Android Malware: Server-Side Polymorphism

Vicki Springmann

February 20, 2012

Why Target Smartphones?

I believe that smart phones are going to become the primary platform of attack for cybercriminals in the coming years.
- Bruce Schneier

Why?

1. Growing Market

Why Target Smartphones?

I believe that smart phones are going to become the primary platform of attack for cybercriminals in the coming years.
- Bruce Schneier

Why?

1. Growing Market
2. Personal Information

Why Target Smartphones?

I believe that smart phones are going to become the primary platform of attack for cybercriminals in the coming years.
- Bruce Schneier

Why?

1. Growing Market
2. Personal Information
3. Limited Resources (Memory and Battery)

How?

Social Engineering

1. More common on unofficial app stores

How?

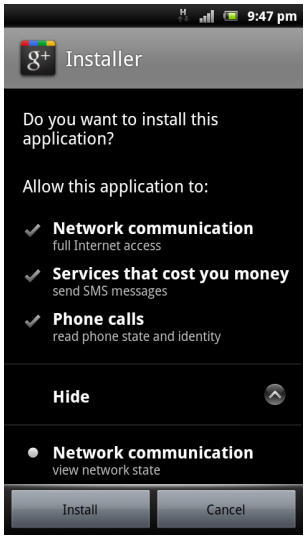
Social Engineering

1. More common on unofficial app stores
2. Pose as a popular game (Angry Birds, etc.)

How?

Social Engineering

1. More common on unofficial app stores
2. Pose as a popular game (Angry Birds, etc.)
3. Trick the user into granting excessive permissions



Then what?

SMS Fraud

1. Messages are sent from the smartphone without the user's knowledge

Then what?

SMS Fraud

1. Messages are sent from the smartphone without the user's knowledge
2. User gets stuck with premium charges

Avoiding Detection

Server-Side Polymorphism

1. Effective against signature-based known malware detection

Avoiding Detection

Server-Side Polymorphism

1. Effective against signature-based known malware detection
2. Variable data changes - Content of SMS messages changes

Avoiding Detection

Server-Side Polymorphism

1. Effective against signature-based known malware detection
2. Variable data changes - Content of SMS messages changes
3. File re-ordering - Causes different manifest and signature files

Avoiding Detection

Server-Side Polymorphism

1. Effective against signature-based known malware detection
2. Variable data changes - Content of SMS messages changes
3. File re-ordering - Causes different manifest and signature files
4. Insertion of dummy files - Variable numbers of useless files

Prevention

1. Bouncer - Scans Android Market for malicious software

Prevention

1. Bouncer - Scans Android Market for malicious software
2. Common Sense - Pay attention to terms of use and permissions

Sources

http://www.securityweek.com/fake-google-android-app-store-lures-users-malware

http://www.symantec.com/connect/blogs/server-side-polymorphic-android-applications

http://www.schneier.com/blog/archives/2011/11/android_malware.html

http://googlemobile.blogspot.com/2012/02/android-and-security.html