The Mobile Criminal: A Pocket Full of Maliciousness

Gunter Ollmann

CTO, DAMBALLA

Session ID: MBS-107

Session Classification: Intermediate

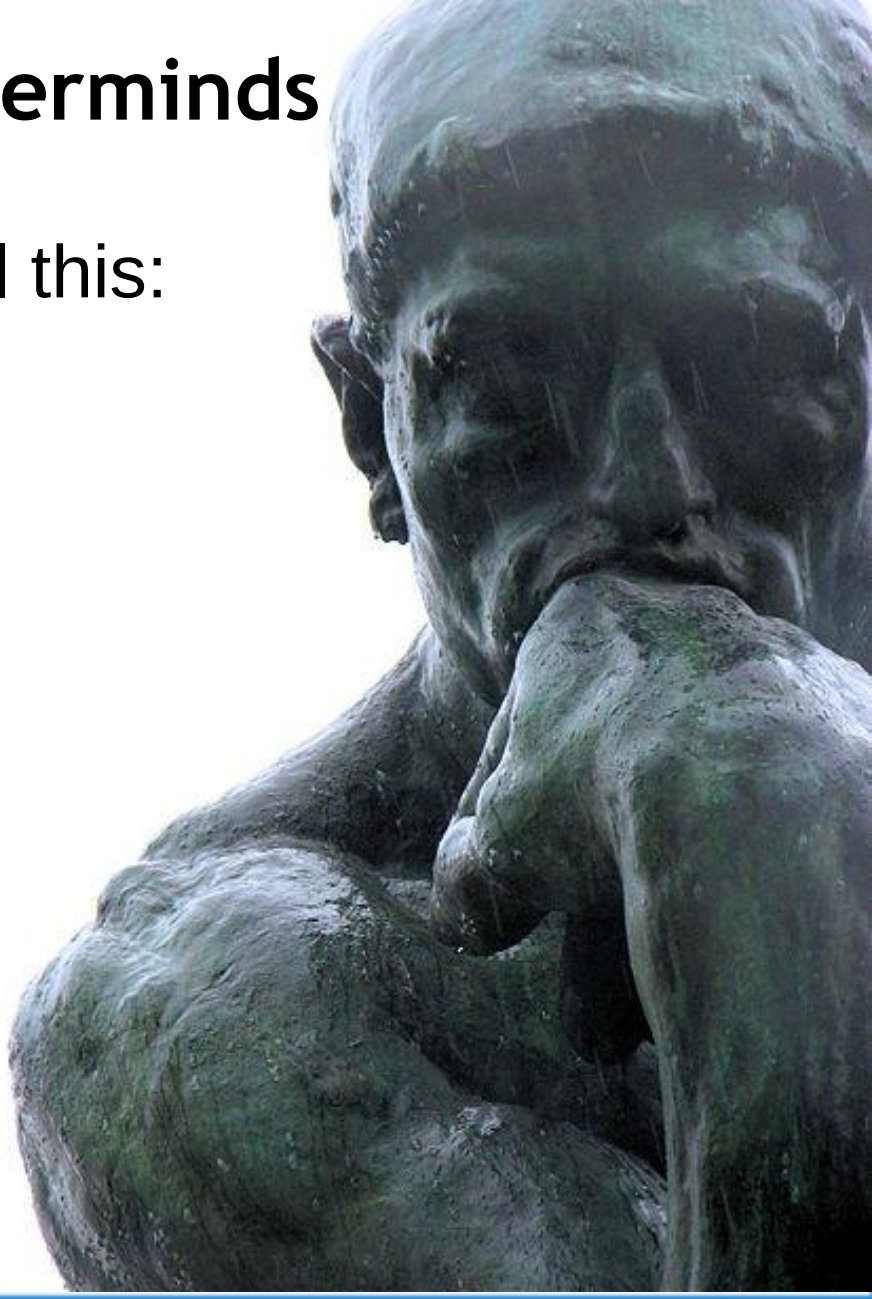
RSA CONFERENCE EUROPE 2012

About Me

- Gunter Ollmann
  - CTO & VP Research @ Damballa
    - IOActive – Advisory board
    - UGA – Advisory board
    - M3AAWG – Board of directors
  - Formerly:
    - IBM – Chief Security Strategist
    - ISS – Director of X-Force
    - NGS – Professional Services Director
  - Can be found/followed/located at:
    - Email – gollmann<at>damballa<dot>com
    - Twitter - @gollmann
    - Blog – http://blog.damballa.com
    - Blog - http://technicalinfodotnet.blogspot.com

About the research masterminds

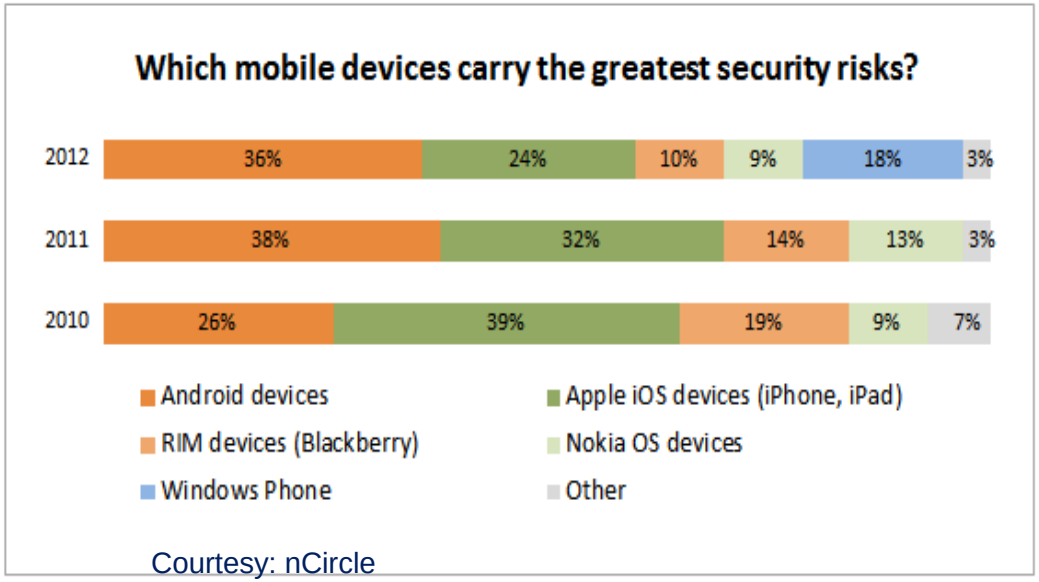
- The masterminds behind all this:
  - Chaz Lever
  - Manos Antonakakis



