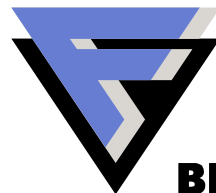


# State of CELL PHONE Malware in 2007

Mikko Hypponen, Chief Research Officer

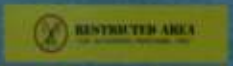
**F-SECURE®**



**BE SURE.**

A photograph of a laboratory door. The door is closed and has a large white warning sign with black text. To the right of the door, there is a control panel with several buttons and a red light that is illuminated. A yellow and black striped caution tape is attached to the door handle. The walls are a light blue color.

**WARNING!**  
LIVE WIRELESS VIRUSES  
DO NOT OPEN THE DOOR!  
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING  
IN PROGRESS



RESTRICTED AREA

## 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
-

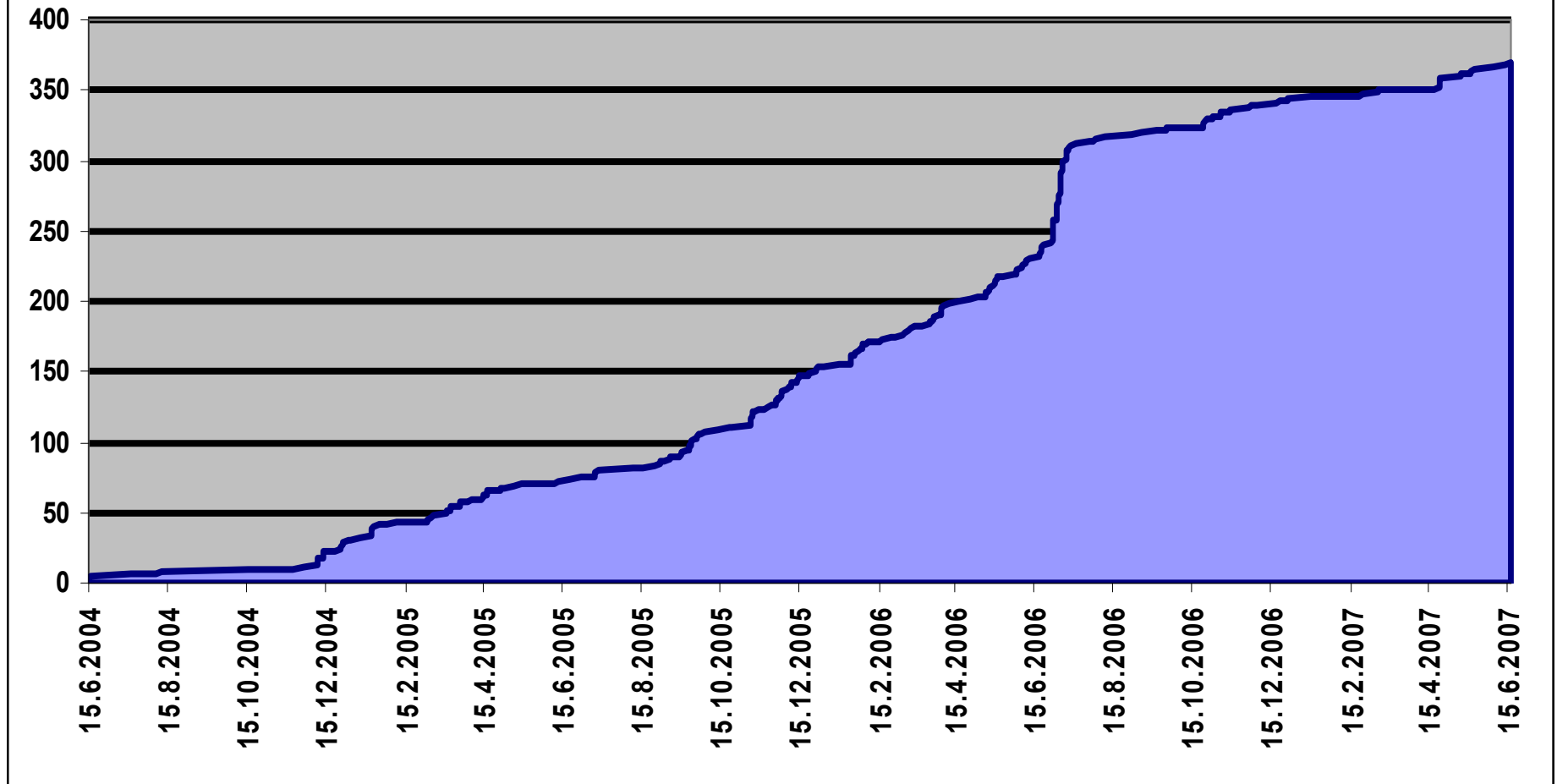
## Smartphone markets

Very important differences on the markets:

- Americas
- EMEA
- APAC



Number of mobile malware



Data source: F-Secure

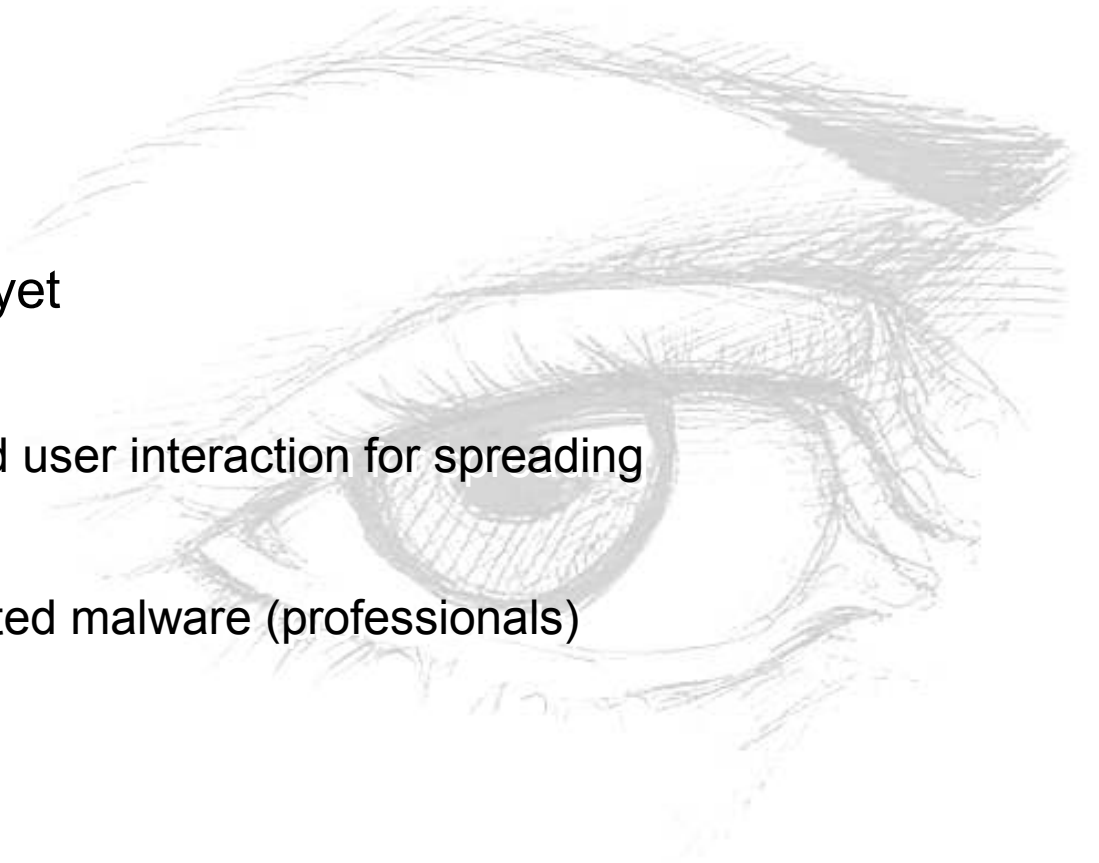
# Types of mobile threats

## 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

Platform	2004	2005	2006	2007
Palm	3	3	3	3
PocketPC	2	2	3	4
Symbian	22	141	337	364
J2ME	0	0	2	2
<b>All</b>	<b>27</b>	<b>146</b>	<b>345</b>	<b>373</b>



