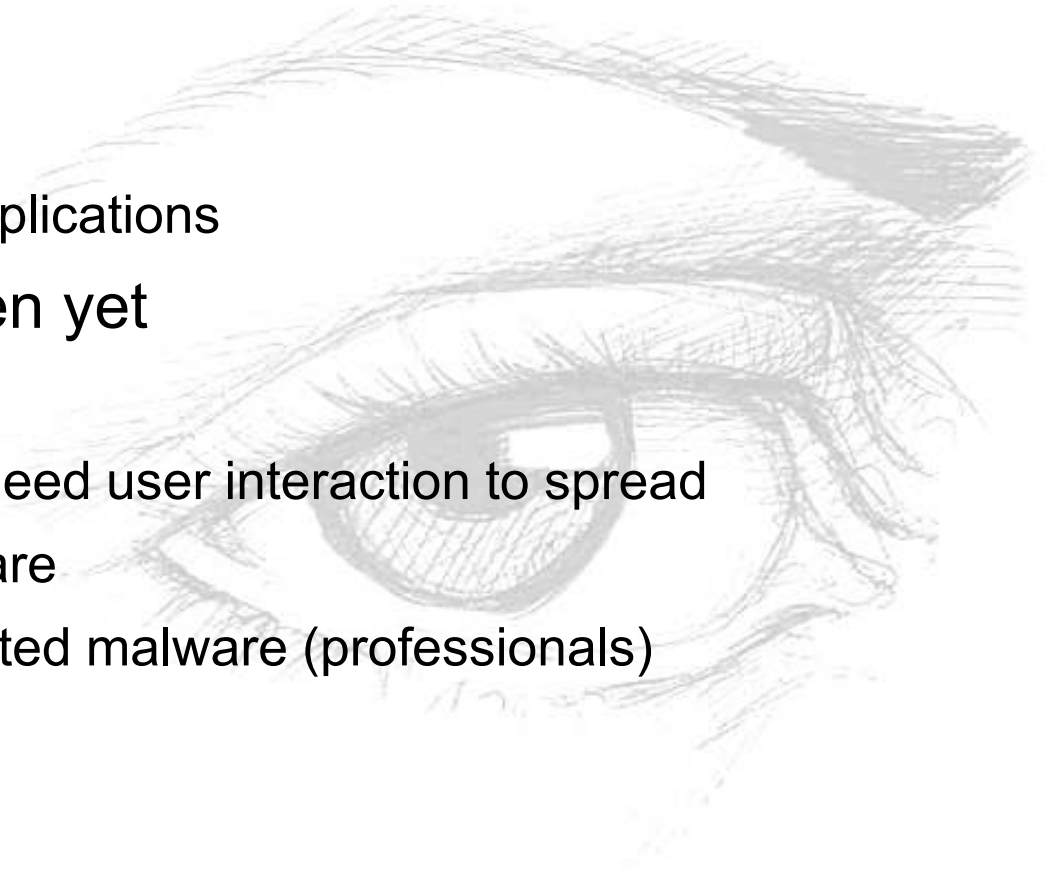# Types of Mobile Threats

What we have seen so far

- Viruses
- Worms
- Trojans
- Single target spying applications

What we have not seen yet

- Rootkits
- A worm that does not need user interaction to spread
- Mass distributed spyware
- Large scale profit oriented malware (professionals)

Mobile Spy Tools

Mobile spy tools are applications that are installed onto a phone to send information out from the phone

- Typical example - an application that forwards all received SMS messages to a third party without the user's permission

Mobile spy tools are not illegal in and of themselves

- Their vendors state (weakly in most cases) that they must only be used for legal purposes

- While in reality most of the things for which people use these tools are illegal; or at least they are in countries that have strong privacy protection laws

F-SECURE®

BE SURE.

Who Would Use Spy Tools

The same people who use PC based spy tools

- Oppressive spouses and other domestic abuse cases
- Private investigators / divorce attorneys
- Managers monitoring their employees
- Industrial spies

Some vendors sell both PC and mobile spy tools

- And give discounts if you buy both
- Spy both on your wife's PC and her mobile phone

F-SECURE ®

BE SURE.

