Mobile phone threats

HITBSecConf2005, Kuala Lumpur, Malaysia

Mikko Hypponen, Chief Research Officer

F-SECURE®

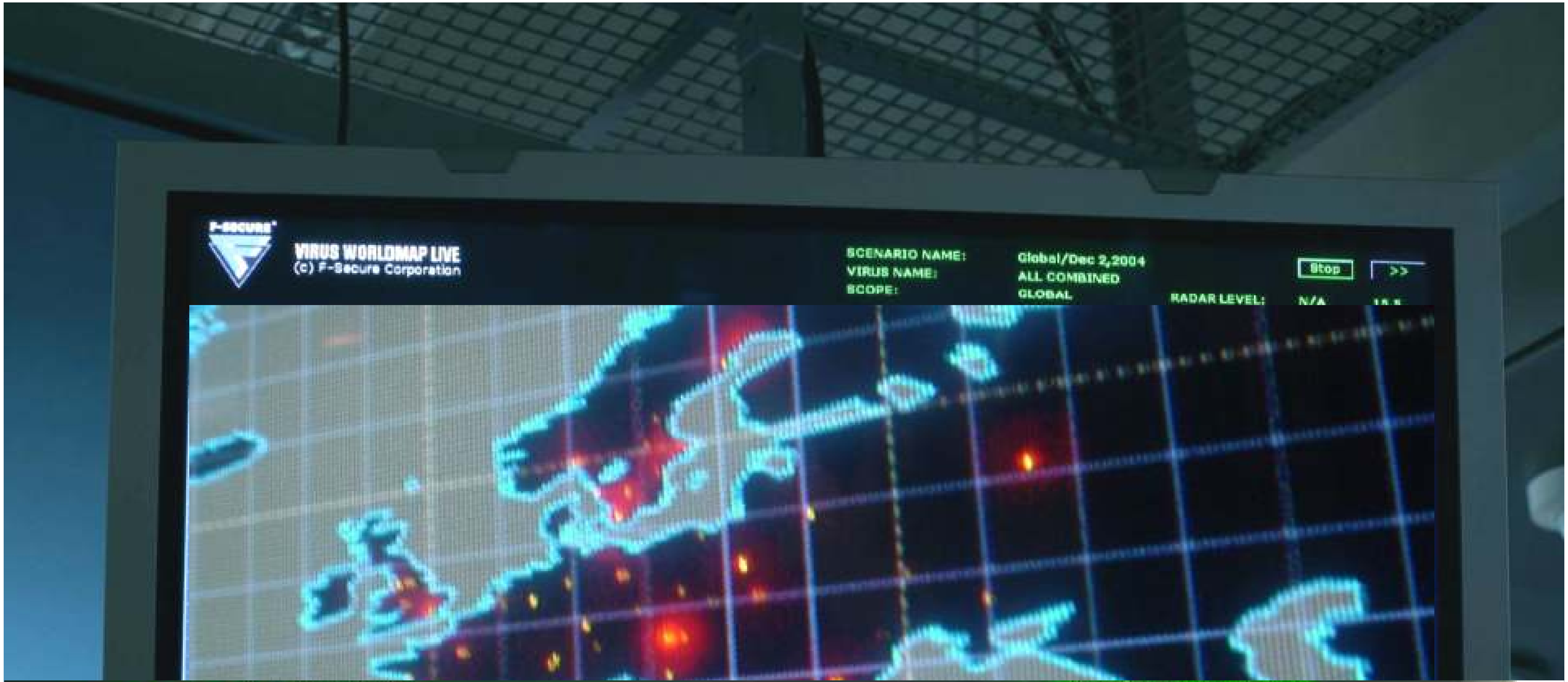
BE SURE.

F-SECURE

F-SECURE
BE SURE.
F-SECURE
BE SURE.

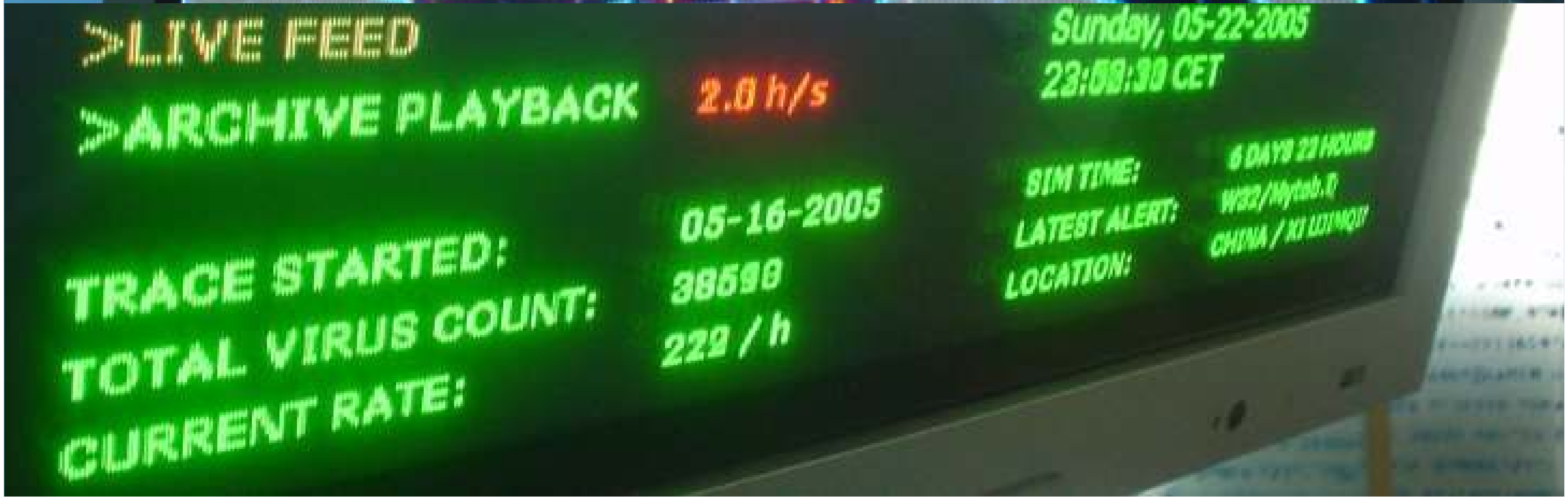
F-SECURE
Got Root?