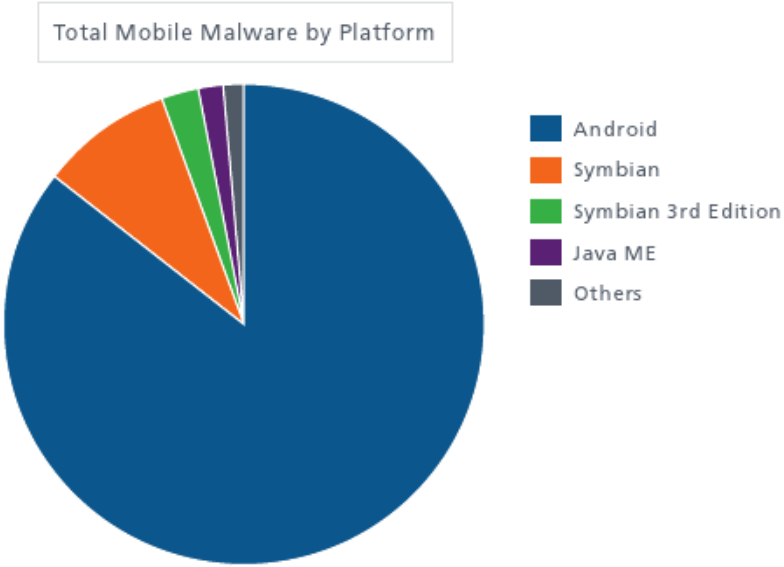
Threat Perspective

Perspective

- What are others saying about the mobile threat?
  - It's getting bigger…
  - It's evolving faster…
  - It's more sophisticated…
  - It's more dangerous than ever…



Courtesy: nCircle



Courtesy: McAfee 2012 Threat Report

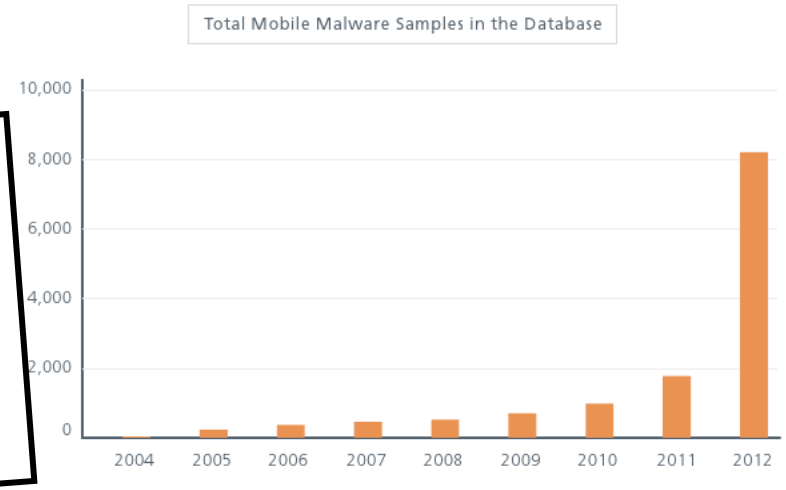
Perspective

- Victims, victims, everywhere…
  - 13 million infected handsets H1 2012 (via NetQin in China)
    - Up 177% from a year ago
    - 3.7m devices infected in June alone
  - 17,676 mobile malware programs H1 2012
    - Up 42% from H2 2011
    - 5,582 android malware in June alone
  - A quarter of the detected malware came from China
    - 17 percent from Russia
    - 16.5 percent from U.S.A

Perspective

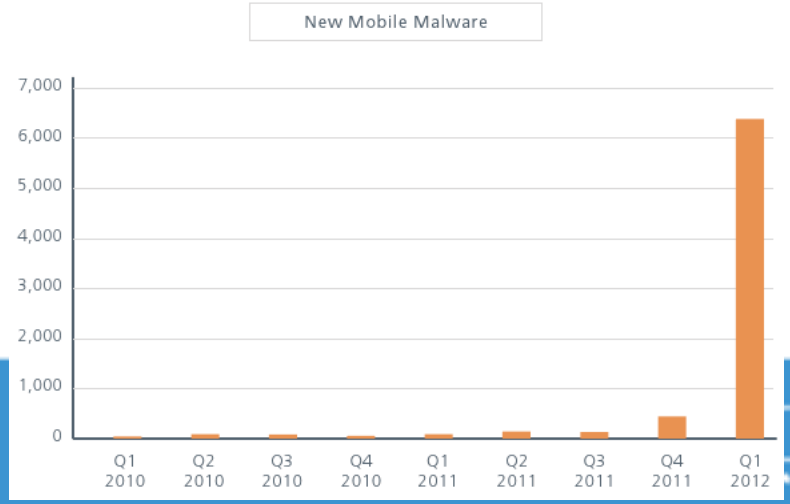
- Where are the numbers/proof coming from?
  - App store monitoring
  - On-device antivirus vendors

McAfee 2012 threat report:
"Android threats now reach almost 7,000, with more than 8,000 total mobile malware in our database."

