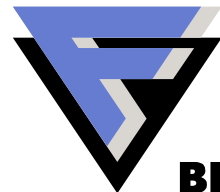


What Makes Symbian Malware Tick

jarno.niemela@f-secure.com

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.



Symbian Malware

Malware that is native on Symbian platform

- 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



Cabir is spreading in the wild

Right Now!

Cabir was found in June 2004

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

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



BE SURE.

Recent Cabir outbreaks

Live 8

10th World Championships in Athletics



F-SECURE



BE SURE.

Cabir Infection



Basics Of Symbian OS

File system that is based on drive letters and directories

- 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

F-SECURE[®]



BE SURE.

Symbian Directory Architecture

All drives have System directory

- The directory is created automatically on a new media when one is inserted

Most important directories

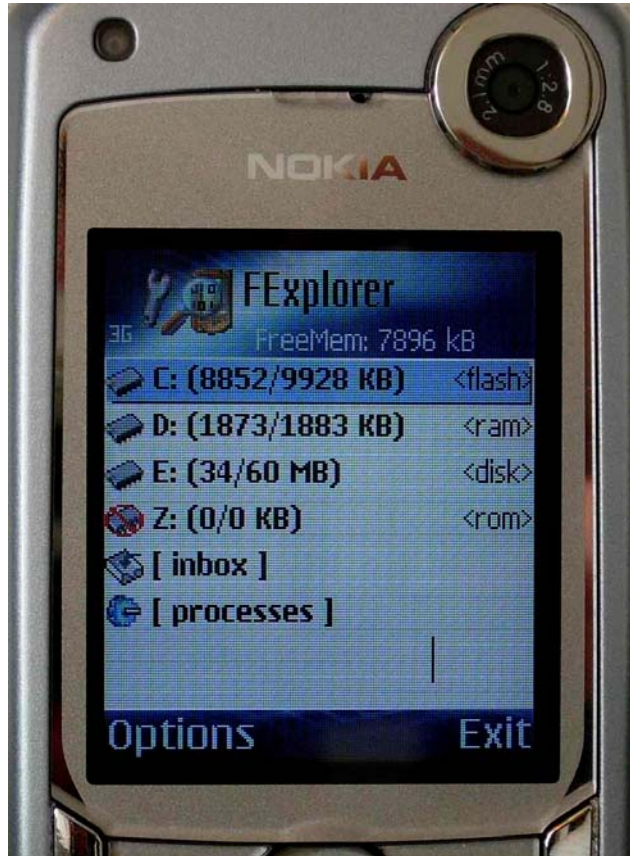
- **System\Apps** Applications that are visible to user
- **System\Recogs** Recognizer components
- **System\Install** Data needed for uninstallation of user installed applications
- **System\libs** System and third party libraries

F-SECURE®



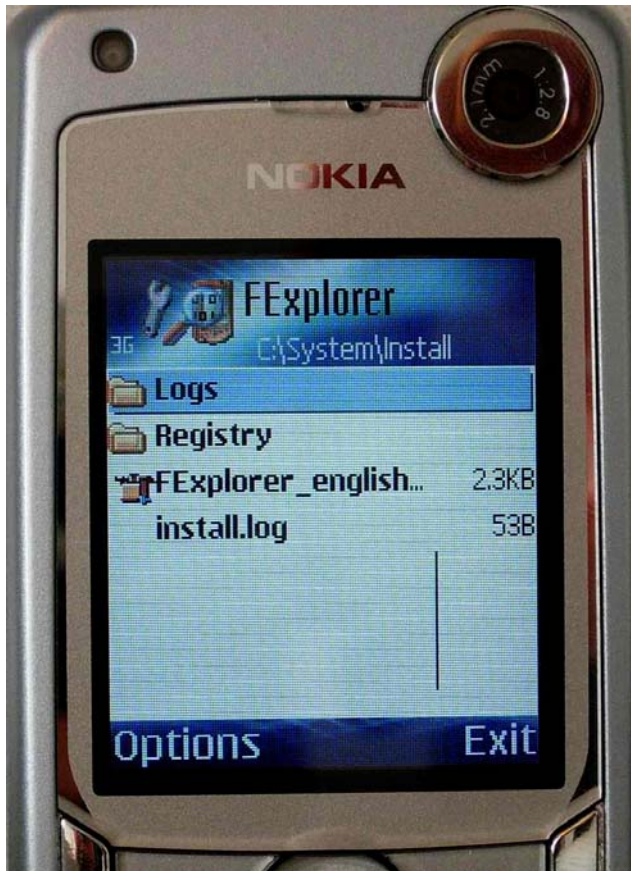
BE SURE.

