Android Malware

Giovanni Russello

g.russello@auckland.ac.nz

Android Under Attack

- Android Malware is on the rise
- In 2012 malware presence has increased by 580% compared to the same period in 2011 (McAfee)
- From 2000 in 2011 to 13000 in 2012
- As for the end of 2012, Android is the most targeted platform surpassing even Windows.

http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf

Malware Types

- SMS-Sending: send/register users to premium numbers
- Spyware: collect sensitive/private information and upload to remote servers
- Destructive Trojans: modify content on the devices
- Mobile botnets: receive command from remote C&C servers
- Ransomware: steal information and ask for money to get back

How do they get to our phones?

- Malware installation is driven by three main social engineering-based techniques
  - Repackaging
  - Update attack
  - Drive-by download
- These techniques can be used in combination
- They require the user intervention

Repackaging

- This is a very common technique among malware authors
- Malicious payload is piggybacked into popular apps
- Users are then lured to download these infected apps

Repackaging

- Locate and download popular apps
- Disassemble apps and enclose malicious payloads
- Re-assemble the apps and upload on official and/or alternative markets
- Apps used include paid apps, popular game apps, utility apps, security tools, and porn-related apps

Repackaging

- To hide malicious payload authors use class names that look legitimate:
  - AnserverBot uses com.sec.android.provider.drm
  - DroidKungFu uses com.google.ssearch and com.google.update
- The malware family jSMSHider has used a private key of the AOSP to sign its apps!

Repackaging

- When the code of an app is changed so is its cryptographic signature
- However, a vulnerability was discovered where the app cryptographic signature is not changed even if the code of the app is modified
- http://bluebox.com/corporate-blog/bluebox-uncovers-android-master-key/

Update Attack

- Repackaging techniques put the whole malicious code in the host apps
- This might expose them to the risk of being detected
- Update attacks lower this risk by inserting only an update component as payload
- This component can be still inserted in a repackaged popular app

Update Attack

- BaseBridge malware requests the user that a new version of the app is available
  - The new version contains the malicious payload
  - Note that the updated version is hidden within the main app!
- DroidKungFuUpdate is similar to BaseBridge
  - However the malicious payload is download remotely

Update Attack

- The whole update of an app requires user intervention to be successful
- AnserverBot and Plankton update only part of the host app not the entire app
  - In this way, they do not require the user permission
- Plankton fetches a jar file from a remote server
- AnserverBot retrieves a public (encrypted) entry from a blog containing the malicious payload

Drive-by Download

- This technique is similar to the one used in PC through the browsers
- Lure the user to click a link to download some cool stuff!
- However, Android malware does not require the browser for performing this attack

Drive-by Download

- GGTracker uses an in-app advertisement
- When the user clicks a special link on an adv it will redirect to a malicious website
- The website claims to analyse the phone battery for increasing its performance
- Instead a malicious payload is downloaded that will register the user to a premium-rate service without the user’s consent

Drive-by Download

- Jifake uses a similar technique of GGTracker
- Instead of a link in an advert, it uses a QR code
- The code downloaded is a repackage ICQ client
- Once installed it will send SMS to premium numbers

Drive-by Download

- Spitmo and ZitMo are two variants of the SpyEye and Zeus PC banking malware
- While the user is using an infect PC for her banking, a link will prompt to download a smartphone app to better protect online banking activities.
- The app is actually a malware that will collect banking credential from mTAN and SMS
- In Europe, these two malware have stolen US $40M

Other Attack Vectors

- Apps that claim themselves as spyware – no need to hide!
- Apps that masquerade as legitimate apps but then perform malicious actions
- Apps that provide the functionality claimed plus perform malicious actions
- Apps that rely on root-exploits to gain root privileges

Malware Activation

- Once malware is installed it will listen to events to start its malicious activity
  - BOOT_COMPLETE and SMS_RECEIVED are the most common
- Hijacking events to substitute the legitimate app activity with the malicious one
  - ACTION_MAIN or the user click the app icon

Attack Types

- Financial charges – SMS Trojan
- Communication with C&C servers – Botnets
- Information Stealing – Spyware/Ransomware/Destructive Trojan
- Root-kit exploit – all the above and much more!

Financial Charges

- One of the main reason behind these attacks is for monetary gain
- Subscription to premium SMS services that are often owned by the malware authors
- Use the permission sendTextMessage that allows an app to send SMS in background (no user in the loop)

Financial Charges

- FakePlayer uses a hard-coded message “798657” and sends it to several premium numbers in Russia
- GGTracker automatically signs up users to premium-rate services in the US
- Malware can download premium numbers from C&C to avoid detection

Hijacking Confirmations

- In China, registration to premium service requires second-confirmation SMS
- To avoid that users are notified, malware uses permission ReceiveSMS and registers a broadcast receiver with highest priority
- When the confirmation SMS arrives it is hijiacked and a reply is sent with an activation code
- The code can also be delivered by the C&C server

C&C Remote Control

- Malware can turn your phone into a bot to be controlled by a remote C&C
- To avoid detection they encrypt the URL of the C&C
  - Pjapps use the following string

    2maodb3ialke8mdmeme3gkos9g1icaofm

    To encode the domain mobilemeego91.com
  - DroidKungFu3 uses AES with key Fuck_sExy-aLl!pw
  - Geinimi use DES to encrypt its comm with the C&C

Information Stealing

- Malware also collects information from the devices
  – SMS, phone numbers, user account numbers
- SndApps collects email addresses
- FakeNetflix collect user name and password from Netflix users
- Once the data is collected it is sent over to the C&C servers

Root-kit Exploit

- Android has at its core a Linux kernel and more than 90 open-source libraries
- Some vulnerabilities exist that can be exploited for gaining root privileges
- Android Malware families have malicious payload that performs these root exploits
    - Some even more than one

Root-kit Exploit

- These exploits are public available
- Most of the malware just copy them verbatim
  - However, this also increase detection
- Recently, malware started to encrypt these exploits and store them as app asset files
- Also obfuscation techniques are used
  - Store the file and then change the extension (.jpeg)
- At runtime they are recovered and then executed
- This makes detection much more difficult.