Targeted and Untargeted Spy Tools

Targeted spy tools are limited by the vendor

- A spy must know the victim before obtaining the spy tool

- Limitations are usually applied by requiring the target device's IMEI code in order to obtain the spy software

- So the spy needs to have access to the device at least twice

- This is done by spy tool authors more as copy protection than concern on how their software is going to be used

Untargeted spyware can be installed onto any device

- The victim of the spy tool can be picked at random

- The spy needs to access the device only once

F-SECURE®

BE SURE.
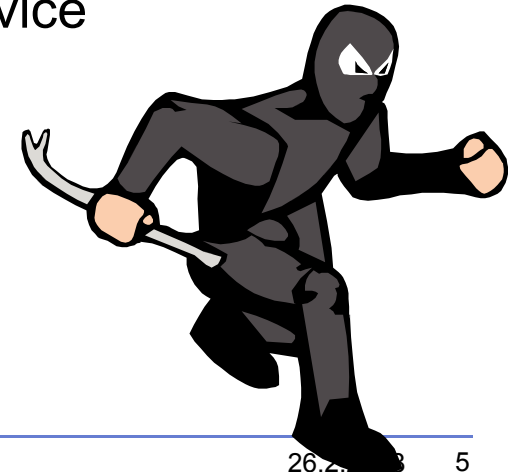
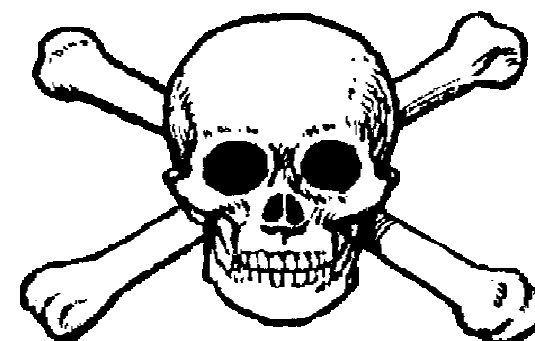# Information That Can Be Stolen

SMS and MMS traffic information and content

- Sender and receiver phone numbers and phone book names
- The content of the SMS or MMS message

E-Mail traffic information and content

- Sender and receiver addresses
- E-mail text and attachments

SIM card information

- Sends the SIM IMSI and phone number as soon as new SIM is inserted

F-SECURE ®

BE SURE.

Information That Can Be Stolen

Call information

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

Voice recording

- Application can record all phone calls to memory card
- The attacker either needs to access the card to get the recordings or they are sent over Bluetooth, MMS, or HTTP

Call interception

- Allows for tapping into voice conversations by setting a covert conference call

F-SECURE ®

BE SURE.

Information That Can Be Stolen

Remote listening

- When a specific number calls, the phone will answer silently
- The phone will not give any indication that a call is open
- Some spyware will even allow automatic conference calls

Physical location

- Some tools are capable of using built-in GPS in modern phones, and to send GPS coordinates
- Those that don't use GPS send GSM cell ID and signal info

User key presses

- All user key presses can be logged and sent over SMS

F-SECURE®

BE SURE.

Typical Spy Tool Operation

Installation

- Spy applications are installed using the normal application install like any other application

- Although most of them fail to mention what the application is

Hiding

- When the spy application has activated it will hide itself

- The application will not be visible in application task list

- It will not be visible in user interface or application manager

- All log information of sent SMS messages or data connections will be erased as soon as the spy messages have been sent

F-SECURE ®

BE SURE.

Typical Spy Tool Operation

Information gathering

- Spy tool hooks all messaging APIs in which it is interested

- Or it simply reads the content from application data files

Leaking user personal data back to attacker

- Spy tool sends the information either in SMS messages or connects to a remote server and sends data over TCP/IP

- Some tools send data instantly after user event and others use timed delay or a certain number of messages in order to minimize number of transmissions

F-SECURE ®

BE SURE.

Methods of Selling Spy Tools

Web shops

- Licences and software sold on typical E-store
- Software is either IMEI locked or uses server to store info
- Payment over credit card, Paypal, E-gold, etc

Spy shops

- Most spying equipment shops also sell software or phone modification services

OEM spy tools

- Some spy tool manufacturers sell easy to use spy tool generators for spy shops

F-SECURE ®

BE SURE.

Devices affected by spyware

Software

- Symbian OS 6.x-8x
  - 6670, 6630, N70,6680,9210,etc
- Symbian S60 3rd edition
  - E60,E61,E50,E70,E90,etc

Windows mobile
  - 2003, 2003 SE, 5.0 and 6.0

LG
  - LG JOY

- Sony Ericsson
  - P800, P900, M600, W950

Hardware

- Flash OS "upgade"
  - Nokia 1100, 3120,3310

- Modifications on actual harware
  - Remote listening is available for most phone models

F-SECURE®

BE SURE.