Symbian C: Drive



BE SURE.

C:\System\install Directory



F-SECURE®



BE SURE.

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

F-SECURE®



BE SURE.

Symbian Executables

- Foo.EXE Command line applications and servers
 - Cannot be accessed by normal user. EXE files are either services or utilities used by GUI applications
- Foo.MDL Recognizer components
 - Provide file association services for rest of the OS
 - 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

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



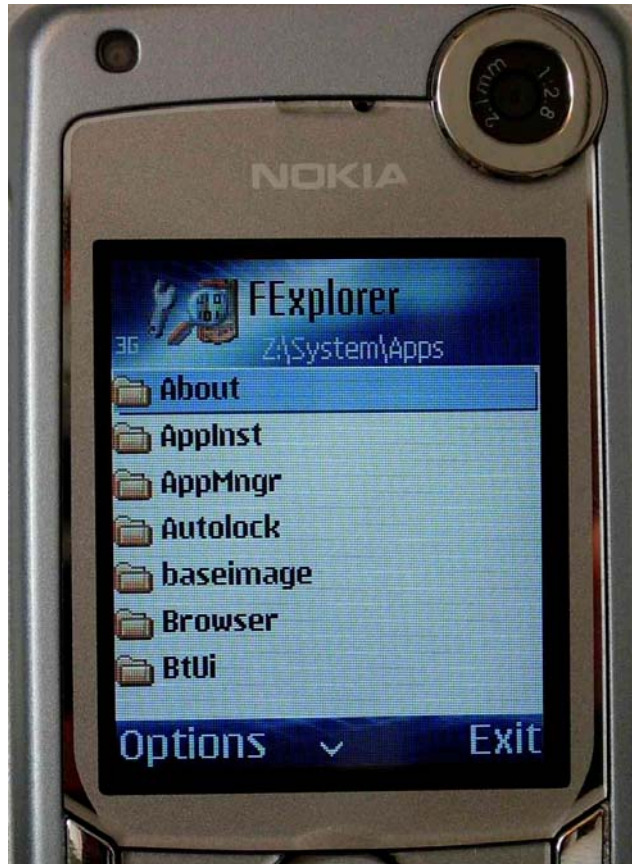
Implementation Of User Services

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

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



Installing A SIS File

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

F-SECURE®



BE SURE.

Removed From Public Version

Some of the slides are removed as the information can be used for creating malware.

If you attended VB 2005, you can request full version from Jarno.



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



BE SURE.

Avoiding Uninstallation

Malware can prevent it's uninstallation by

- Removed



Removed From Public Version

Some of the slides are removed as the information can be used for creating malware.

If you attended VB 2005, you can request full version from Jarno.

F-SECURE®



BE SURE.

ROM Application Overriding

If an application in C: or E: has exactly the same name and path as one in Z: it will get executed instead of original application in ROM

- F.ex c:\system\apps\menu.app replaces z:\system\apps\menu.app
- This feature was intended for patching of binary in ROM without needing to re-flash the device
- Obviously this feature is very open for misuse by malware



Removed From Public Version

Some of the slides are removed as the information can be used for creating malware.

If you attended VB 2005, you can request full version from Jarno.

F-SECURE®



BE SURE.