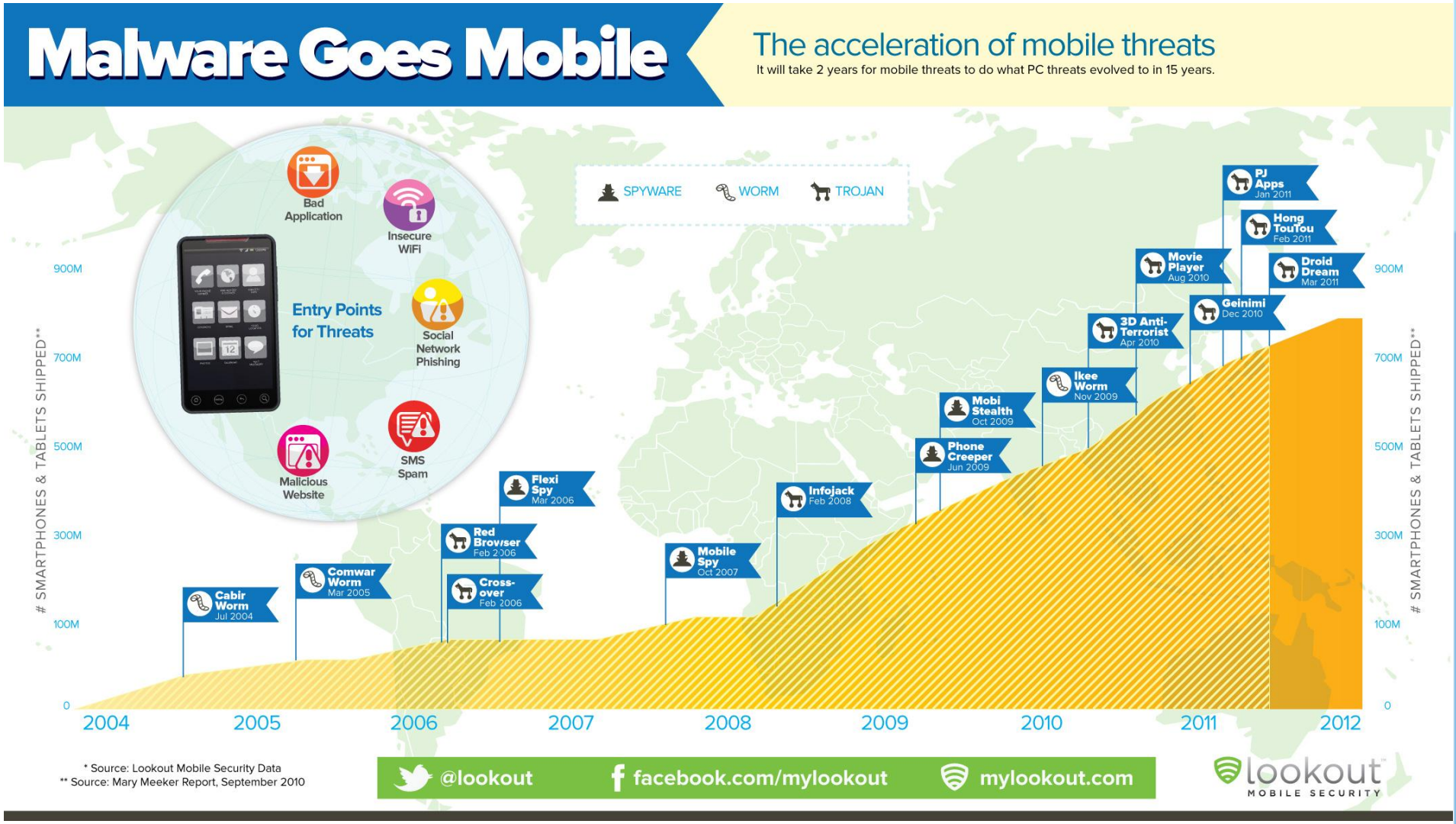


The number of modifications and families of mobile malicious programs in Kaspersky Lab's records as of 1 January 2012 is shown in the table below.

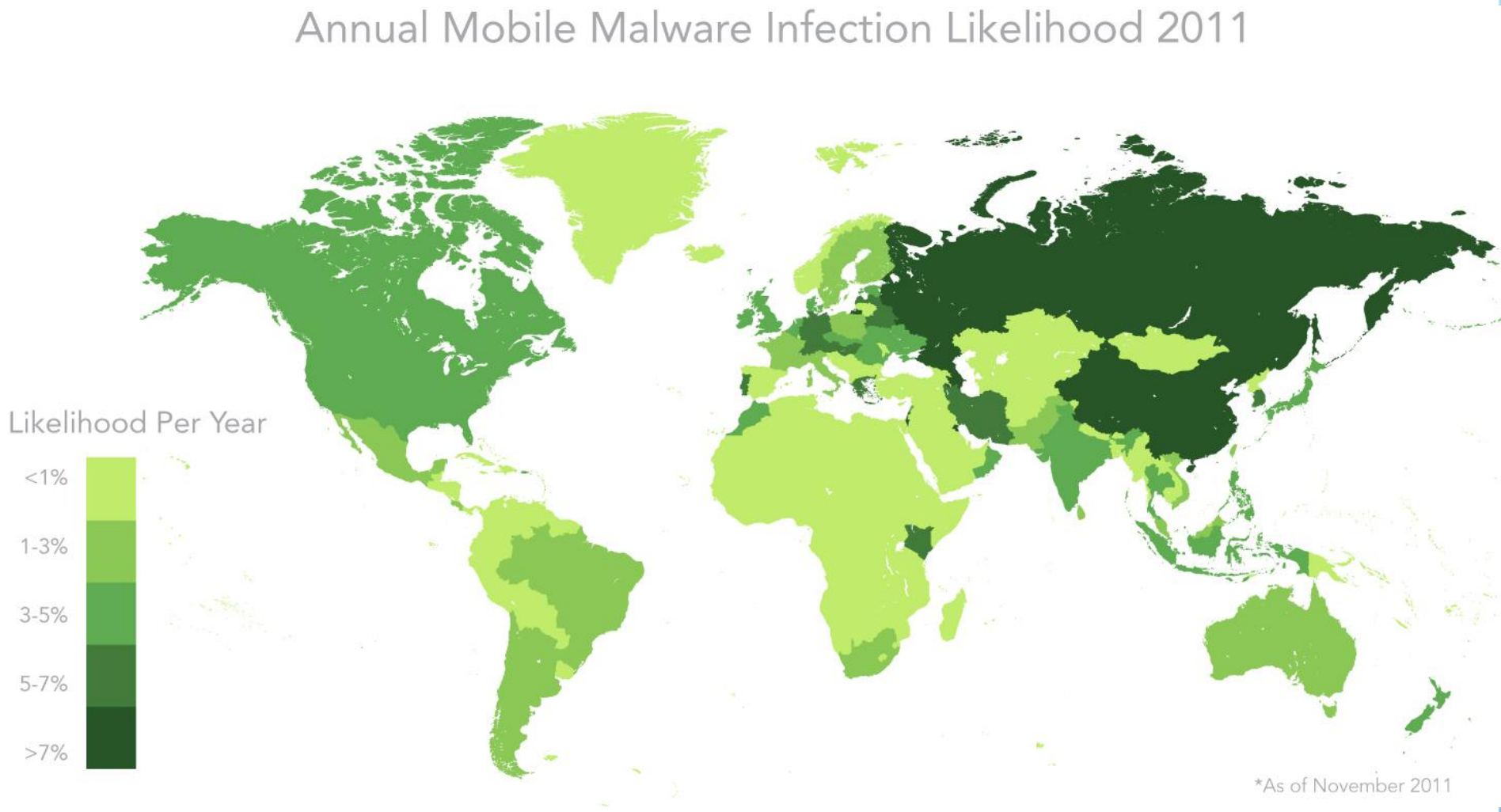
Platform	Modifications	Families
Android	4139	126
J2ME	1682	63
Symbian	435	111
Windows Mobile	81	23
Others	19	8