Neo-Call

Neo-Call spy software for Symbian phones sends information directly to another phone

- When the spy orders the software from Neo-Call he specifies the phone number to forward the information to
- The software is IMEI locked so spy must know his target

Neo-call offers a wide range of features

- SMS spying
- Call list spying
- Location spying
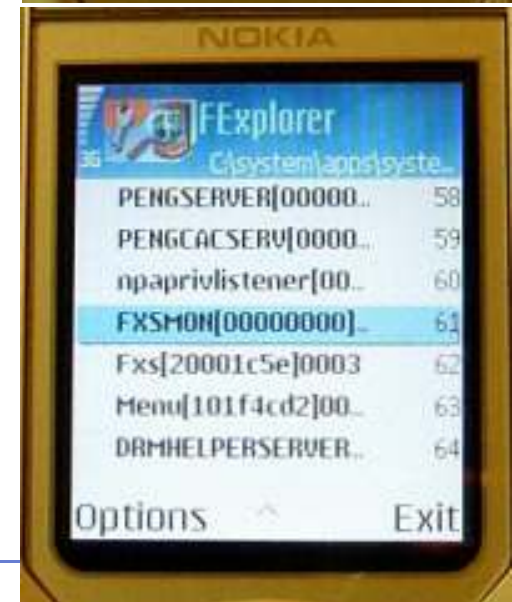- Remote listening
- Key logging

F-SECURE®

BE SURE.

FlexiSpy

FlexiSpy.A was invasive enough to be classified as a trojan
Later variants are classified as riskware

FlexiSpy monitors

•Voice call destinations

•Voice call times dates and duration

•SMS messaging and contents

Software itself is not illegal

•Unauthorized installation of it is

F-SECURE®

BE SURE.

FlexiSpy web interface

All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help

ALL EVENTS 1 - 10 of 413records   Row Per Page 10

	▲ Type ▼	▲ Direction ▼	▲ Duration ▼	▲ Contact Name ▼	▲ Mobile Time ▼	▲ Server Time ▼
☐	SMS			15400	30/01/08 09:54:07	29/01/08 08:55:01
☐	SMS			15400	30/01/08 09:54:03	29/01/08 08:55:00
☐	SMS			+358407175873	08/01/08 15:22:52	07/01/08 14:23:49
☐	VOICE		0:00:07	0407175873	08/01/08 15:22:09	07/01/08 14:23:16
☐	VOICE		0:00:13	0407175873	08/01/08 14:52:38	07/01/08 13:53:50
☐	VOICE		0:00:00	0405081712	08/01/08 14:51:59	07/01/08 13:53:22
☐	E-MAIL			"Fred Savage" <fred....	07/01/08 13:25:57	07/01/08 14:26:57
☐	SMS			+358400648180	04.01.08 10:42:09	03/01/08 09:43:05
☐	VOICE		0:00:06	0400648180	04.01.08 10:41:08	03/01/08 09:42:13
☐	VOICE		0:00:14	0405862908	04.01.08 09:15:36	03/01/08 08:16:49

✗ Delete   🔄 Refresh   🪄 Report Setting   First | Previous | 1 | 2 | 3 | 4 | 5 | Next | Last

F-SECURE®

BE SURE.

SMS Messages

All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help

Log Detail

IMEI:	353659013790262
Client Time:	**16/01/08 13:25:05**
Server Time:	16/01/08 12:25:20
Event Type:	SMS
Direction:	OUT
Phone Number:	+358407175873
Contact Name:	Boss
Contents:	Hello.?Was the meeting about merger with Acmeco tomorrow or friday.?

back

F-SECURE®

BE SURE.

Voice Call Information

GPS Location Information

Länsiväylä 51

Länsiväylä 51

Länsiväy

Länsivä

60.163258, 24.912461

+60° 9' 47.73", +24° 54' 44.86"

Get directions: To here - From here
Search nearby - Save to My Maps

Salmisaarenkatu

Suhasenkuja

Salmisaarenkatu

Porkkalankatu

Salmisaarenranta

Tallberginkatu

Salmisaari

Porkalagatan

Kauppakeskus
Ruoholahti

Ruoholahti

Sundholmsstranden

Porkalagatan

Länsisatamankatu

Itämerenkatu

Östersjögatan

Itämerenkatu

Harmajankatu

Itämerenkuja

Bottenhavsgatan

Lauttasaaren Silta

Kasuunikuja

Loistokuja

Lauttasaaren Silta

en Silta

Tallberginkatu

Länsisatamankatu

Kellosaarenkatu

Tammasaarenkatu

Kellosaarenranta

FlexiSpy on Symbian S60 3rd Edition

The latest versions also work on S60 3rd edition phones

- Nokia E60, E61, E65, E70, E95, N73, N95 and all other new models
- The software is **Symbian Signed**, so it passes all security checks

So how did spy tool pass Symbian Signed?