Data source: F-Secure

## Mobile malware by Type

### Types

Viruses	58
Trojans	297
Spyware	9



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

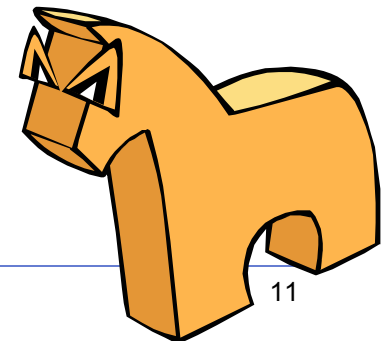
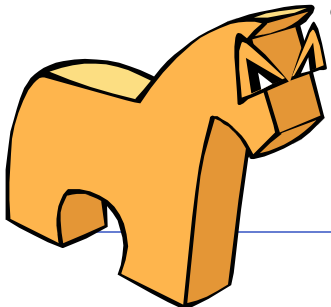
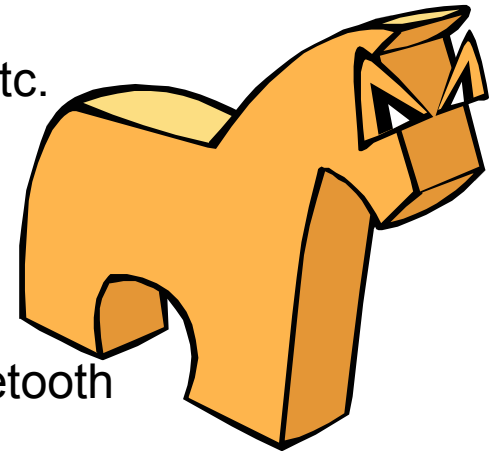
- *SymbOS/Pbstealer family*

