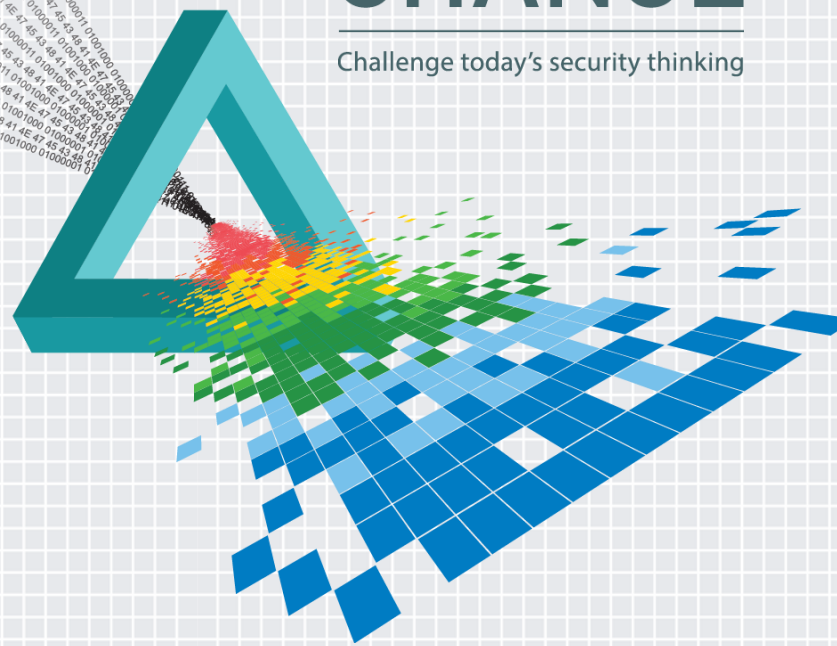
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: MBS-W01

Characterizing Malicious Traffic on Cellular Networks

A Retrospective

Chaz Lever

Researcher
Damballa, Inc
@chazlever

Mobile Malware

New Android Malware Steals Your Money Via SMS

FBI issues Android malware warning

Android Malware Infections Increase By 700%

Report: Android Has Become the Ultimate Malware Platform

Mobile malware jumped 75 percent in 2014: Report

Android is under attack: New malware threats tripled in Q2

PHONES

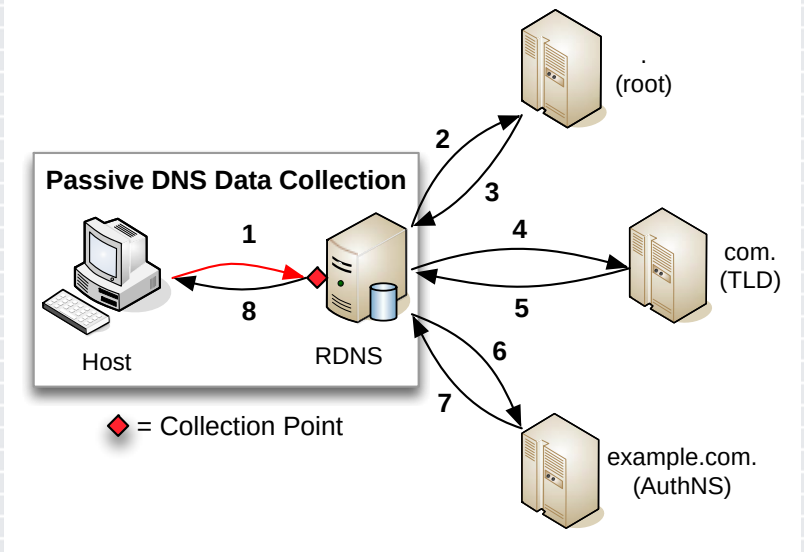
Mobile Malware Epidemic Looms

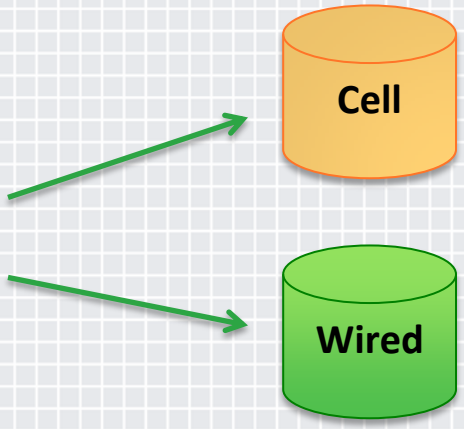
Mobile Malware Research

- Significant effort has been spent by researchers to characterize mobile applications and markets.
- Market operators have invested significant resources in preventing malicious applications from being installed.
- Extent to which mobile ecosystem is actually infected is *still* not well understood.

Use network level analysis to better understand the threat.