© 2005 Mikael Albrecht



VIRUS WORLDMAP LIVE
(c) F-Secure Corporation

SCENARIO NAME: Global/Dec 2,2004
VIRUS NAME: ALL COMBINED
SCOPE: GLOBAL
RADAR LEVEL: N/A

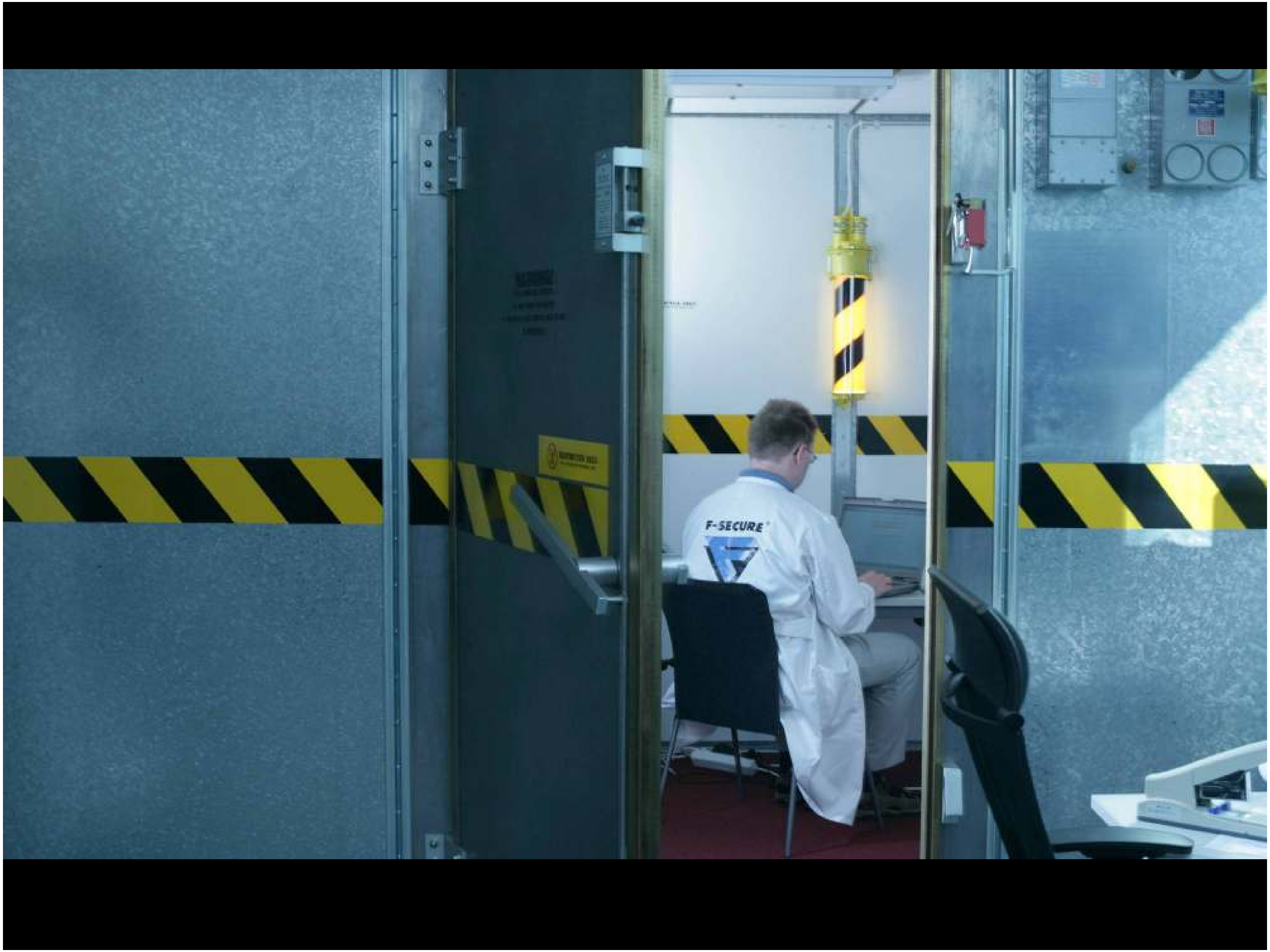


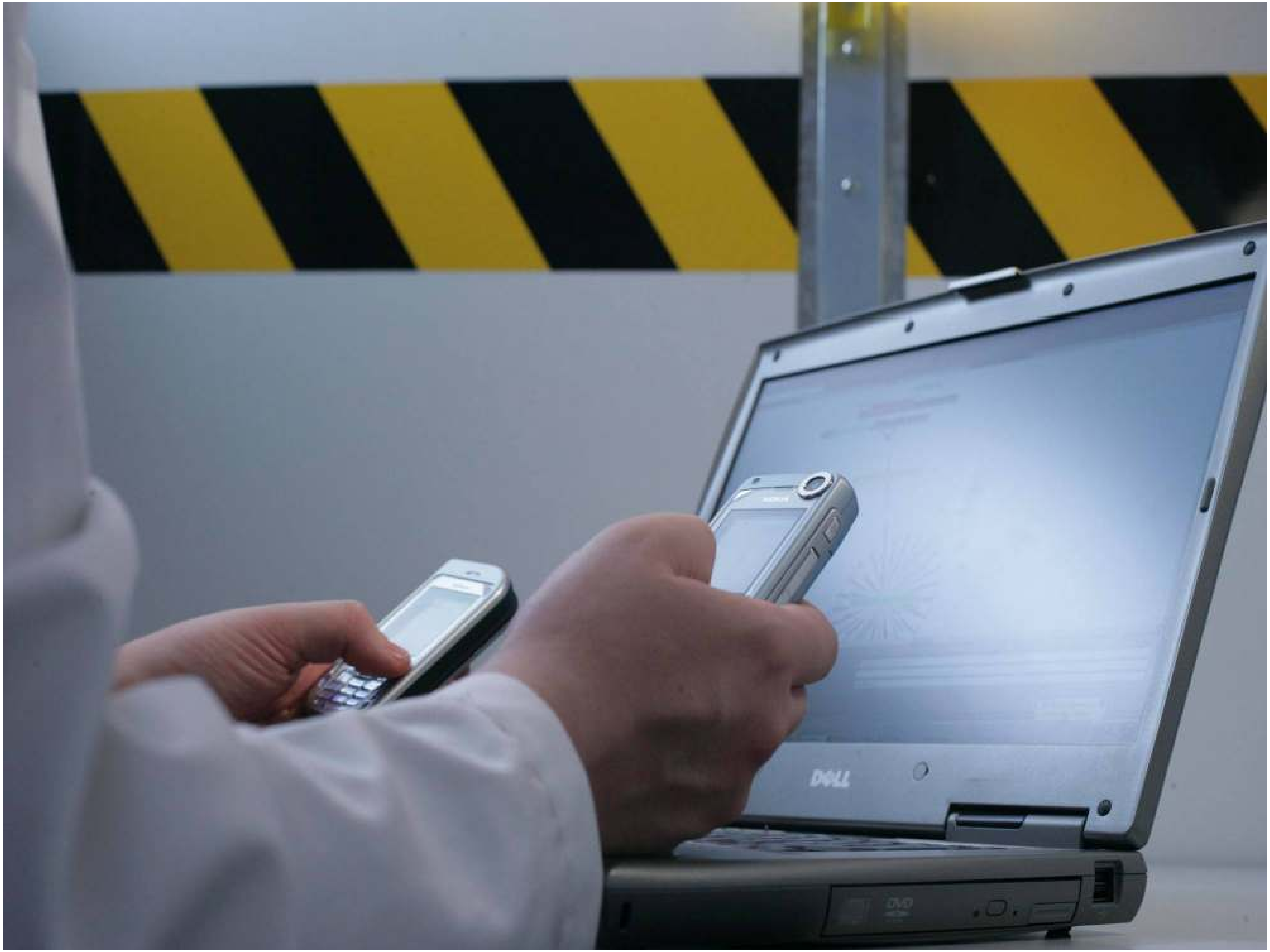
>LIVE FEED
>ARCHIVE PLAYBACK 2.0 h/s

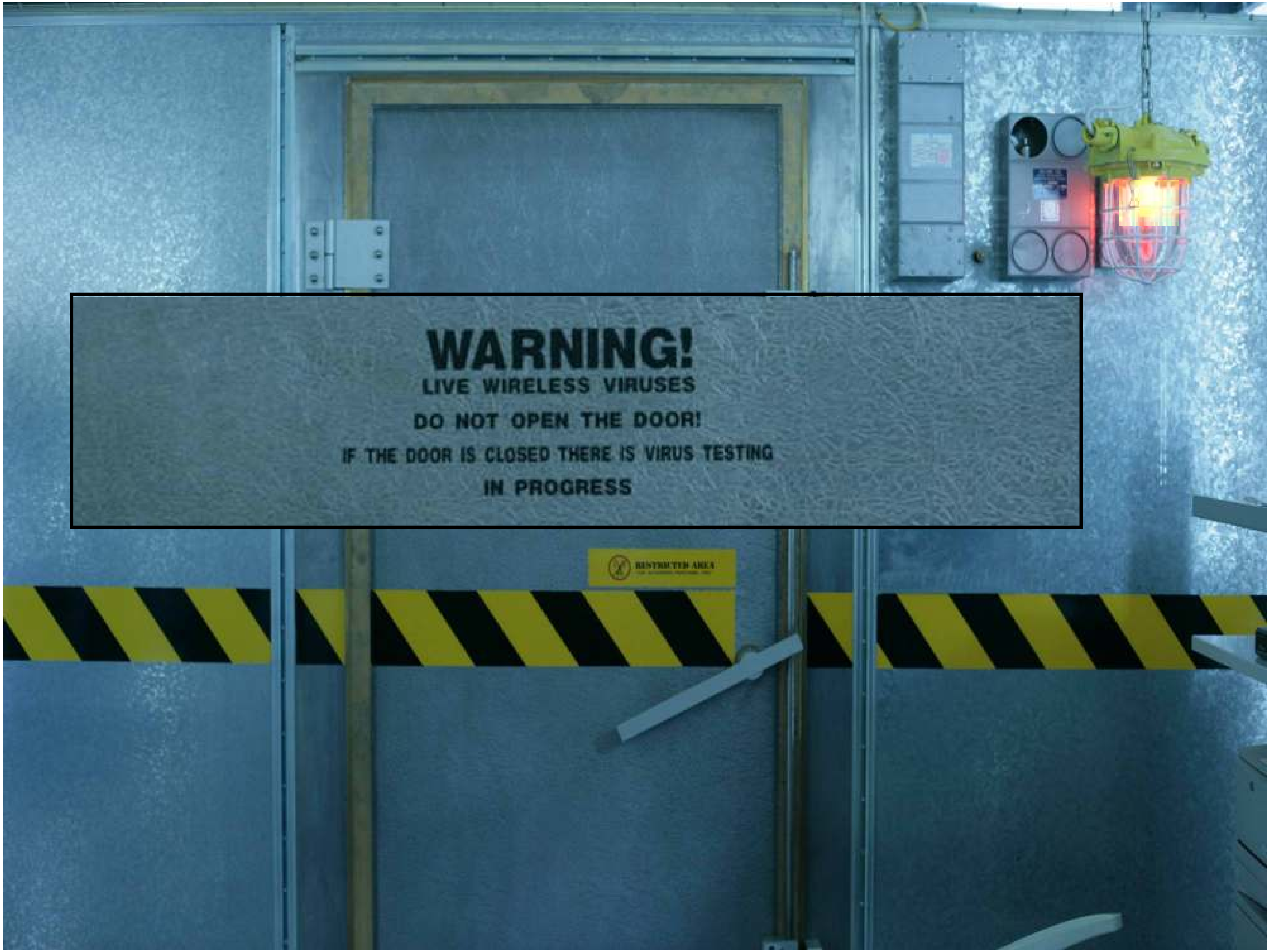
Sunday, 05-22-2005
23:59:30 CET

TRACE STARTED: 05-16-2005
TOTAL VIRUS COUNT: 38598
CURRENT RATE: 229 / h

SIM TIME: 6 DAYS 23 HOURS
LATEST ALERT: W32/Mytob.D
LOCATION: CHINA / XI LUNQI


F-SECURE


DELL
DVD

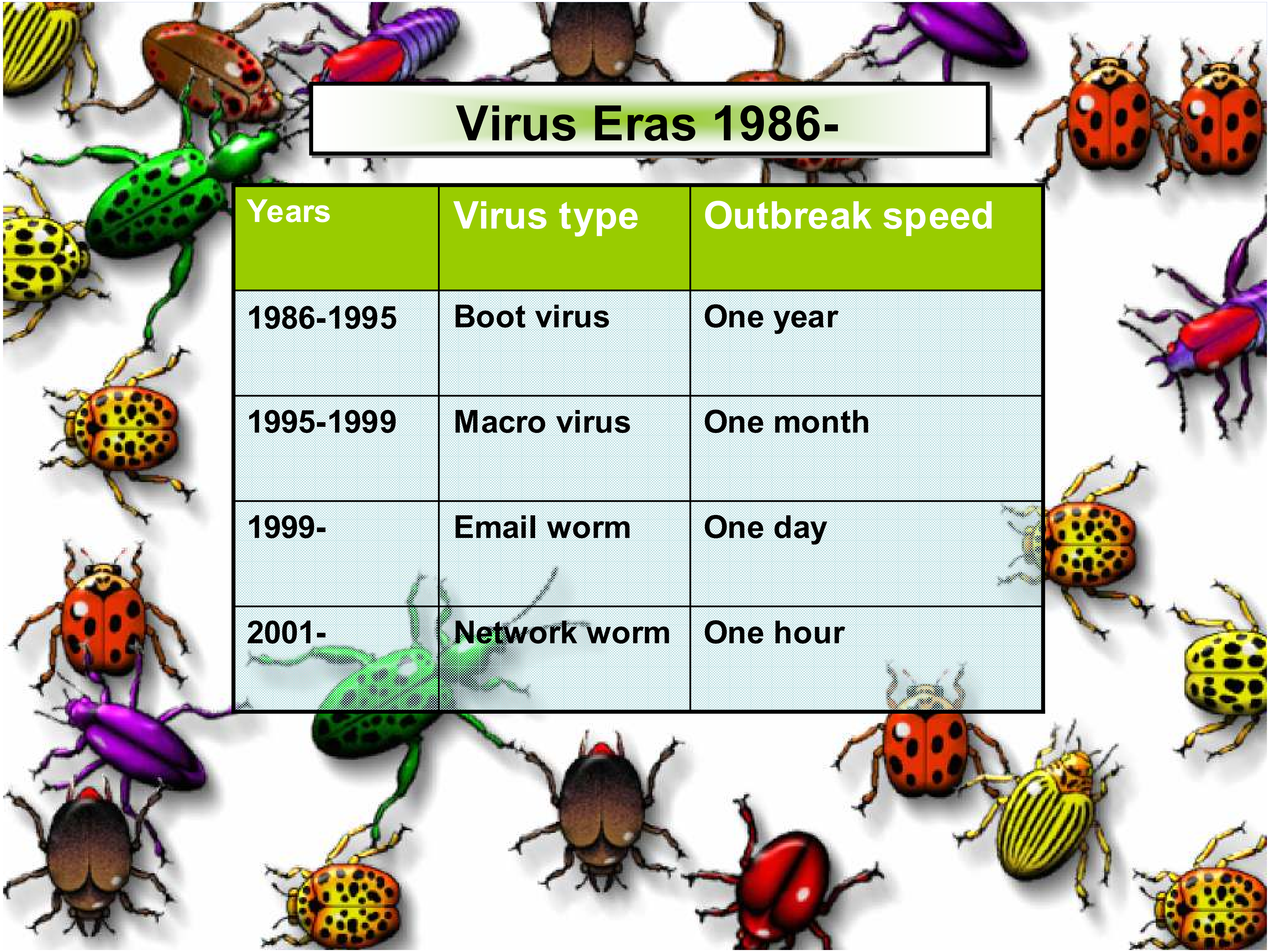

WARNING!
LIVE WIRELESS VIRUSES
DO NOT OPEN THE DOOR!
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING
IN PROGRESS
RESTRICTED AREA

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...

Nope, this is already happening...

- Tens of thousands of infections worldwide
- Reports about Cabir and Commwarrior from over 30 countries
- A company with 8 m mobile subscribers says it has disinfected 13000 phones
- An operator with 9 million customers reports 200 infections a day