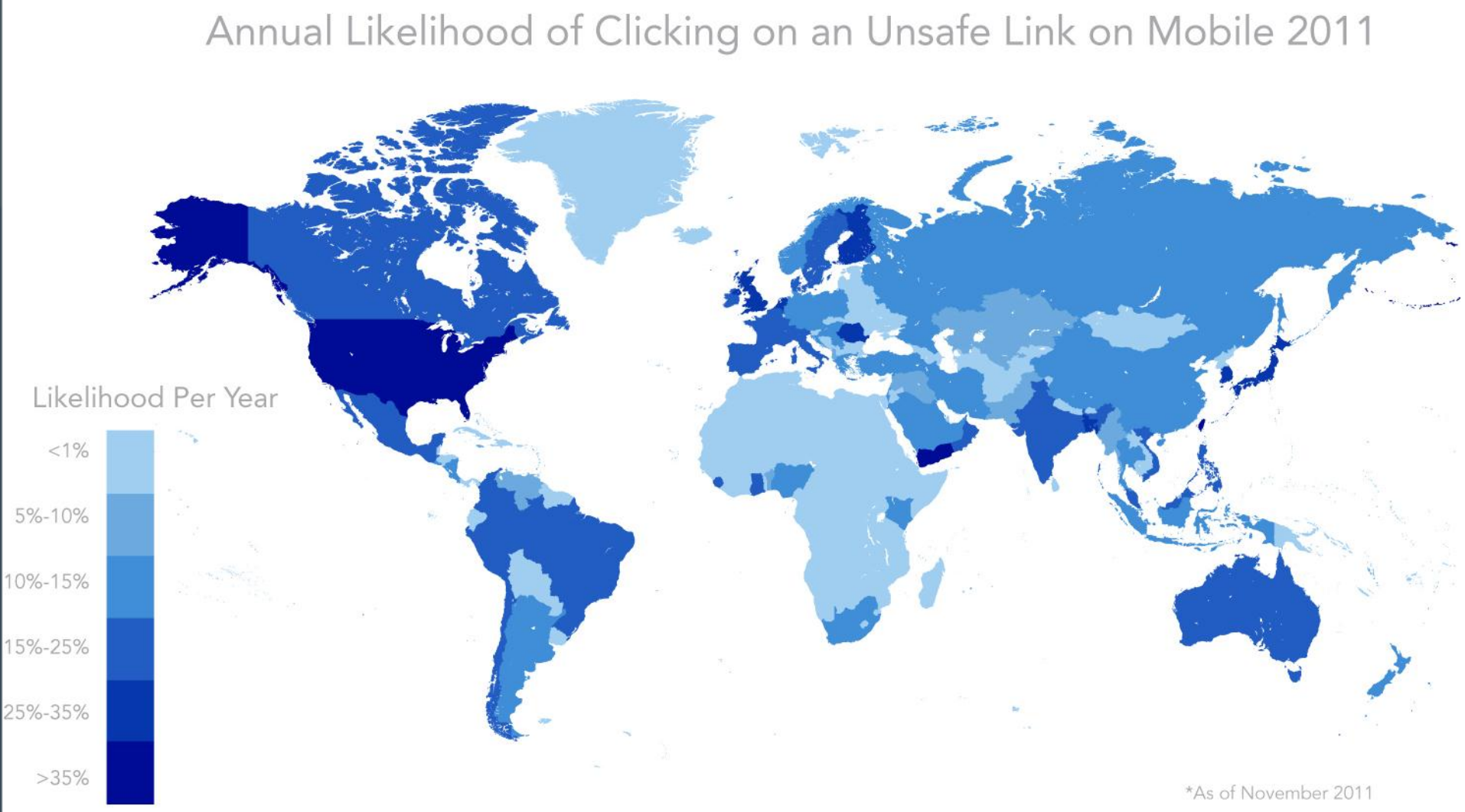
What's the story?



Evolving landscape

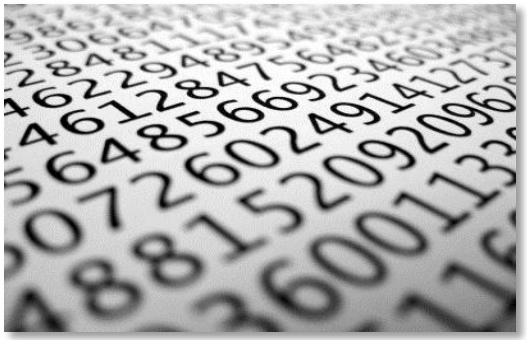


Evolving landscape



Are the threat numbers real?

- There's a difference…
  - Between malware samples and malware families
  - Between malware downloads and malware infections
  - Between attempts to install and successfully installed malware



- Measurements reflect visibility
  - Static analysis of new apps on stores
  - Monitoring app store download statistics
  - Vendor specific antivirus stats on their *own* customers
  - Criminal operator's C&C connections

The “Malware”

Malware objectives

- Malware functionality and objectives changing
  - Evolution of device capabilities
  - Reflects changing user requirements

