The Core of the Matter: Characterizing Malicious Traffic in Cellular Carriers

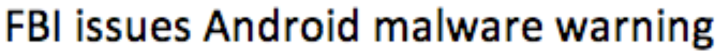
Chaz Lever*, Manos Antonakakis†, Brad Reaves*
Patrick Traynor*, Wenke Lee*

** Georgia Institute of Technology*
† Damballa, Inc.

NDSS, February 2013, San Diego, CA

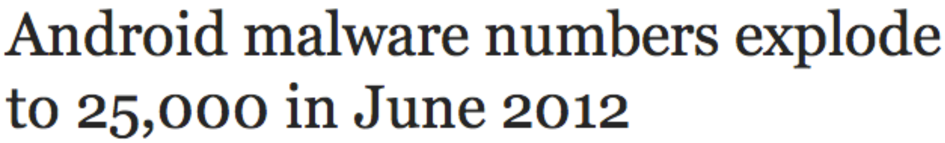
Mobile Malware

New Android Malware Steals Your Money Via SMS

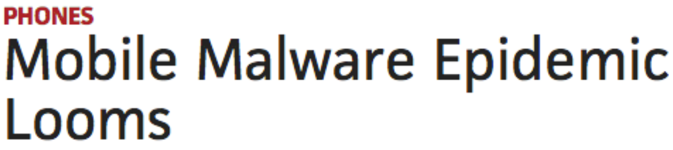

FBI issues Android malware warning

Android Malware Infections Increase By 700%

Report: Android Has Become the Ultimate Malware Platform


Android malware numbers explode to 25,000 in June 2012

Android is under attack: New malware threats tripled in Q2


PHONES

Mobile Malware Epidemic Looms

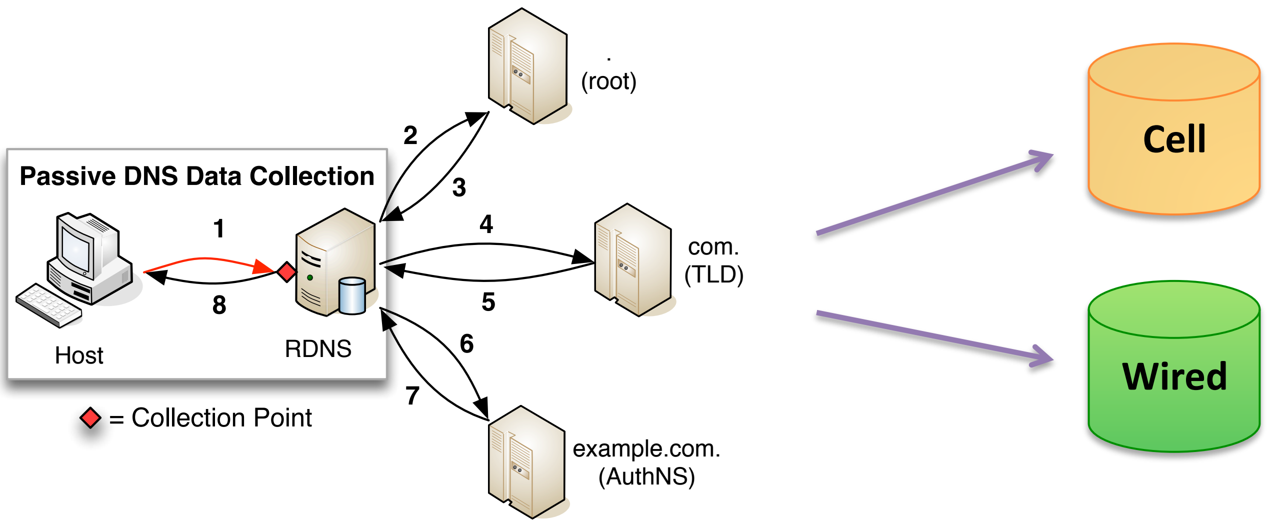
Malware Going Nuclear

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 not well understood.