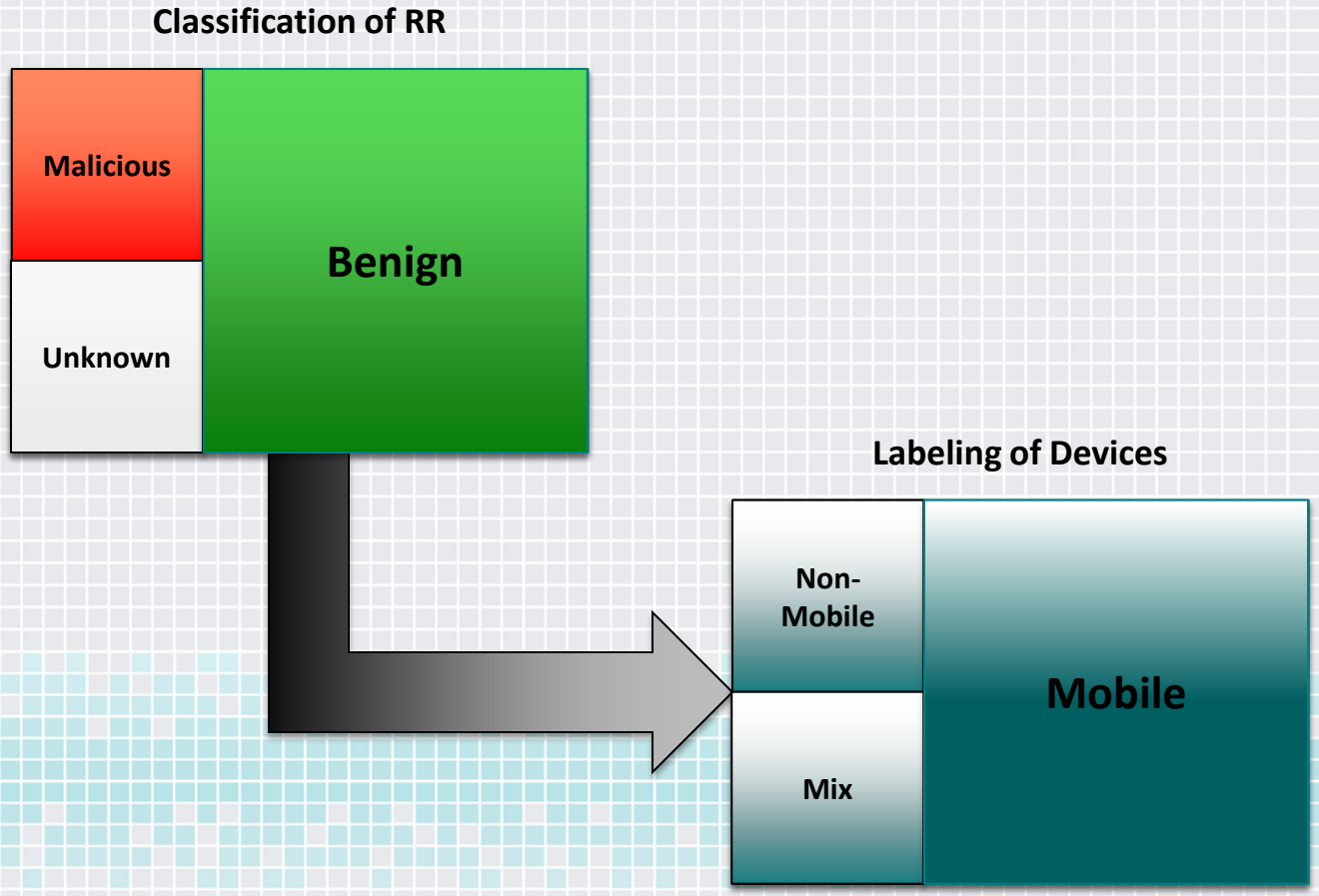
Data Collection





- Use passive DNS (pDNS) data collected at the recursive DNS (RDNS) level.
- Data collected from a major US cellular provider and a large traditional, non-cellular ISP.

Characterizing Cellular Traffic



Cellular pDNS Data Summary

Week (2012)	Hours	RRs	Domains	Hosts	Devices (Avg)
4/15 - 4/21	168	8,553,155	8,040,141	2,070,189	22,469,561
5/13 – 5/19	168	9,240,372	8,711,704	2,168,266	24,223,108
6/17 – 6/23	168	8,660,555	8,109,536	2,050,168	21,932,245
Total (Unique)	**504**	**16,298,114**	**14,828,149**	**3,053,704**	**22,874,971**

