Mobile Malware

John Mitchell

Acknowledgments: Lecture slides are from the Computer Security course taught by Dan Boneh and John Mitchell at Stanford University. When slides are obtained from other sources, a reference will be noted on the bottom of that slide. A full list of references is provided on the last slide.
Outline

• Mobile malware
• Identifying malware
  – Detect at app store rather than on platform
• Target fragmentation in Android
  – Out-of-date Apps may disable more recent security platform patches
Malware Trends

- Aggressively displaying ads
- Sending SMS
- Potentially malicious software
- Remote control over device
- Download malware
- Stealing user's data
- Stealing money from bank accounts
- Others

© Kaspersky Lab
Apple pulls popular Instagram client 'InstaAgent' from iOS App Store after malware discovery

By AppleInsider Staff
Tuesday, November 10, 2015, 03:51 pm PT (06:51 pm ET)

A popular Instagram profile analyzer was on Tuesday pulled from the iOS App Store after being outing as malware by a German developer who found the app harvesting usernames and passwords.
ACEDECEIVER: FIRST IOS TROJAN EXPLOITING APPLE DRM DESIGN FLAWS TO INFECT ANY IOS DEVICE

POSTED BY: Claud Xiao on March 16, 2016 5:00 AM

FILED IN: Unit 42
TAGGED: AceDeceiver, FairPlay, OS X, Trojan, ZergHelper

We’ve discovered a new family of iOS malware that successfully infected non-jailbroken devices we’ve named “AceDeceiver”.

What makes AceDeceiver different from previous iOS malware is that instead of abusing enterprise certificates as some iOS malware has over the past two years, AceDeceiver manages to install itself without any enterprise certificate at all. It does so by exploiting design flaws in Apple’s DRM mechanism, and even as Apple has removed AceDeceiver from App Store, it may still spread thanks to a novel attack vector.

AceDeceiver is the first iOS malware we’ve seen that abuses certain design flaws in Apple’s DRM protection mechanism — namely FairPlay — to install malicious apps on iOS devices regardless of whether they are jailbroken. This technique is called “FairPlay Man-In-The-Middle (MITM)” and has been used since 2013 to spread pirated iOS apps, but this is the first time we’ve seen it used to spread malware. (The FairPlay MITM attack technique was also
Based on FairPlay vulnerability

- Requires malware on user PC, installation of malicious app in App Store
- Continues to work after app removed from store
- Silently installs app on phone
Android malware 2015

CYREN noted a 61% increase in the amount of mobile malware targeting Android devices.

©2015. CYREN Ltd. All Rights Reserved. Proprietary and Confidential.
# Current Android Malware

<table>
<thead>
<tr>
<th>Malware</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccuTrack</td>
<td>This application turns an Android smartphone into a GPS tracker.</td>
</tr>
<tr>
<td>Ackposts</td>
<td>This Trojan steals contact information from the compromised device and uploads them to a remote server.</td>
</tr>
<tr>
<td>Acnetdoor</td>
<td>This Trojan opens a backdoor on the infected device and sends the IP address to a remote server.</td>
</tr>
<tr>
<td>Adsms</td>
<td>This is a Trojan which is allowed to send SMS messages. The distribution channel ... is through a SMS message containing the download link.</td>
</tr>
<tr>
<td>Airpush/StopSMS</td>
<td>Airpush is a very aggressive Ad-Network.</td>
</tr>
<tr>
<td>BankBot</td>
<td>This malware tries to steal users’ confidential information and money from bank and mobile accounts associated with infected devices.</td>
</tr>
</tbody>
</table>

[http://forensics.spreitzenbarth.de/android-malware/](http://forensics.spreitzenbarth.de/android-malware/)
Android free antivirus apps ...

1. Comodo Security & Antivirus
2. CM Security Antivirus AppLock
3. 360 Security - Antivirus Boost
4. Sophos Free Antivirus and Security
5. Malwarebytes Anti-Malware
6. Bitdefender Antivirus Free

http://www.androidcentral.com/top-free-antivirus-apps-android
Android malware example

22 March 2013  World Uyghur Congress

In what was an unprecedented coming-together of leading Uyghur, Mongolian, Tibetan and Chinese activists, as well as other leading international experts, we were greatly humbled by the great enthusiasm, contribution and desire from all in attendance to make this occasion something meaningful, the outcome of which produced some concrete, action-orientated solutions to our shared grievances. The attachment is a letter on behalf of WUC, UNPO and STP.
Install malicious “conference app”
Malware behavior triggered by C&C server (Chuli)

WUC’s Conference in Geneva

On behalf of all at the World Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia. In what was an unprecedented
Outline

• Mobile malware

  ➔ Identifying malware
  – Detect at app store rather than on platform

• Target fragmentation in Android
  – Out-of-date Apps may disable more recent security platform patches
STAMP Admission System