Use network level analysis to better understand the threat.

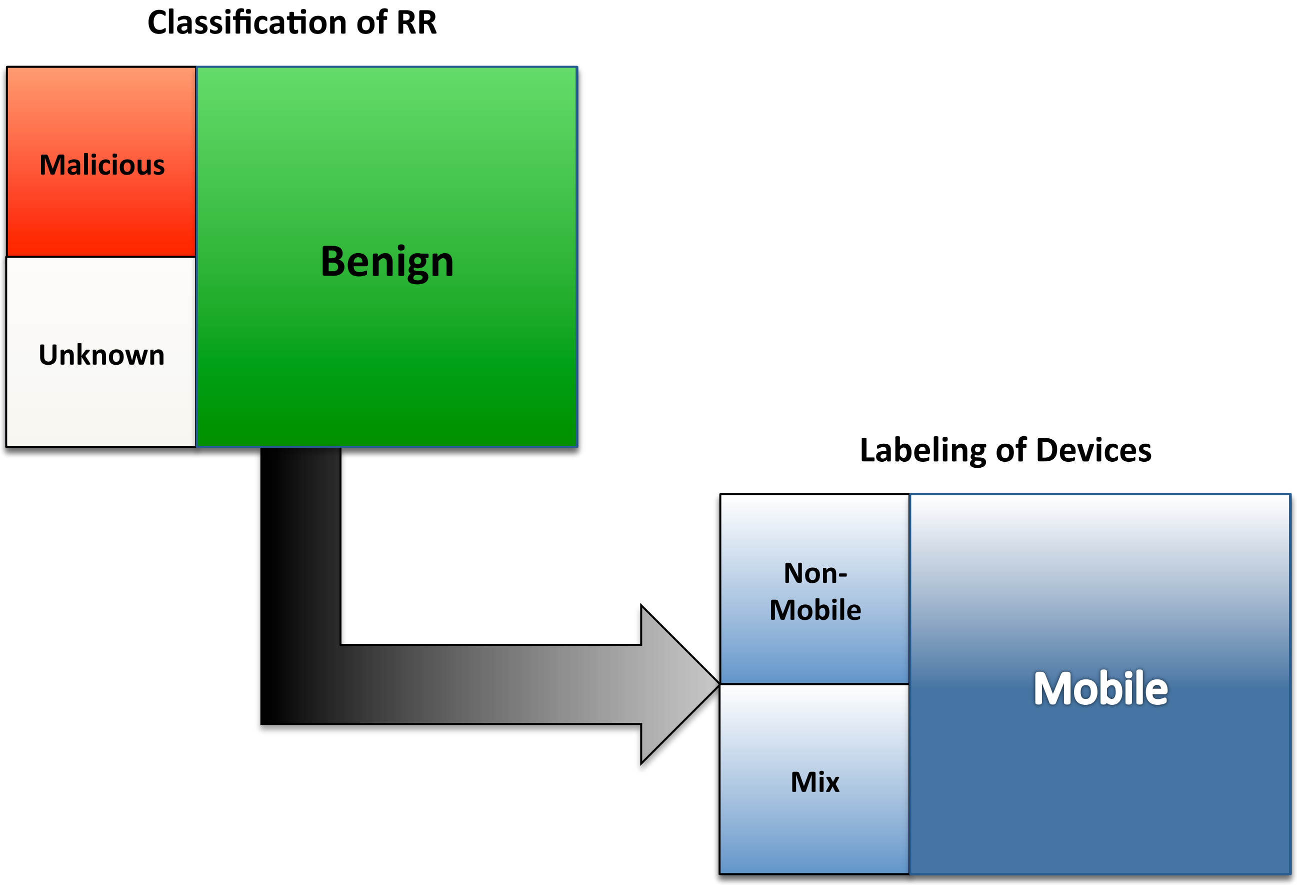
Data Collection



- 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

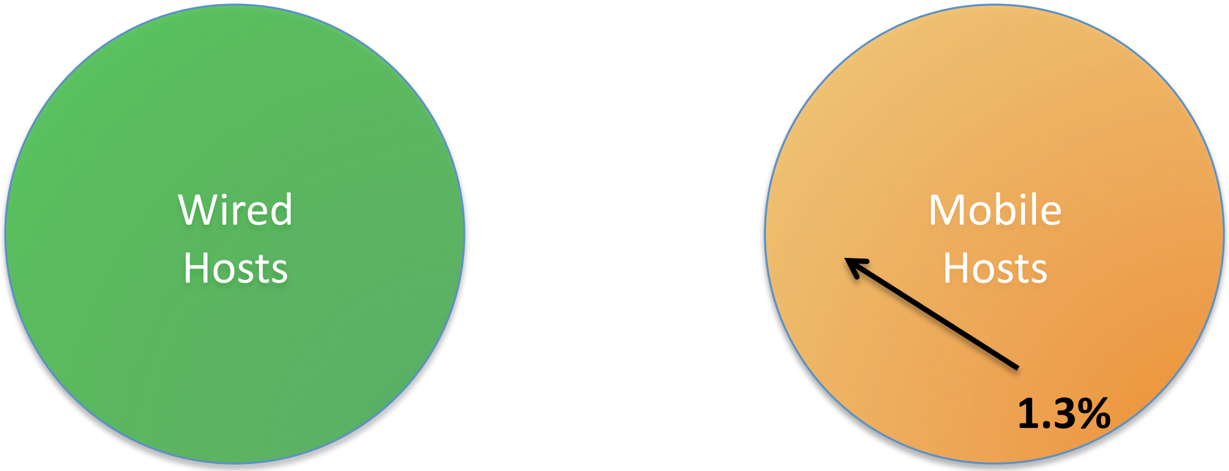


Cellular pDNS Data Summary

Observation Period	Duration (hours)	RRs		Domains	
		Total	*New*	*Total*	*New*
4/15 - 4/21	168	8,553,155	8,553,155	8,040,141	8,040,141
5/13 – 5/19	168	9,240,372	4,498,765	8,711,704	4,042,009
6/17 – 6/23	168	8,660,555	3,246,194	8,109,536	2,745,999
Total	504	26,454,082	16,298,114	24,861,381	14,828,149

Observation Period	Duration (hours)	Hosts		Devices	
		Total	*New*	*Total*	*Mobile*
4/15 - 4/21	168	2,070,189	2,070,189	157,286,931	121,497,066
5/13 – 5/19	168	2,168,266	606,467	169,561,760	136,292,358
6/17 – 6/23	168	2,050,168	377,048	153,525,716	122,747,704
Total	504	6,288,623	3,053,704	**480,374,407**	**380,537,128**