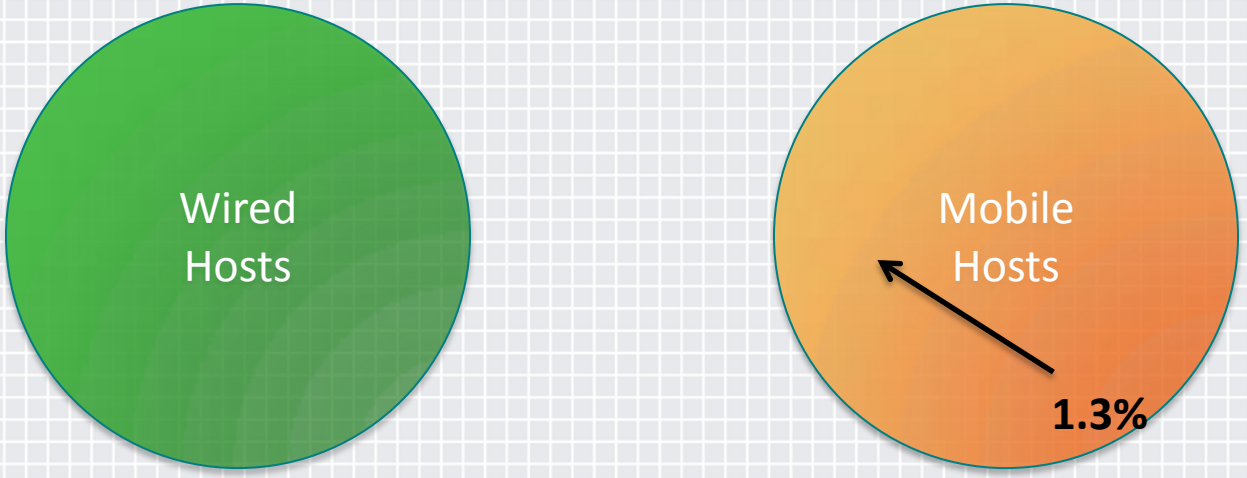
Week (2014)	Hours	RRs	Domains	Hosts	Devices (Avg)
11/01 – 11/07	168	178,752,268	158,214,788	18,673,671	132,152,348
11/08 – 11/14	168	185,125,832	163,740,910	21,179,148	152,832,654
11/15 – 11/21	168	188,458,108	166,929,111	18,617,397	159,200,303
11/22 – 11/28	168	183,678,777	162,213,521	8,963,386	160,788,608
11/29 – 11/30	48	60,706,045	53,244,354	5,768,628	137,285,304
Total (Unique)	**720**	**684,641,271**	**613,350,819**	**28,799,008**	**151,858,362**

Cellular pDNS Data Summary

Week (2012)	Hours	RRs	Domains	Hosts	Devices (Avg)
4/15 - 4/21	168	8,553,155	8,040,141	2,070,189	22,469,561
5/13 – 5/19	168	9,240,372	8,711,704	2,168,266	24,223,108
6/17 – 6/23	168	8,660,555	8,109,536	2,050,168	21,932,245
Total (Unique)	**504**	**16,298,114**	**14,828,149**	**3,053,704**	**22,874,971**

Week (2014)	Hours	RRs	Domains	Hosts	Devices (Avg)
11/01 – 11/07	168	178,752,268	158,214,788	18,673,671	132,152,348
11/08 – 11/14	168	185,125,832	163,740,910	21,179,148	152,832,654
11/15 – 11/21	168	188,458,108	166,929,111	18,617,397	159,200,303
11/22 – 11/28	168	183,678,777	162,213,521	8,963,386	160,788,608
11/29 – 11/30	48	60,706,045	53,244,354	5,768,628	137,285,304
Total (Unique)	**720**	**684,641,271**	**613,350,819**	**28,799,008**	**151,858,362**