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

Bluetooth	71
MMS	23
Memory cards	3
User download	373



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

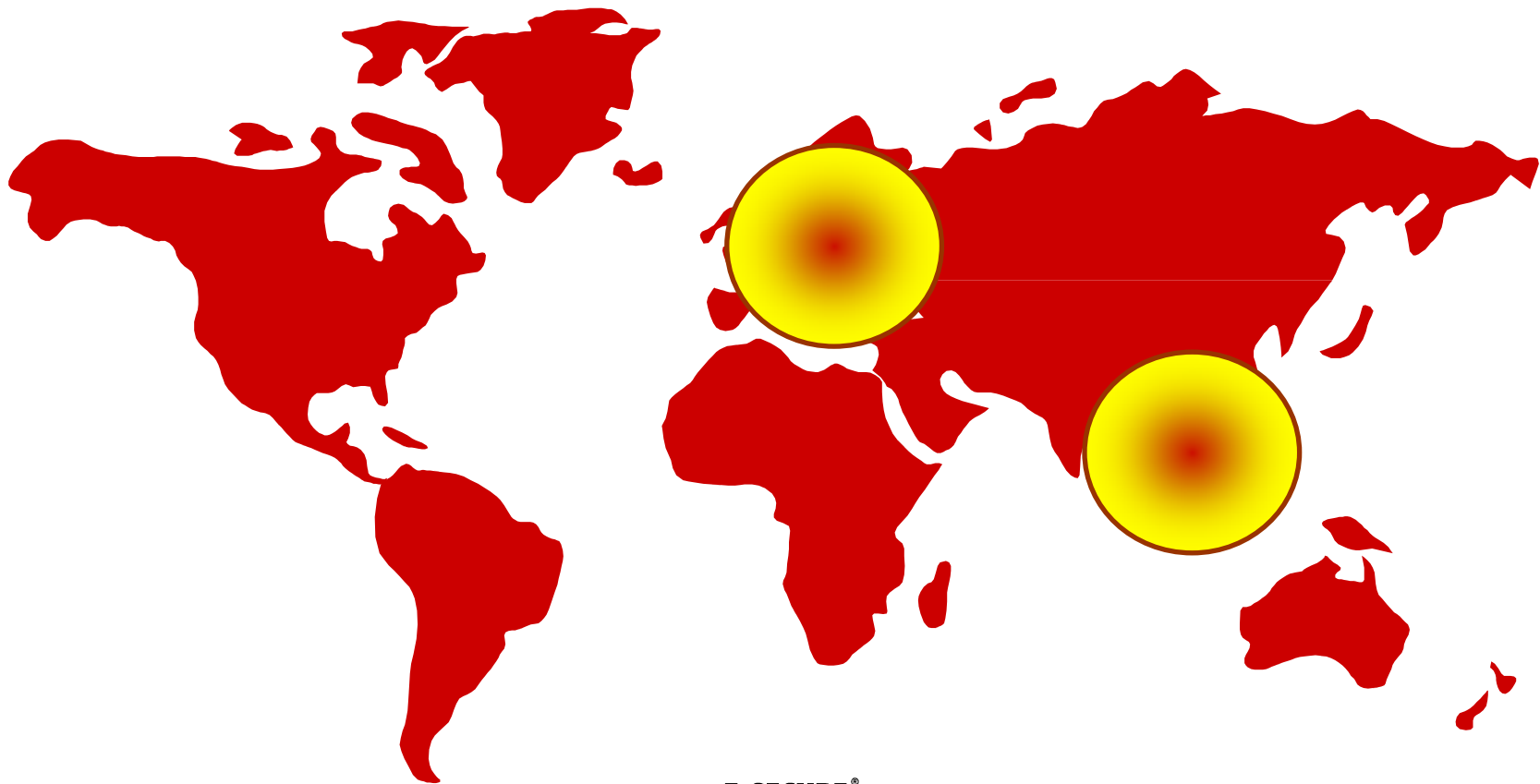
## Asia

- India
- Malaysia
- Indonesia
- Philippines
- China

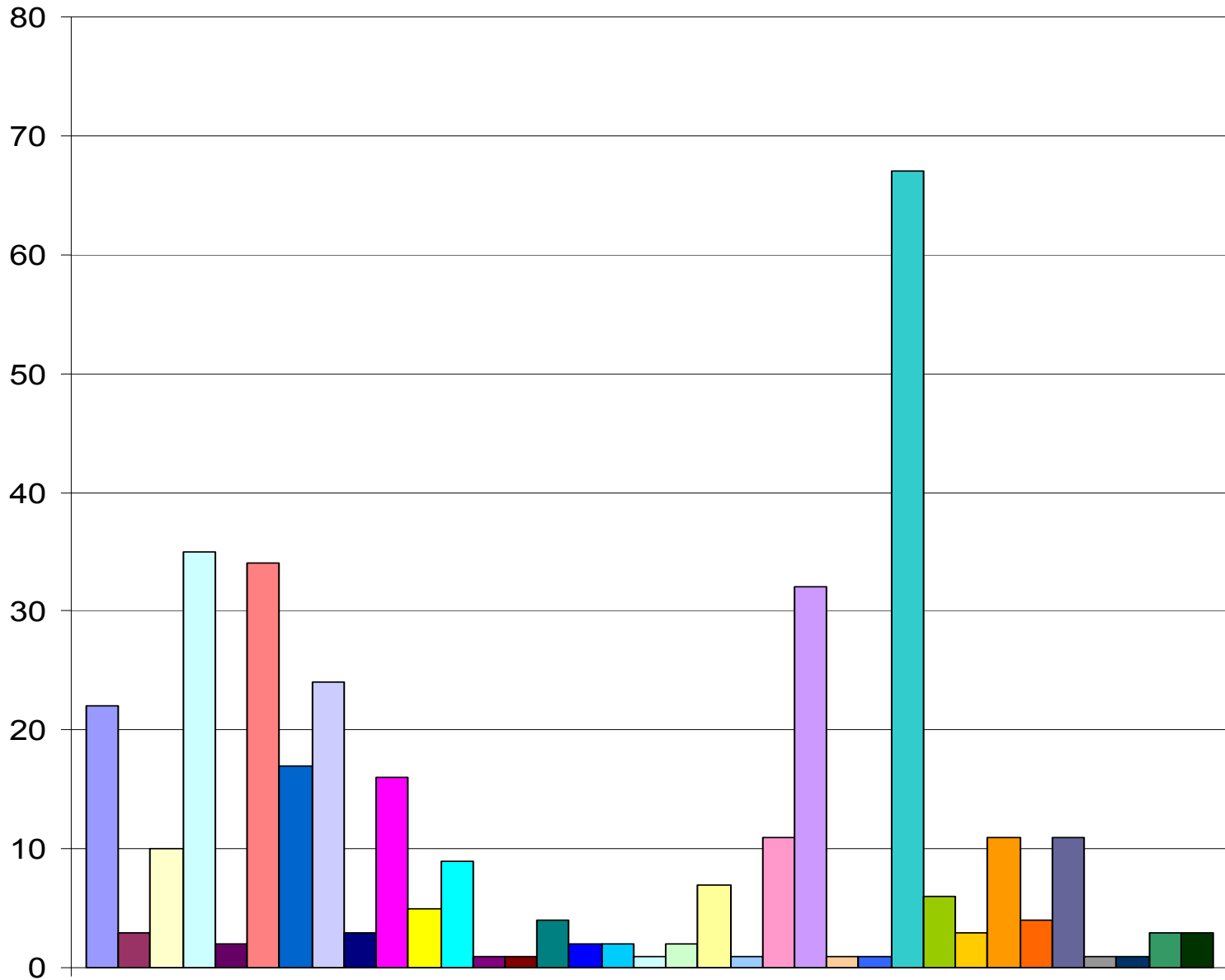
F-SECURE®



# Where in the world is the problem?



## Variants in families



- Appdisabler
- Blankfont
- Bootton
- Cabir
- Cardblock
- Cardtrap
- Cdropper
- Commwarrior
- Dampig
- Doomboot
- Drever
- Fontal
- Hobbes
- Lasco
- Locknut
- Mabir
- Mabtal
- Mquito
- Nogav
- Pbstealer
- Sendtool
- Singlejump
- Skulls
- Redbrowser
- Cxover
- Sdropper
- Stealwar
- Trojan-spy.FlexiSpy
- Commdropper
- Rommwar
- Romride
- Acallno
- Wesber
- Flerprox
- Feak



# 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	Hong Kong
UAE	France
China	South Africa
India	Australia
Finland	The Netherlands
Vietnam	Egypt
Turkey	Luxembourg
Russia	New Zealand
UK	Switzerland
Italy	Germany
USA	
Japan	