Hosting Infrastructure



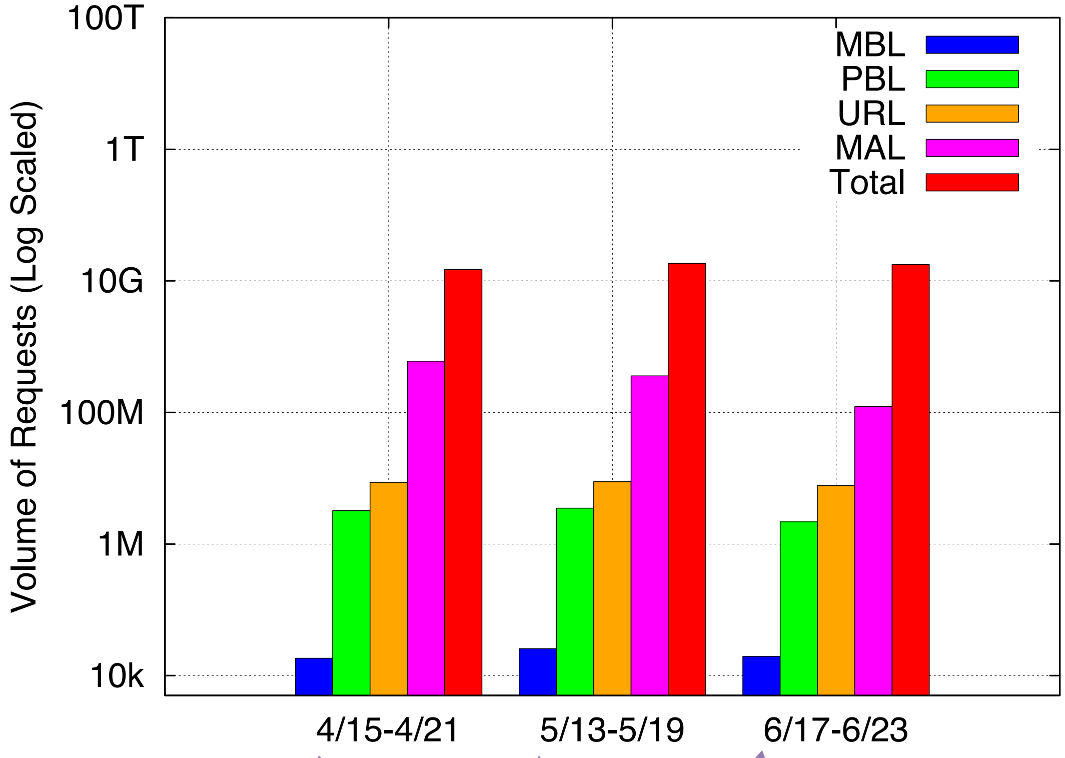
- Observed 2,762,453 unique hosts contacted by *mobile devices*.
- Only 1.3% (35,522) of “mobile” hosts were not in the set of hosts contained by historical non-cellular pDNS data.

The mobile Internet is really just the Internet.

Evidence of Malware

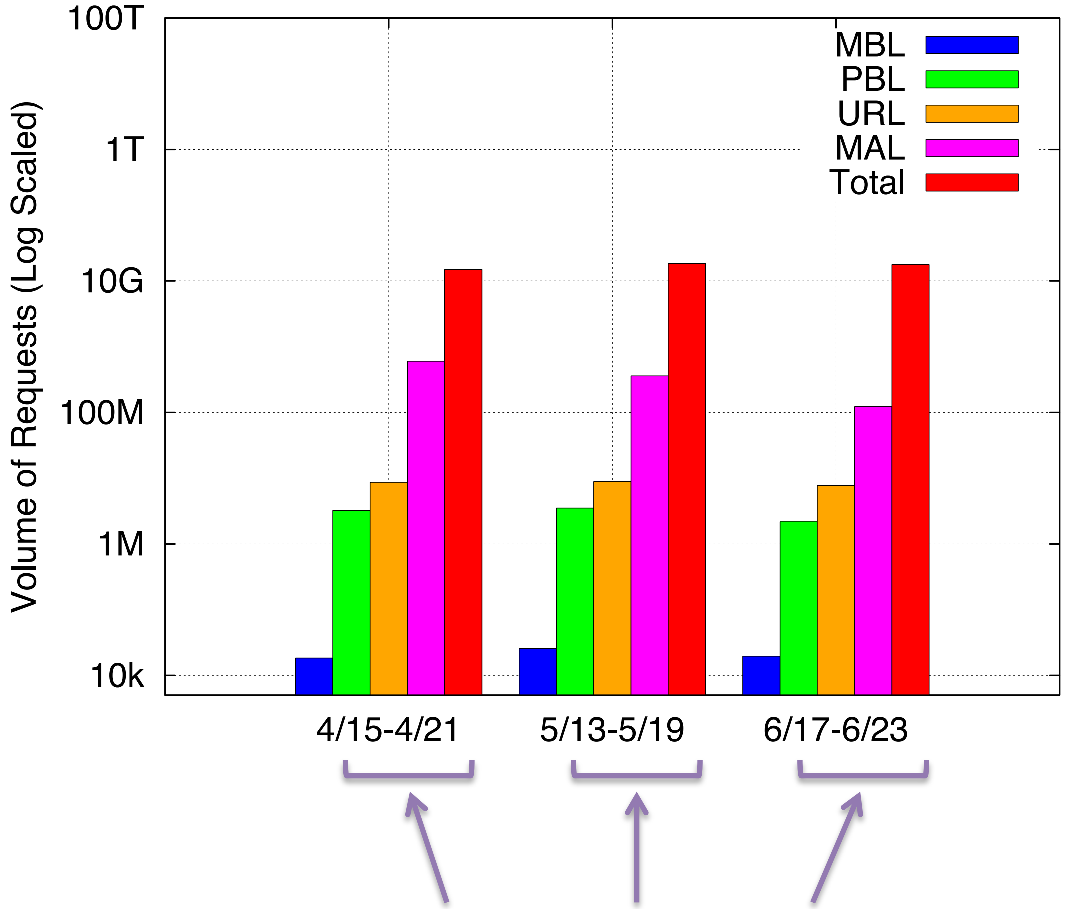
- Public Blacklist (PBL)
- Phishing and Drive-by-Downloads (URL)
- Desktop Malware Association (MAL)
- Mobile Blacklist (MBL)