Symbian Application Loading

In Symbian application icons and launch are not directly linked to any given binary

- When user launches application Symbian will search what binary to execute
- The search is done by enumerating directories in C:,E: and Z: looking for first binary with correct UID
- The first match is then executed
- Thus, if there are several binaries with same UID only one will get executed



File Parsing And Crashing Symbian

Symbian file parsing is quite poor and trusts own files

- It is quite easy to craft files that crash the phone

So far we have seen fatal parsing errors on following file formats

- RSC String resource files
- GDR Font files

F-SECURE®



BE SURE.

Locknut.A Using Corrupted RSC File To Crash The Device

Locknut.A drops drops following files to
C:\System\Apps\Gavno

- Gavno.app, Gavno.rsc, Gavno_caption.rsc
- Gavno_caption.rsc is a corrupted icon caption file
- When Application launcher enumerates applications, it finds Gavno.app and tries to load caption string from Gavno_caption.rsc
- This results into system crash
- Apologies for those who understand Russian



<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 Refresh Home Search Favorites Home Mail Print Word Pad Find Bluetooth People

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.

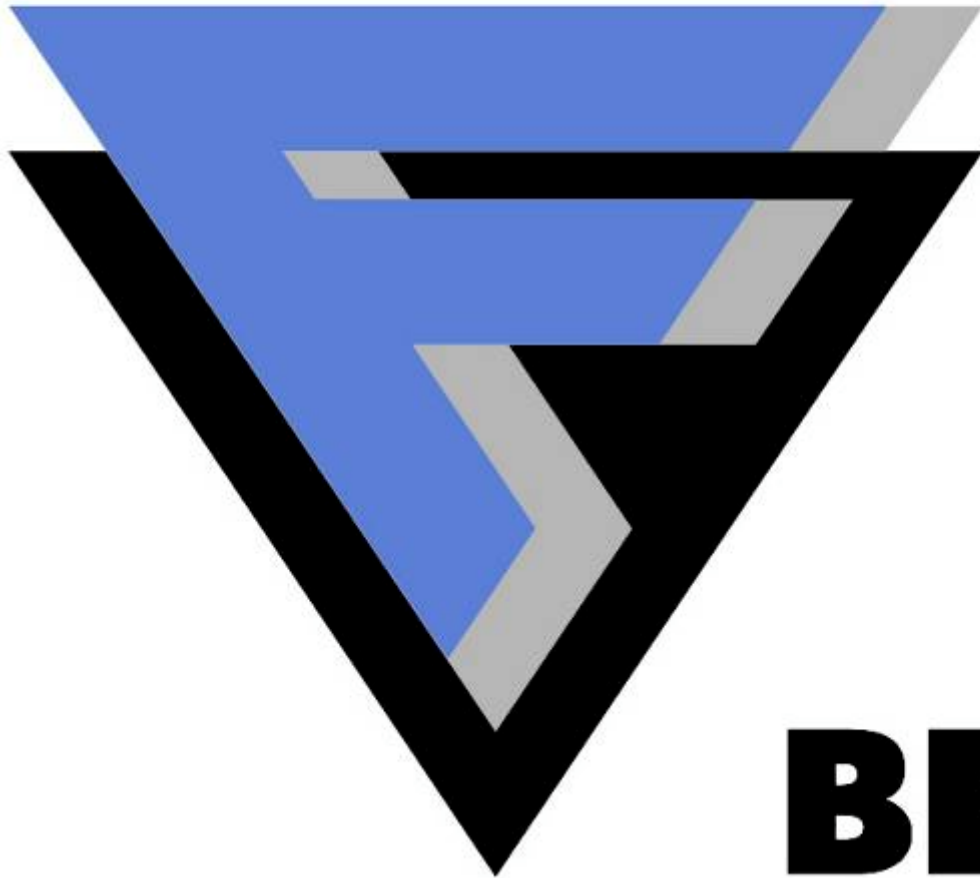
And for those who are curious, please use [F-Secure Mobile Anti-Virus](#) which detects Cabir and all other known Symbian Viruses, worms and trojans.

So now we have 16 countries with Cabir sightings:

1. Philippines
2. Singapore



F-SECURE[®]



BE SURE.

F-Secure 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



United States
11/04



United Kingdom
10/04