# F-Secure Bluetooth Honeypot Prototype

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

#	Bluetooth Device
1.	Jaana Nokia Smart Phone (00:11:9f:c1:1d:d6)
2.	Nokia 6230 Nokia Cellular (00:12:62:d6:8d:0a)
3.	TABLETPC2 Laptop (00:0b:5e:a0:1a:7b)
4.	Exploit Cellular (00:60:57:9a:6b:56)
5.	RAUM30_10 Desktop (00:20:a0:7c:bb:71)
6.	TR100674 Laptop (00:0b:5d:a0:9a:7c)
7.	Nokia 6310i Cellular (00:60:57:2c:81:29)
8.	Nokia 6310i Cellular (00:0e:5d:20:b7:46)
9.	BlackBerry 7100 Smart Phone (00:0c:86:1a:76:d1)
10.	Nokia 6230i Nokia Cellular (00:15:0a:22:33:5c)
11.	Ruedi Nokia Cellular (00:12:62:c2:04:f6)
12.	Nokia 6820 Nokia Cellular (00:02:aa:d3:8c:3c)
13.	Honeypot ~~~~~ Nokia Smart Phone (00:0e:ad:b2:a2:80)
14.	IBM-EK Laptop (00:0e:96:4a:41:26)

09-Mar-2006 11:00:41 - Status: (same) 1/844 - 1/212

Top bluetooth viruses  
(total 10 files received)

#	Virus name
1.	SymbOS/Skulls.A 1 infected devices 09-Mar-2006 10:31:45 (00:0e:ad:b2:a2:80)
2.	EICAR test file 1 infected devices 09-Mar-2006 10:38:05 (00:0e:ad:b2:a2:80)

