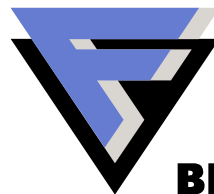


# **Symbian Malware What It Is And How To Handle it**

**Jarno Niemelä**

**F-Secure Corporation**

**F-SECURE®**



**BE SURE.**

# Introduction

Jarno Niemelä

- Senior Anti-Virus Researcher
- Has been working at F-Secure Corporation from 2000
- Specialized in Mobile and PDA malware



# F-Secure Corp



**BE SURE.**



© 2005 Mikael Albrecht

# Symbian Malware

Malware that is native on Symbian platform

- Symbian malware is still quite primitive, but has some properties and vectors that are not really used much on other platforms
- Unlike in most other platforms, majority of Symbian malware is not executable code
- Most of the currently known cases misuse features of Symbian OS without needing any executable code at all



# Symbian Basics

- Basics of Symbian OS
- Symbian file System
- Symbian executables
- Symbian user Services
- Application installation and uninstallation



# Basics Of Symbian OS

Calling Symbian devices as Smartphones is misleading

- These devices are general purpose computing devices that also function as phones
- One should think Symbian device as small computer

Symbian OS provides

- File system
- Multitasking operating system
- Very complete system libraries and relational database
- In other words all the same features as desktop OS





# Symbian File System

Symbian file system is based on drive letters, directories and files

- C: FLASH RAM User data and user installed applications
- D: TEMP RAM Temporary file storage for applications
- E: MMC card Removable disk for pictures and applications
- Z: OS ROM Flash drive that contains most of the OS files





# Symbian Directory Architecture

All drives have System directory

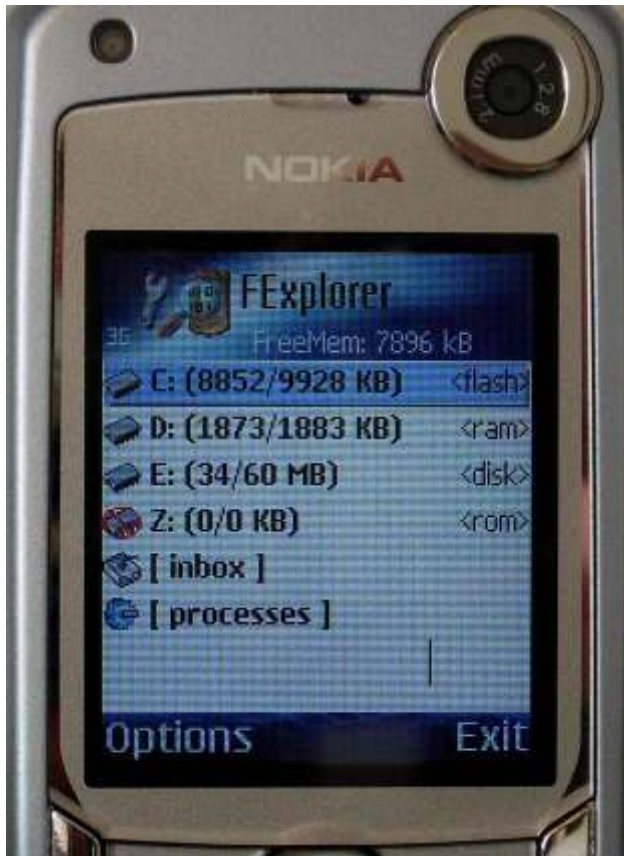
- The directory is created automatically on a new media when one is inserted
- The System directory contains directory tree that contains OS and application files. Very much the same as C:\windows

Most important directories

- **System\Apps** Applications that are visible to user
- **System\Recogs** Recognizer components
- **System\Install** Data needed for uninstallation of user installed applications
- **System\libs** System and third party libraries



# Symbian C: Drive



**BE SURE.**

# C:\System\install Directory



# Symbian Executables

Symbian executables use unique identifiers

- Each application has unique 32-bit UID
- Thus any executable files with same UID are assumed to be copies of same application

Symbian native executables come in three flavors

- Foo.APP GUI applications
  - End user applications, accessible from applications menu
  - Each application must have own directory under System\apps in some drive in order to be visible for user in application launch menu



# Symbian Executables

- Foo.EXE Command line applications and servers
  - Cannot be accessed by normal user, but can be executed with third party file manager or other software
  - EXE files are either services or utilities used by GUI applications
- Foo.MDL Recognizer components
  - Provide file association services for rest of the OS
  - Also the most common method for starting applications at boot
  - Start automatically at boot or from inserted memory card
  - Must be located on System\recogs directory