- Operator with 2 million customers: 3.5% of MMS traffic infected
- Operators have given money back to customers who had Commwarrior
- An antivirus service was needed during the athletics world championships



Virus Eras 1986-

Years	Virus type	Outbreak speed
1986-1995	Boot virus	One year
1995-1999	Macro virus	One month
1999-	Email worm	One day
2001-	Network worm	One hour

We used to be fighting these...

Chen-Ing Hau
Author of
the CIH virus

Joseph McElroy
Hacked the Fermi lab
network

Benny
Ex-29A

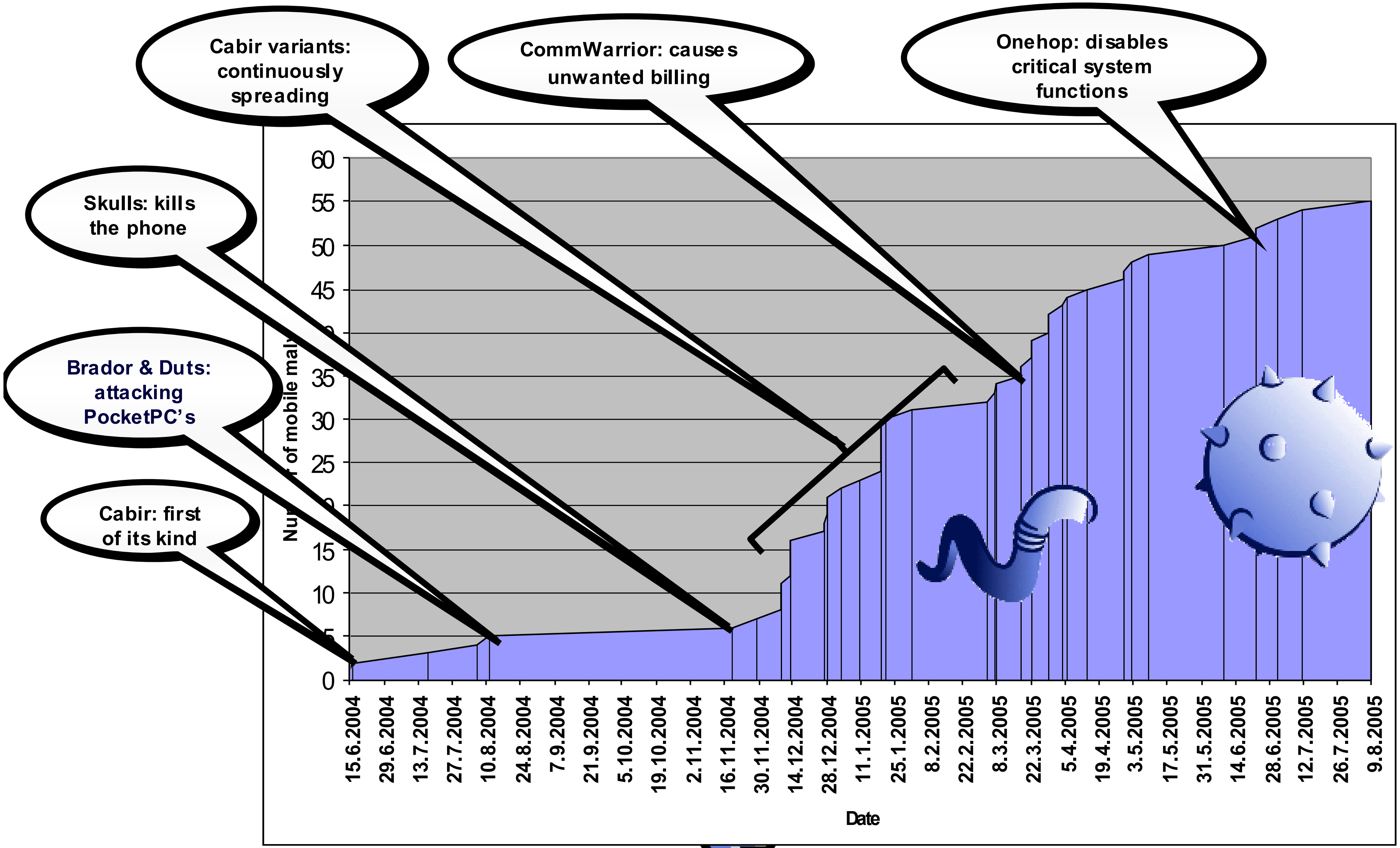
Today we are fighting these!

Jeremy Jaynes
Millionaire,
and a spammer

Jay Echouafni
CEO,
and a DDoS attacker

Andrew Schwarmkoff
Member of Russian mob,
and a phisher

The Increasing Amount of Mobile Malware



Cabir variants: continuously spreading

CommWarrior: causes unwanted billing

Onehop: disables critical system functions

Skulls: kills the phone

Brador & Duts: attacking PocketPC's

Cabir: first of its kind

So, where are they coming from?

