State of Cell Phone Malware in 2007

Mikko Hypponen, Chief Research Officer

F-SECURE®

BE SURE.
WARNING!
LIVE WIRELESS VIRUSES
DO NOT OPEN THE DOOR!
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING IN PROGRESS
But surely you’re not serious?

...mobile phone viruses are just an urban legend...
...they are not really spreading anywhere...
...you are just hyping them...

...and stop calling me Shirley.
Mobile viruses: this is already happening...

- More than **370** mobile phone viruses so far
- Tens of thousands of infections worldwide
- Reports about Cabir and Commwarrior from over **30** countries
- Operator with 9 million customers: almost **5%** of MMS traffic infected
- Operator with 14 million customers: Over **8000** infected devices have sent over **450000** MMS messages. Largest number of messages sent by one phone: **3500**.
- Operators have given money back to customers who had Commwarrior
Prerequisites for any Malware Outbreak

Enough functionality
  • for the malware to work

Enough connectivity
  • for the malware to spread

Enough target terminals
  • for the platform to become an interesting target
Smartphone markets

Very important differences on the markets:

• Americas
• EMEA
• APAC
Number of mobile malware

Data source: F-Secure
Types of mobile threats

What we have seen so far

• Viruses
• Worms
• Trojans
• Spy tools

What we have not seen yet

• Rootkits
• Worms that do not need user interaction for spreading
• Mobile botnets
• Large-scale profit-oriented malware (professionals)
### Malware per Platform by Year

Data source: F-Secure

<table>
<thead>
<tr>
<th>Platform</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palm</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>PocketPC</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Symbian</td>
<td>22</td>
<td>141</td>
<td>337</td>
<td>364</td>
</tr>
<tr>
<td>J2ME</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>All</strong></td>
<td>27</td>
<td>146</td>
<td>345</td>
<td>373</td>
</tr>
</tbody>
</table>
Mobile malware by Type

<table>
<thead>
<tr>
<th>Types</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>58</td>
</tr>
<tr>
<td>Trojans</td>
<td>297</td>
</tr>
<tr>
<td>Spyware</td>
<td>9</td>
</tr>
</tbody>
</table>

Data source: F-Secure
What do the trojans do?

Break the phone so that it crashes and will not boot again
  • SymbOS/Doomboot family

Break phone services like Messaging, Web, Camera etc.
  • SymbOS/Skulls family

Cause monetary loss by sending messages
  • SymbOS/Mquito.A, Java/Redbrowser.A

Steal user's private information and send it out via bluetooth
  • SymbOS/Pbstealer family

Set random password to phone memory card, making it useless
  • SymbOS/Cardblock.A

Delete user E-Mail, SMS messages and other critical information
  • SymbOS/Cardblock.A
## Infection mechanisms

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth</td>
<td>71</td>
</tr>
<tr>
<td>MMS</td>
<td>23</td>
</tr>
<tr>
<td>Memory cards</td>
<td>3</td>
</tr>
<tr>
<td>User download</td>
<td>373</td>
</tr>
</tbody>
</table>

Data source: F-Secure
In-the-wild Spreading vectors

1. Bluetooth
2. MMS
3. User downloads
4. Memory cards

Not yet:
- Email
- SMS
- WLAN
- P2P
- IM
So, where are they coming from?

Europe
- Norway
- Spain

South America
- Brazil

Asia
- India
- Malaysia
- Indonesia
- Philippines
- China
Where in the world is the problem?
How come Windows Mobile is not targetted more?

Good question.
It will be.
Low marketshare explains a bit, but not everything
So, why do people get infected?

Because of the user interface
**Cabir is still spreading in the wild**

Cabir was found in June 2004

First in-the-wild report from Philippines in August 2004

Still in-the-wild in 2007

- Singapore
- UAE
- China
- India
- Finland
- Vietnam
- Turkey
- Russia
- UK
- Italy
- USA
- Japan
- Hong Kong
- France
- South Africa
- Australia
- The Netherlands
- Egypt
- Luxembourg
- New Zealand
- Switzerland
- Germany
F-Secure Bluetooth Honeypot Prototype

Closest 14 discoverable bluetooth devices (currently 134 devices in range, total 828)