## Implementation Of User Services

All phone features are implemented using .APP GUI applications. Anything that is visible in phone menu or started through buttons, is actually application under z:\System\apps\

- Z:\System\Apps\Menu\Menu.app
  - Phone main menu and application launching service
- Z:\System\Apps\AppInst\Appinst.app
  - Application installation
- Z:\System\Apps\AppMngr\AppMngr.app
  - Application uninstallation



# Implementation Of User Services

- Z:\System\Apps\MMM\Mmm.app
  - Messaging application for sending and receiving SMS,MMS,BT
- Z:\System\apps\phonebook\Phonebook.app
  - Phonebook
- Z:\System\apps\btui\btui.app
  - Bluetooth control panel

If any of the user service applications is disabled, user cannot use that feature anymore





# Symbian Z: Drive



**F-SECURE®**



**BE SURE.**

# SIS Files And Installing Symbian Applications

SIS files are the only currently known method for normal user to import executable code to a device

- Any malware that wants to run on the device has to get installed as a SIS file. Thus all known malware uses SIS files

A SIS file is an archive file with header parameters used by the system installer

- When a user opens a SIS file the installer is automatically started and starts installing the file



# User Installing Symbian Application

Stage 1: A SIS file arrives to the device

- Bluetooth, IRDA, MMS, USB cable, MMC

Stage 2: The SIS file gets executed

- Either automatically (bluetooth) or user clicks file

Stage 3: Symbian SIS installer parses file and installs

- Copies files to locations specified in SIS
- Installs any embedded SIS files
- Starts installed application automatically (optional)
- Writes uninstall data



## What A SIS File Can Do

When contents of a SIS file are installed the SIS file can affect following properties that interest malware

- Exact name and path where a file is installed
- Automatic execution of a file that is installed
- Displaying text to user during installation
- Embedding additional SIS files that are automatically installed after the main file is installed



# Uninstalling Installed Applications

When a SIS file is installed, the system creates uninstall data

- The data is stored with identical name to original SIS into System\install of the drive where application is installed

The uninstall data is used by the Application Manager

- When application manager is started it enumerates System\install of each drive and uses the data provided for uninstall



# Avoiding Uninstallation

Malware can prevent it's uninstallation by

- Breaking the Application Manager software
- Copying it's files to another location and using from there
- Crashing the Application Manager by dropping corrupted uninstall SIS to system\install



# Symbian Malware

Worms: Cabir, Commwarrior, Mabir and Lasco

- Spread over bluetooth and MMS

Viruses: Lasco, Commwarrior.C

- Spread by infecting other SIS installation files or MMC cards that are inserted into the phone

Trojans: Skulls, Locknut, Fontal, PBstealer, etc.

- Don't spread, most common way to get infected is to download pirate copied software
- Symbian has two flavors of trojans, typical binary trojans and SIS file trojans that abuse features of Symbian OS





# Cabir Bluetooth Worm

Cabir is a worm that tries to spread over bluetooth

- Cabir spreads by creating a SIS file of itself and sending that to any phones it finds over bluetooth connections
- When Cabir finds another phone, it tries to send itself as bluetooth file transfer
- User of the target phone has to accept the file transfer before Cabir can arrive to receiving phone
- When the Cabir has arrived the file is shown in inbox, and will not install automatically.
- User has to answer yes several times for the Cabir to install and start



# Cabir Infection



# Cabir Bluetooth Replication

Cabir spreads by using standard Bluetooth functionalities

- No exploits or anything else suspicious is used
- Cabir opens the bluetooth connection and searches devices with same BT properties as the infected phone
- When suitable target is found, Cabir opens bluetooth connection and initiates file transfer

Most Cabir variants lock to single target

- User receives unlimited number of file transfer request
- If user answers no, he will get asked immediately again, if he answers yes, he will get a moment of peace
- Some later variants (H,I,J,K,L, AA and AB) switch target after bombarding one target for a while.



