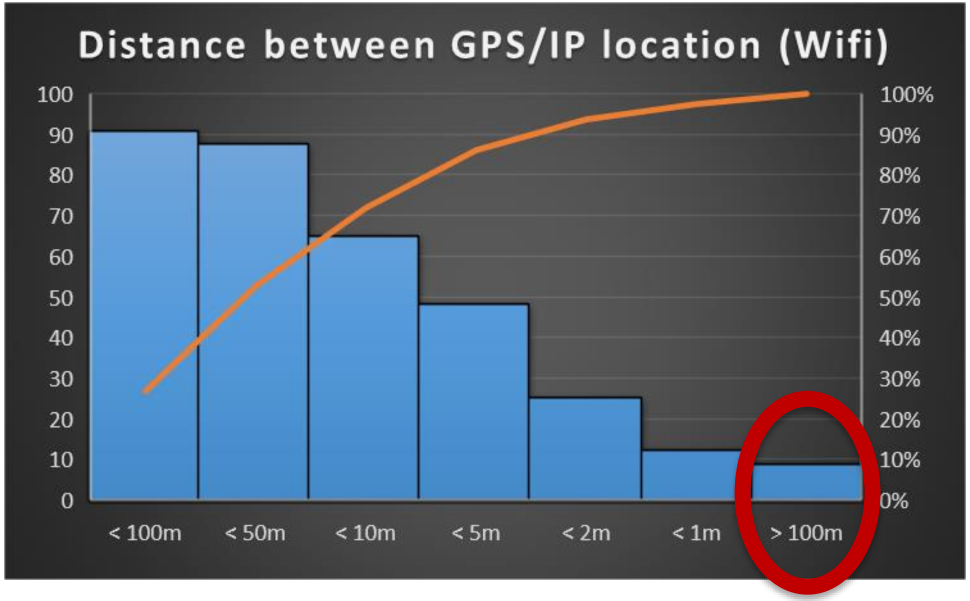
How accurate is the IP Address Location?

Connection type: Cellular



How accurate is the IP Address Location?

Connection type: Wifi



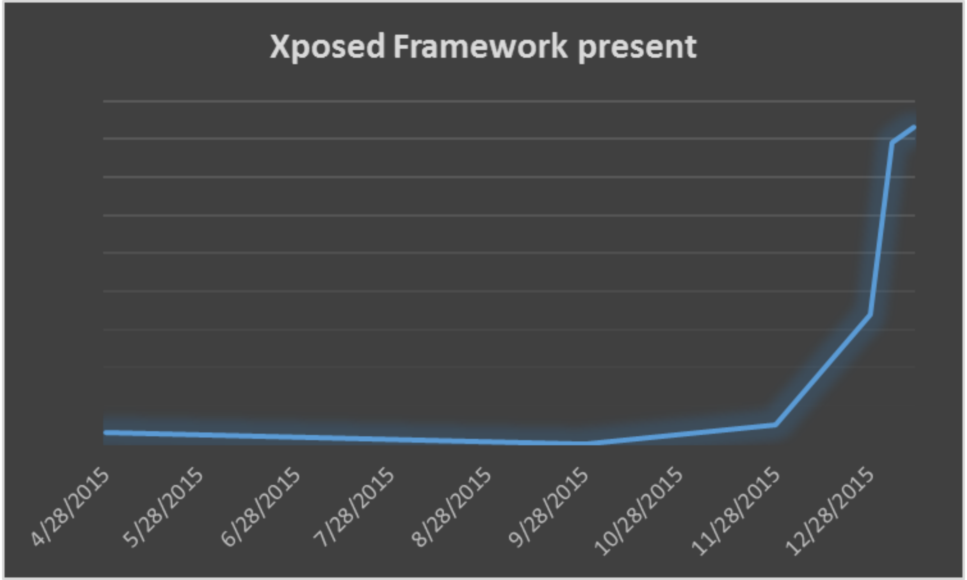
IP Address Anomalies

- Interesting anomalies can be found by interrogating the IP address of the device and comparing it to the IP address of its used DNS server

