Ubiquitous and Mobile Computing CS 528: *A Survey of Mobile Malware in the Wild*

Alex Fortier

Computer Science Dept.

Worcester Polytechnic Institute (WPI)

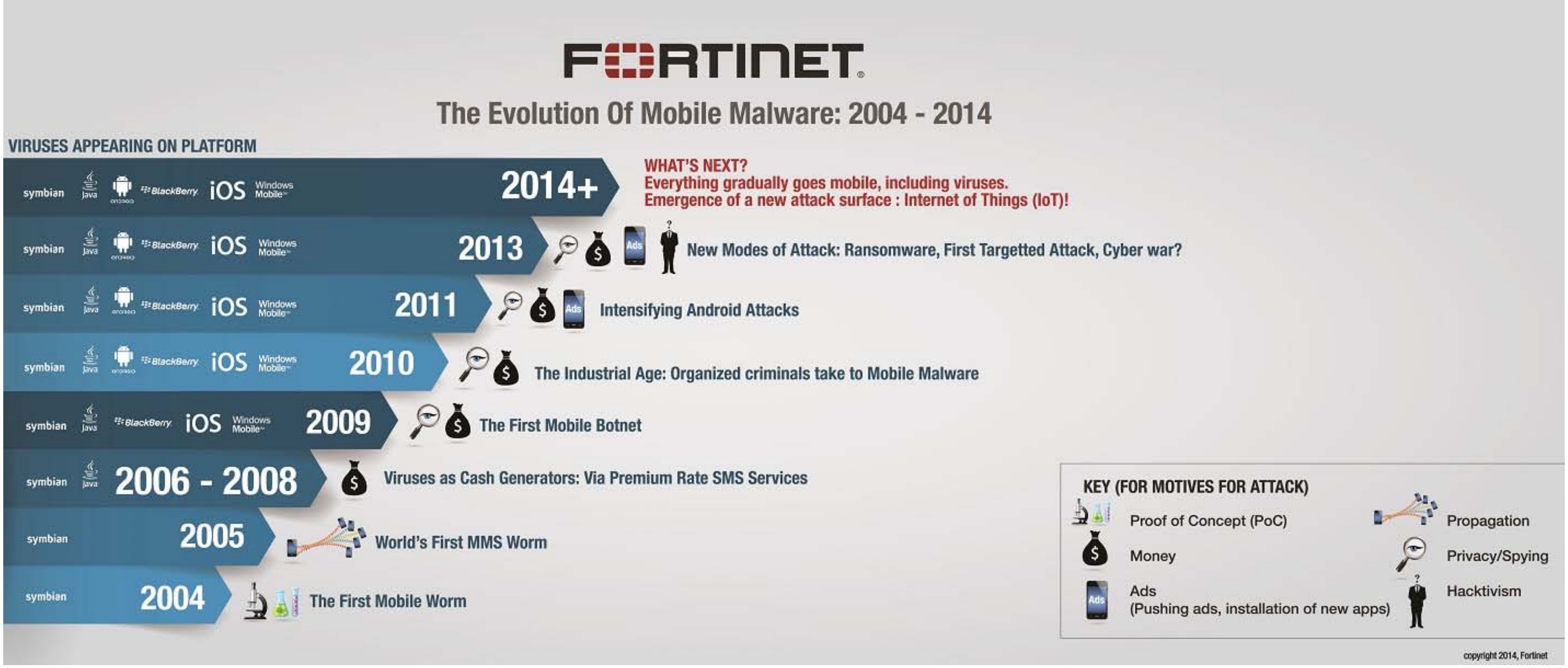
What is mobile malware?

- Targeted at Android, iOS, Symbian (discontinued), Windows Phone
- Gather data, send premium-rate SMS messages, credential theft, novelty or amusement
- Is it more of a problem than traditional malware for PCs?

Root and Motivation

- Quick comparison: PCs vs. Smartphones

When did this become a problem?



The Evolution Of Mobile Malware: 2004 - 2014

2014+ WHAT'S NEXT?
Everything gradually goes mobile, including viruses.
Emergence of a new attack surface : Internet of Things (IoT)!