Europe

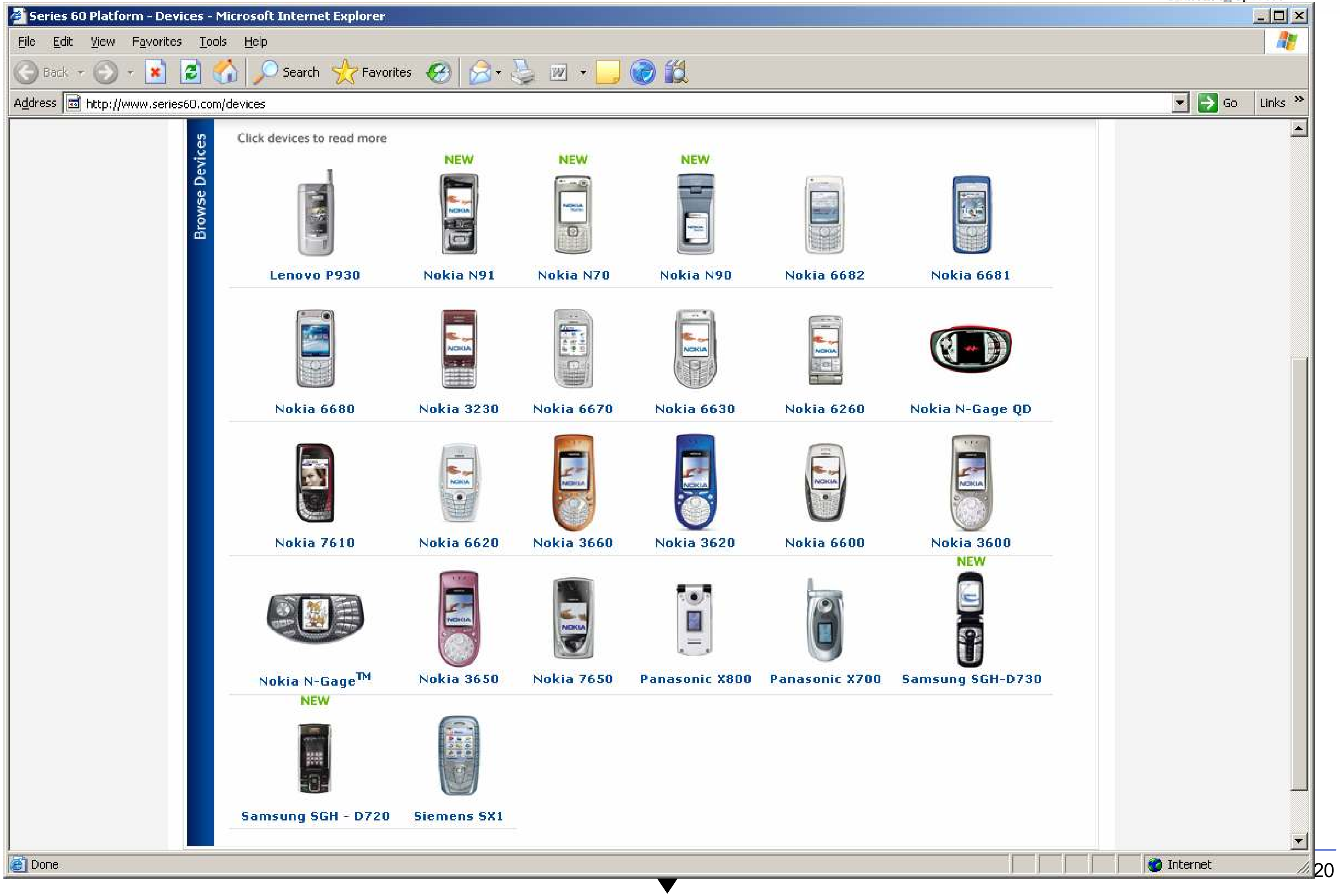
Brazil

Asia

Malaysian virus writers who have written mobile viruses or trojans:

- Calvin
- Yuan
- Tee-222
- Blue

So, why Symbian?



Series 60 Platform - Devices - Microsoft Internet Explorer

http://www.series60.com/devices

Click devices to read more

Lenovo P930

NEW Nokia N91

NEW Nokia N70

NEW Nokia N90

Nokia 6682

Nokia 6681

Nokia 6680

Nokia 3230

Nokia 6670

Nokia 6630

Nokia 6260

Nokia N-Gage QD

Nokia 7610

Nokia 6620

Nokia 3660

Nokia 3620

Nokia 6600

Nokia 3600

Nokia N-Gage™

Nokia 3650

Nokia 7650

Panasonic X800

Panasonic X700

NEW Samsung SGH-D730

NEW Samsung SGH - D720

Siemens SX1

Mobile threats:
Virus-writing community is awake

"Let's go to work . We are starting Cell Phone Virus Challenge. Any contribution welcomed (the more funny solution, the better). Deadline has not been set"

- Statement from an underground website at virus.cyberspace.sk

Fred Burg/ArtFactory

Case Cabir

First real mobile phone virus

Found in June 2004

Runs on Symbian Series 60

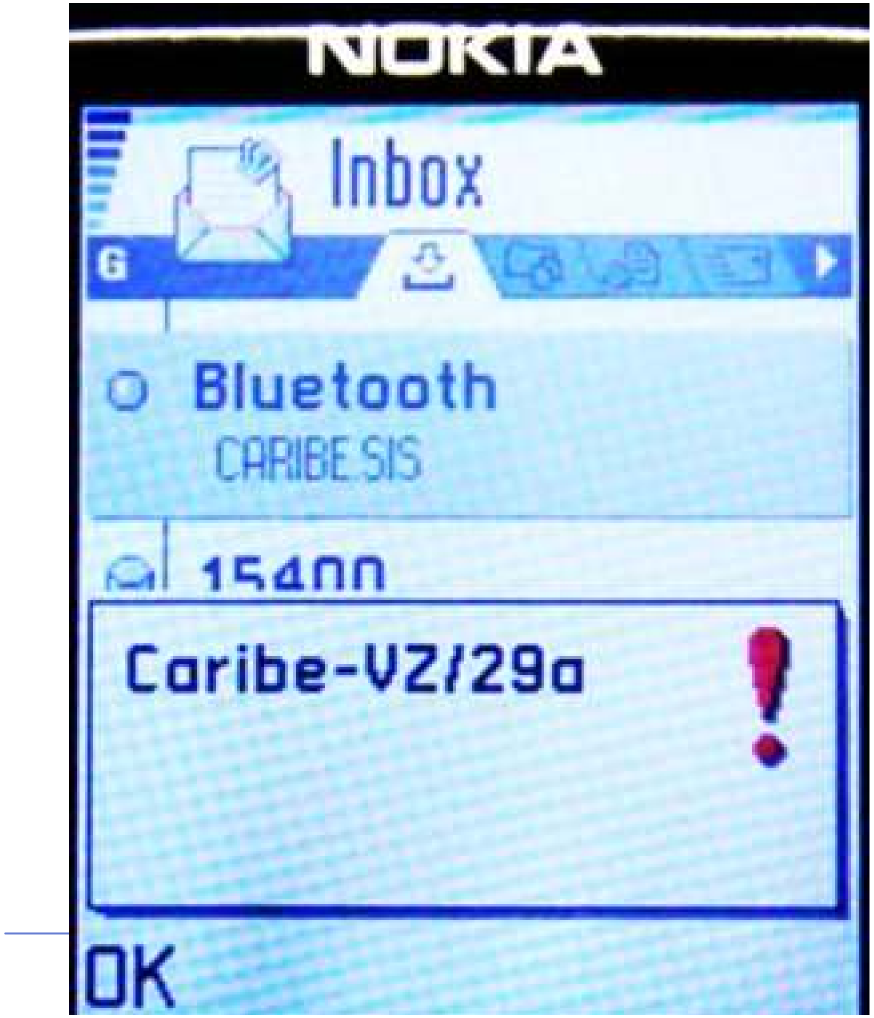
Proof-of-concept

By 29A

Spreads via Bluetooth

Kinda like the flu

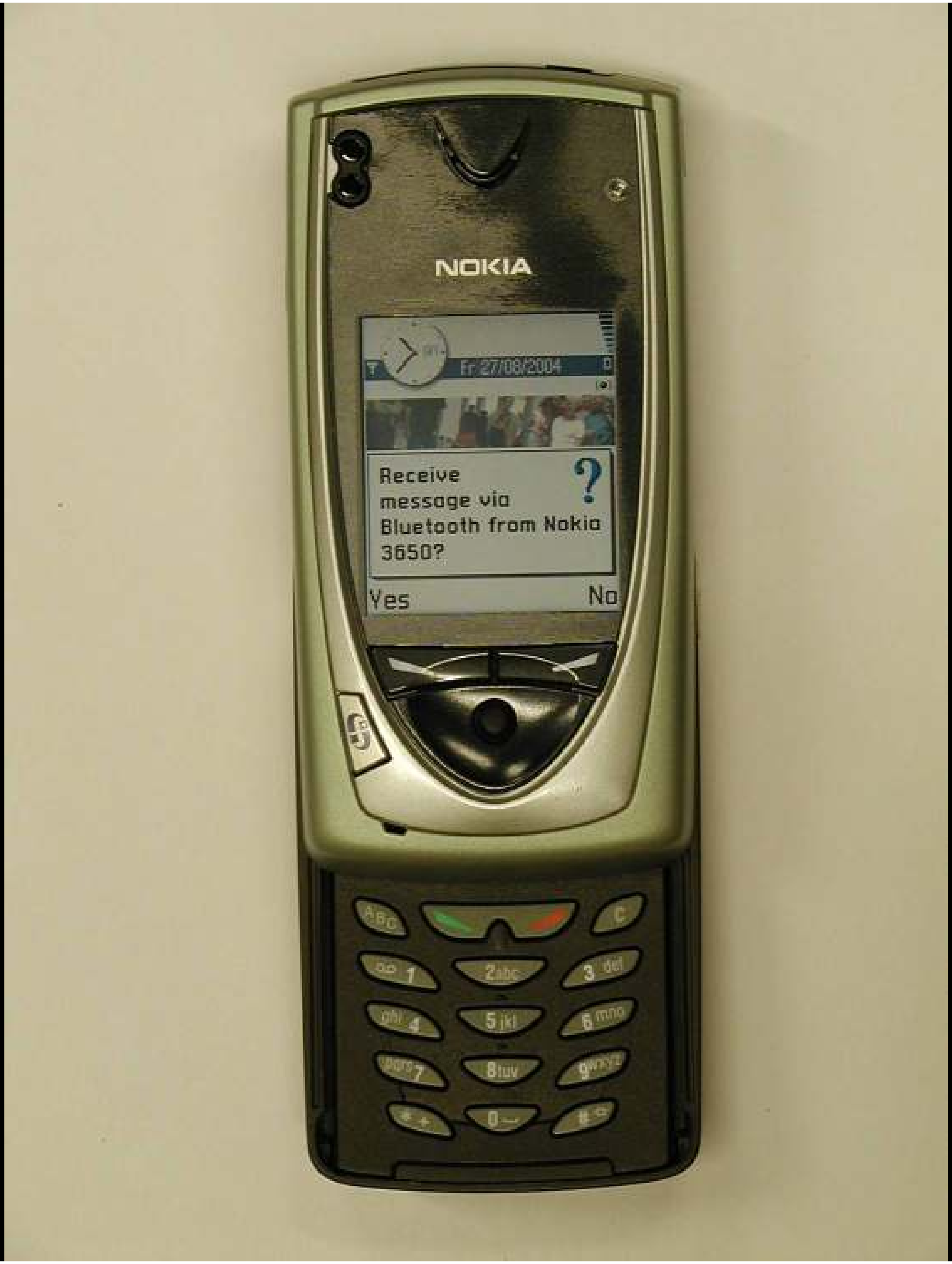
<u>Doesn't break Series 60 security model in any way!</u>