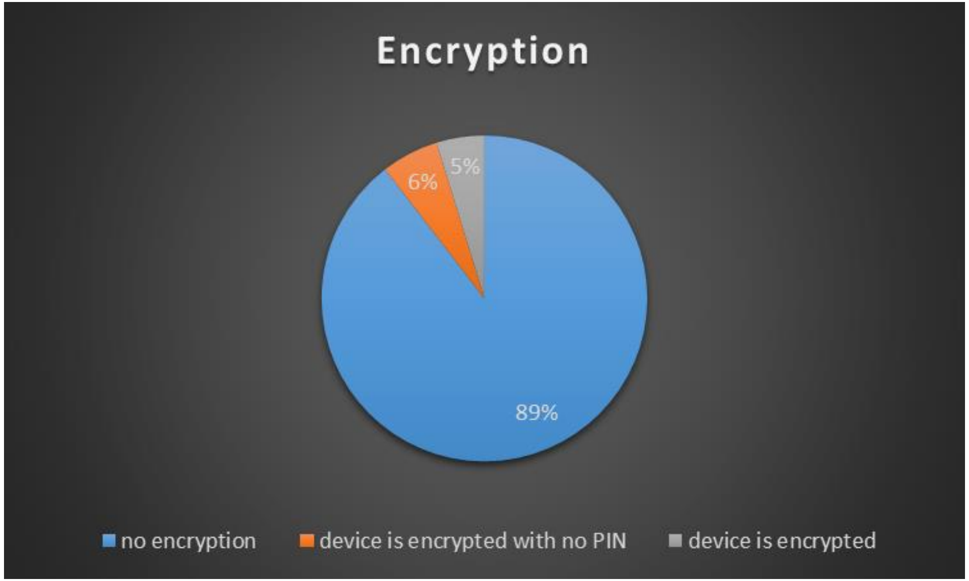
IP Geo	DNS IP Geo
Russia	USA
Ukraine	USA
USA	Russia
USA	Iran, Islamic Republic of
…	…

Other anomalies (Xposed)

