Tools and Processes for Forensic Analyses of Smartphones and Mobile Malware

Michael Spreitzenbarth

March 21st 2011
Agenda

• About the Project
• Introduction
• Android Forensics
  • ADEL & Panoptes
• Mobile Malware
• Further Work
About MobWorm

• Aims of the project:
  • Development of forensic methods and tools
  • Development of mobile Honeypots / Honeynets
  • Development of mobile Sandbox
  • POC of attack and defense scenarios

• Participants:
  • Ruhr University Bochum
  • University of Erlangen-Nuremberg
  • G-Data
  • Security Labs
Why Android?

• Open Source mobile OS
• Biggest growth rate in sector
• Many different manufacturers
• Many different fields of application (smartphone, tablet, TV......)
• According to the leading market research companies THE mobile OS of the future
### Top Smartphone Platforms

#### 3 Month Average

<table>
<thead>
<tr>
<th>Market-Share (%) of Smartphone Subscribers</th>
<th>January 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>US</td>
</tr>
<tr>
<td>Apple</td>
<td>24.7</td>
</tr>
<tr>
<td>Google</td>
<td>31.2</td>
</tr>
<tr>
<td>Microsoft</td>
<td>8.0</td>
</tr>
<tr>
<td>Palm</td>
<td>3.2</td>
</tr>
<tr>
<td>RIM</td>
<td>30.4</td>
</tr>
<tr>
<td>Symbian</td>
<td>--</td>
</tr>
</tbody>
</table>

Source: comScore MobiLens & IDC European Quarterly Mobile Phone Tracker
Android Forensics

- Security restrictions of the Android platform
- SQLite databases
- Filesystem:
  - YAFFS2
  - EXT4
Android Forensics

Panoptes
Software-Agent

ADEL
„Forensic“ Software
Panoptes

- Software Agent (on-phone-toolkit)
- JAVA App
- Uses Content Provider to access the databases
- Generates CSV-files

- Has to be installed on the device
ADEL
(Android Data Extractor Lite)

- Modular design
- Connection through adb
- Dumps SQLite databases
- Uses its own SQLite parser
- Generates XSL / XML report
Forensic Analysis of Smartphones: The Android Data Extractor Lite

Felix Freiling, Michael Spreitzenbarth, Sven Schmitt

Conference on Digital Forensics, Security and Law

Richmond, Virginia, USA

May 25-27, 2011
Mobile Malware

- Smartphones have powerful hardware
- First malware sighted:
  - ZeuS-MITMO
  - DroidDream
  - zHash
- Only few detection processes
- Nearly no defensive measures
Mobile Sandbox

- Android based sandbox for malware analysis
- Fully automated analysis process and reporting

- Is it possible to adopt known approaches?
  - CWSandbox or MobileSandbox
  - pTrace or sTrace
  - sebek
Further Work

• Creation of forensic tools and procedures for YAFFS2 and EXT4

• Increased functionality of ADEL

• Analyze and „understand“ Android malware

• Building a Mobile Sandbox for Android
Questions?
Thank you very much for your Attention

- Michael Spreitzenbarth
- Chair for IT Security Infrastructures
- University of Erlangen-Nuremberg
- 91058 Erlangen-Tennelohe
- michael.spreitzenbarth@informatik.uni-erlangen.de
References


• M. Becher, „Mobile Sandbox“, http://mobilesandbox.org

• TuX-Logos from the website http://tux.crystalxp.net/