The “Five W’s” of Mobile Device Malware: Who, What, When, Where, and Why? ... and What Can be Done About It?

Kevin McPeak, CISSP, ITILv3
Technical Architect, Security
Symantec Public Sector Strategic Programs
Who Can Be Affected by Mobile Malware?

School Administrators, Teachers, Students, and Home Users

Apple iOS  
Android
BlackBerry  
Windows Mobile

Who Creates & Distributes Mobile Malware?

Cyber Criminals and their Accomplices

Malware Developers  
Mules
Mobile Botnet Operators  
Cyber Thieves
Criminal Elements  
Hacktivists
What is Mobile Malware and How Do We Count Them?

- Each of these applications contain the same piece of malware embedded in them
- Each piece of malware is counted as one Family
  - If this malware is modified the new version counts as a Variant
- We would count the five apps as Samples
- We do not report on Samples, but many vendors do
What is the Growth Rate of Android Malware?
What Mobile Platform Has the Most Vulnerabilities? ...

What Mobile Device Type Has the Most Threats?

Vulnerabilities & Mobile Malware

<table>
<thead>
<tr>
<th>Platform</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iOS</td>
<td>387</td>
</tr>
<tr>
<td>Android</td>
<td>13</td>
</tr>
<tr>
<td>Blackberry</td>
<td>13</td>
</tr>
<tr>
<td>Windows Mobile</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Type</th>
<th># of Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iOS Malware</td>
<td>1</td>
</tr>
<tr>
<td>Android Malware</td>
<td>103</td>
</tr>
<tr>
<td>Symbian Malware</td>
<td>3</td>
</tr>
<tr>
<td>Windows Malware</td>
<td>1</td>
</tr>
</tbody>
</table>
What Types of Mobile Malware Exist?


- **Track User**: 36%
  - Risks that spy on the individual using the device, collecting SMS messages or phone call logs, tracking GPS coordinates, recording phone calls, or gathering pictures and video taken with the device.

- **Collect Data**: 23%
  - This includes the collection of both device- and user-specific data, such as device information, configuration data, or banking details.

- **Traditional Threats**: 22%
  - Threats that carry out traditional malware functions, such as back doors and downloaders.

- **Change Settings**: 12%
  - These types of risks attempt to elevate privileges or simply modify various settings within the operating system.

- **Adware/Annoyance**: 24%
  - Mobile risks that display advertising or generally perform actions to disrupt the user.

- **Send Content**: 7%
  - These risks will send text messages to premium SMS numbers, ultimately appearing on the bill of the device’s owner. Other risks can be used to send spam messages.
When is Mobile Malware Active?

When Mobile Data is Collected: When IMEI7 and IMSI8 numbers are taken by attackers as a way to uniquely identify a device.

When Users Are Tracked: When communication data such as SMS messages, call logs, GPS coordinates, calendar events, or personal photos are exfiltrated.

When Bad Apps Send Out Content: When an app sends a text message to a premium SMS number, ultimately appearing on the mobile bill of the device’s owner.

Or when a device is hijacked to serve as an e-mail spam relay system, thus allowing unwanted e-mails to be sent from addresses registered to the device.

When Device Settings are Changed: When an attempt is made to elevate privileges or modify OS settings to perform further actions on the compromised devices.
Where is Mobile Malware Found?

Third-party app stores hosting the most malware from January to June 2013

Where is Mobile Malware Found?

• In 2018, App revenues will be worth $92 Billion
• Currently there are 70 app stores
• The big 5 app stores contain approx. 1.9 Million apps
• Approx. 25% of apps downloaded are used just once
• Most used app: Facebook
Why is Mobile Malware Developed?

... because There is Significant Illicit Money Being Made

- Premium SMS Messages
- Mobile Adware (Madware)
- Stealing Information
- Bank Fraud
- Ransomware
- Botnets and Spam
Information Stealing Malware

Android.Sumzand

1. User received email with link to download app
2. Steals contact information
3. Sends email promoting app to all contacts
... Lastly, What Can be Done About It?

Vulnerability Patching

Google

OEMs

Service Providers

iOS

... What Can be Done About It? (Continued)

What Can be Done About It? (Continued)

**Enforce User Mobile Security Training:** School employees must be constantly reminded to avoid clicking on suspicious links in messages, to keep their personal mobile devices updated, and to only download apps from officially sanctioned App Stores.

**Deploy Mobile Security Software Throughout Your School:** At a minimum, this software should scan and identify threats from any mobile apps or content that the user downloads.

**Establish a Robust, Highly Secure Mobile Device Management Framework for Your School:** Managing your school’s mobile devices is not just about remote wipe commands for lost/stolen devices and OTA password resets. You should also setup a system for mobile app management across the entire app lifecycle. Likewise, you should manage your school’s mobile content ecosystem in the same secure end-to-end manner.
Thank you!

**Kevin McPeak**
kevin_mcpeak@symantec.com
@kevin_mcpeak

**mobilesecurity.com/**

**symantec.com/threatreport**