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

SAMSUNG

SynchMaster 192r



# DEMO



# Commwarrior

By "e10d0r"

Symbian Series 60 virus

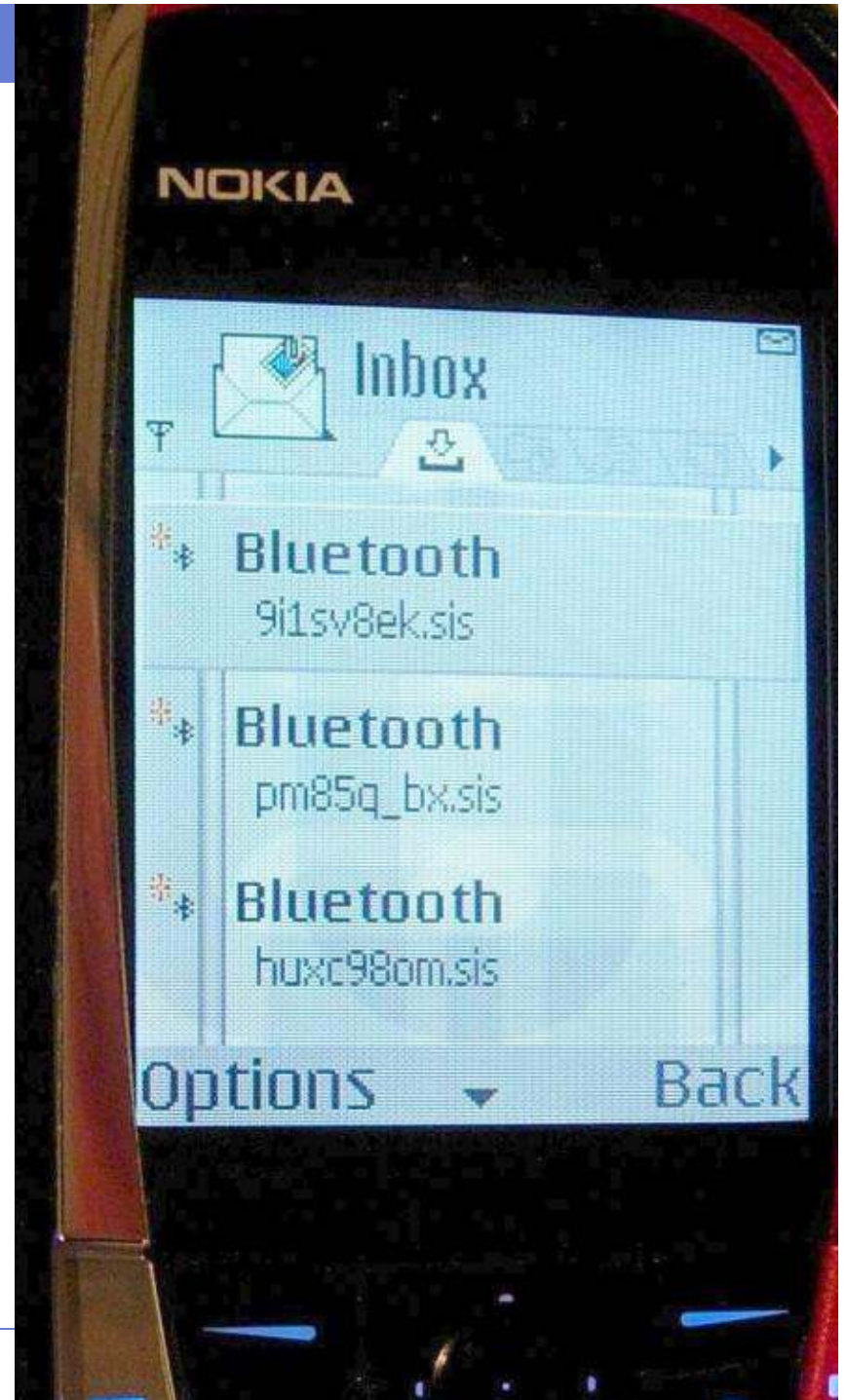
First virus to spread over  
MMS messages