2013 New Modes of Attack: Ransomware, First Targetted Attack, Cyber war?

2011 Intensifying Android Attacks

2010 The Industrial Age: Organized criminals take to Mobile Malware

2009 The First Mobile Botnet

2006 - 2008 Viruses as Cash Generators: Via Premium Rate SMS Services

2005 World's First MMS Worm

2004 The First Mobile Worm

KEY (FOR MOTIVES FOR ATTACK)

- Proof of Concept (PoC)
- Money
- Ads (Pushing ads, installation of new apps)
- Propagation
- Privacy/Spying
- Hacktivism

copyright 2014, Fortinet

Threat Types

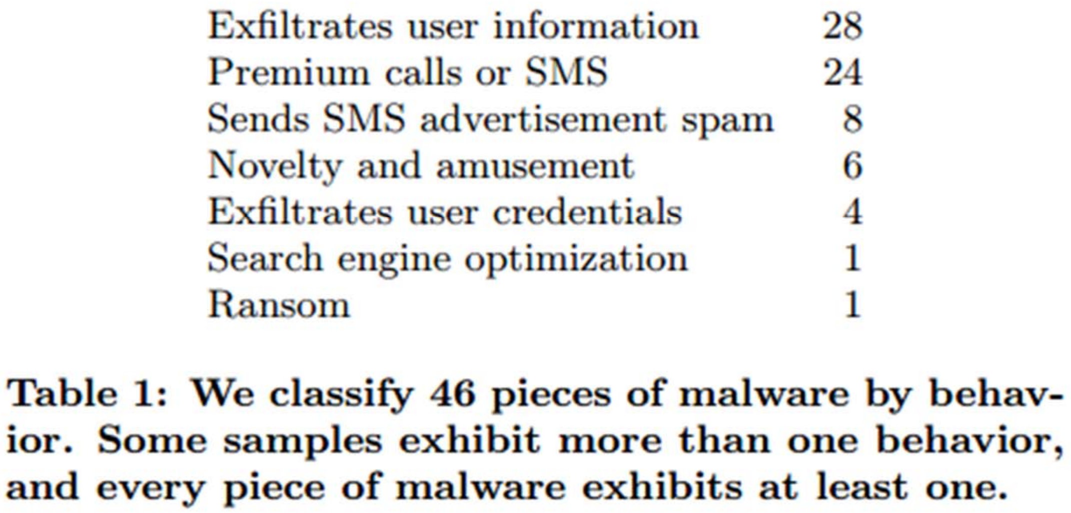
- Malware
  - Gains access for the purpose of stealing data, damaging the device, annoying user, etc.
- Personal Spyware
  - Collects personal information over a period of time
- Grayware
  - Collect data on user, but with no intention to harm user

Security Measures

- App Markets
  - Apple App Store highly regulated; Apple approves all apps after review
  - Android Market (Google Play Store) similar, but user’s can install applications from elsewhere
- Permissions
  - Android informs all users of requested permissions at install-time
  - iOS less comprehensive

Incentives

- Selling user information
- Stealing credentials
- For fun!



Exfiltrates user information	28
Premium calls or SMS	24
Sends SMS advertisement spam	8
Novelty and amusement	6
Exfiltrates user credentials	4
Search engine optimization	1
Ransom	1

Table 1: We classify 46 pieces of malware by behavior. Some samples exhibit more than one behavior, and every piece of malware exhibits at least one.