- By using social engineering
- Software was submitted as a fictional application **"RBackupPRO"**
- "RBackupPRO" was described as a remote backup software that copies user data to a remote server. And thus needs access to user data and network.
- So when the application was approved, everything was working as documented!

F-SECURE®

BE SURE.

The Other Side of the Coin

When Flexispy is installed spying features are disabled

- The attacker must enter a secret code to access the hidden user interface

- From this interface the software is activated and spying features are enabled

- Thus a remote backup tool is suddenly a very capable spy tool

Symbian has no resources for exhaustive checks

- Thus any other application with hidden functionality can pass the checks with high probability of success

F-SECURE ®

BE SURE.

Magic Spy suite is a spy tool generator for spy shops

- Anyone can buy the generator and set up their own spy shop

- We have seen similar tools for PCs

- But this is first for mobile devices

- It's a good bet that many of the spy shops that can be found with Google actually use this tool

- Current license price 12,500 $US

Detecting Spy Tools

Spy tools are problematic to detect

- Spy tool vendors have an interest in staying below the radar of security companies

- Which means that AV companies do not have full sample set, and therefore we do not have near full detection coverage like we have with other threats

F-Secure Anti-Virus detects everything we have seen

- But let's have a look at tools and methods to handle cases that we have not yet seen

F-SECURE ®

BE SURE.

Is This Phone Being Spied On?

Like any other investigation, collect what you know

What made the user suspicious of spying?

- Were there extra charges on the phone bill, or new activity?

- Did someone else appear to know something that was he or she should not known?

Does the phone behave strangely?

- Did the phone open data connections out of the blue?

- If the phone is rebooted, are there any dialogs or screens that flash and suddenly disappear?

F-SECURE®

BE SURE.

Analyzing the Suspected Phone

- Traffic analysis

- Process analysis

- File system analysis

Detecting Spy Tools Using Traffic Costs

A spy tool must be able to send user data out

- Practically, this means over an SMS, MMS, or Data channel

- And even if the tool is able to completely hide on the device without any indication it is there…

- No tool can escape the operator's billing system

- Of course, the user probably has an SMS/Data plan that will hide almost any traffic, if he ever even sees the phone bill

- So what you need is an investigation SIM card

- One that is not used for anything else, is as expensive as it can be and from operator that has real-time bill monitoring

F-SECURE ®

BE SURE.

Using Basic SIM Card To Catch A Spy

Insert your investigation SIM card into the phone

- Send 20 or more SMS messages to the phone

- Make 10 phone calls to the phone

- This of course might tip off the spy, so use your imagination

- All of this should be free for the receiver

- So if there are charges in the phone bill, something bad is going on

- The same can be done with e-mail but then there will be some transfer costs for retrieving the mail to the phone

F-SECURE®

BE SURE.

Trying SIM Trick With E90

Remaining free data before spy activity

Liittymän saldo

Liittymä:

Laskutuskausi: 13.1.2008 - 22.2.2008

Liittymäsi laskun summa ajalta 13.1.2008-20.1.2008 on noin: 10,19 €.

Kotimaan puhelut	0,00 €
Ulkomaan puhelut	0,00 €
Tekstiviestit	0,40 €
Kuukausimaksuun sisältyvää tiedonsiirtoa jäljellä	8,77 Mt

After spy activity

Liittymän saldo

Liittymä:

Laskutuskausi: 13.1.2008 - 22.2.2008

Liittymäsi laskun summa ajalta 13.1.2008-20.1.2008 on noin: 10,79 €.

Kotimaan puhelut	0,00 €
Ulkomaan puhelut	0,00 €
Tekstiviestit	1,00 €
Kuukausimaksuun sisältyvää tiedonsiirtoa jäljellä	8,75 Mt

BE SURE.

Detecting Spy Tools By TCP/IP Monitoring

Some spy tools leak data over TCP/IP

- So simply watching the GPRS data icon after an SMS gives a clue

- But TCP/IP can also be sniffed, so you can actually see what is happening

- A word of warning, make sure that sniffing your own data is still legal in the country that you are operating within

Tools needed

- WLAN access point

- PC with two network ports, or good old 10BaseT hub

- Wireshark or other sniffer

F-SECURE ®

BE SURE.