Hosting Infrastructure



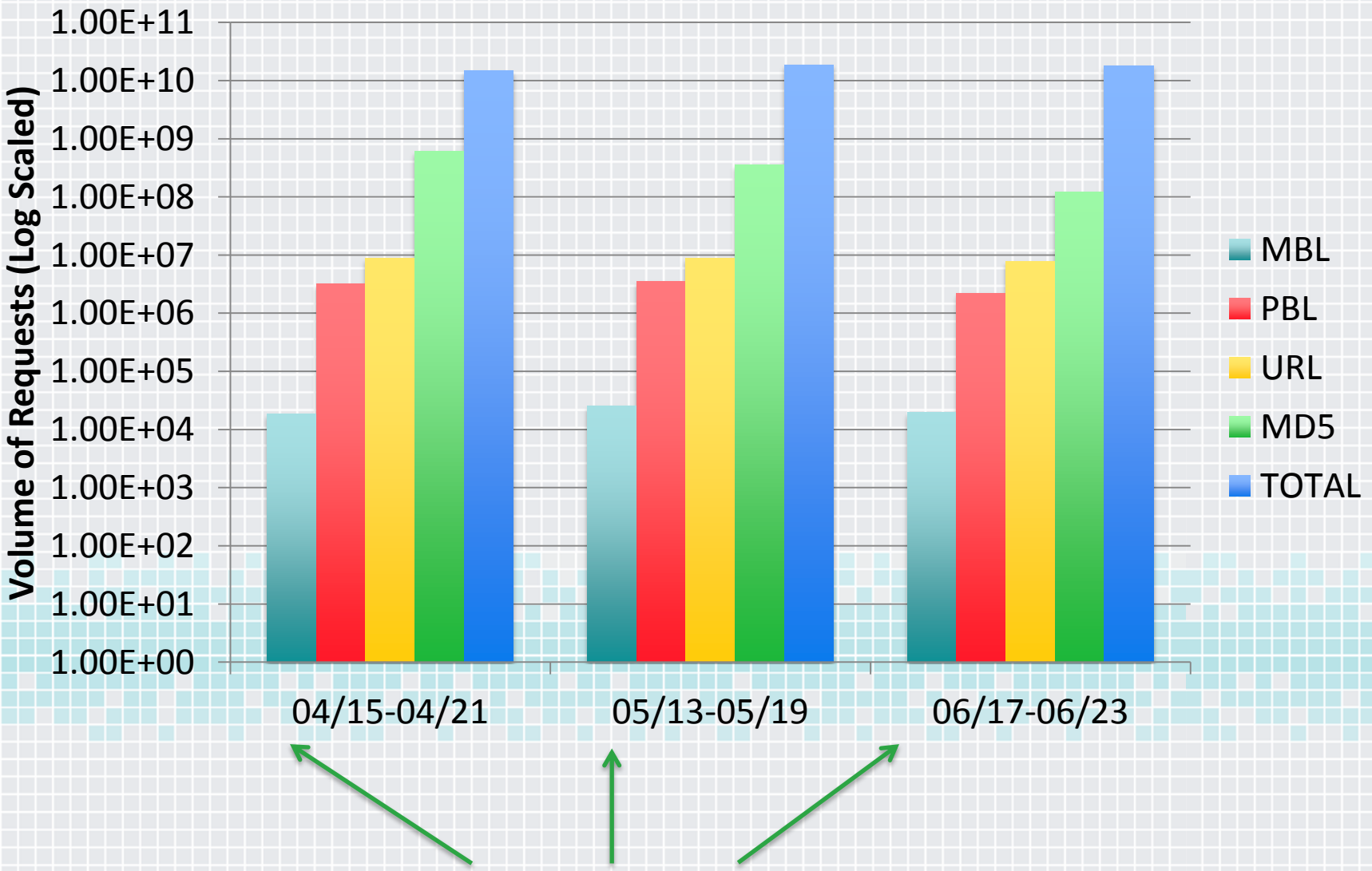
- Observed 2,762,453 unique hosts contacted by *mobile devices*.
- Only 1.3% (35,522) of “mobile” hosts were not in the set of hosts contained by historical non-cellular pDNS data.

The mobile Internet is really just the Internet.