Findings

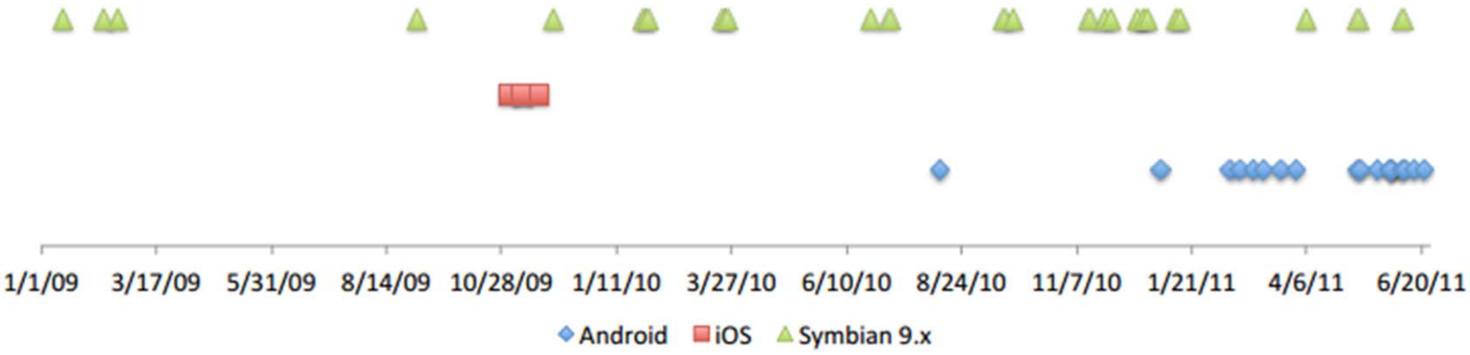
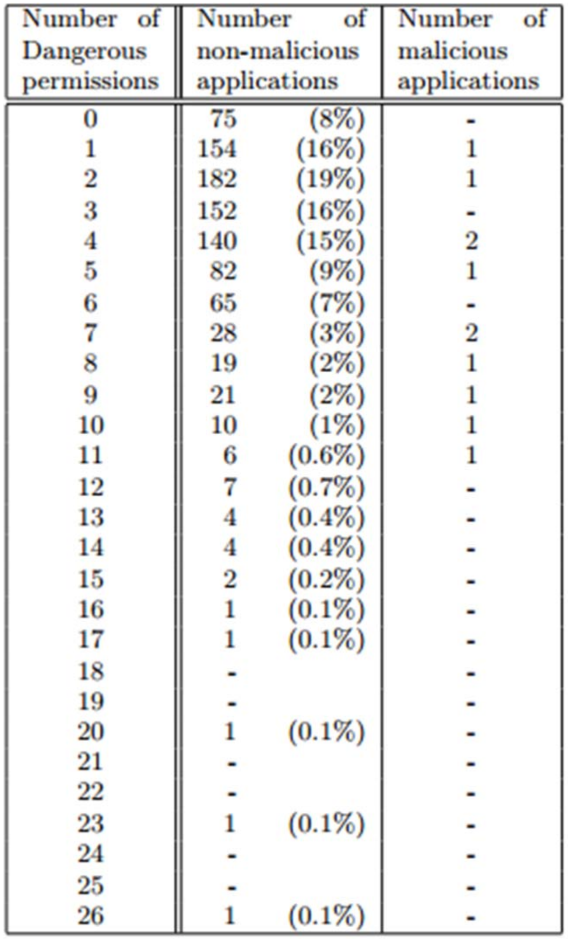


Figure 1: A timeline of when the 46 pieces of malware in our data set were detected by malware researchers.

Malware Detection

Number of Permissions

- Malicious applications request an average of 6.18 “Dangerous” permissions
- Non-malicious apps request an average of 3.46 “Dangerous” permissions



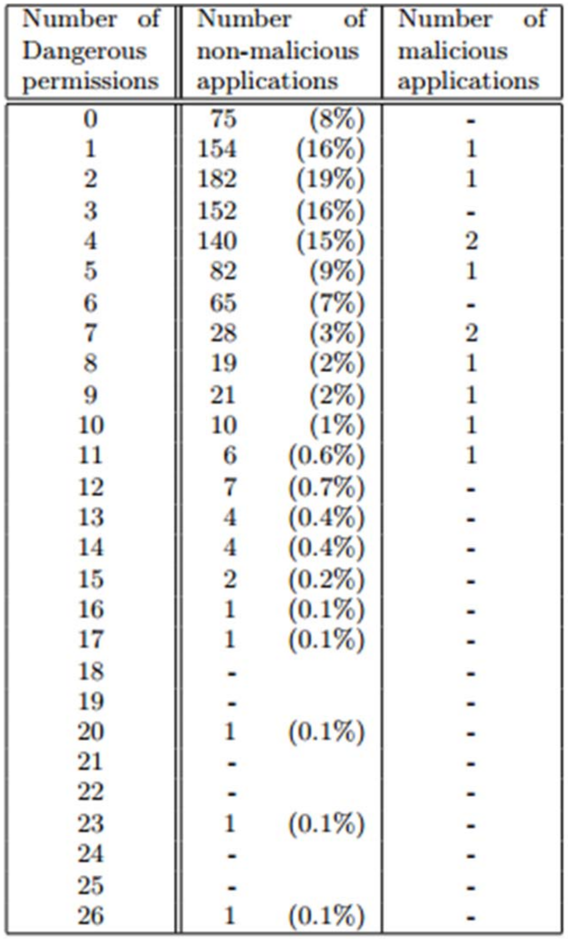
Number of Dangerous permissions	Number of non-malicious applications		Number of malicious applications
0	75	(8%)	-
1	154	(16%)	1
2	182	(19%)	1
3	152	(16%)	-
4	140	(15%)	2
5	82	(9%)	1
6	65	(7%)	-
7	28	(3%)	2
8	19	(2%)	1
9	21	(2%)	1
10	10	(1%)	1
11	6	(0.6%)	1
12	7	(0.7%)	-
13	4	(0.4%)	-
14	4	(0.4%)	-
15	2	(0.2%)	-
16	1	(0.1%)	-
17	1	(0.1%)	-
18	-		-
19	-		-
20	1	(0.1%)	-
21	-		-
22	-		-
23	1	(0.1%)	-
24	-		-
25	-		-
26	1	(0.1%)	-