Setting Up Phone For Wireshark

Windows Mobile

- Connect to WLAN access point

- All data should now be automatically routed over WLAN

Symbian

- Modify all existing access points so that they use WLAN instead of packet data

- Reboot the phone and web browse a bit to open connection

- FlexiSpy insists on using GPRS, and creates own access point "ACN GPRS"; probably there are other tools that behave the same, but extra access point is a dead giveaway

F-SECURE ®

BE SURE.

Monitoring Traffic Caused By Mobile Spy

```
427 556.694331  192.168.6.100    216.239.138.236    HTTP   POST /webapi/sms.php HTTP/1.1
430 556.988250  192.168.6.100    216.239.138.236    TCP    hpvmmdata > http [ACK] Seq=1221
431 557.143565  192.168.6.100    216.239.138.236    HTTP   GET /webapi/calllog.php?sID=530
435 557.561013  192.168.6.100    216.239.138.236    TCP    hpvmmdata > http [ACK] Seq=1329
441 569.228295  192.168.6.100    216.239.138.236    TCP    ardus-cnt1 > http [RST] Seq=1
443 572.558710  192.168.6.100    216.239.138.236    TCP    hpvmmdata > http [ACK] Seq=1329
```

```
⊞ Frame 427 (1100 bytes on wire, 1100 bytes captured)
⊞ Ethernet II, Src: Cisco-Li_d8:4e:3c (00:18:f8:d8:4e:3c), Dst: Wincomm_00:6f:ee (00:01:da:00:6f:ee)
⊞ Internet Protocol, Src: 192.168.6.100 (192.168.6.100), Dst: 216.239.138.236 (216.239.138.236)
⊞ Transmission Control Protocol, Src Port: hpvmmdata (1126), Dst Port: http (80), Seq: 177, Ack: 26, Le
⊞ [Reassembled TCP Segments (1222 bytes): #424(176), #427(1046)]
⊟ Hypertext Transfer Protocol
   ⊞ POST /webapi/sms.php HTTP/1.1\r\n
     Content-Type: application/x-www-form-urlencoded\r\n
     Content-Length: 1046
     Connection: Keep-Alive\r\n
     Expect: 100-continue\r\n
     Host: www.mobile-spy.com\r\n
     \r\n
⊟ Line-based text data: application/x-www-form-urlencoded
     sID=530&content=2008-02-16\t14:29:00\t15400\t0\t2/5: KONTAKTIT(osoitemuistio), MAPPI(teksti- ja mms
     2008-02-16\t14:29:00\t15400\t0\t5/5:ASETUKSET (wap- ja mms-asetukset sek\344 gprs-kytkent\344 nross
     2008-02-16\t14:29:00\t15400\t0\t4/5: Ohjeita palvelujen k\344ytt\366\366n saat lis\344\344m\344ll\3
     2008-02-16\t14:29:00\t15400\t0\t1/5: Soneran palvelujen hakusanat numerossa 15400 ovat: LASKU, BILL
     2008-02-16\t14:29:00\t15400\t0\t3/5: NET(www.sonera.fi/omatsivut -salasana),TEKSTI,SPOSTI(ryhm\344t
     2008-02-16\t14:33:00\t15400\t0\tPalvelu on tilap\344isesti pois k\344yt\366st\344. Yrit\344 my\366h
     2008-02-16\t14:29:33\t0\t15400\tlista\r\n
     2008-02-16\t14:33:00\t0\t15400\tmaksupaiva\r\n
```

BE SURE.

Process Analysis

Check every running process on the phone

- Reboot the phone and check suspected the process list against a clean phone's list

- Normally there should be very few third party tools starting right at boot

- Also on a normal phone, most processes start from the ROM image, so anything that uses a "system-ish" process name and starts from C: is interesting

- For every process that you cannot verify to be part of the OS or a clean install, check from where the image was loaded and get the sample file for closer study

F-SECURE®

BE SURE.

File System Analysis

So far we have not seen mobile rootkits

- If you know where to look, you can find any spy tool

Get an identical clean phone and compare with that

- Check what applications start at boot

- Get a full copy of the file system and compare against clean

- Check application install logs; any third party application without install log history is very interesting

- Install a file monitor and compare file access behavior on clean and suspected devices when receiving SMS or incoming call

F-SECURE ®

BE SURE.

Analysis Tools For S60 2nd Edition

File manager and process viewer

- F-Explorer http://www.gosymbian.com/

- Efileman http://www.psiloc.com

File monitor

- EzFileMon http://www.epocsoft.com/ezfilemon.htm

Traffic monitor

- EzSniffer http://www.epocsoft.com/ezsniffer.htm

F-SECURE®

BE SURE.