- Still on a very low level (< 0.1%), but growing

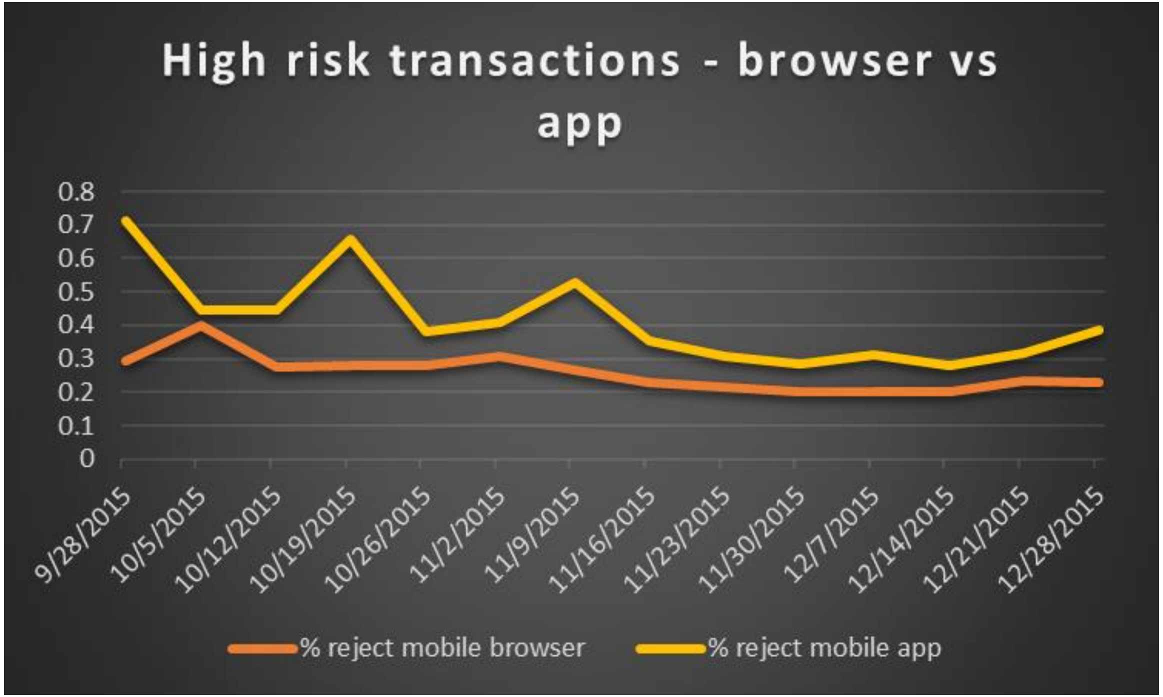


Device Encryption



Android only

Surprisingly, mobile app transactions represent more high risk transactions



Myths / Assumptions

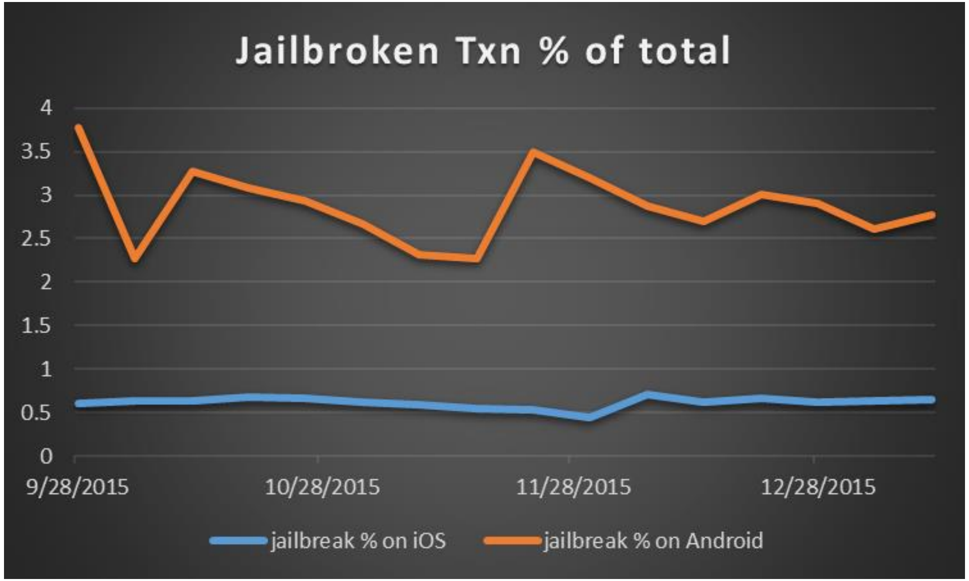
Operating systems are converging

- Windows 10
- Mac OS/X – iOS
- Android – Chrome

- When is an OS a mobile OS?

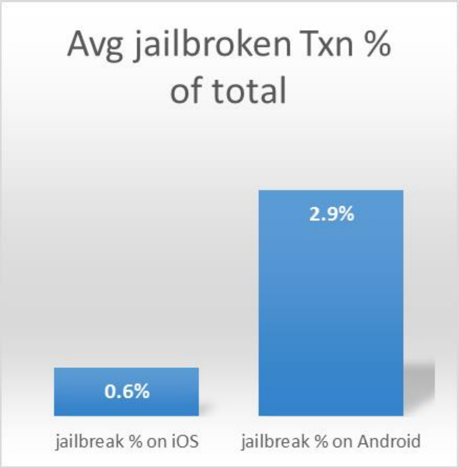
Different OS's have different attack surface

- No surprise
  - Ecosystem
- Mobile Ecosystem is much more diverse



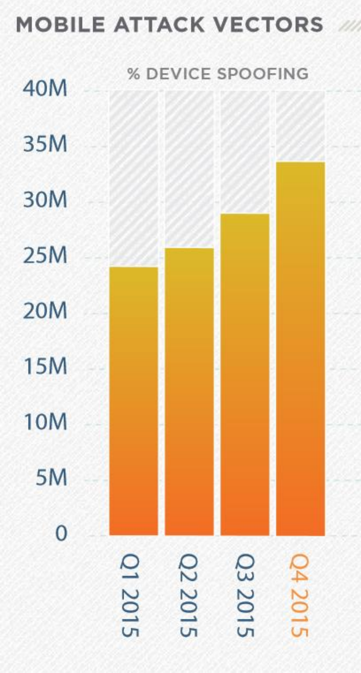
Jailbreaking

- Jailbroken devices are not as commonly used on a global scale
- But they do represent a significantly higher risk if they are being used