<table>
<thead>
<tr>
<th>#</th>
<th>Bluetooth Device</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jaana</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Nokia Smart Phone</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Nokia 6230</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Exploit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>RAUM30_10</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>TR100674</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Nokia 6310i</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Nokia 6310i</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>BlackBerry 7100</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Nokia 6230i</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Ruedi</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Nokia 6820</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Honeypot</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>IBM-EK</td>
<td></td>
</tr>
</tbody>
</table>

Top bluetooth viruses (total 10 files received)

<table>
<thead>
<tr>
<th>#</th>
<th>Virus name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SymbOS/Skulls:A</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>EICAR test file</td>
<td></td>
</tr>
</tbody>
</table>

Search for discoverable devices: Enabled (Disabled)
Bluetooth Honeypot: Enabled (Disabled)
Alert infected phones: Disabled (Enabled)
Commwarrior

By "e10d0r"
Symbian Series 60 virus
First virus to spread over MMS messages
Also spreads over Bluetooth
Worst we've seen so far
Could be really expensive
"OTMOP03KAM HET!"
Cardtrap

First mobile phone virus that tries to infect Windows PCs too
Drops two Windows viruses to phone’s memory card
Case Viver

May 18th 2007: First international $M$ trojans found from a Symbian download site

Three different fake applications

When installed, they start to send expensive premium-rate SMS messages to an international service number

Each SMS costs about US$7
What are the vendors doing?

Phone manufacturers: fixing the Bluetooth user interface issue
Symbian: shipped Symbian 9
**Symbian Signed** introduced
Video: Improved Bluetooth user interface
Welcome
Symbian Signed promotes best practice in designing applications to run on Symbian OS phones. Symbian Signed applications follow industry-agreed quality guidelines and support network operator requirements for signed applications. More details about Symbian Signed can be found [here](https://www.symbiansigned.com/app/page).

Understanding the Signing Process
In order to Symbian Sign your application there are a number of steps that need to be followed. [More](https://www.symbiansigned.com/app/page).

Symbian Signed Test Criteria
Applications submitted to Symbian Signed will be validated against specific test criteria. [More](https://www.symbiansigned.com/app/page).

Symbian Developer Network
The Symbian Developer Network is the primary source of solutions for all developer requirements. [More](https://www.symbiansigned.com/app/page).

SYMBIAN SIGNED WEBSITE UPDATE - SITE FULLY FUNCTIONAL FOR REGISTERED ACCOUNTS
The Symbian Signed web site has now been migrated, with the following functionality now available.

- Applications may be submitted via the site for testing via TEST HOUSES.
Mobile Spyware

Mobile spying tools are applications that are installed into a smartphone and send information out from the phone

- Typical example would be an application that sends all received SMS message to a third party without permission from the user

Mobile spying tools might **not** be illegal by itself

- Spyware vendors insist that their spyware must be used only for legal purposes
Targeted and untargeted spying tools

Targeted spying tools are limited by the vendor
- A spy must know the victim before obtaining spying tool
- Usually limiting is done by requiring the target devices IMEI code in order to be able to obtain the spying software
- So the spy needs to have access to the device twice
- This is done by spyware authors more as a way of copy protection than concern on how their software is going to be used

Untargeted spyware can be installed into any device
- The victim of the spying tool can be picked at random
- The spy needs to access the device only once
Information that can be stolen by spyware

Text messages
- Sender and receiver phone numbers and phonebook names
- The content of the SMS messages (think two-factor passwords)

Call information
- Incoming or outgoing call and to what number
- Time and duration of the call

Voice recording
- Application can record all phone calls
- Application can also record anything that's spoken near the phone

Physical location
- Spyware records in which GSM cell it is and how strong the field is
So…what about iPhone viruses?

- Closed platform
- No SDK
- Hard to program
- No Bluetooth file transmissions
- File system not accessible

+ Has the userbase
+ Lots of eager hackers
+ First attempt from Apple

Verdict: I'd give it a 90% chance that we'll see an iPhone virus. Perhaps spreading via SMS or email.
Oh, and one more thing…

How well does iPhone work in Nordic Wintern conditions?

http://www.youtube.com/fslabs
Feel free to try us out

Visit: www.f-secure.mobi

Contains an Antivirus and a Firewall.
And in the future?

More for-profit malware
Native malware for S60 3rd edition
More Java malware
More Windows Mobile malware
SMS worms
Wi-Fi worms – for Windows
Mobile worms using exploits (perhaps exploiting things like MMS, OTA, reflashing etc)
Mikko Hypponen
Chief Research Officer
F-Secure Corporation

www.f-secure.com
www.hypponen.com