Cleaning Up Infected Symbian Phones

Version 1.1

13.12.2005

What To Do If You Get an Infected Phone?

Calm down!

- Don’t reboot the phone before you know what is wrong with it!

Find out where the infection came from

- Bluetooth? MMS? Or download from web?
- If you have the original malware SIS, don’t delete it

Check Symbian own process listing

- Press ‘Menu’ button for 5 seconds to get process list, then select process and press ‘C’ button
- Kill all unknown processes. free$8, Caribe, Tee222

Does the phone send bluetooth requests?

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

Tools You Need

F-Secure Mobile Anti-Virus Installation File

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

F-Skulls Disinfection Tool

- http://www.f-secure.com/tools/f-skulls.sis

F-Locknut Disinfection Tool

- http://www.f-secure.com/tools/f-locknut.sis

F-Commwarrior Disinfection Tool

- http://www.f-secure.com/tools/f-commwarrior.sis

FExplorer file manager (not F-Secure product)

- http://www.gosymbian.com

MMC card reader for PC

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/

F-SECURE®

BE SURE.

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

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 F-Secure

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

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.

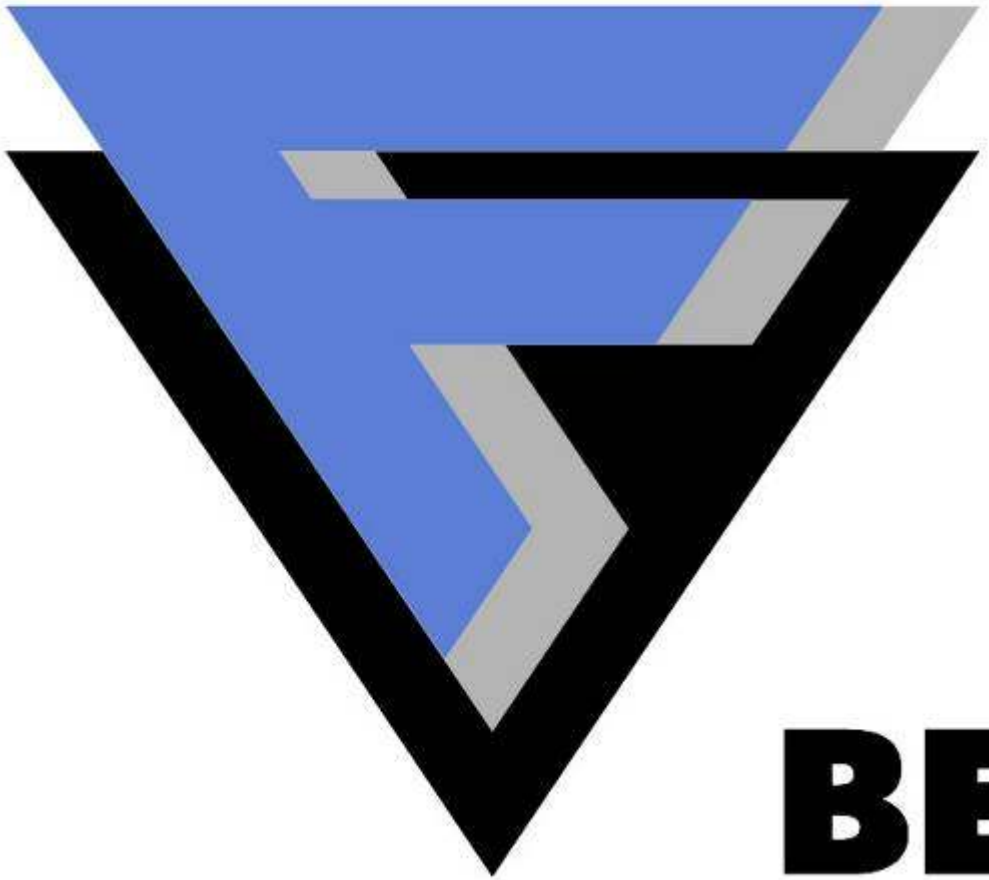
If your phone receives any SIS file from someone that you were not expecting, please do not install it. Instead, send the file to vsamples@f-secure.com. We are rather interested about just what variants are on the move.

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
3. UAE
4. China
5. India

F-SECURE®



BE SURE.

F-Secure Awards

Austria

04/05

Spain

04/05

Serbia

04/05

Norway

04/05

UK

04/05

Finland

04/05

United Kingdom

03/05

United Kingdom

02/05

Italy

12/04

Italy

12/04

United States

12/04

Sweden

11/04

United States

11/04

United Kingdom

10/04