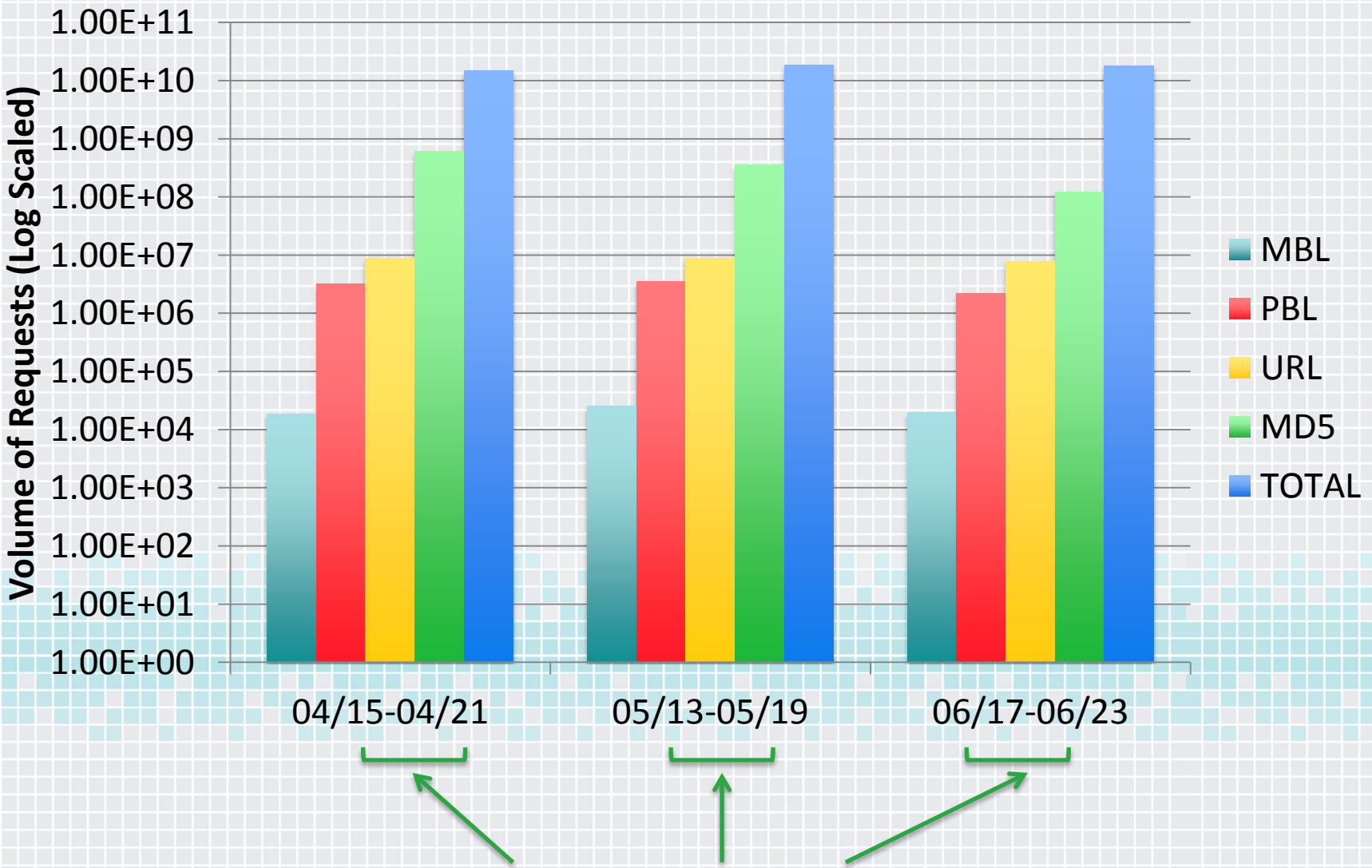
Evidence of Malware

- Public Blacklist (PBL)
- Phishing and Drive-by-Downloads (URL)
- Desktop Malware Association (MAL)
- Mobile Blacklist (MBL)