File Analysis On S60 2nd Edition

Drive letters

- C:\ User data and applications D:\ Temp RAM drive
- E:\ Memory card Z:\ OS ROM

Applications can be executed from anywhere

- So, well behaving ones are at c:\system\apps
- Those that don't behave well, happy hunting

Locating applications that start on boot

- Check C:\System\recogs and E:\system\recogs
- All third party applications must have .MDL file there. Typically there should be only couple well known recognizers; treat anything you don't know with suspicion

F-SECURE®

BE SURE.

Process Analysis On S60 2nd Edition

Processes can do whatever they wish on S60 2nd ed

- Hide from normal process list

- Assume system process name

- Fake their UID

Locating suspicious processes is a lot of work

- Fortunately most spy tools don't try to hide their processes

- And even those that do cannot fake the information from where executable was loaded

Analysis Tools On Symbian S60 3rd Edition

File managers

- F-Explorer Beta http://www.gosymbian.com
- You need to get devcert on the phone in order to use it
- Y-Browser http://www.drjukka.com/YBrowser.html
- Does not show everything, but doesn't require dev cert

Process viewers

- Y-Tasks http://www.drjukka.com/YTasks.html
- Good collection of tools for getting information on running processes

F-SECURE ®

BE SURE.

Symbian Security Model On S60 3rd

The Symbian security model makes our life difficult

- Normal applications cannot see executable install dir

- So a file manager that runs with normal rights is of no use

- What you need is developer cert that has "all files" capability

- Dev certs have to be requested individually for each phone

    - www.symbiansigned.com

- The good news is that applications are also limited on where they are located and how they can hide in the system

F-SECURE ®

BE SURE.

26.2.2008   38

Symbian Security Restrictions On Applications

Applications must be installed from SIS files

- Any application with significant access must be signed

- Thus for every interesting application you know who made it and what capabilities it has

Applications must be installed to proper path

- Executables must be in C:\sys\bin\

- Private data c:\private\APPUID\

- Resource data c:\resource\apps

- So applications cannot hide in location X

F-SECURE ®

BE SURE.

File Analysis On S60 3ʳᵈ Edition

Check auto start programs

- Get all files from c:\PRIVATE\101f875a\startup\

Check all executables

- C:\sys\bin if it executes, it has to be here

- For interesting applications

  - Check Application UID, litte endian DWord at 0x08-0xC

  - Check applications private data, f.ex C:\PRIVATE\2000B2C2

  - Check C:\system\apps\, f.ex C:\system\apps\2000B2C2

F-SECURE ®

BE SURE.

Process Analysis On S60 3rd Edition

Use Y-tasks to browse through process info

- Check all apps that are hidden or launched in background

- Check all running tasks, check whether they are hidden and what capabilities they have

    - Anything that has NetworkServices, PowerMgmt, location or other not so common capability is interesting

If still nothing, check all processes

- Focus especially on those that start from C:\ are third party and have interesting capabilities

F-SECURE ®

BE SURE.

Analysis Tools on Windows Mobile

File managers

- Resco Explorer http://www.resco.net/

Registry editors

- Resco registry editor http://www.resco.net/

Process monitors

- acbTaskMan http://www.acbpocketsoft.com

F-SECURE ®

BE SURE.

File Analysis on Windows Mobile

Check application install data

- HKEY_LOCAL_MACHINE\security\AppInstall

Check auto start information

- C:\windows\startup

- HKEY_LOCAL_MACHINE\init

- HKEY_LOCAL_MACHINE\services

Use process monitor and check all running files

- Unlike Symbian even plain vanilla WM has lot of third party tools, but those are well known and easily googled

F-SECURE ®

BE SURE.

Ok, So You Found Something Interesting

The next step is to analyze and identify the file

- Double check that the file you found is indeed the culprit

- Kill the suspicious process, and see if the spying continues

- The spy tool most likely uses some kind of resource file to contain user ID for server, or SMS number where to leak info

- In case it is a known spy tool, someone else might have already analyzed it. Google using file names or other info

And of course your friendly AV company appreciates any samples of interesting cases you find

- http://www.f-secure.com/samples/

F-SECURE ®

BE SURE.

Preventing Spy Tools on Phones

Use Anti-Virus

- Good AV detects the most commonly used spy tools

All phones must have up to date OS

- Some installation methods rely on OS bugs

Every phone must have lock code

- While phone is locked no new applications can be installed

Have users personalize their phones

- Prevents quick swapping of the phone

Configure the phone to allow only signed applications

F-SECURE®

BE SURE.