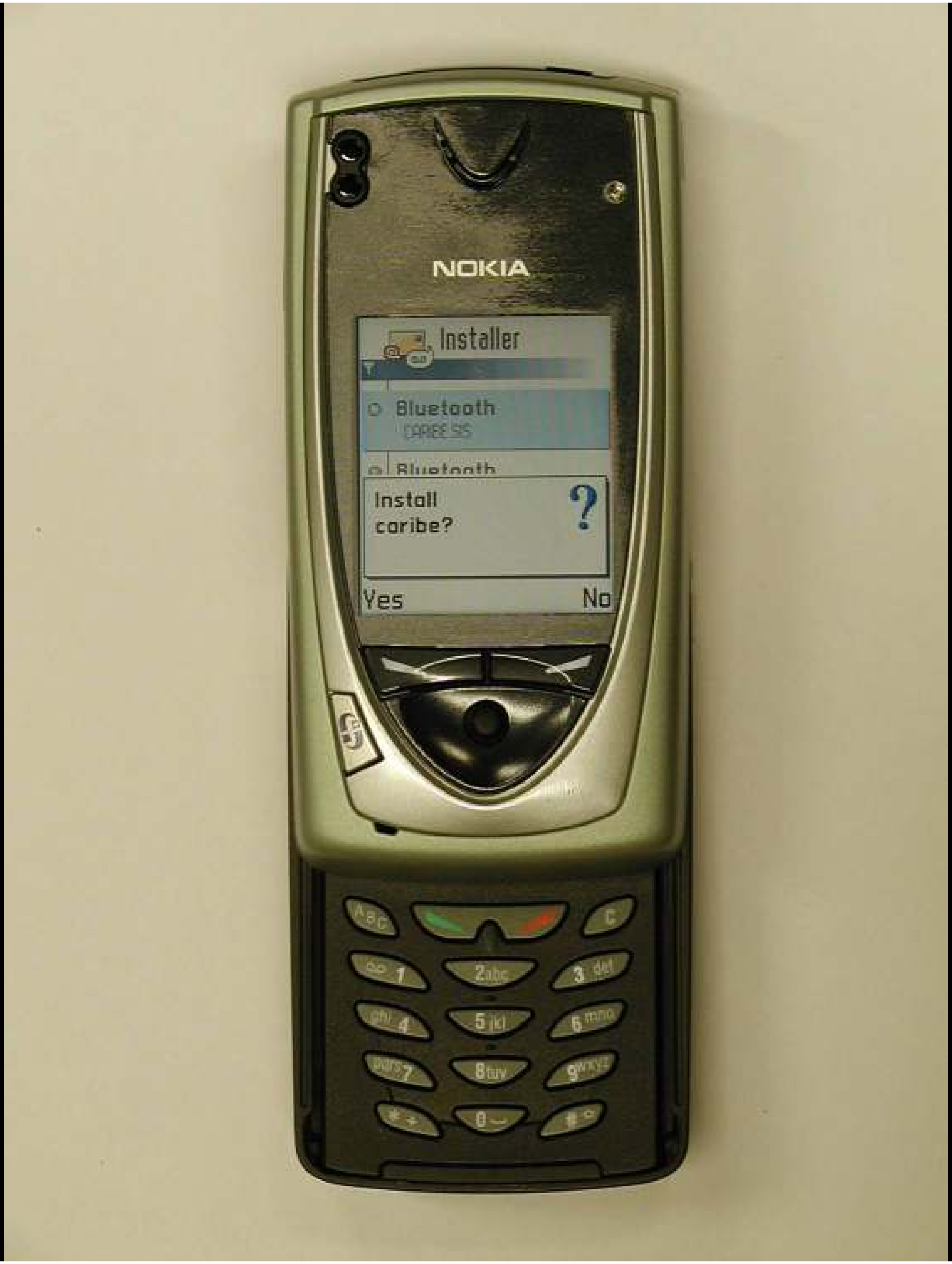
Bluetooth
CARIBE.SIS

15400

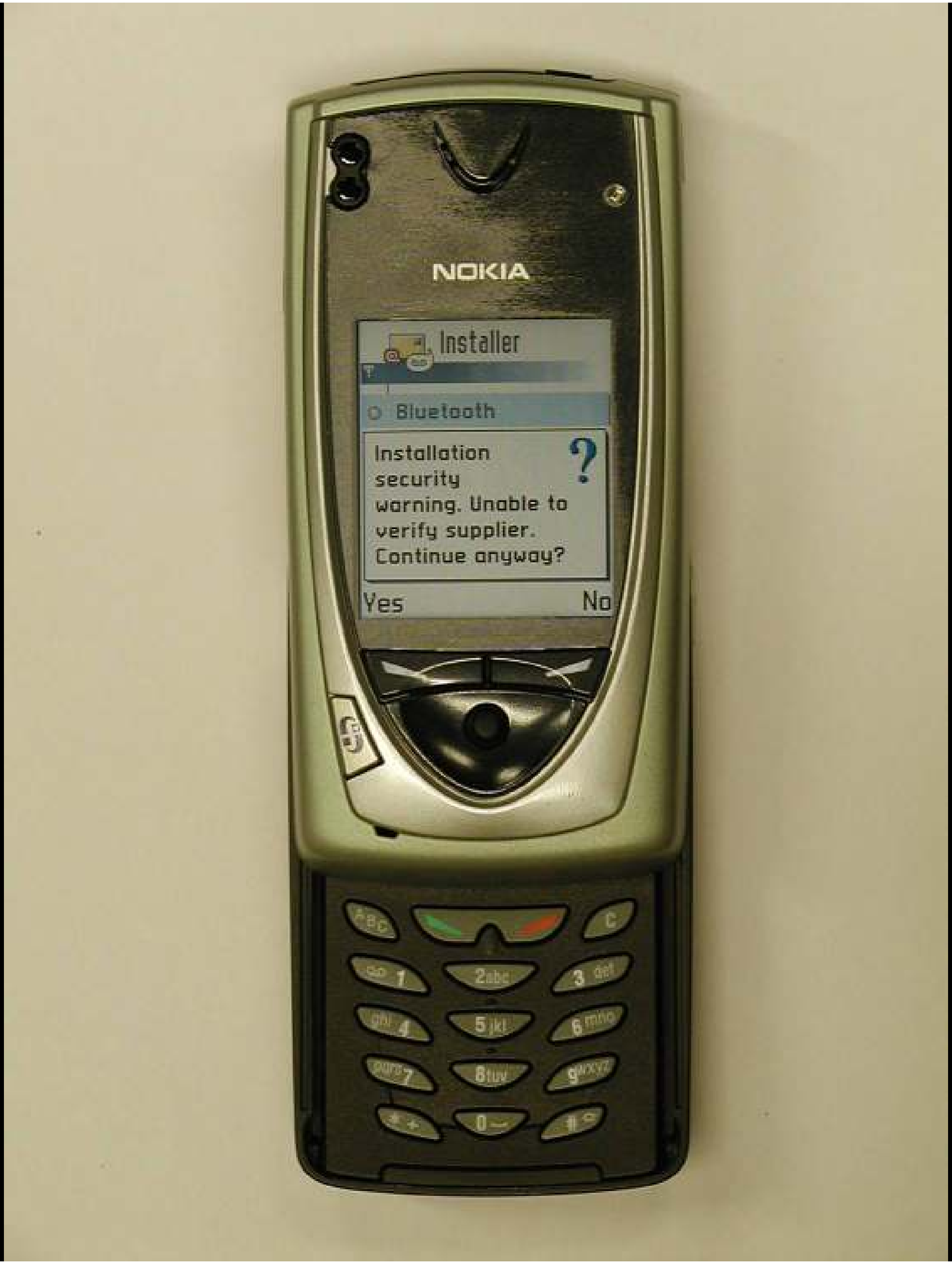
Caribe-VZ/29a



Receive message via Bluetooth from Nokia 3650?