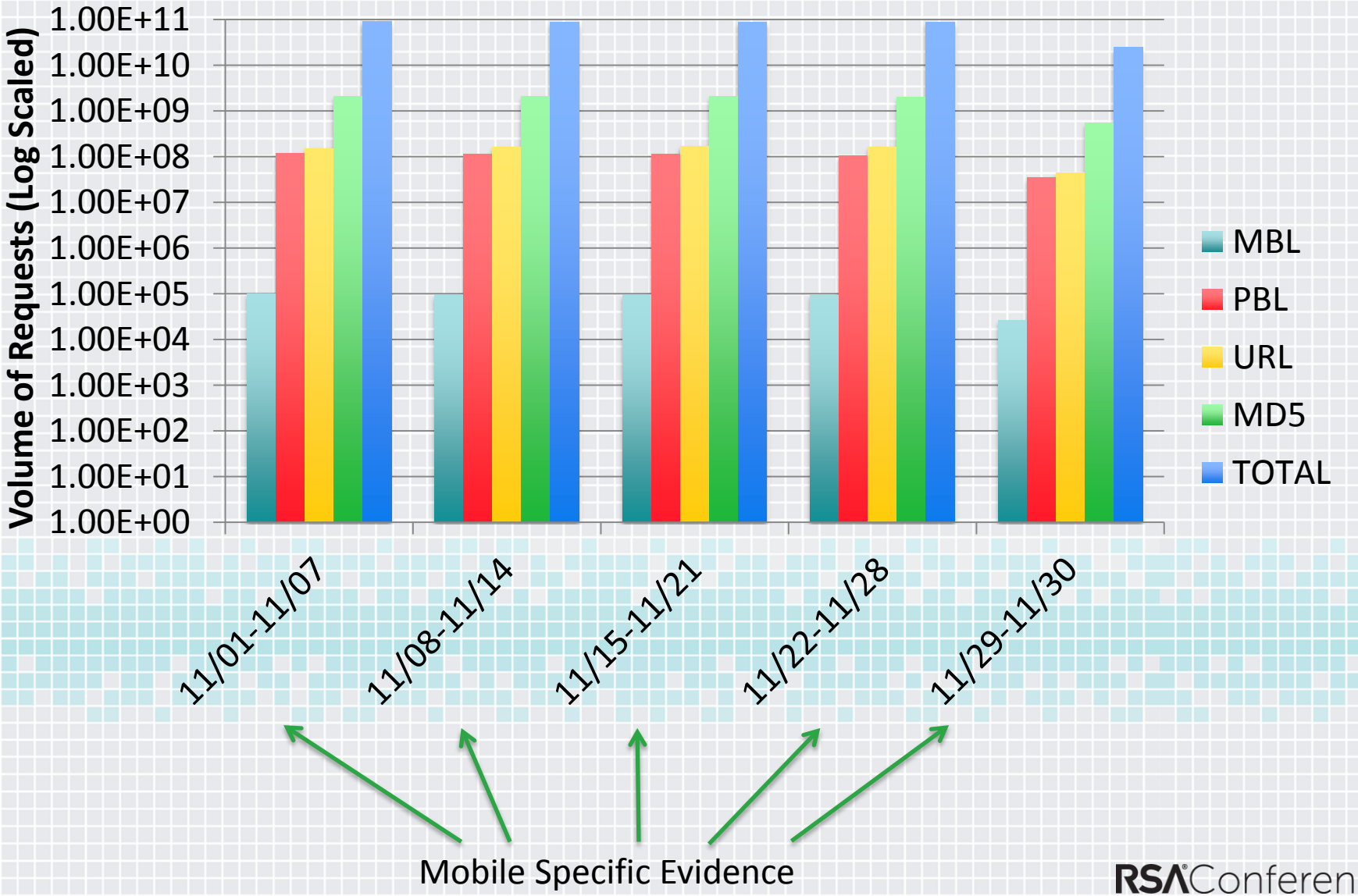
Observed Historical Evidence



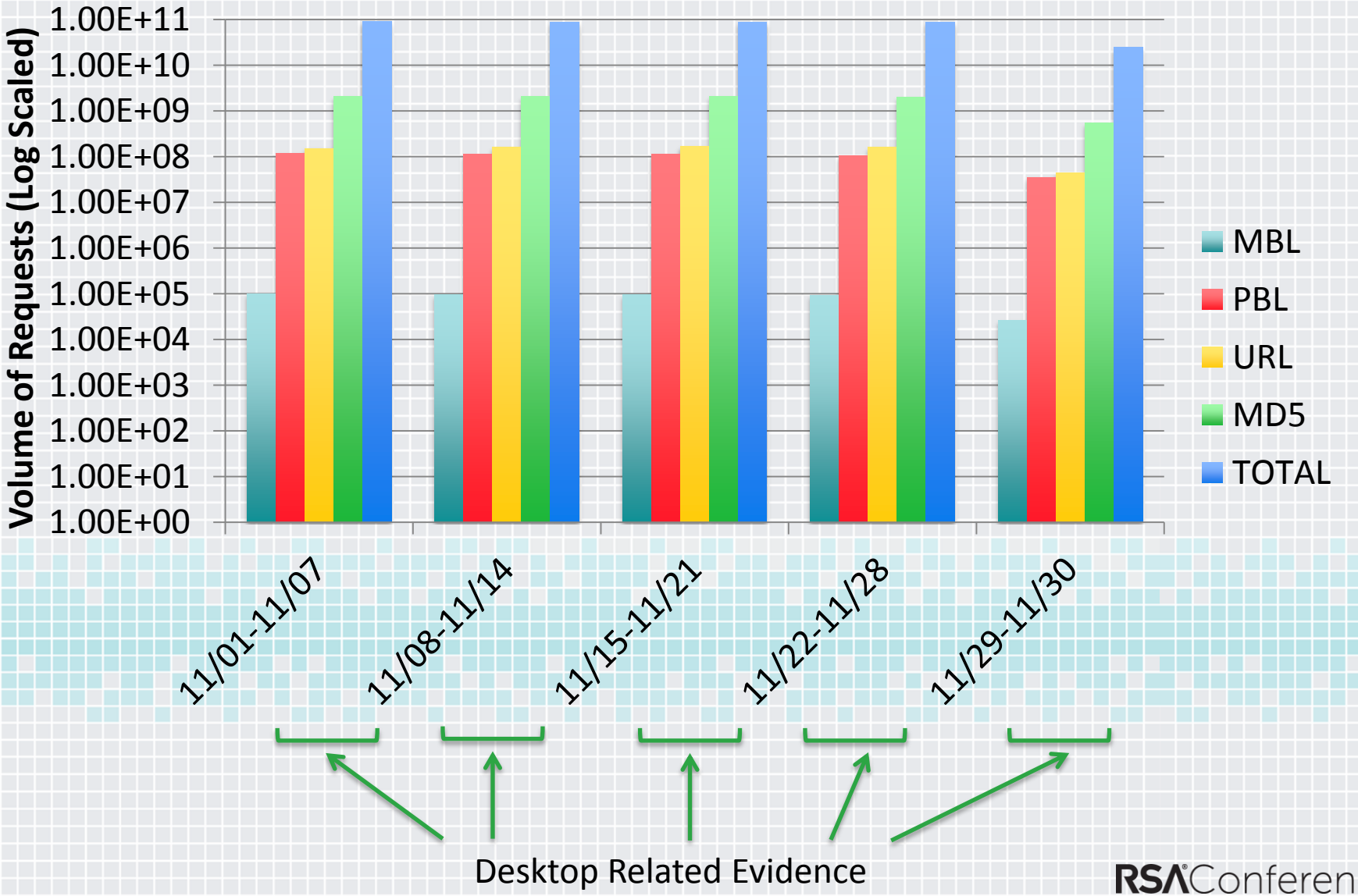
Observed Historical Evidence



Observed Historical Evidence (Redux)



Observed Historical Evidence (Redux)



Tainted Hosts and Platforms

Platform	% Population requesting tainted hosts (2012)	% Population requesting tainted hosts (2014)
iOS		
All other mobile (Android, etc.)		