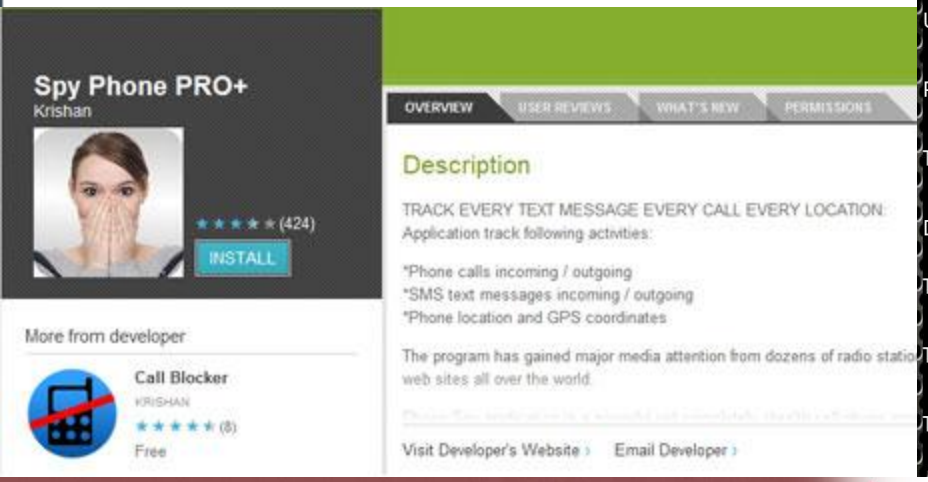
- What's guiding the evolution of mobile threats?
  - Understand where the money is…
  - Figure out how to "launder" the money…

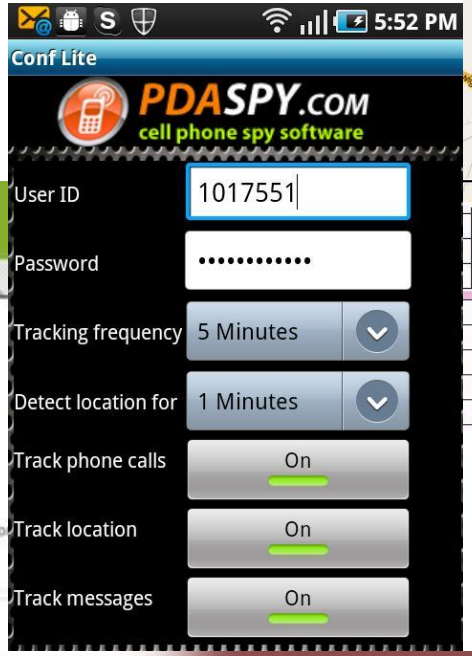
Evolving threat sophistication

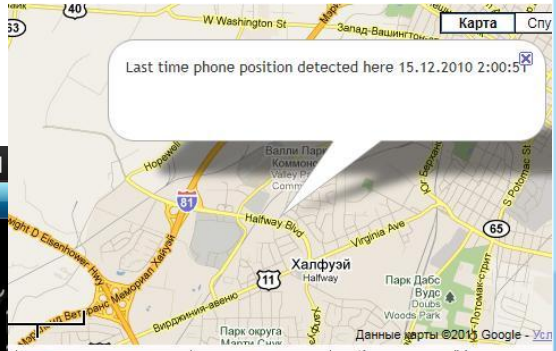
- Pain-in-the-arse botherware
- Premium-rate SMS
- Ad substitution
- Click-fraud
- Pay-per-install
- TAN/out-of-band interception
- Rootkits and backdoors
- Identity hijacking

Opt-in spyware

- Commercial spying applications
  - Spouse monitoring etc.







15.12.2010 2:00:51	+39° 37' 57.40"	-77° 45' 6.30"	Google Maps
15.12.2010 1:49:46	+39° 37' 57.40"	-77° 44' 6.30"	Google Maps
15.12.2010 1:35:59	+42° 37' 57.40"	-77° 44' 6.30"	Google Maps

Type	Number	Duration	Time
	Sweetheart <+1324xxxxxxx>	00:01:08	15.12.2010 9:09:48
	Honey<+132xxxxxxx>	00:00:24	15.12.2010 9:04:17
	+1732xxxxxxx	00:00:11	15.12.2010 0:04:20
	+1201xxxxxxx	00:00:18	15.12.2010 0:03:41

SMS

Type	Number	Message	Time
	+1201xxxxxxx	I want you NOW	15.12.2010 3:41:28
	+1732xxxxxxx	Hubby at home, don't call me now	15.12.2010 1:12:41
	+1221xxxxxxx	as always, come and get it	15.12.2010 0:35:35
	+1732xxxxxxx	You rock darling, my wife leaving tomorrow	15.12.2010 0:33:51
	221xxxxxxx	have some pot ? need asap	15.12.2010 0:33:51
	201xxxxxxx	I miss you a lot	15.12.2010 0:26:57

Government malware/spyware

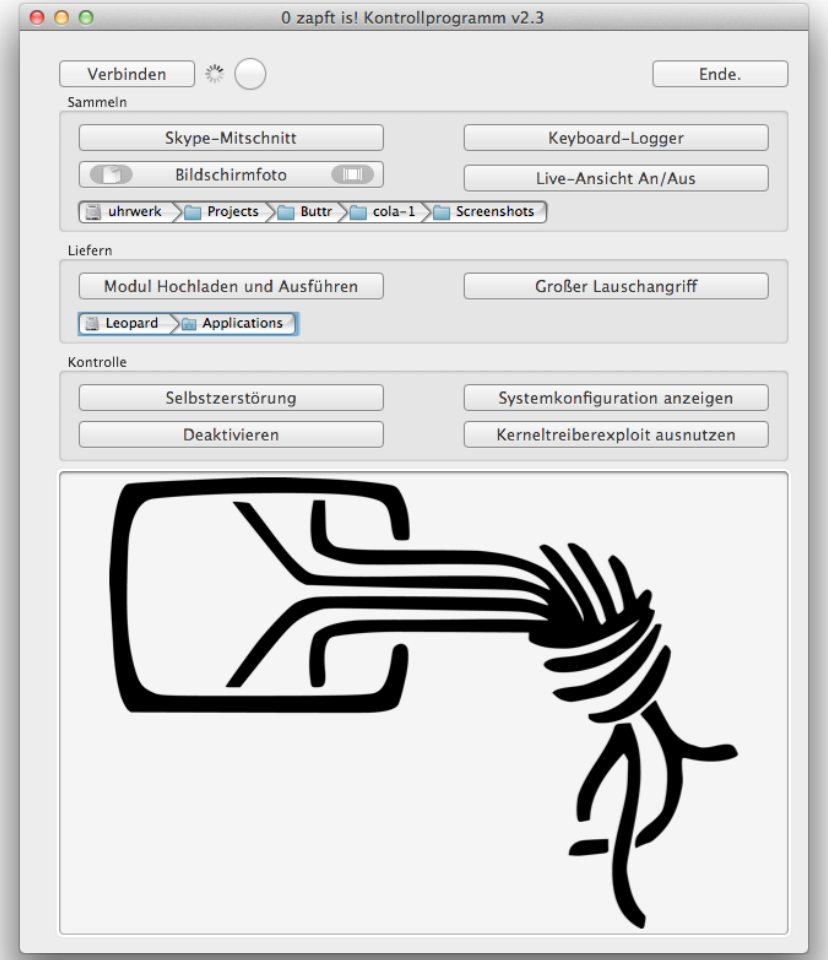
- FinFisher for iOS
  - Developed for Arm7, built against iOS SDK 5.1 on OSX 10.7.3 and it appears that it will run on iPhone 4, 4S, iPad 1, 2, 3, and iPod touch 3, 4 on iOS 4.0 and up.
  - IOS,Android, Symbian, Blackberry, Windows Mobile