NOKIA
Installer
Bluetooth
CARIBE.SIS
Bluetooth
Install caribe?
Yes
No

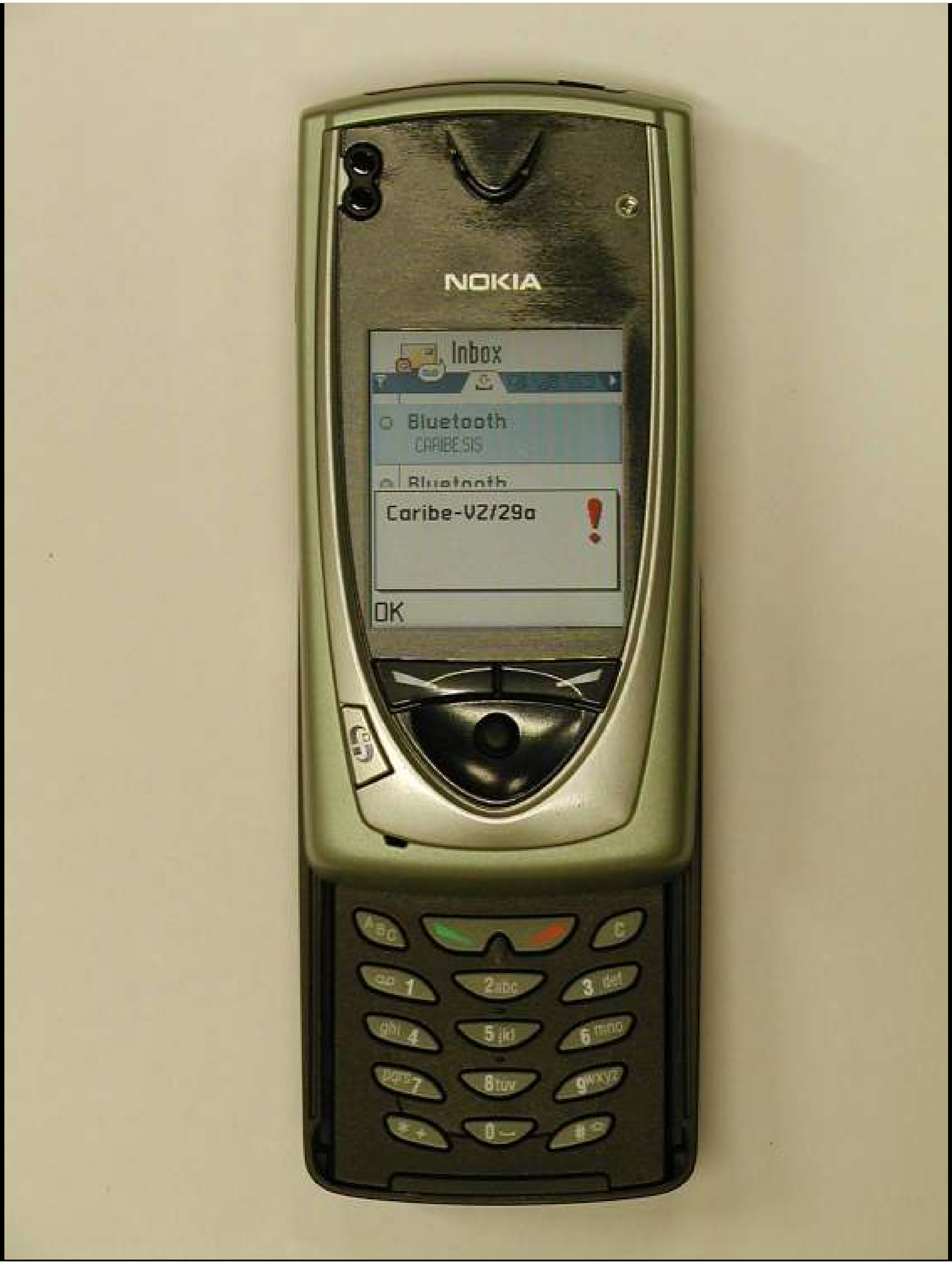


Installer

Bluetooth

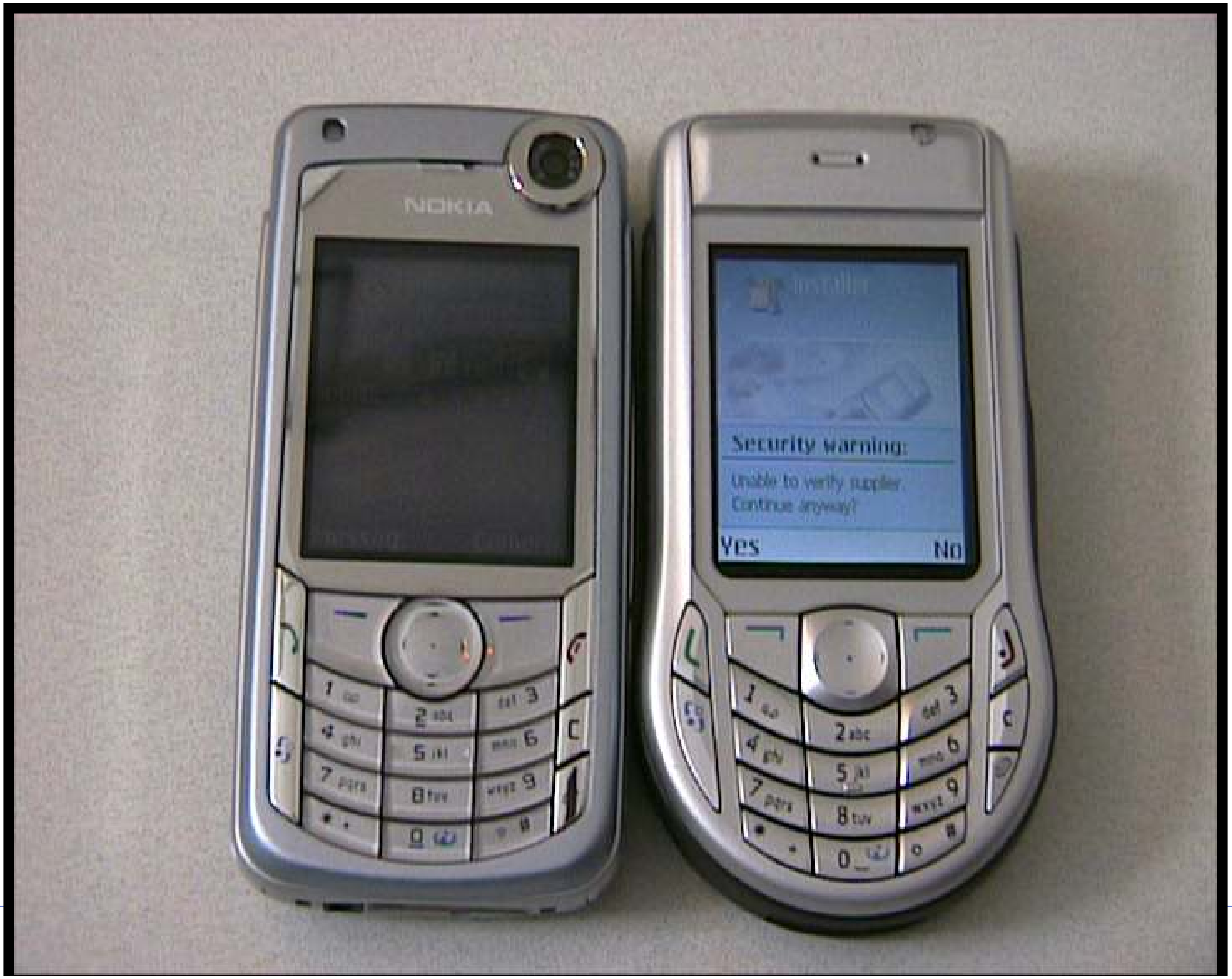
Installation security warning. Unable to verify supplier. Continue anyway?

Yes No


NOKIA
Inbox
Bluetooth
CARIBE SIS
Bluetooth
Caribe-VZ/29a
OK

So, why do people still get infected?

Because of the user interface



Security warning:

Unable to verify supplier. Continue anyway?