Tainted Hosts and Platforms

Platform	% Population requesting tainted hosts (2012)	% Population requesting tainted hosts (2014)
iOS	31.6%	
All other mobile (Android, etc.)	68.4%	

Tainted Hosts and Platforms

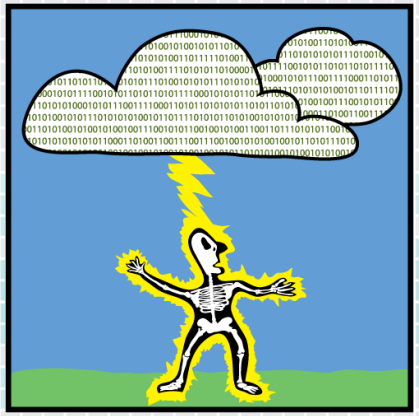
Platform	% Population requesting tainted hosts (2012)	% Population requesting tainted hosts (2014)
iOS	31.6%	38.9%
All other mobile (Android, etc.)	68.4%	61.1%

Tainted Hosts and Platforms

Platform	% Population requesting tainted hosts (2012)	% Population requesting tainted hosts (2014)
iOS	31.6%	38.9%
All other mobile (Android, etc.)	68.4%	61.1%

Mobile Malware in Numbers

- Only ***0.015% (3,492)*** out of a total of 23M *mobile* devices contacted MBL domains (observation period 2012).
- Only ***0.0064% (9,688)*** out of a total of 151M *mobile* devices contacted MBL domains (observation period 2014).
- According to National Weather Service, odds of an individual being struck by lightning in a lifetime is **0.01% (1/10,000)**!



Mobile malware is currently a real but small threat.

Market and Malware (M&A) Dataset

Market Name	Market Country	Date of Snapshot	# Unique Apps	# Unique Domains	# Unique IPs
Google Play*	US	09/20/11, 01/20/12	26,332	27,581	47,144
SoftAndroid	RU	02/07/12	3,626	3,028	8,868
ProAndroid	CN	02/02/12, 03/11/12	2,407	2,712	8,458
Anzhi	CN	01/31/12	28,760	11,719	24,032
Ndoo	CN	10/25/12, 02/03/12, 03/06/12	7,914	5,939	14,174

* Top 500 free applications per category only

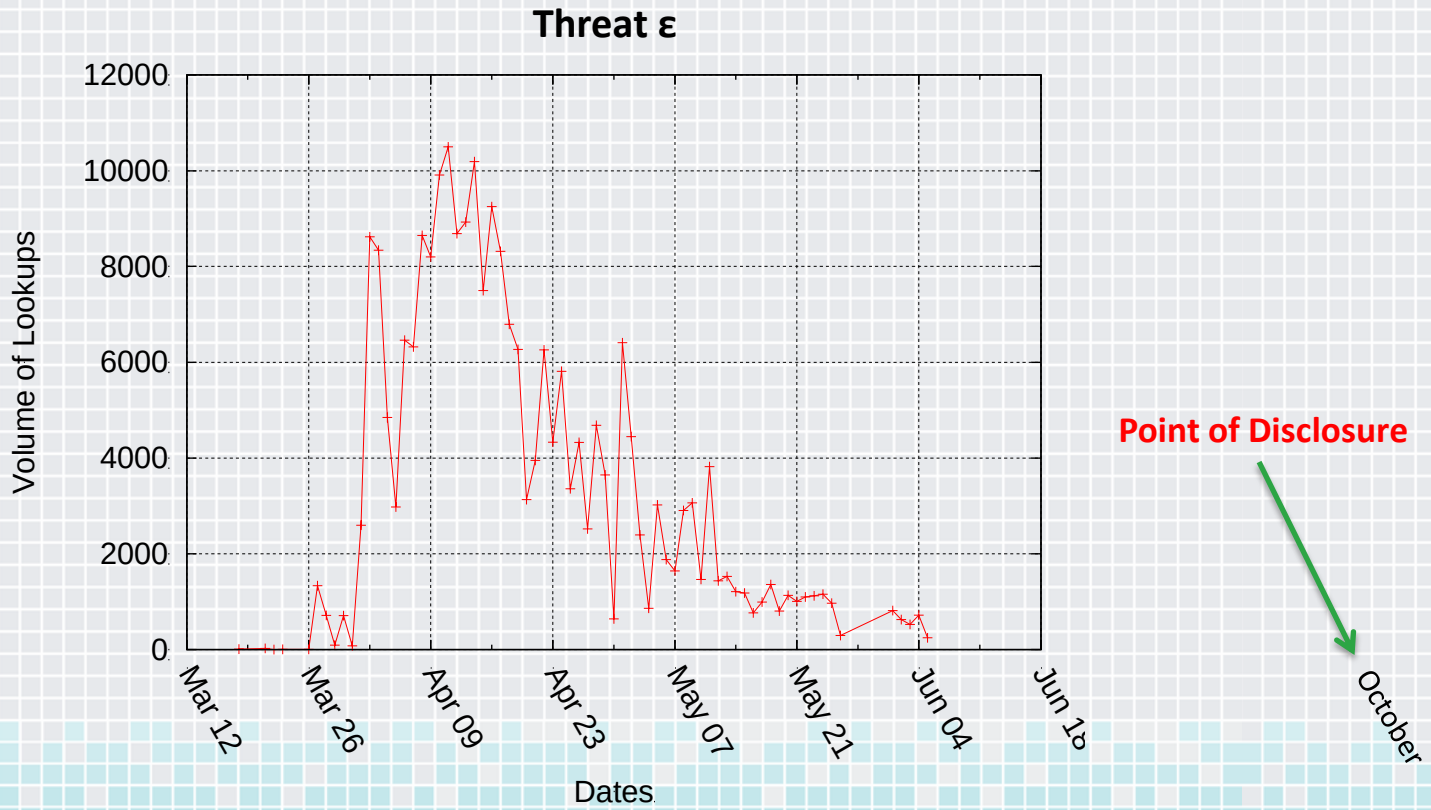
Malware Dataset Name	Date of Snapshot	# Unique Apps	# Unique Domains	# Unique IPs
Contagio	03/27/12	338	246	2,324
Zhou et al	02/2012	596	281	2,413
M1	03/26/2012	1,485	839	5,540