Preventing Spy Tools on Phones

Have the phone OS of key personal flashed at regular intervals

- OS reinstallation removes possible firmware modifications

Leave phones out of critical meetings or remove batteries

But when in unfamiliar territory, it is a very good idea not to leave your phone out of sight either

- If you know that you are going to a place where your phone has to be left at reception, take a tamper evident envelope or other container with you

F-SECURE ®

BE SURE.

What might be coming in the future?

The large number of spy tool vendors indicates that there is money in creating mobile software that exists within a grey area

- Most likely we will soon see mass distributed mobile spy software
- Also phishing, data stealing trojans, backdoors, and other criminals tools that are used in Windows will migrate to phones

Experience has shown that where there is money there will be crime

- We fear that we are going to see the same development as on PCs
- On PCs first we had hobbyists and people with too much curiosity
- Now more than 95% of malware is created for commercial gain
- The same development will follow in the mobile field

F-SECURE®

BE SURE.

http://www.f-secure.com/weblog

F-Secure : News from the Lab - March of 2005 - Microsoft Internet Explorer provided by F-Secure Corporation

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites

Address   D:\weblog\archive-032005.html   Links »

Thursday, March 3, 2005

Cabir now in Hongkong and Japan   Posted by Jarno @ 12:30 GMT

It seems that as long as people are not using Anti-Virus and are curious, the Cabir phone worm just keeps spreading.

Now we have received confirmed report from our Japan office of Cabir in Hongkong and Japan; a Japanese visitor in Hong Kong picked up the infection to his phone in late February and returned to Tokyo with the infected handset. He noticed that something is wrong because his battery life had reduced to 30 minutes per recharge. However, it is likely that the infection has spread to at least some handsets before this.

If your phone receives any SIS file from someone that you were not expecting, please do not install it. Instead, send the file to vsamples@f-secure.com. We are rather interested about just what variants are on the move.
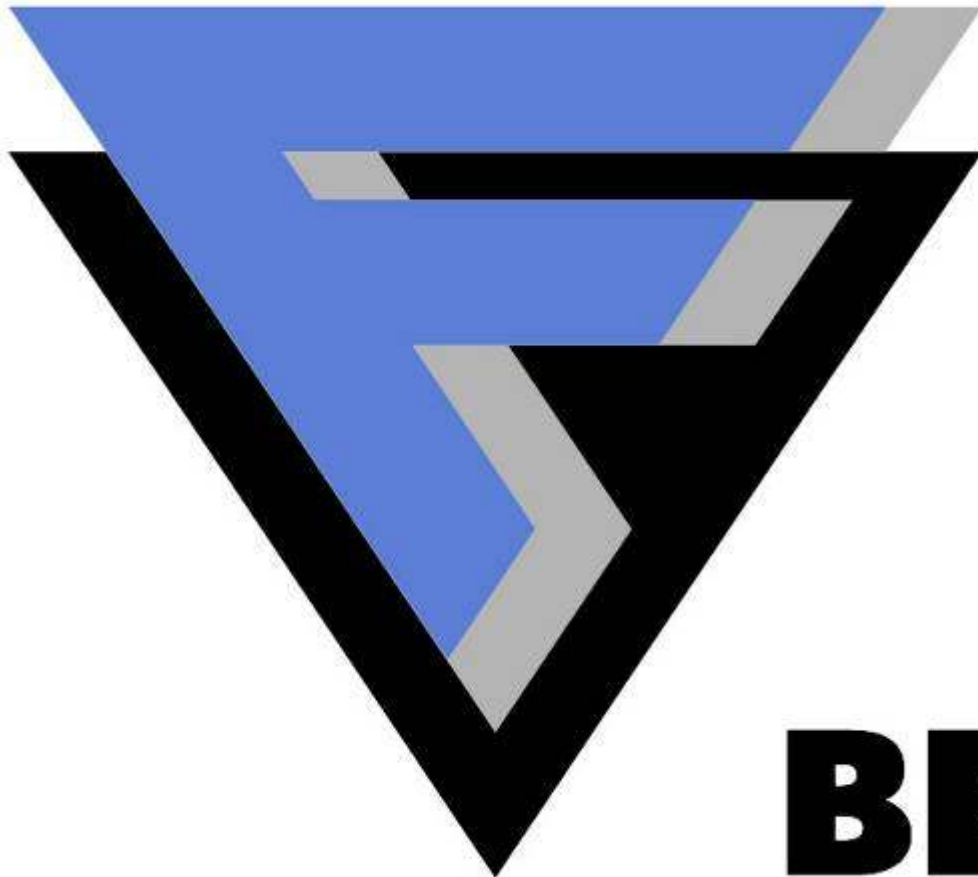
And for those who are curious, please use F-Secure Mobile Anti-Virus which detects Cabir and all other known Symbian Viruses, worms and trojans.