# Cabir Installation

Cabir installation starts automatically when BT message is read

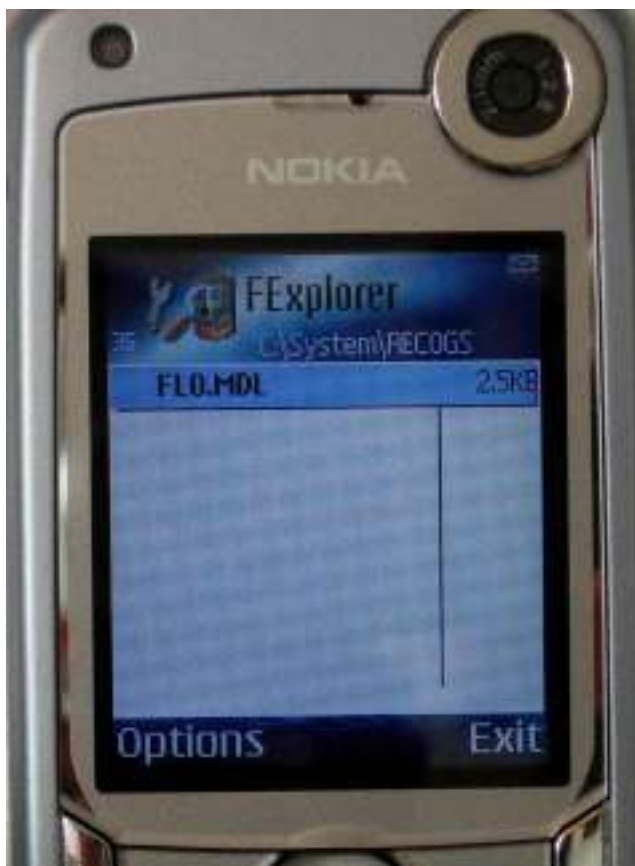
- User doesn't realize that he is installing something
- User must answer yes to several questions, but most people don't even realize that they are installing something
- And many who do, install Cabir anyway
  - Either because they trust the sender, or are plain curious

The installation copies the Cabir files and start the worm

- First Cabir copies it's recognizer component to System\Recogs so that it would start automatically on boot
- The Cabir copies it's own files away from the location where system installer copied them.
- Thus it can avoid removal by system uninstaller.



## Files Copied By Cabir



# Commwarrior MMS And Bluetooth Worm

Installs and spreads over Bluetooth like Cabir

- Attempts file transfer to several targets at the same time

Spreads as attachment in MMS multimedia messages

- Commwarrior.A and B, use local address book for numbers
- Commwarrior.C also listens for incoming and outgoing traffic

MMS replication works much in the same manner as E-Mail

- Receiver sees social engineering text and attached file
- Text is either from users own messages, or from predefined list
  - 3DGame from me, Nokia RingtoneManager for all models
- Because message comes from known sender, people are trusting



# Commwarrior Bluetooth Replication





# Commwarrior MMS Message



Image Copyright © F-Secure Corporation



Image Copyright © F-Secure Corporation



Image Copyright © F-Secure Corporation



## Viral Behavior In Symbian OS

In addition of being worms, some Symbian malware also use viral spreading methods

Lasco.A infects SIS installation files

- When executed Lasco.A searches for any SIS installation files on the device or card and embeds itself to all files found

Commwarrior.C infects MMC cards

- When a clean MMC card is inserted, Commwarrior.C copies its executable and MDL recognizer to the card
- Thus if the card is inserted to another phone, it will get infected without any question or warning
- The behavior is rather similar to old DOS boot sector viruses



# Binary Trojans

Symbian binary trojans are malicious application files that cause some damage to the system

- SymbOS/Mquito sends SMS messages without permission
- SymbOS/Cardblock sets random password to the MMC card so that the card contents are inaccessible
- SymbOS/PBStealer reads user phonebook, calendar, etc and sends the contents to first device it finds over bluetooth



# SIS File Trojans

SIS file trojans are based on installing file that breaks something in the System

- Either location where the file is installed causes problems
- Or the file itself is corrupted so that it causes problems

The key point is that SIS file trojans don't need to have any executable code to cause problems

- Some trojans do have executables, but usually they cause some of the side effects of the malware, not the main damage



# Skulls Trojans

Skulls trojans are based on installing file into location that causes problems

- In Symbian file in C: overrides with same path on E: or Z:
- For example a nonfunctional C:\System\Apps\Menu\Menu.App overrides Z: menu.app in Z: and the phone UI doesn't work anymore at next boot
- Skulls variants and other similar trojans, contain a large number of applications that override system applications, trying to render the phone non-functional
- Most Skulls variants also drop Cabir or other worms on the device



## Demo Skulls.A



**BE SURE.**

# Skulls.D





## Locknut/Doomboot trojans

Locknut type trojans are based on installing a corrupted file

- Certain files can be corrupted so that Symbian OS crashes when trying to load them

Locknut attacks application startup

- Breaks application startup routine so that new processes cannot be created.