OS anomalies

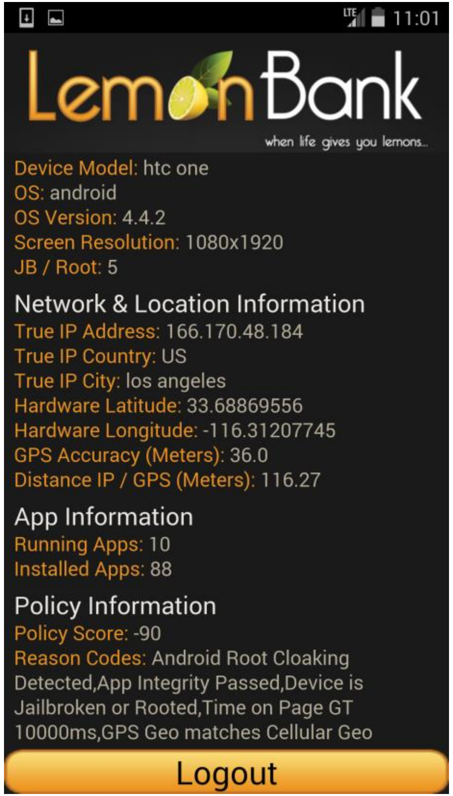
- There are plenty of anomalies with mobile traffic that is there for the taking
- Browser-string vs TCP fingerprint



Take advantage of additional information from mobile devices

Mobile Location

- IP Address Location
- DNS IP Address Location
- Hardware / GPS Location
- Carrier Location



Device Model: htc one
OS: android
OS Version: 4.4.2
Screen Resolution: 1080x1920
JB / Root: 5

Network & Location Information
True IP Address: 166.170.48.184
True IP Country: US
True IP City: los angeles
Hardware Latitude: 33.68869556
Hardware Longitude: -116.31207745
GPS Accuracy (Meters): 36.0
Distance IP / GPS (Meters): 116.27

App Information
Running Apps: 10
Installed Apps: 88

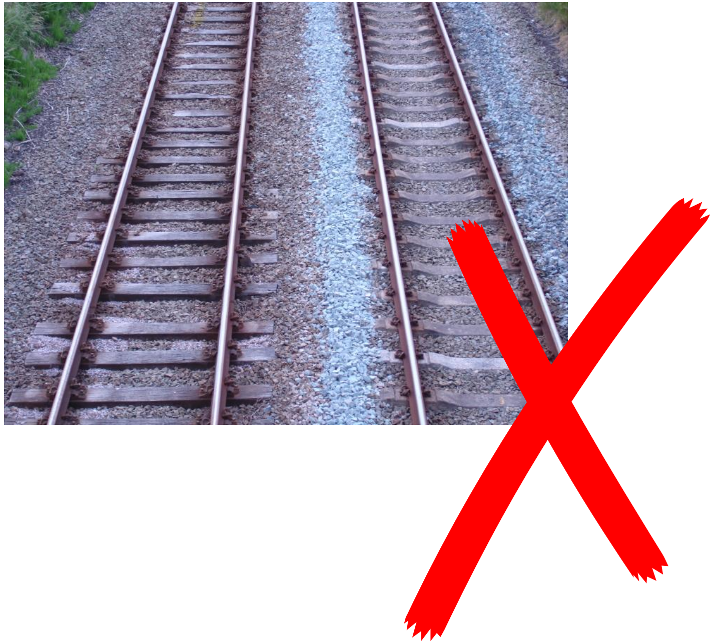
Policy Information
Policy Score: -90
Reason Codes: Android Root Cloaking Detected,App Integrity Passed,Device is Jailbroken or Rooted,Time on Page GT 10000ms,GPS Geo matches Cellular Geo