The bundle is called "install_manager.app" and the contents of it are:

```
99621a7301bfd00d98c222a89900aeef ./data
1f73ebf8be52aa14d4d4546fb3242728 ./_CodeSignature/CodeResources
9273880e5baa5ac810f312f8bd29bd3f ./embedded.mobileprovision
2cbe06c89dc5a43ea0e0600ed496803e ./install_manager
23b7d7d024abb0f558420e098800bf27 ./PkgInfo
11e4821d845f369b610c31592f4316d9 ./Info.plist
ce7f5b3d4bfc7b4b0da6a06dccc515f2 ./en.lproj/InfoPlist.strings
3fa32da3b25862ba16af040be3451922 ./ResourceRules.plist
```

Lawful interception

- German police Trojan
- German constitutional court ("Bundesverfassungsgericht")
  - February 27 2008 forbade the use of malware to manipulate German citizen's PCs
  - "Quellen-TKÜ" (the term means "source wiretapping" or lawful interception at the source).
- Bundestrojaner light
  - Concealed as "Quellen-TKÜ"
  - The trojan can, for example, receive uploads of arbitrary programs from the Internet and execute them remotely. This means, an "upgrade path" from Quellen-TKÜ to the full Bundestrojaner's functionality is built-in right from the start.
  - Activation of the computer's hardware like microphone or camera can be used for room surveillance.



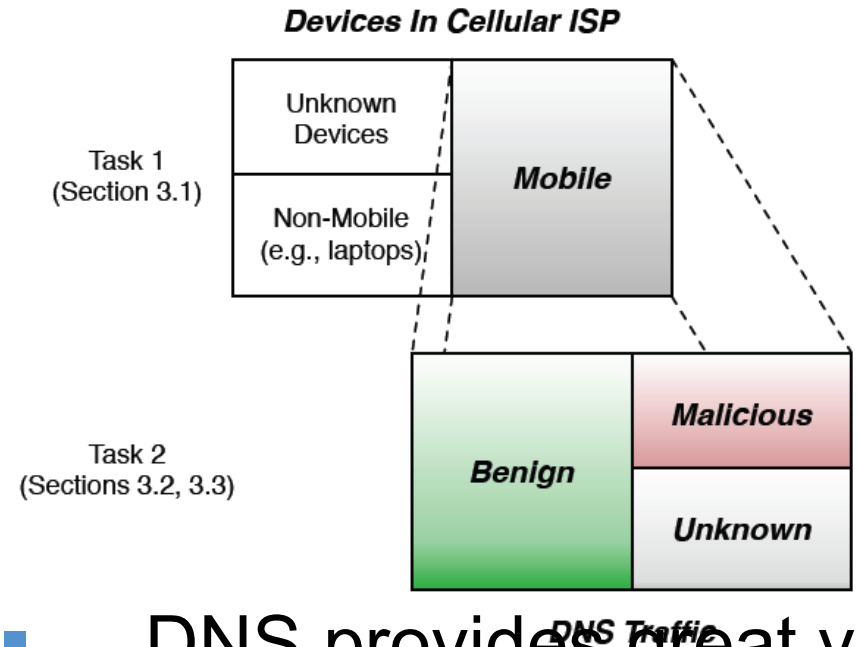
The Control

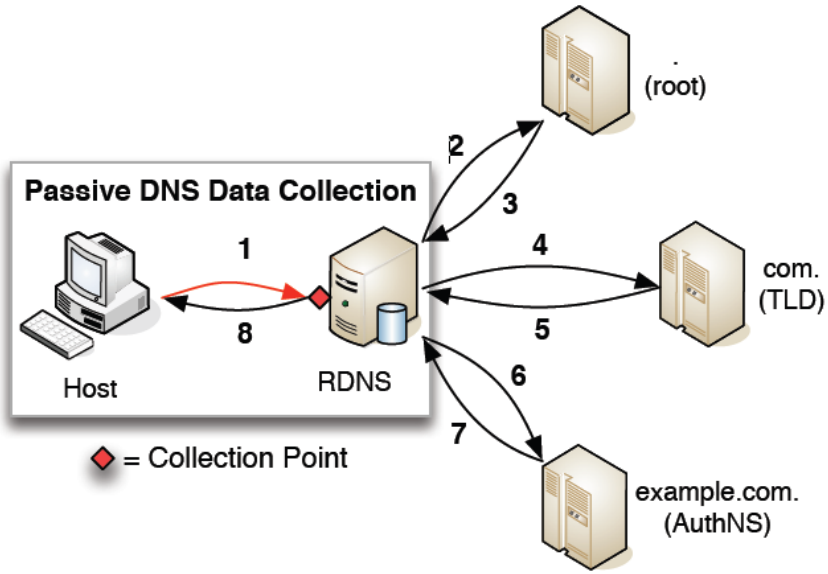
- “Malware” is just a tool
  - Modern malware communicates with its owners/controllers
  - Knowing who controls the malware defines the threat
- What is the “malware” talking to?
  - What and where are the C&C infrastructure?
- Network traffic can yield answers…

Malicious Traffic

Cellular ISP Visibility

- If you want to know what infections are *really* out there, you need to be a cellular ISP!