Also spreads over Bluetooth

Worst we've seen so far

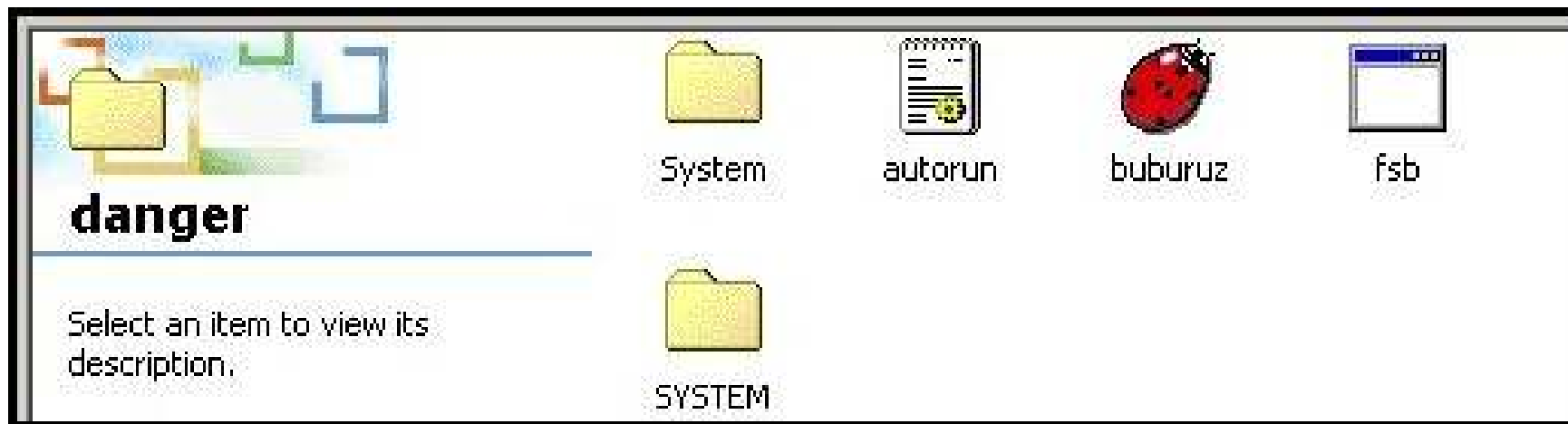
Could be really expensive

"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



S60 3rd Edition  
(or S60 3.0),

Vs

S60 3rd Edition Feature  
Pack 1 (or S60 3.1).



You are not logged in

Symbian Signed Overview

My Symbian Signed

Account Settings



### 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](#).

Get your freeware




Username:

Password:

[Register now!](#) [Lost password?](#)



### Understanding the Signing Process

In order to Symbian Sign your application there are a number of steps that need to be followed. [▶ More](#)



### Symbian Signed Test Criteria

Applications submitted to Symbian Signed will be validated against specific test criteria. [▶ More](#)



### Symbian Developer Network

The Symbian Developer Network is the primary source of solutions for all developer requirements. [▶ More](#)

### Symbian Signed News

- ▶ [Symbian Signed launches new Certificate Authority](#)
- ▶ [Fast-Track signing process now available](#)
- ▶ [Test Criteria \(v2.11.0\) - Updated!](#)
- ▶ [Developer Certificate changes](#)

### Symbian News

- ▶ [OMTP PRODUCT PROFILE PROCESS](#)
- ▶ [FOMA™ SH903i launched today is based on Symbian OS](#)
- ▶ [Symbian Signed launches new initiatives to make application signing faster](#)
- ▶ [Symbian launches new book for Accredited Symbian Developer exam](#)
- ▶ [Sling Media and Symbian partner to bring personal TV home viewing to consumers](#)
- ▶ [Symbian welcomes the Samsung SGH-i520](#)
- ▶ [LG Electronics introduces HSDPA Symbian smartphone](#)

### Product updates

- ▶ [A new tool to export TrustCenter Publisher Ids is available](#)
- ▶ [A new version of "VerifySymbianSigned" tool is available](#)
- ▶ [A new version of DevCertRequest is available](#)
- ▶ [A new version of AppTest Lite for Symbian OS phones](#)