Fontal and Doomboot break phone startup

- Breaks OS startup so that the phone wont start anymore



# Investigating Infected Phones

- Building a toolkit for investigating phones
- Gathering information from infected phone
- Disinfecting infected phones
  - Information provided in separate document, included in the Black Hat CD



# Tools For Investigating S60 phones

## F-Secure Mobile Anti-Virus

- <http://mobile.f-secure.com>

## F-Secure disinfection tools

- F-Commwarrior
- F-Cabir
- F-Skulls
- F-Locknut

Clean Symbian phone, preferably identical to the investigated one



# Tools For Investigating S60 phones

MMC card reader for PC

Symbian built in process list tool

- Press menu button for 5 seconds
- Shows all GUI processes, Cabir is shown, Commwarrior not

Task spy

- Shows all processes <http://www.pushl.com/taskspy/>

File manager programs

- Fexplorer <http://users.skynet.be/domi/>
  - Free, light and easy to use, but cannot make proper copy of full drive
- EFileManager <http://www.psiloc.com/>
  - Commercial, heavier, but makes a good copy of full drive



## Create Investigation MMC card

Install following software to MMC using clean phone

- Task Spy
- FExplorer
- E-File manager
- Anti-Virus Installation files
- F-Commwarrior
- F-Cabir

Make separate cards for F-Skulls and F-Locknut

Remember to rebuild cards for each investigation!



# What To Do If You Get Infected Phone?

**Calm down!**

**The phone has probably been infected already for a while**

- 10 Minutes more to figure what's going on doesn't make it worse
- If possible, spend that 10 minutes away from crowds

Find out where the infection came from

- Bluetooth? MMS? Or download from web?
- Recover the original SIS file if possible

Check Symbian own process listing

- Record names of all unknown processes. free\$8, Caribe, Tee222

Does the phone send bluetooth requests?

- Is the Bluetooth icon active?
- Do people around the phone get file transfer requests



## Gather Information From The Infected Phone

Remove original MMC card from the phone

Check does the phone menu work

- If menu works, check does application manager start

Insert investigation MMC card

- Use E-File Manager to make full copy of the C: drive to card



## Disinfecting Phone Easy Cases

Remove original MMC card from the phone

Check does the phone menu work

- If phone menu doesn't work proceed to page 7

Install F-Secure Mobile Anti-Virus into the phone and scan the phone

- Select all infected files (hold pen key) and delete files with 'C'

Uninstall the SIS file in which the malware was installed

- If you don't know in which, ask user what application he installed

Reboot the phone

Malware specific instructions are available from F-Secure web

- <http://www.f-secure.com/v-descs/>





## Creating F-Skulls Or F-Locknut MMC Card

Get a phone that is known to be clean of viruses

- Insert empty MMC card to the phone
- Installs F-Skulls into the phone
- F-Skulls automatically installs to MMC card and is now usable
- Remove card with F-Skulls from the phone
- Now you have card that can be used for removing Skulls trojan from phones

Repeat same for F-Locknut



## If F-Secure Mobile Anti-Virus Installs Correctly But Disappears Immediately After Install

Phone may be infected with Commwarrior.C which attacks any known antivirus application

- Install F-Commwarrior
- Scan the phone with F-Commwarrior
- If Commwarrior is found, the phone reboots automatically after killing the worm
- Install F-Secure Mobile Anti-Virus and proceed as in page 4



## If Phone Menu Doesn't Work Or Applications Wont Install

Insert the MMC card that has F-Skulls

- If possible do this without removing the battery, on most new phone models card can be inserted without powering off the phone
- F-Skulls tool starts automatically on card insertion or when phone powers up
- F-Skulls deletes the trojan components that block the menu or application install

When the menu works again

- Install F-Secure Mobile Anti-Virus and proceed as in page 4



# If The Phone Complains System Error And Does Not Start Properly

Insert the MMC card that has F-Locknut

- If possible do this without removing the battery, on most new phone models card can be inserted without powering off the phone
- F-Locknut tool starts automatically on card insertion or when phone powers up
- F-Locknut deletes the trojan components that application startup

When the menu works again

- Install F-Secure Mobile Anti-Virus and proceed as in page 4



# What To Do After F-Secure Mobile Anti-Virus Has Been Installed

Put the original MMC card back to the phone

- Scan the phone, if there are any infected files on the card the F-Secure Mobile Anti-Virus will detect and remove them
- If you managed to get the original SIS file from where user installed the malware, check it with PC antivirus.
- If the SIS file is not detected, send it to F-Secure for analysis
- <http://support.f-secure.com/enu/home/virusproblem/sample>
- If you have problems with using Anti-Virus or disinfecting phone, please contact our support at [mobile-support@f-secure.com](mailto:mobile-support@f-secure.com)