Observed Historical Evidence



Mobile Specific Evidence

Observed Historical Evidence



Desktop Related Evidence

Tainted Hosts and Platforms

Platform	% Of All Devices	% Population requesting tainted hosts	% Total tainted host requests
iOS	31.6%	8.8%	33.2%
All other mobile (Android, etc.)	68.4%	8.2%	66.8%

Tainted Hosts and Platforms

Platform	% Of All Devices	% Population requesting tainted hosts	% Total tainted host requests
iOS	**31.6%**	8.8%	**33.2%**
All other mobile (Android, etc.)	**68.4%**	8.2%	**66.8%**

Tainted Hosts and Platforms

Platform	% Of All Devices	% Population requesting tainted hosts	% Total tainted host requests
iOS	31.6%	**8.8%**	33.2%
All other mobile (Android, etc.)	68.4%	**8.2%**	66.8%

iOS equally likely to reach out to tainted hosts as other platforms.

Mobile Malware Families and Devices

Malware Family	# Assoc. Domains	#Devices (Any type)	#Devices (Mobile only)
DroidDreamLight*†	3	150	44
DroidKungFu*	1	19	6
FakeDoc*†	1	5417	2145
Fatakr*	1	328	151
GGTracker*	3	1	1
Gone60*†	1	1	1
NotCompatible	3	2198	762
Plankton*†	4	686	286
Malware β*	1	18	1
WalkInWat*	1	215	95

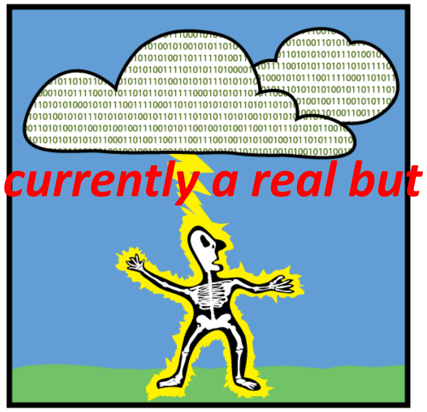
* Disclosed before any of our epochs
† Distributed in Google Play market

Mobile Malware in Numbers

- Only ***0.001% (9,033)*** out of 480M *total* devices contacted MBL domains.

- Only ***0.0009% (3,492)*** out of a total of 380M *mobile* devices contacted MBL domains.

- According to National Weather Service, odds of an individual being struck by lightning in a lifetime is **0.01% (1/10000)**!



Mobile malware is currently a real but miniscule threat.