### 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.



### Basic Capabilities

- LocalServices
- UserEnvironment
- NetworkServices
- Location
- ReadUserData
- WriteUserData

### Generic Symbian Signed Test Criteria

### Extended Capabilities

- ReadDeviceData
- WriteDeviceData
- SWEvent
- ProtSrv
- Power Mgmt
- SurroundingsDD
- TrustedUI

*Declarative  
statements and  
API declarations*

### Phone Manufacturer Approved

- DRM
- NetworkControl
- MultimediaDD
- TCB
- AllFiles
- CommDD
- DiskAdmin

*Licensee defined  
additional tests  
through Channel  
Certification*



# 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



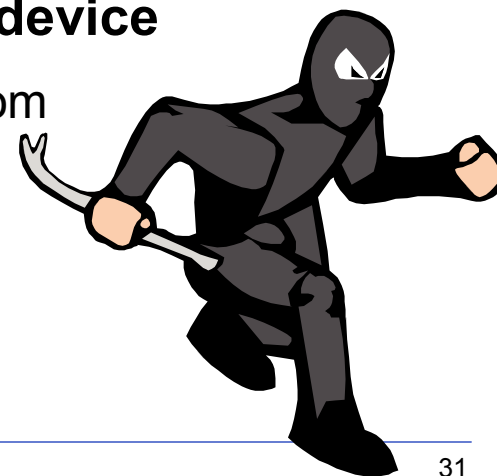
# Targeted and untargeted spying tools

## 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

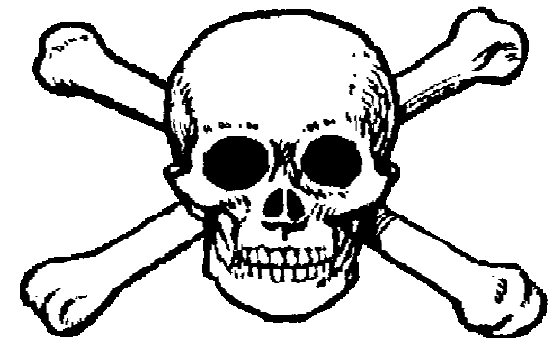
- Incoming or outgoing call and to what number
- Time and duration of the call

## 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







# DEMO



## 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 Winter conditions?

<http://www.youtube.com/fslabs>



# Feel free to try us out

**Visit: [www.f-secure.mobi](http://www.f-secure.mobi)**

**With a [Windows Mobile | Symbian] phone.**

**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

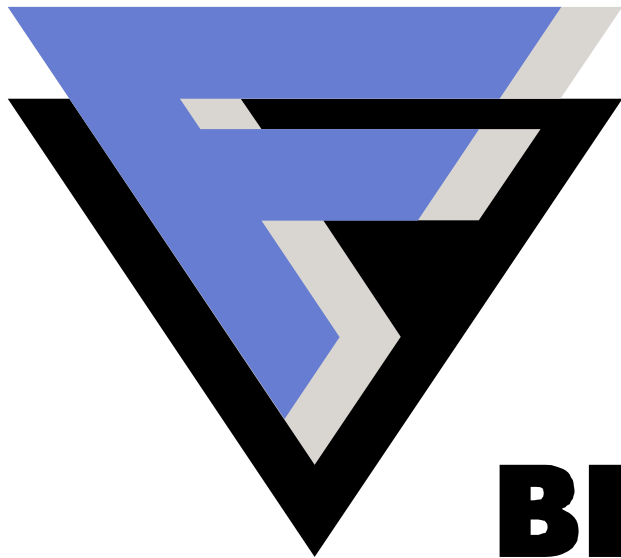
SMS worms

Wi-Fi worms – for Windows

Mobile worms using exploits  
(perhaps exploiting things like  
MMS, OTA, reflashing etc)



**F-SECURE**®



**BE SURE.**

**Mikko Hypponen**  
**Chief Research Officer**  
**F-Secure Corporation**

**[www.f-secure.com](http://www.f-secure.com)**

**[www.hypponen.com](http://www.hypponen.com)**