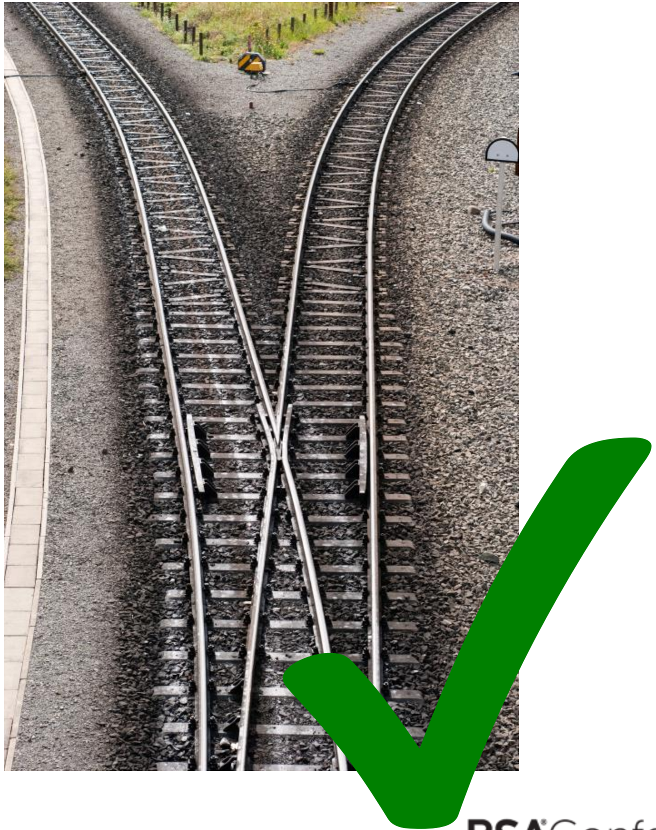
Huge amount of forensics information available

- Jailbreak detection
- Root Cloaking detection
- OS anomalies
- Mobile App Integrity
- Mobile App Reputation

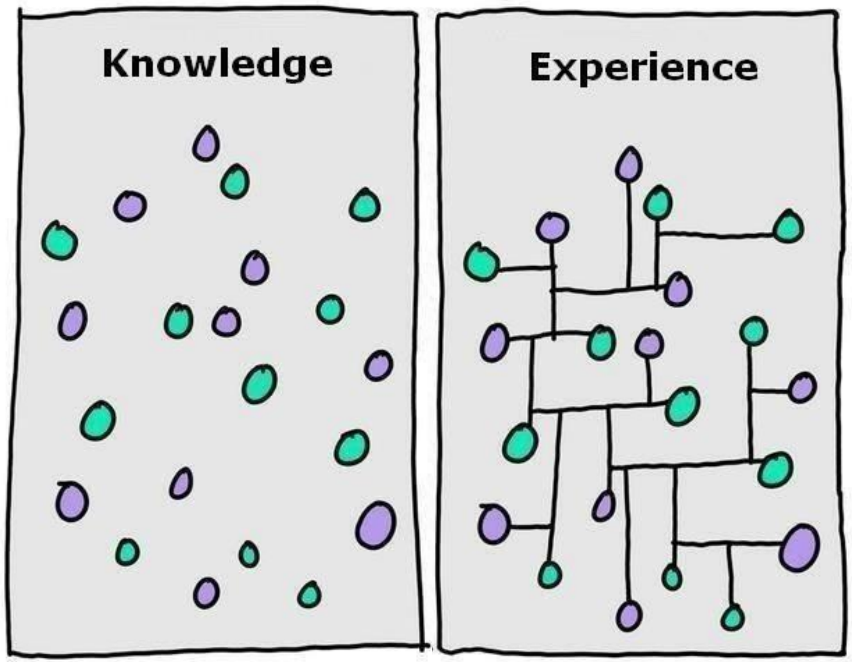
Conclusion

Mobile is part of the omni-channel





Rich data + advanced models = win


Knowledge
Experience