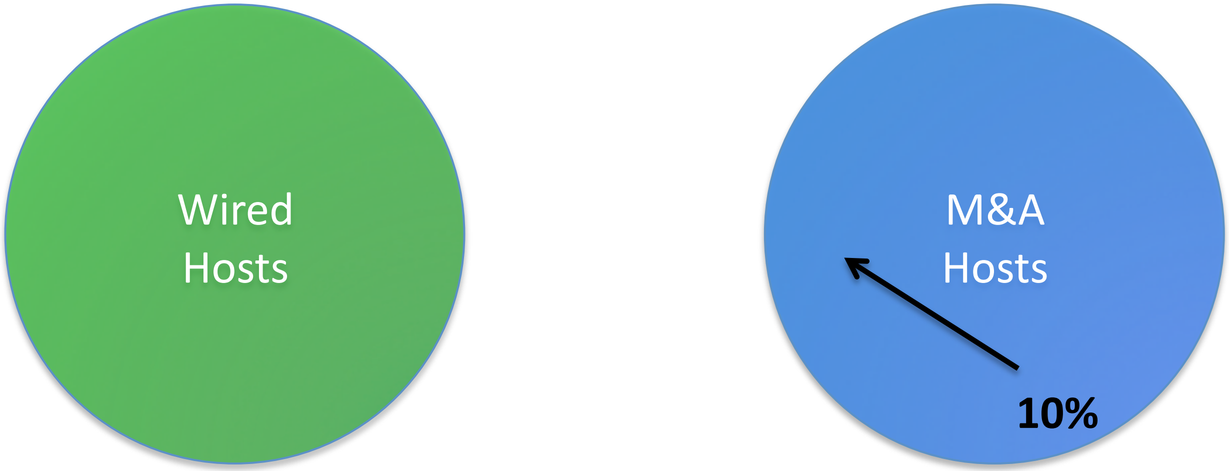
Market and Malware (M&A) Dataset

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

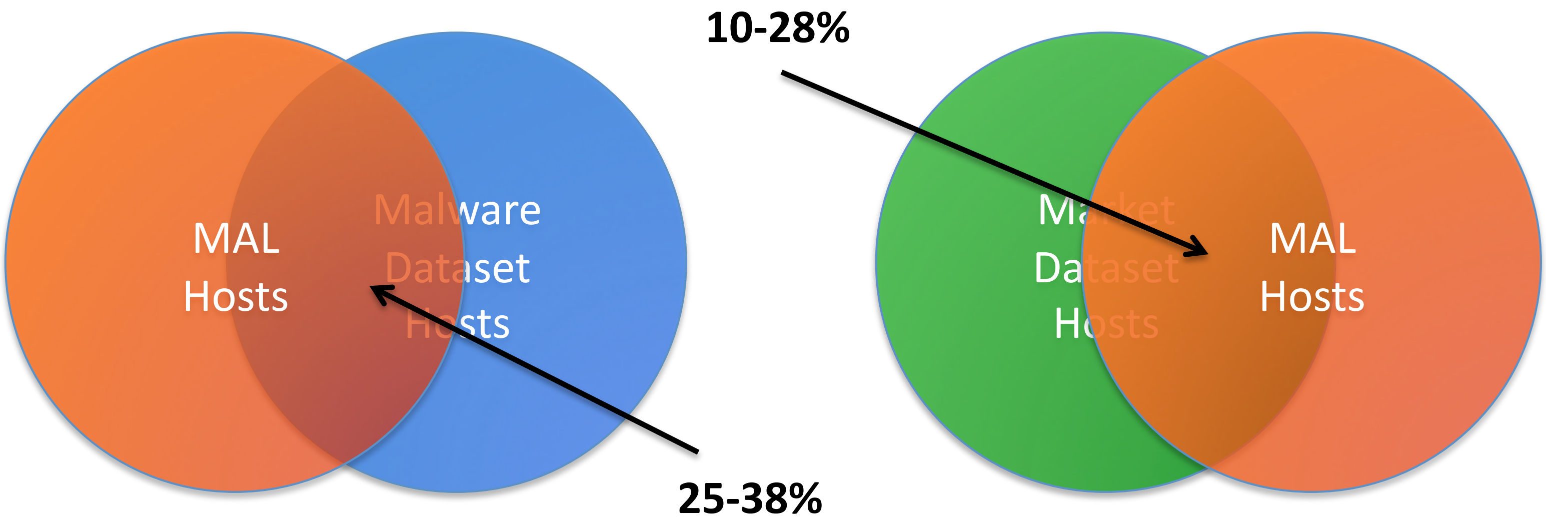
M&A Overlap with Wired pDNS