- …DNS provides great visibility and retains privacy

Qualifying maliciousness

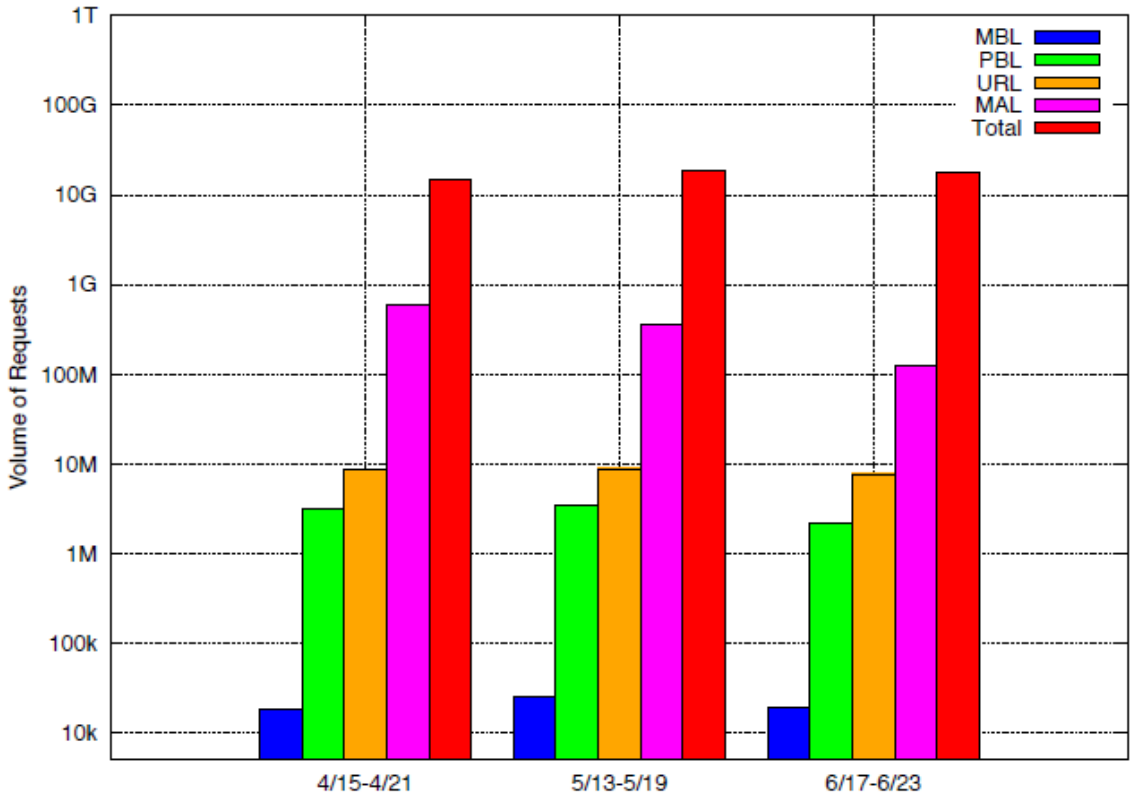
- Questionable destinations (by domain name):
  - Public blacklist data (PBL),
  - Phishing and drive-by download evidence (URL),
  - Hosts accessed by known malicious applications (MAL)
  - Mobile blacklist (MBL) containing 2,914 domains known to be associated with mobile malware or mobile malware operators

Overlapping Hosting Infrastructure

- After characterizing the cellular pDNS data, we observed XXXX unique hosts contacted by mobile devices over a period of six days.
- Only 3.3% (XXXX) of these hosts were outside of the non-cellular pDNS evidence we used for this work.

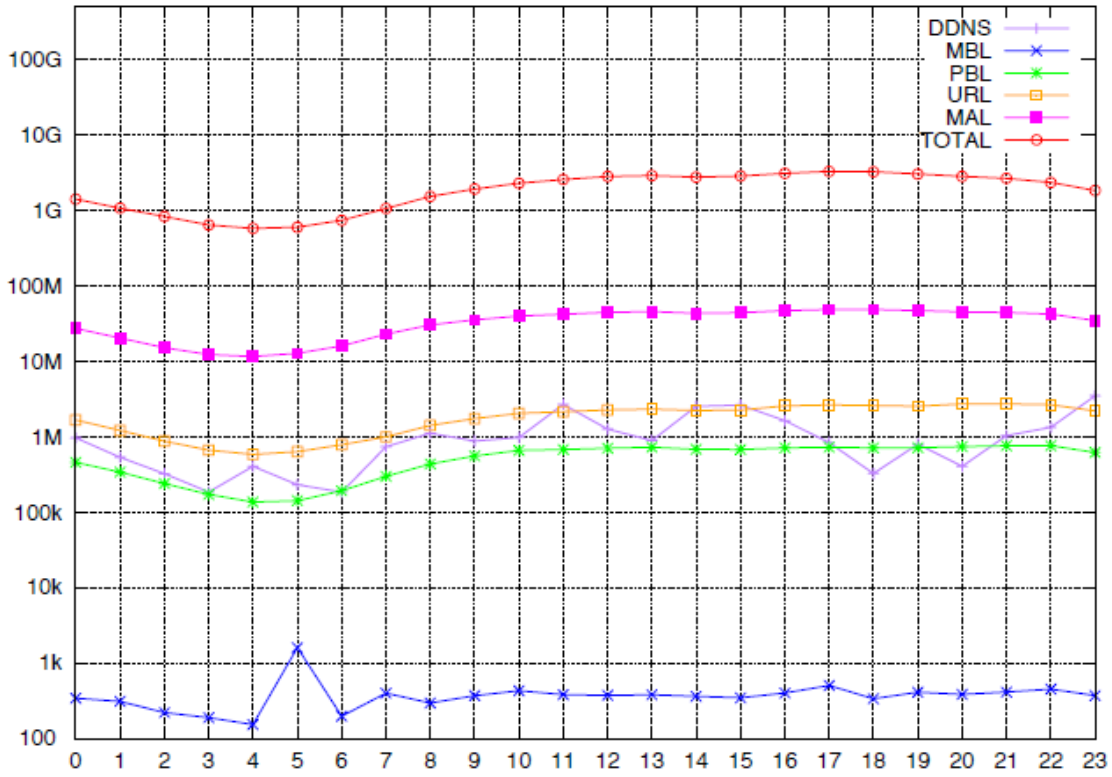
Malicious domain requests

- Volume of requests to domains with malicious
- evidence visited by mobile devices in cellular network.



Malicious domain requests

- Hourly analysis of request volume for various
- types of domains observed from mobile devices.



Domains from Malicious Apps

Malware Family	# Assoc. Domains	#Devices (Any type)	#Devices (Mobile only)
Crusewin	1		
DroidKungFu	1		
Fatakr *	1		
Geinimi	10		
GGTracker	2		
Plankton	1		
SndApps †	1		
SymbOS.Fakenotify *	1		
Threat ε *	1		
WalkInWat	1		

- Very few domains associated with discovered malicious apps were seen in pDNS data.