Table 2: The number of “Dangerous” Android permissions requested by 11 pieces of malware and 956 non-malicious applications [28].

Malware Detection

Common Permissions

- 73% of malicious apps requested SMS sending permission
  - 4% of non-malicious apps requested that permission
- 73% of malicious apps requested READ_PHONE_STATE (IMEI info)
  - 33% of non-malicious apps requested that permission



Number of Dangerous permissions	Number of non-malicious applications		Number of malicious applications
0	75	(8%)	-
1	154	(16%)	1
2	182	(19%)	1
3	152	(16%)	-
4	140	(15%)	2
5	82	(9%)	1
6	65	(7%)	-
7	28	(3%)	2
8	19	(2%)	1
9	21	(2%)	1
10	10	(1%)	1
11	6	(0.6%)	1
12	7	(0.7%)	-
13	4	(0.4%)	-
14	4	(0.4%)	-
15	2	(0.2%)	-
16	1	(0.1%)	-
17	1	(0.1%)	-
18	-		-
19	-		-
20	1	(0.1%)	-
21	-		-
22	-		-
23	1	(0.1%)	-
24	-		-
25	-		-
26	1	(0.1%)	-

Table 2: The number of "Dangerous" Android permissions requested by 11 pieces of malware and 956 non-malicious applications [28].

Malware Detection

Application Review

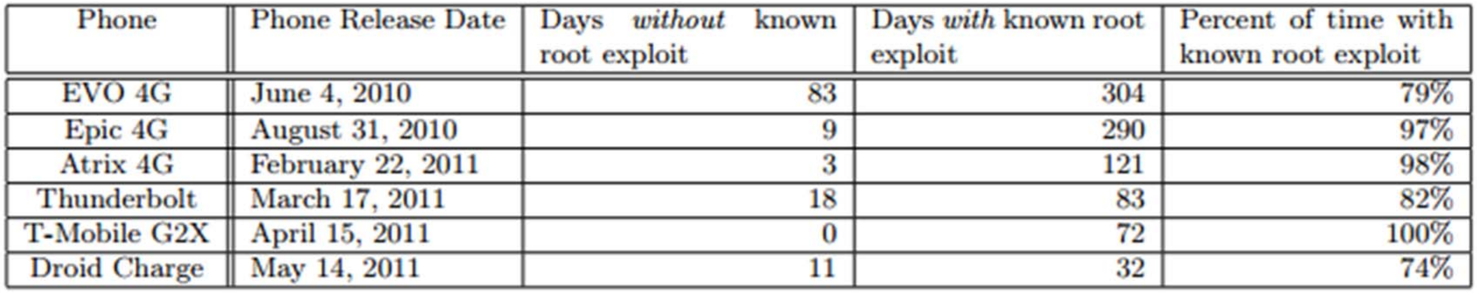
- iOS: All 4 pieces of Apple malware were spread through jailbroken devices; not found on App Store
- Symbian: 5 of 24 pieces of malware were Symbian Signed
  - Passed automated review
  - 30% passed or evaded Symbian signing process

Root Exploits

Who?	Why?
Malware authors	• Gain extra privileges • Perform any action on the phone
Users who want to modify their phone	• Install homebrew versions of operating system

- Can install only applications that are distributed through official application store
- Cannot perform complete system backups
- Carriers forbid or restrict tethering (in order to pay additional fee)
- Carrier pre-install applications (bloatware) and disable their removal
- Cannot install custom versions of OS that may have additional features