- 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.

M&A Overlap with MAL

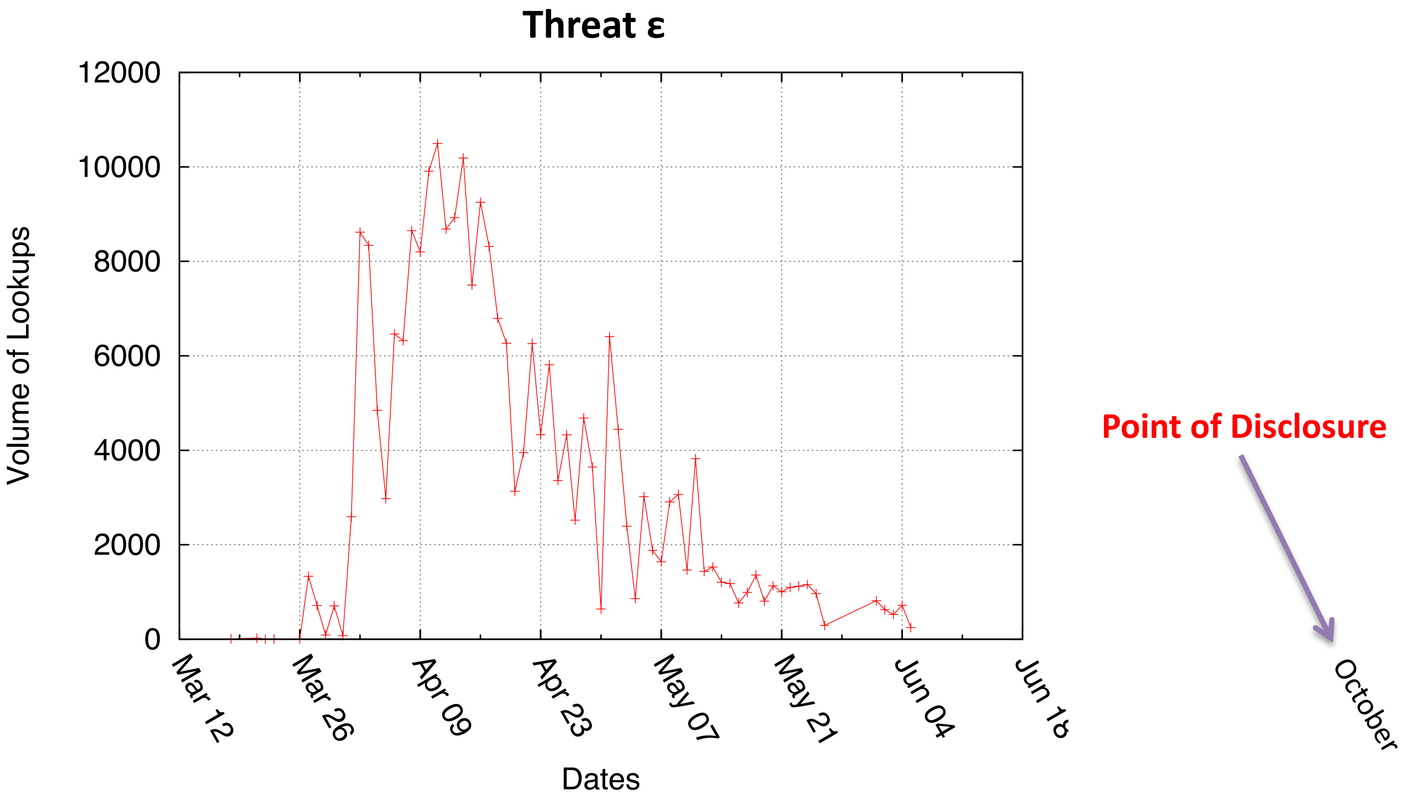


- Between 25-38% of hosts in *malware datasets* overlap MAL hosts.