Tainted Hosts and Platforms

Platform	% Of All Devices	% Population requesting tainted hosts	% Total tainted host requests
iOS			
Android			
iOS or Android			
Indistinguishable Platform			

- Using the domains visited by a device, we can make educated guesses regarding the types of devices seen.
- iOS and Android devices visit similar percentages of tainted (i.e., potentially malicious hosts)

Shared Infrastructure

More of the same

- Same bad actors
  - C&C domains (and credentials) typically the same
  - C&C servers independent of malware agent and infected platform
  - Developing/distributing different malware

- More complex fraud systems
  - Desktop and smartphone agents to bypass multifactor auth
  - Phishing campaigns to deliver both malware elements
  - Social engineering of victims

Example: ZitMo

Trusteer Building trust online

Dear Customer!

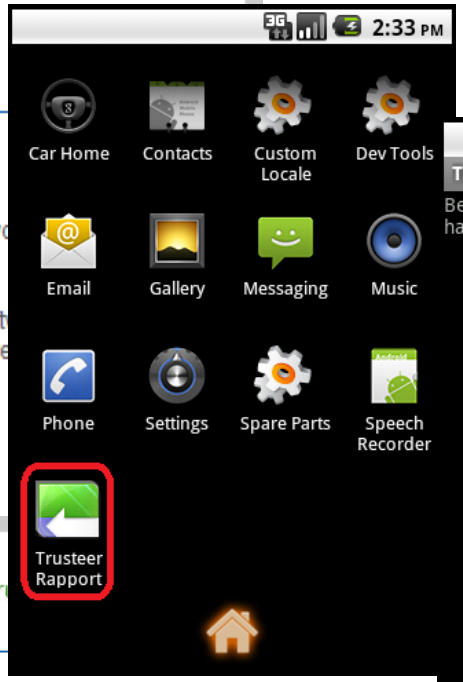
Trusteer is glad to announce the new mobile app which protects your phone while wo
banking, receiving and sending SMS and making calls.

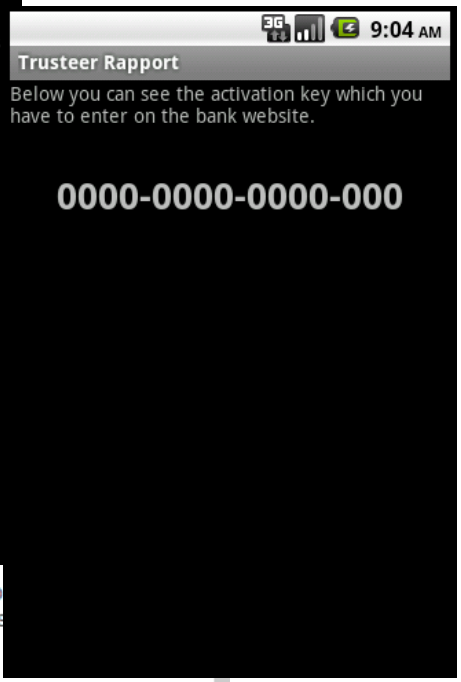
Over 22 millions customers, banks and financial instututions use our programm soft
payments, transfers and other operations securely. If you're working with our software
protected by professionals.

Please chose your phone's operating system:

- iOS (iPhone)
- BlackBerry
- Android
- Symbian (Nokia)
- Other

Continue





Trusteer Building tru

Due to the becoming more frequent internet fraud cases with text messages it is stro
recommended to the customers owning mobile phones with Android OS to install a s
which will help to protect you from fraud.

For the software installation open the internet browser on the mobile and enter the following URL address:

http:/[redacted].com/tr.apk

When the installation is completed you'll see a new program called "Trusteer Rapport" in the Application folder on your mobile. You need to start the program then enter the activation code indicated there into the field below and press "Activate".

Activation code: Activate

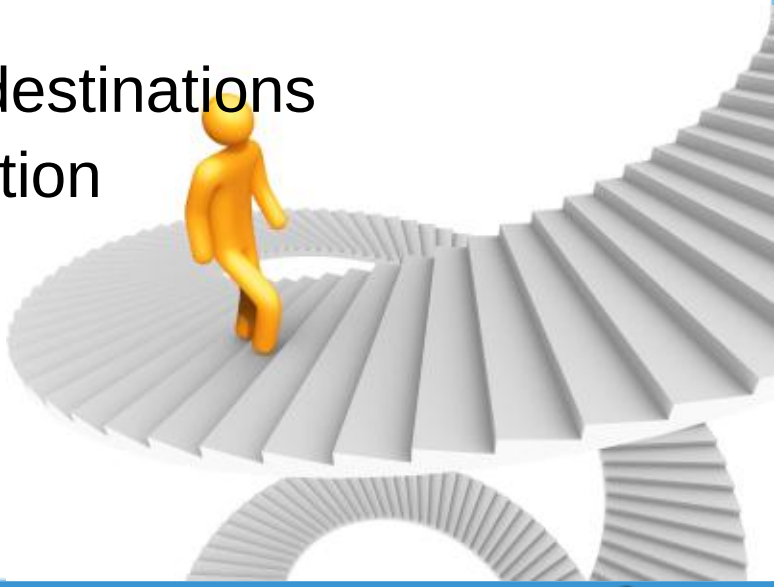
Dealing with the Mobile Threat

- What's changed/changing:
  - The malware agent (adding new OS's)
  - The social engineering message
  - The exploits

- What's NOT changed/changing:
  - The C&C language
  - The C&C hosting
  - The individuals behind the threat
- Evolution of the threat, not a new threat!

Next steps

- Host-based defenses:
  - Multi-platform support and correlation of events
  - New agents and signatures for each threat component
- Network-based detection:
  - Communication channels and destinations
  - Hosting infrastructure classification



Apply…

How to Apply What You Have Learned Today

- In the first month following this presentation you should:
  - Educate your coworkers that any mobile device can be compromised and controlled by a remote entity… not just hackers
  - Review what technologies you already possess that could detect egregious communications
- Within six months you should:
  - Develop policies that govern the agents deployed within mobile devices that are/will connect to the corporate network
  - Deploy technologies capable of detecting and reporting the presence of mobile threats

Thank you

Email – gollmann<at>damballa<dot>com
Twitter - @gollmann