The incident response playbook: For Android and iOS
Andrew Hoog
NowSecure CEO and Co-founder

- Computer scientist & mobile security researcher
- Author of three mobile security books
- Enjoyer of science fiction, running and red wine
Mobile incident response challenges
DFIR professionals vs. giants

Titans of industry, governments, organized crime

- Mobile defenders have few allies
- Apple and Google making strides to make iOS and Android more secure
- Restricted platforms amplify attackers’ asymmetric advantage
- (Attackers know something their targets don’t)
Broad attack surface

Resulting from large user base, dual-use devices, rapid development, and continuous connectivity
The challenges of mobile IR

- **DUAL-USE**
- **ALWAYS-ON CONNECTIVITY**
- **NO ADMIN ACCESS**
- **DIFFERENT TOOLS**
Building blocks for your mobile incident response plan
You need to start somewhere

- Identify assets:
  - Devices
  - Operating systems
  - Installed apps

- SCAN Principle
  - System
  - Configuration
  - Apps
  - Network

- Historical data is crucial to response
Your mobile IR “jump bag”

Install and configure your tools and know how to use them

CONTINUAL ANALYSIS TOOLS

ACQUISITION TOOLS

FORENSIC ANALYSIS TOOLS (& more)

See a detailed list at
Phases of incident response

Playbooks are an output of the preparation phase

Great reference: Mason Pokladnik’s “Checklist for incident response capability”
## Types of mobile incidents

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Prevalence</th>
<th>Max Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNAL INVESTIGATION</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>INSIDER ATTACK</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>LOST OR STOLEN DEVICE</td>
<td>HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>VULNERABLE OR LEAKY APP</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>MALICIOUS IMPOSTER APP</td>
<td>LOW</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>DATA BREACH</td>
<td>LOW</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>DEVICE ACTING SUSPICIOUSLY</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>MALWARE ON DEVICE</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
</tr>
</tbody>
</table>
Mobile incident response playbook
It all began on Saturday, February 13

Here's the data you might get from an end user
Step 1 — Identification

- Device Indicators of Compromise (IoCs)
  - Battery drain
  - Unusual network traffic
  - Certificate errors
  - Unusual log messages
  - Crash reports
- App reputation monitoring
  - Unauthorized use of brand
  - Apps connecting to your transactional servers
- User reported
Step 2 — Containment

Once you have identified and logged an incident

- Gain access to device, if possible
- Capture device, OS, and app baseline
- Determine if network analysis is appropriate
- Isolate the device
  - Airplane mode
  - Faraday bag
  - Etc.
- Perform full forensic acquisition
Step 3 — Eradication

- Analyze attack artifacts
- Determine if threat can be removed
- Identify all impacted (if malware on app store)
- Remove threat or wipe corporate data
Mobile recovery typically involves
● Re-provision mobile devices
● Ensure attacker didn’t move laterally
● Monitor accounts and systems connected to mobile device and impacted user(s)
● Effectiveness of social engineering attacks is greatly increased
Step 5 — Debriefing

- **Team debrief:**
  - What worked, what can be improved
  - Policies & procedures changes, user education
- **Determine IOCs**
  - Attribution
  - Share threat intel data
- **Inoculate against future attacks**
  - Static signatures generally ineffective
  - Focus on anomaly detection
  - Shared insights and cross-referenceable data
Don’t panic

Andrew Hoog // CEO & Co-founder

NowSecure
ahoog@nowsecure.com
+1.312.878.1100
@ahoog42