Ubiquitous and Mobile Computing CS 403x: A Survey of Mobile Malware in the Wild

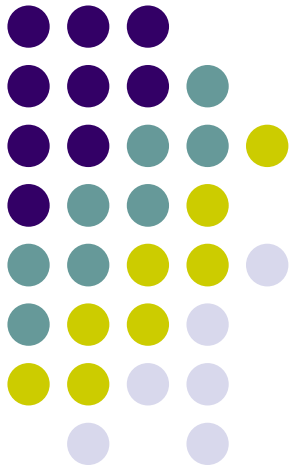
James Megin,

Saraf Rahman,

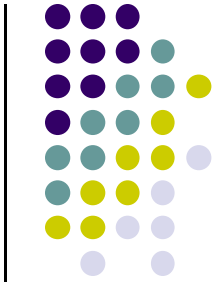
Jordan Wetzel

Computer Science Dept.

Worcester Polytechnic Institute (WPI)

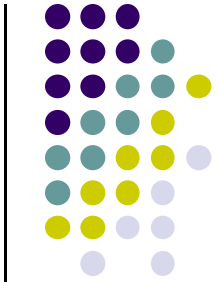


Introduction/Motivation



- Mobile malware is becoming a serious threat
- Used for many of the same purposes as desktop computers
- Smartphone users' information would be compromised

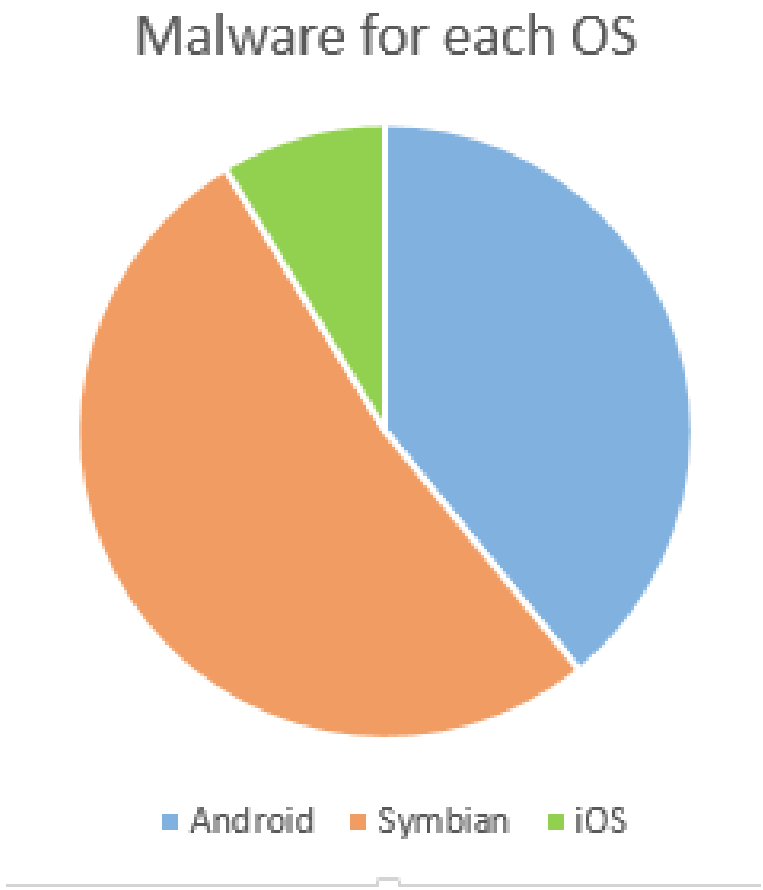
Vision



- Understand underlying motivations for malware
- How to defend against each threat
- Prevent malware in the future

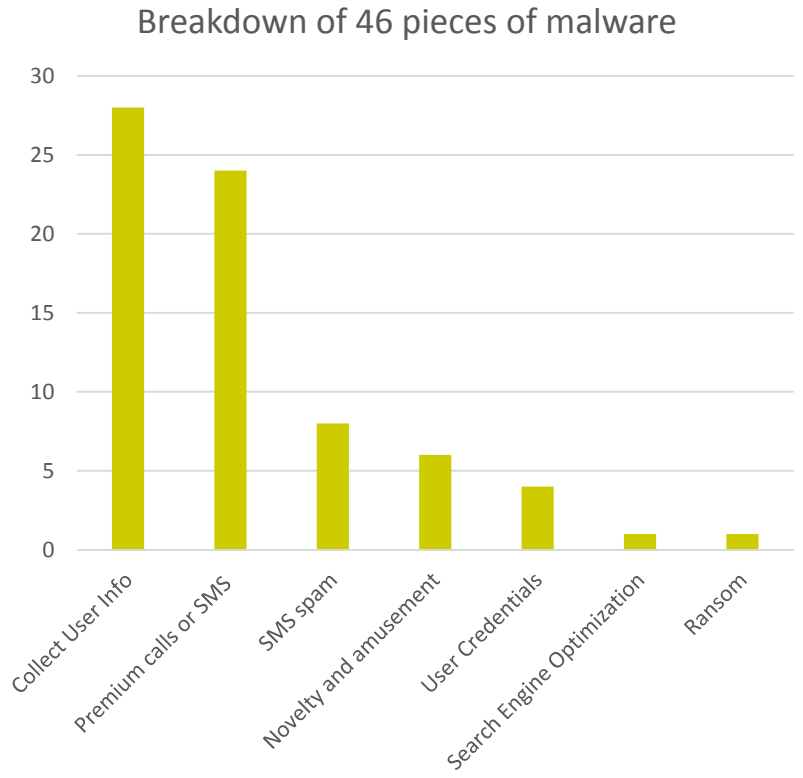
Background

- 46 pieces of malware in iOS, Android, and Symbian
- 3 types of threat models:
  - Malware
  - Grayware
  - Personal Spyware