Root Exploits



Phone	Phone Release Date	Days *without* known root exploit	Days *with* known root exploit	Percent of time with known root exploit
EVO 4G	June 4, 2010	83	304	79%
Epic 4G	August 31, 2010	9	290	97%
Atrix 4G	February 22, 2011	3	121	98%
Thunderbolt	March 17, 2011	18	83	82%
T-Mobile G2X	April 15, 2011	0	72	100%
Droid Charge	May 14, 2011	11	32	74%

Table 3: We report the number and percentage of days between a handset's release date and June 26, 2011 in which there was a publicly available root exploit published by the Android homebrew community.

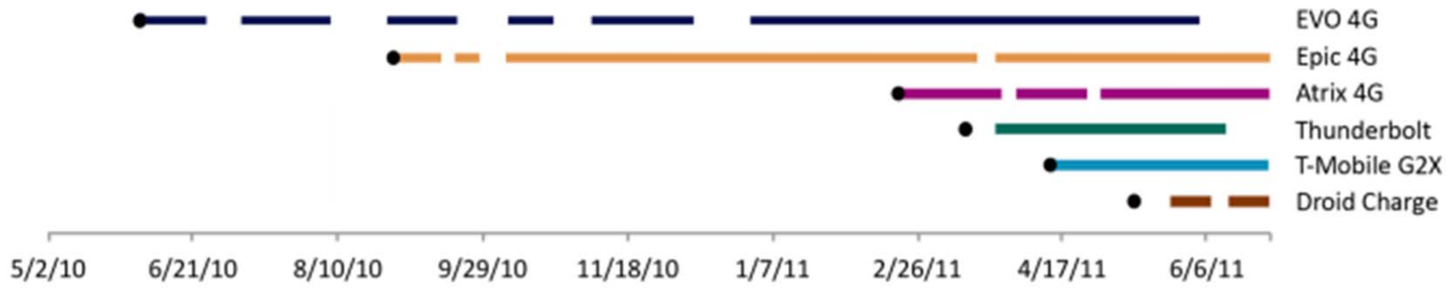
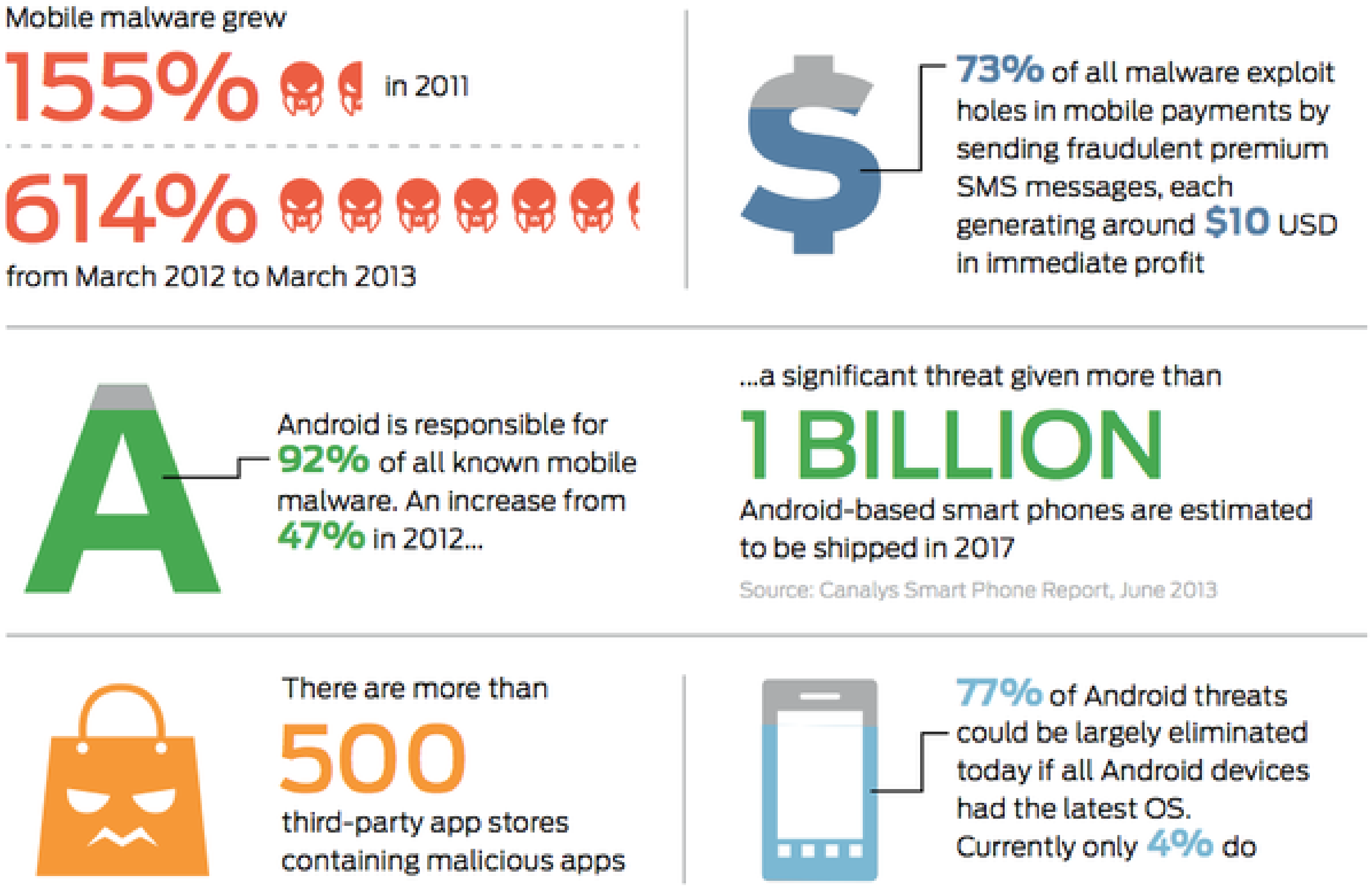