So now we have 16 countries with Cabir sightings:

1. Philippines
2. Singapore

F-SECURE®

BE SURE.

F-Secure Mobile Anti-Virus (+ Firewall)
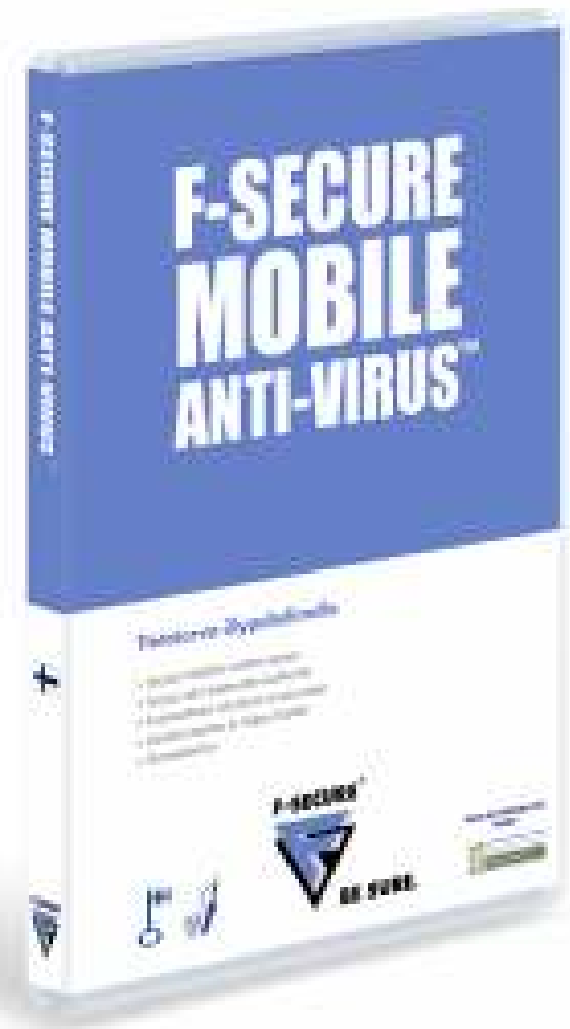
F-Secure Mobile Anti-Virus

Runs on lots of platforms

F-Secure Mobile Anti-Virus™

- S60 2nd and 3rd edition (Symbian 7.x, 8.x and 9.x)

- Windows Mobile 2003 for Pocket PC 2003 SE/Phone edition

- Windows Mobile 2003 for Smartphone 2003 SE

- Windows Mobile 5.0 for Pocket PC

- Windows Mobile 5.0 for Smartphone

F-Secure Mobile Security™

- Series 80 (Nokia Communicators 9300, 9300i, 9500)

- S60 3rd edition (Symbian 9.x)

F-SECURE ®

BE SURE.

Awards

PC Magazin sehr gut — www.pc-magazin.de 12/2006 **Saksa**	**PC Today** Recomendado **Espanja**	REKOMMENDERAS AV **PC FÖR ALLA** **Ruotsi**	**Windows** CHOIX DE LA RÉDACTION December 2006 **Ranska**
PC PRO RECOMMENDED **Iso-Britannia**	**PCgo** 1/07 sehr gut **Saksa**	Empfehlung CD INFO CD Austria **Itävalta**	**Webwereld** 10 JAAR **Alankomaat**	**PC MAGAZINE** EDITOR RATING GOOD **Yhdysvallat**	BEST I TEST **PC WORLD** NORGE **Norja**
Computer **act!ve** Simple Clear Advice ★★★★☆ **Iso-Britannia**	**MIKROBITTI** ★★★★★ Toimituksen valinta 2/2007 **Suomi**	**PCM** **Hong Kong**	NAJLEPSZA **PC Format** 4/2007 JAKOŚĆ/CENA **Puola**	**PC Japan** **Japani**	BEST BUY ★ COMPUTER SHOPPER **Iso-Britannia**
CHIP COMPUTER & COMMUNICATIONS QUALITA COMPLESSIVA **Italia**	**HARDWARE UPGRADE** **Excellent** **Italia**	**PC MAGAZINE EDITORS' CHOICE** **Serbia**	**Säkerhet&sekretess** BETYG: ●●●●○ **Ruotsi**	**c|net** Editors' rating: Good 7.8 out of 10 **Yhdysvallat**	TOP **50 Buyer BEST BUY** **Iso-Britannia**