# What To Do If Disinfection Instructions Didn't help

If the phone boots, install FExplorer File Manager and get samples to send to F-Secure for analysis

- If you have original SIS file send that
- If not, contents of following directories
  - C:\system\install
  - C:\system\apps
  - C:\system\recogs
  - C:\system\mail (if there is no confidential data)

Pack the files into a ZIP package and send them to US

- <http://support.f-secure.com/enu/home/virusproblem/sample>



# What To Do If The Phone Doesn't Boot at All

The phone has been infected with Doomboot or other trojan that breaks the phone so that it doesn't boot

- The only solution is to reformat the phone or reflash it

Or the phone has some other problem than virus



# Phone Reformat (S60)

## Soft format

- Reinitializes file system, and removes everything that prevent phone from booting
- Enter code\*#7370# and give security code (default 12345)

## Hard Format

- Shut off the phone
- Press buttons “Answer call” + “\*” + “3” and switch on the phone
- Some phones show text “formatting” others just ask for country settings after successful reformat





## Detailed Investigation Of Malware Cases

- Analyzing original SIS file
- Analyzing phone memory card
- Analyzing backup copied from the phone



# Tools For Investigating SIS files

## UnmakeSIS

- Unpacks a SIS file and has nice GUI browser for analyzing contents
- <http://www.atz-soft.com/unmakesis.html>
- Site license available from [atz@atz-soft.com](mailto:atz@atz-soft.com), say hello from me ☺

## UnSIS

- Simple, but unpacks all SIS files, needs Symbian SDK
- <http://www.symbian.com/developer/downloads/tools.html>

## Desktop Anti-Virus

- F-Secure PC Anti-Virus has detection for all known cases

## Strings tool to extract ASCII and Unicode strings

- <http://www.sysinternals.com/Utilities/Strings.html>



## Analyzing Original SIS File

### Scan the SIS file with PC Anti-Virus

- Most Anti-Virus applications detect known cases by CRC
- If PC Anti-Virus doesn't recognize it, please submit it as sample

### Extract strings information with Strings tool

### Investigate SIS file contents with UnmakeSIS

- UnmakeSIS shows you the SIS file contents, and what is installed where
- Be careful if you unpack the SIS file, some Symbian malwares also drop Win32 malware



# Demo Investigating A SIS File With UnmakeSIS



# Things To Search From A SIS File

What files are installed and where

- Pay Special attention to filenames that match with Z: drive

What files are automatically executed at install

- Cabir.AA  
"spooky.app"- "C:\system\apps\spooky\spooky.app",FR,RI



# Investigating Infected MMC And Files Copied From Phone

Do MMC card investigation in a safe computer

- Some trojans contain Windows malware, you don't want to run those by accident!

Use Anti-Virus to check for any known cases

Check recognizer autostart directory system\recogs

- The MDL files there usually contain string reference to application that they are starting
  - Cabir.AA  
SYSTEM\SCREAMSECUREDATA\SPOOKYSECURITYMANAGER\SPOOKY.APP
- All applications that are started automatically are suspect, until you have verified them to be clean



## Investigating Infected MMC And Files Copied From Phone C:

Compare contents against clean phone and card

- Get clean sample from identical phone, and compare files
- Any files that are extra in the infected phone are potentially malware

Check what SIS files have been installed from System\install

- The System\install contains record of what files are installed on the phone
- If you already know what files are infected, check from which SIS they came from



# Demo Investigating Files From Infected Phone





## What To Do With The Files You Found

Depends much on reasons why you started to investigate the phone

But if there is any reason to suspect that you have found new malware, send samples to Anti-Virus company. Preferably to us ☺

Also if you have files that need to be analyzed, for example comparison between malware binary and what is suspected to be source files for them. We are more than glad to help.