M&A Overlap with Wired pDNS

- At most 10% of M&A hosts are outside our non-cellular pDNS dataset.
- More than 50% of M&A hosts are associated with at least seven domain names.

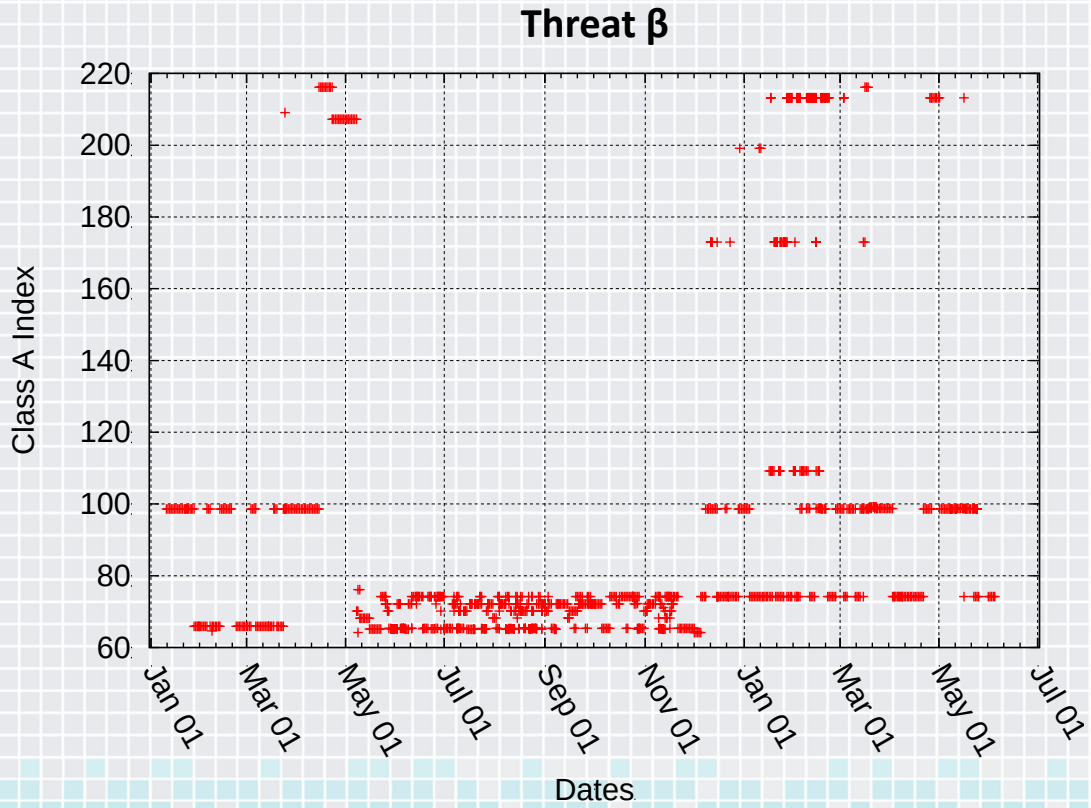
Mobile applications reusing same hosting infrastructure as desktop applications.

Lifecycle of a Threat



- Threat publicly disclosed by security community in October.
- Associated domain no longer resolved at time of disclosure.

Network Behavior



- Mobile threats show high degree of network agility similar to traditional botnets.

Use of network based countermeasures may help better detect and mitigate threats.

Summary of Observations

- Mobile Internet is really just the Internet.
- Mobile malware is still a real but ***small*** threat.
- Mobile applications reusing same infrastructure as desktop applications.
- Analysis of mobile malware slow to identify threats.
- Network based countermeasures can and should be used.

Apply What You Have Learned Today

- What you can do today:
  - When downloading applications for your mobile device, try and stick to first-party application markets.
  - Be mindful that certain threats like phishing can be more effective against mobile users due to limited screen real estate.

- What you should be doing in the future:
  - Leverage your existing network infrastructure to help identify mobile devices.
  - Analyzing the network infrastructure mobile devices are contacting by using new or existing tools to evaluate the reputation of that infrastructure.

Questions?

References

- The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers, Network & Distributed System Security Symposium (NDSS), 2013
- Mobile Malware Sources (Public)
  - Contagio Mobile Malware (http://contagiominidump.blogspot.com)
  - Android Malware Genome (http://www.malgenomeproject.org)
  - VirusTotal (https://www.virustotal.com)