Studying Cabir

Trickier than one might think

Could easily escape by accident

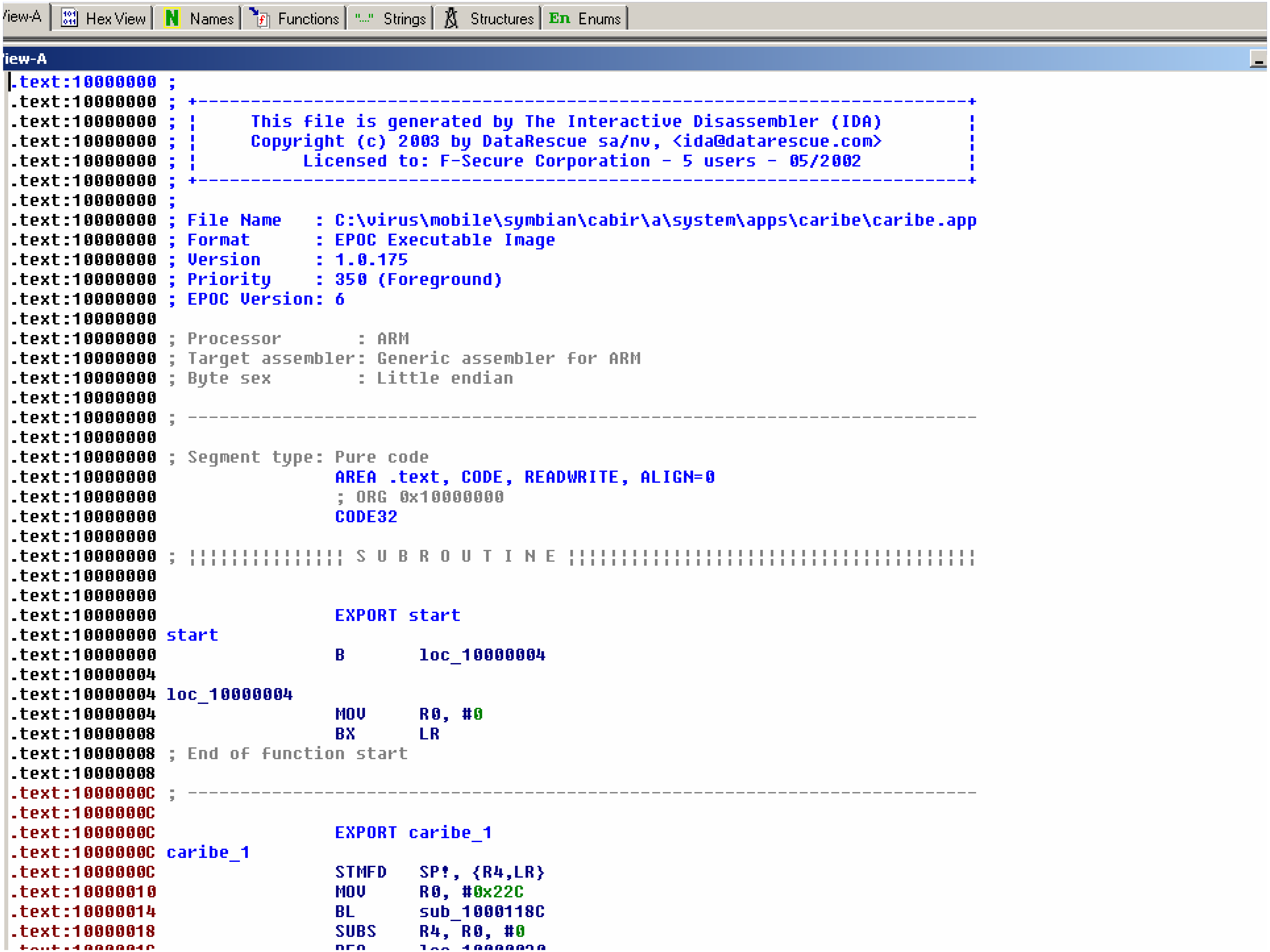
Which would be catastrophic

Needs a safe place for testing purposes

Cabir tries to send itself to **any** Bluetooth device

On newer and fast Series 60 phones it makes lots of connections, fast

But Cabir spreading technique is broken



```
.text:10000000 ;
.text:10000000 ; +-------------------------------------------------------------------------+
.text:10000000 ; ¦     This file is generated by The Interactive Disassembler (IDA)        ¦
.text:10000000 ; ¦     Copyright (c) 2003 by DataRescue sa/nv, <ida@datarescue.com>        ¦
.text:10000000 ; ¦          Licensed to: F-Secure Corporation - 5 users - 05/2002          ¦
.text:10000000 ; +-------------------------------------------------------------------------+
.text:10000000 ;
.text:10000000 ; File Name   : C:\virus\mobile\symbian\cabir\a\system\apps\caribe\caribe.app
.text:10000000 ; Format      : EPOC Executable Image
.text:10000000 ; Version     : 1.0.175
.text:10000000 ; Priority    : 350 (Foreground)
.text:10000000 ; EPOC Version: 6
.text:10000000
.text:10000000 ; Processor       : ARM
.text:10000000 ; Target assembler: Generic assembler for ARM
.text:10000000 ; Byte sex        : Little endian
.text:10000000
.text:10000000 ; ---------------------------------------------------------------------------
.text:10000000
.text:10000000 ; Segment type: Pure code
.text:10000000                 AREA .text, CODE, READWRITE, ALIGN=0
.text:10000000                 ; ORG 0x10000000
.text:10000000                 CODE32
.text:10000000
.text:10000000 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:10000000
.text:10000000
.text:10000000                 EXPORT start
.text:10000000 start
.text:10000000                 B       loc_10000004
.text:10000004
.text:10000004 loc_10000004
.text:10000004                 MOV     R0, #0
.text:10000008                 BX      LR
.text:10000008 ; End of function start
.text:10000008
.text:1000000C ; ---------------------------------------------------------------------------
.text:1000000C
.text:1000000C                 EXPORT caribe_1
.text:1000000C caribe_1
.text:1000000C                 STMFD   SP!, {R4,LR}
.text:10000010                 MOV     R0, #0x22C
.text:10000014                 BL      sub_1000118C
.text:10000018                 SUBS    R4, R0, #0
.text:1000001C                 BEQ     loc_10000020
```

BT DOESN'T WORKING
=> BT flex removal

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

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
Netherlands
Egypt
Luxembourg
New Zealand
Switzerland
Germany

Mad Powerpoint Skills!

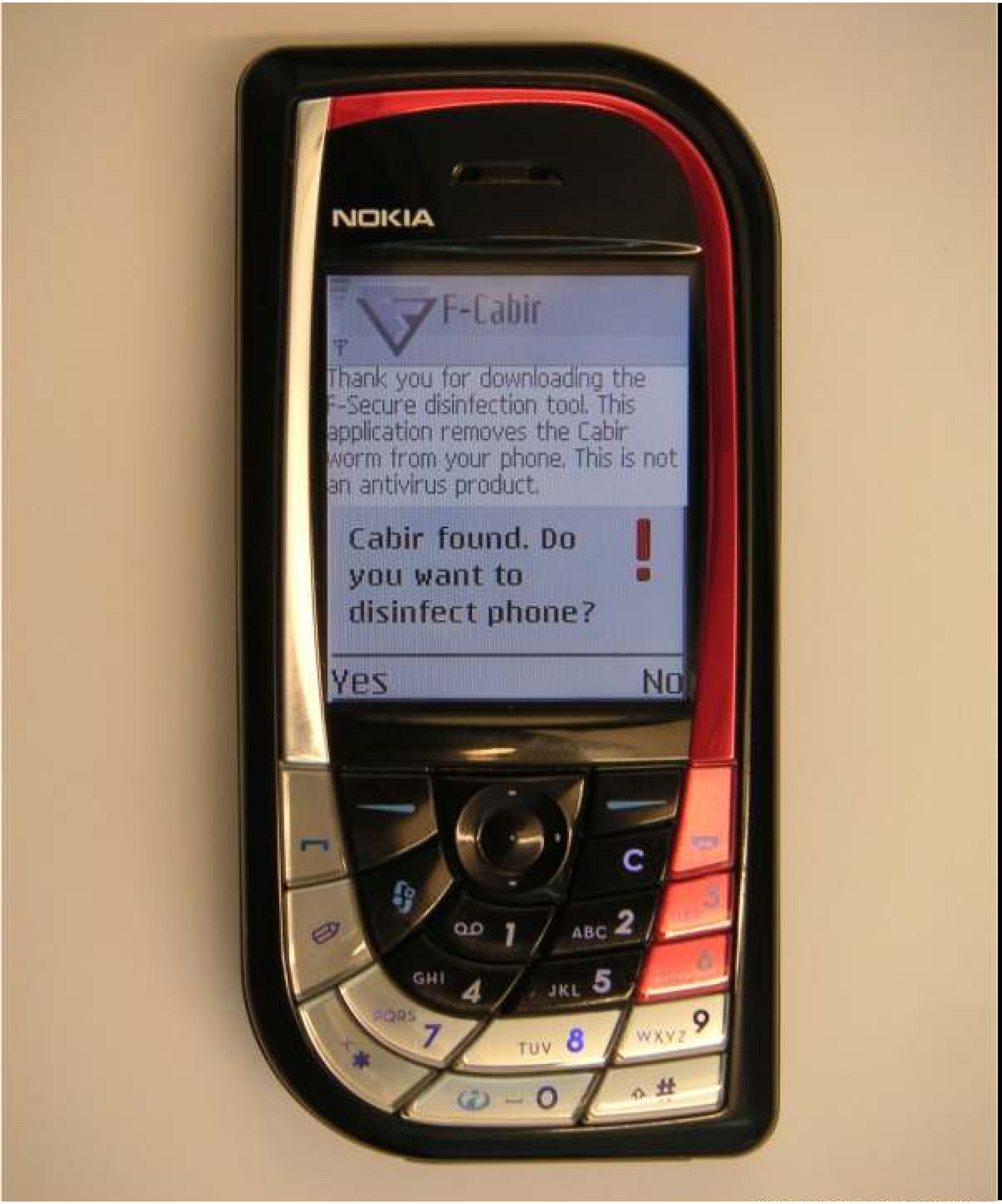
F-SECURE®

Recent Cabir outbreaks

Live 8

10th World Championships in Athletics

Hilton
NOKIA
Messaging
Inbox
Outbox
Drafts
Inbox
922 messages (1 new)
Bluetooth
CARIBE.SIS
10:30
Vendor Watch
Open
Write message



F-Cabir

Thank you for downloading the F-Secure disinfection tool. This application removes the Cabir worm from your phone. This is not an antivirus product.

Cabir found. Do you want to disinfect phone?