# Outbreak Control

- Controlling local outbreak
- Controlling MMS worm outbreak



## Advise For Organizing Cabir Safe Event

If you are organizing large international event, there will be people with infected smart phones

Use honeypots for detecting that there are infected phones

- Simplest way is to have trained people with phone that has Anti-Virus and is visible over bluetooth
- More advanced way is to have dedicated PC honeypot

Have service desk where people with infected phones can get their phones disinfected

- Make a deal with local phone operator or repair shop



# Tools For Controlling Bluetooth Outbreak

Unfortunately the only outbreak control we know, is to have trained people to help people in getting their phones clean

- Advise people to have bluetooth in non-discoverable mode
- Have information which phones can be affected
- Have installation packages for Anti-Virus available and people to instruct in installing them
- Have disinfection tools available for cases that Anti-Virus cannot deal with automatically



## Conclusions

Symbian malware is not nearly as bad threat as Windows malware is

- But for the past year, the situation has been getting worse

The greatest difficulty in handling Symbian malware is the Symbian devices themselves

- It's totally different world compared to windows
- Users don't have experience, and neither do have admins

The best way to combat these problems is to have trained people and tools ready when problem hits



# <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 Forward Stop Reload Home Search Favorites RSS Bluetooth

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](mailto:vsamples@f-secure.com). We are rather interested about just what variants are on the move.

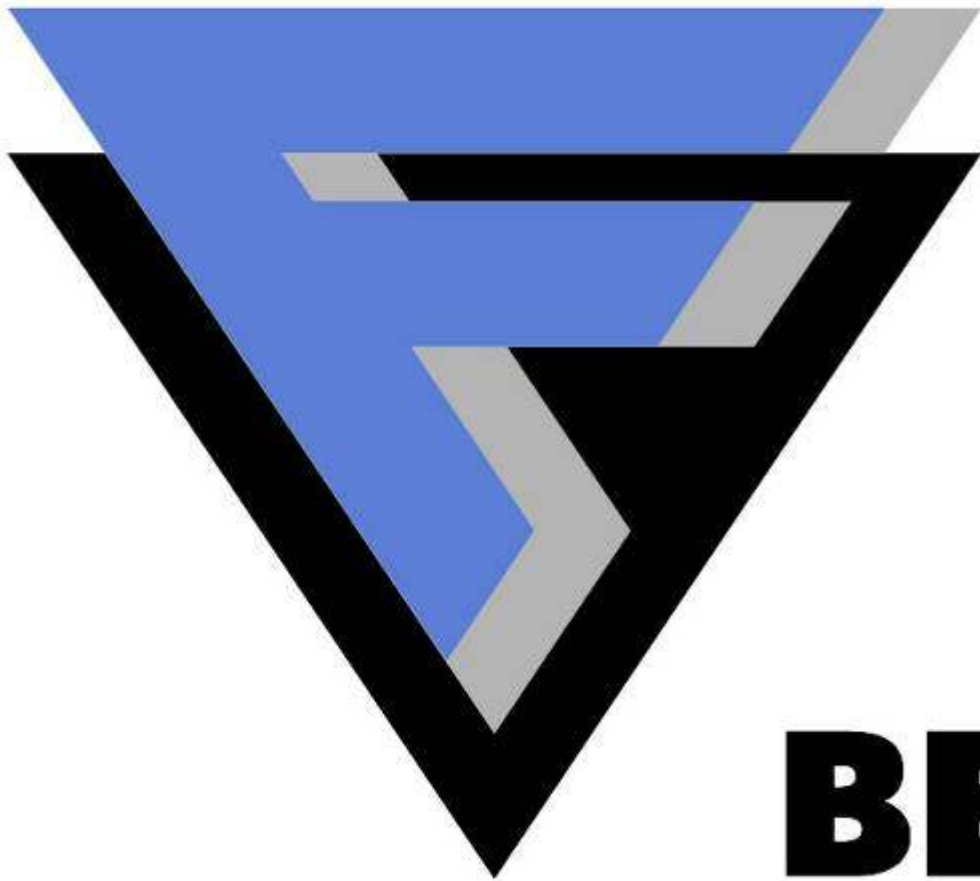
And for those who are curious, please use [F-Secure Mobile Anti-Virus](#) which detects Cabir and all other known Symbian Viruses, worms and trojans.

So now we have 16 countries with Cabir sightings:

1. Philippines
2. Singapore



**F-SECURE<sup>®</sup>**



**BE SURE.**

# F-Secure Awards



Austria  
04/05



Spain  
04/05



Serbia  
04/05



Norway  
04/05



Overall ★★★★★

UK  
04/05



Finland  
04/05



United Kingdom  
03/05



United Kingdom  
02/05



Italy  
12/04



Excellent

Italy  
12/04



United States  
12/04



Sweden  
11/04



Editors' rating:  
Good  
7.8  
out of 10

United States  
11/04



United Kingdom  
10/04