Figure 2: A timeline displaying the dates that known root exploits were available for 6 popular Android phones. Circles mark the release dates of the phones.

Future Incentives (as of 2011)

- Advertising Click Fraud
- Invasive Advertising
- In-Application Billing Fraud
- Governments
- E-Mail Spam
- Distributed Denial of Service (DDoS)
- NFC and Credit Cards

Conclusion



Mobile malware grew

155% in 2011

614% from March 2012 to March 2013

73% of all malware exploit holes in mobile payments by sending fraudulent premium SMS messages, each generating around $10 USD in immediate profit

Android is responsible for 92% of all known mobile malware. An increase from 47% in 2012...

...a significant threat given more than

1 BILLION

Android-based smart phones are estimated to be shipped in 2017

Source: Canalys Smart Phone Report, June 2013

There are more than

500

third-party app stores containing malicious apps

77% of Android threats could be largely eliminated today if all Android devices had the latest OS. Currently only 4% do

Conclusion

- Mobile malware rivals desktop malware
- Human review may be appropriate measure against malware
- Phone manufacturers should support smartphone customization to minimize root exploits

References

1. Mobile Malware: Protect Yourself Against Evolving Threats - InformationWeek. (n.d.). Retrieved April 28, 2015, from http://www.informationweek.com/mobile/mobile-malware-protect-yourself-against-evolving-threats/d/d-id/1099438?
2. (n.d.). Retrieved April 28, 2015, from http://www.fortinet.com/sites/default/files/whitepapers/10-Years-of-Mobile-Malware-Whitepaper.pdf
3. A. P. Felt, K. Greenwood, and D. Wagner. The Effectiveness of Application Permissions. In USENIX WebApps, 2011.
4. Mobile malware grows by 614 percent in last year - CNET. (n.d.). Retrieved April 28, 2015, from http://www.cnet.com/news/mobile-malware-grows-by-614-percent-in-last-year/
5. M. Boodaei. Mobile Users Three Times More Vulnerable to Phishing Attacks. Trusteer Technical Report.
6. W. Enck, M. Ongtang, and P. McDaniel. On Lightweight Mobile Phone Application Certification. In CCS, 2009.
7. P. Porras and H. Saidi and V. Yegneswaran. An Analysis of the Ikee.B (Duh) iPhone Botnet. SRI International, 2009. http://mtc.sri.com/iPhone.
8. A. Schmidt, H. Schmidt, L. Batyuk, J. H. Clausen, S. A. Camtepe, and S. Albayrak. Smartphone Malware Evolution Regisited: Android Next Target? In MALWARE, 2009.