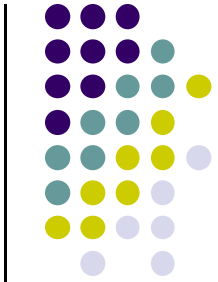


Background

- Most common malicious activities:
  - Collecting user information (61%)
  - Sending premium-rate SMS messages (52%)

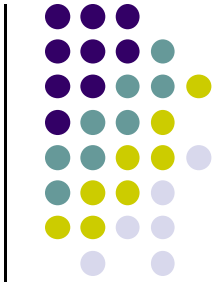


Current Incentives



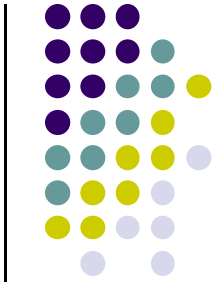
- Selling User Information (28)
  - Ex. IMEI, location, contact lists
  - Sold to companies, scammers, spammers, etc.
  - E-mail addresses worth between $0.33/MB and $40/MB on the black market in 2008
- Defense
  - Provide an alternate, globally-unique ID for IMEI theft

Current Incentives



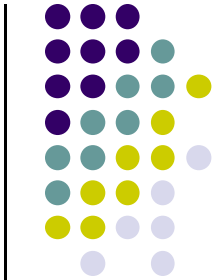
- Premium-Rate Calls and SMS messages (24)
  - Delivers valuable content like stock quotes or tech support
  - Cost is charged to sender's phone bill
- Defense
  - Require user confirmation

Current Incentives



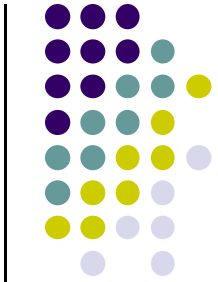
- Novelty and Amusement (6)
  - Causes mischief/damage intended to amuse the author
- Stealing User Credentials (4)
  - Can steal bank information, launch phishing attacks
  - Capture using keylogging or scanning documents
- Defense
  - Strengthen application isolation mechanisms

Current Incentives



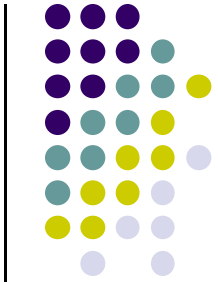
- SMS Spam (8)
  - Commercial advertising
  - Phishing links
- Defense
  - Prevent apps from directly sending SMS messages

Current Incentives



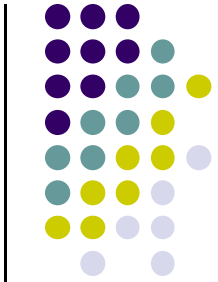
- Search Engine Optimization (1)
  - Used by many sites for traffic
  - Malware used to improve a site's ranking
- Defense
  - Add metadata to request headers
- Ransom (1)
  - Used for blackmail

Future Incentives



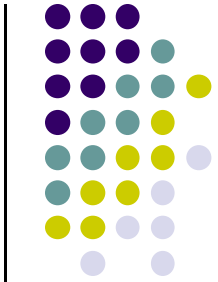
- Advertising Click Fraud
- Invasive Advertising
- In-application Billing Fraud
- Government Spying
- E-Mail Spam
- DDoS Attacks via NFC

Related Work



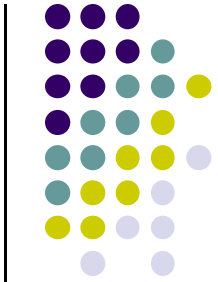
- Mobile Malware
- Underground Economies
- DDoS on Cellular Networks

Permissions



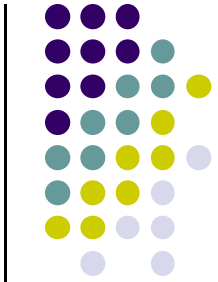
- Could help users identify malware
- Android applications:
  - Identified 11 out of 18 malware apps
  - Malicious apps make 6.18 requests on average
  - Non-malicious apps make 3.46 requests on average
- Number of permission requests is not sufficient
- Observing SMS and IMEI permissions are effective

Root Exploits/Jailbreaks



- Used by malware authors and smartphone owners
- Modifications using a jailbreak
- Available for 74% of a device's lifetime

Conclusions



- Mobile malware will rival desktop malware
- Motivated by premium-rate SMS messages
- Recommendation:
  - Allow owners to customize their devices

References

[1] Felt, Adrienne P. et al. "A Survey of Mobile Malware in the Wild". Web. 25 April 2015. http://www.cs.swarthmore.edu/~bylvisa1/cs97/f13/Papers/mobilemalware.pdf