Static Analysis
More behaviors, fewer details

Dynamic Analysis
Fewer behaviors, more details

Alex Aiken,
John Mitchell,
Saswat Anand,
Jason Franklin
Osbert Bastani,
Lazaro Clapp,
Patrick Mutchler,
Manolis Papadakis
Data Flow Analysis

- Source-to-sink flows
  - Sources: Location, Calendar, Contacts, Device ID etc.
  - Sinks: Internet, SMS, Disk, etc.
Data Flow Analysis in Action

• Malware/Greyware Analysis
  ○ Data flow summaries enable enterprise-specific policies

• API Misuse and Data Theft Detection

• Automatic Generation of App Privacy Policies
  ○ Avoid liability, protect consumer privacy

• Vulnerability Discovery

Privacy Policy
This app collects your:
Contacts
Phone Number
Address
Challenges

- Android is 3.4M+ lines of complex code
  - Uses reflection, callbacks, native code
- **Scalability**: Whole system analysis impractical
- **Soundness**: Avoid missing flows
- **Precision**: Minimize false positives
STAMP Approach

- Model Android/Java
  - Sources and sinks
  - Data structures
  - Callbacks
  - 500+ models

- Whole-program analysis
  - Context sensitive

Too expensive!
Data We Track (Sources)

- Account data
- Audio
- Calendar
- Call log
- Camera
- Contacts
- Device Id
- Location
- Photos (Geotags)
- SD card data
- SMS

30+ types of sensitive data
Data Destinations (Sinks)

- Internet (socket)
- SMS
- Email
- System Logs
- Webview/Browser
- File System
- Broadcast Message

10+ types of exit points
Currently Detectable Flow Types

396 Flow Types

Unique Flow Types = Sources x Sink
Example Analysis

Contact Sync for Facebook (unofficial)

Description:
This application allows you to synchronize your Facebook contacts on Android.

IMPORTANT:
* "Facebook does not allow [sic] to export phone numbers or emails. Only names, pictures and statuses are synced."
* "Facebook users have the option to block one or all apps. If they opt for that, they will be EXCLUDED from your friends list."

Privacy Policy: (page not found)
Expected Flows

Sources
- READ_CONTACTS
- READ_SYNC_SETTINGS
- READ_SYNC_STATS
- GET_ACCOUNTS
- INTERNET

Sinks
- INTERNET
- WRITE_SETTINGS
- WRITE_CONTACTS
- WRITE_SECURE_SETTINGS
- WRITE_SETTINGS
Observed Flows

Source: FB_Data

Write Contacts

Sink: Contact_Book

Sink: Internet

Source: Contacts

Send Internet
Chuli source-to-sink flows
• **Mobile malware**
• **Identifying malware**
  – Detect at app store rather than on platform

**Target fragmentation in Android**
  – Out-of-date Apps may disable more recent security platform patches
Target Fragmentation in Android Apps

Patrick Mutchler
John Mitchell

Yeganeh Safaei
Adam Doupe
Android apps can run using outdated OS behavior
- The large majority of Android apps do this
- Including popular and well maintained apps

Outdated security code invisibly permeates the app ecosystem
- “Patched” security vulnerabilities still exist in the wild
- “Risky by default” behavior is widespread
Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences
“If the [operating system version of the device] is higher than the version declared by your app’s targetSdkVersion, the system may enable compatibility behaviors to ensure that your app continues to work the way you expect.”

- Android Developer Reference
Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences
Dataset

1,232,696 Android Apps

Popularity, Category, Update, and Developer metadata

Collected between May 2012 and Dec 2015

Broken into five datasets by collection date
Android 5.0 Released
Android 5.1 Released
Android 6.0 Released
App Collected
Outdatedness

Android 5.0 Released

Android 5.1 Released

App Updated

Android 6.0 Released

App Collected

Negligent Outdatedness
Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences
Mixed Content in WebView

⚠️ Mixed Content: The page at 'https://googleamples.github.io/web-fundamentals/samples/discovery-and-distribution/avoid-mixed-content/simple-example.html' was loaded over HTTPS, but requested an insecure script 'http://googleamples.github.io/web-fundamentals/samples/discovery-and-distribution/avoid-mixed-content/simple-example.js'. This request has been blocked; the content must be served over HTTPS.
Mixed Content in WebView

Major web browsers block Mixed Content

In Android 5.0, WebViews block Mixed Content by default

Can override default with `setMixedContentMode()`
SOP for file:// URLs in WebView

Android 4.1 separate file:// URLs are treated as unique origins

Can override with `setAllowFileAccessFromFileURLs()`
% Apps Using Unsafe file:/// SOP

Target API Version

- <16
- >=16
Recap

Android apps can run using outdated OS behavior
- The large majority of Android apps do this
- Including popular and well maintained apps

Outdated security code invisibly permeates the app ecosystem
- “Patched” security vulnerabilities still exist in the wild
- “Risky by default” behavior is widespread
Summary

• Mobile malware
• Identifying malware
  – Detect at app store rather than on platform
• Target fragmentation in Android
  – Out-of-date Apps may disable more recent security platform patches
The END