- Between 10-28% of hosts in *mobile markets* overlap MAL hosts.

Mobile applications reaching out to same tainted hosting infrastructure as desktop malware.

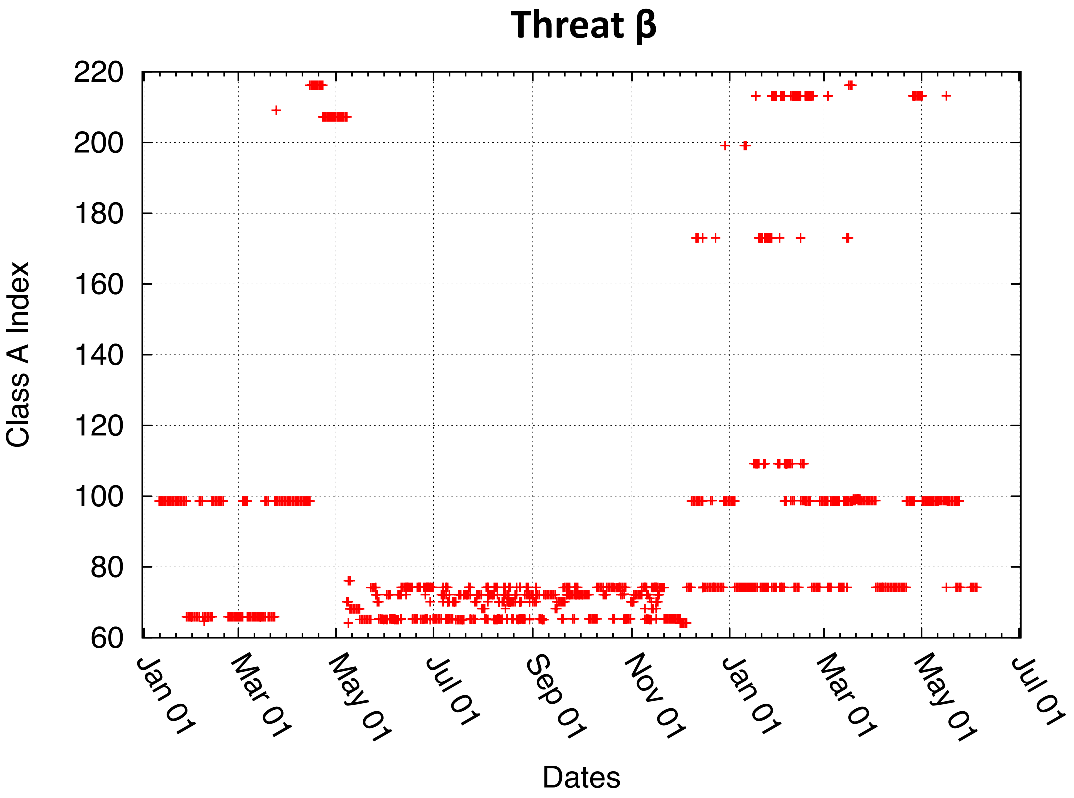
Lifecycle of a Threat



- Threat publicly disclosed by security community in October 2011.
- Associated domain no longer resolved at time of disclosure.

Network Behavior

Georgia Tech College of Computing



- 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 platforms equally likely to reach out to tainted hosts.
- Mobile malware is currently a real but ***small*** threat.
- Mobile applications reusing same infrastructure as desktop applications.
- Analysis of mobile malware slow to identify threats.

Questions?