Case Duts

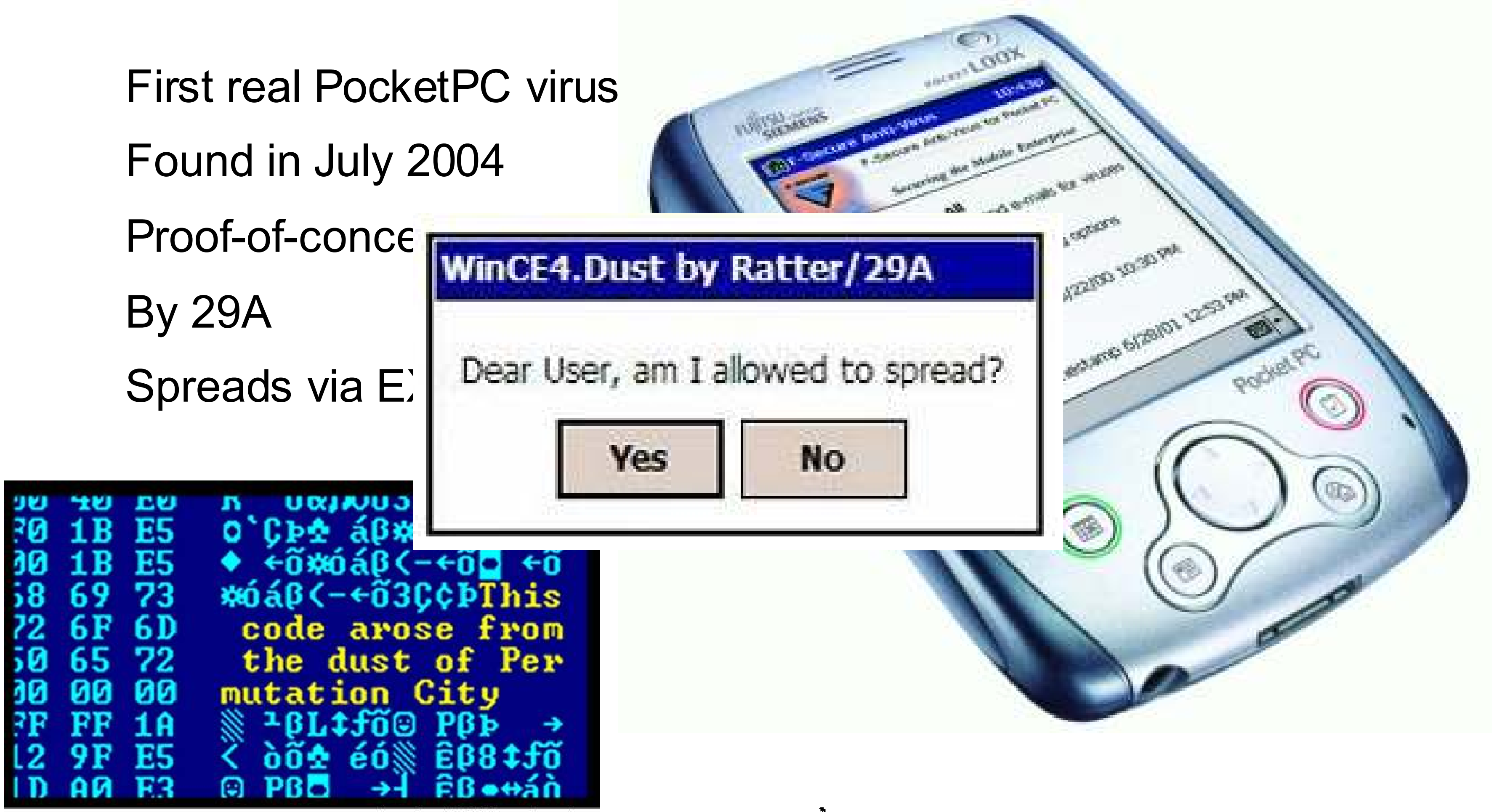
First real PocketPC virus

Found in July 2004

Proof-of-conce

By 29A

Spreads via E



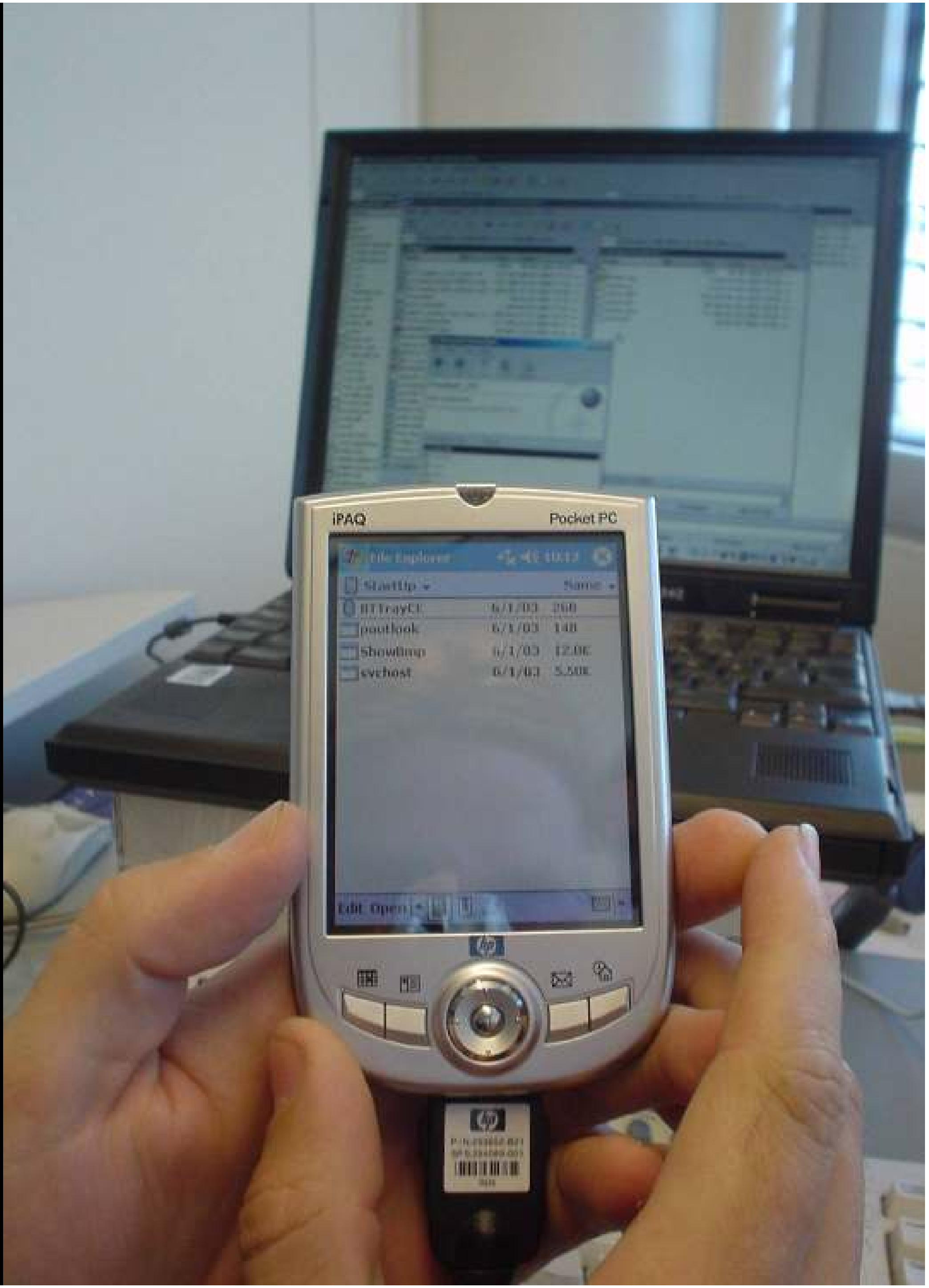
WinCE4.Dust by Ratter/29A

Dear User, am I allowed to spread?

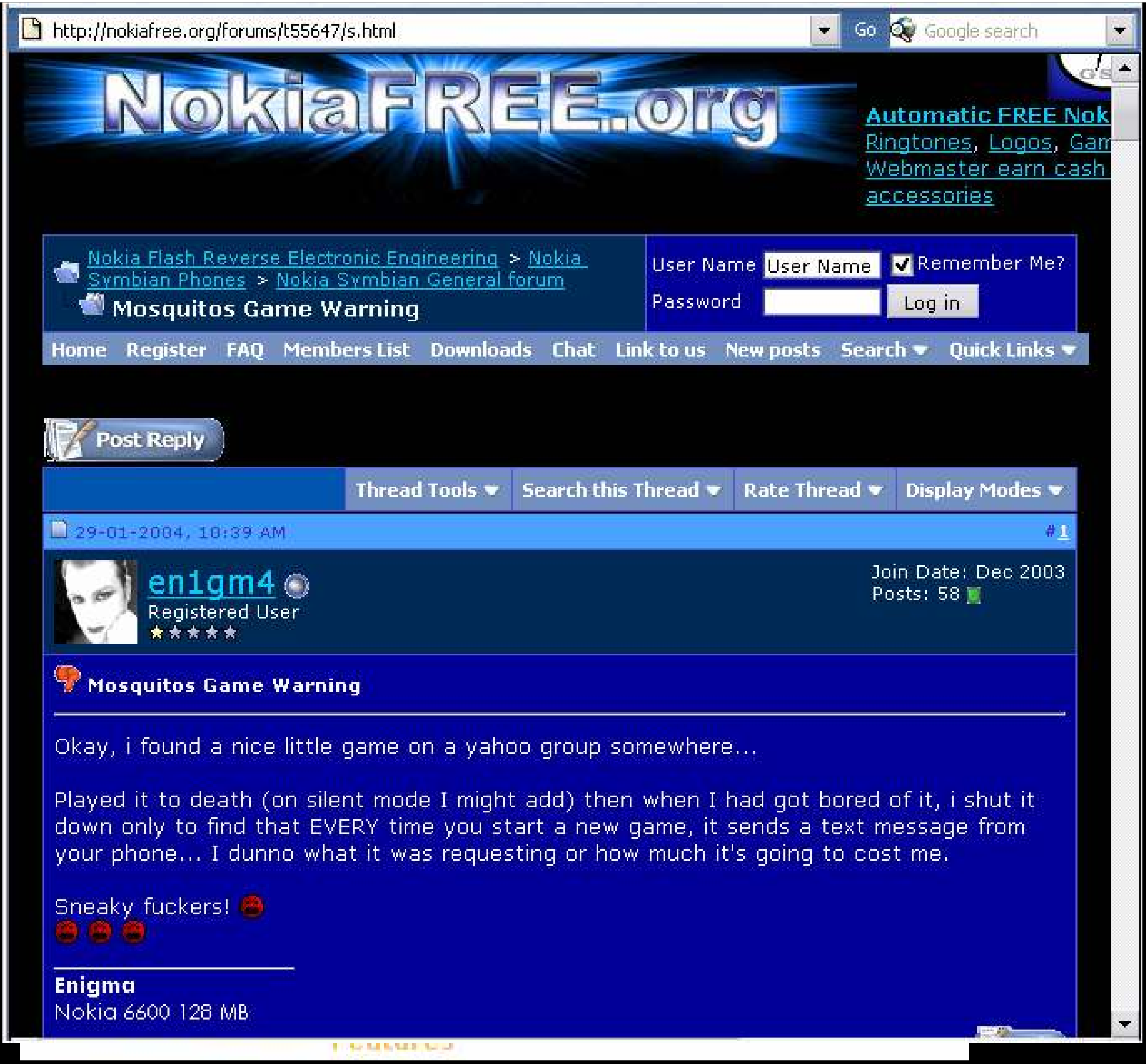
```
F0 1B E5   o`ÇÞ♣ áß☼
00 1B E5   ◆ ←õ☼óáß<-←õ▄ ←õ
58 69 73   ☼óáß<-←õ3Ç¢ÞThis
72 6F 6D    code arose from
50 65 72    the dust of Per
00 00 00   mutation City
FF FF 1A   ▒ ¹ßL↕ƒõ☺ Pßþ  →
12 9F E5   < òõ♣ éó▒ Êß8↕ƒõ
1D A0 E3   ☺ Pß▀  →┤ Êß●↔áǹ
```

Image Copyright © F-Secure Corporation

Case Brador



```
BTTrayCE   6/1/03  26B
pouttlook  6/1/03  14B
ShowBmp    6/1/03  12.0K
svchost    6/1/03  5.50K
```



Nokia Flash Reverse Electronic Engineering > Nokia Symbian Phones > Nokia Symbian General forum

Mosquitos Game Warning

29-01-2004, 10:39 AM #1

en1gm4
Registered User

Join Date: Dec 2003
Posts: 58

Mosquitos Game Warning

Okay, i found a nice little game on a yahoo group somewhere...

Played it to death (on silent mode I might add) then when I had got bored of it, i shut it down only to find that EVERY time you start a new game, it sends a text message from your phone... I dunno what it was requesting or how much it's going to cost me.

Sneaky fuckers!

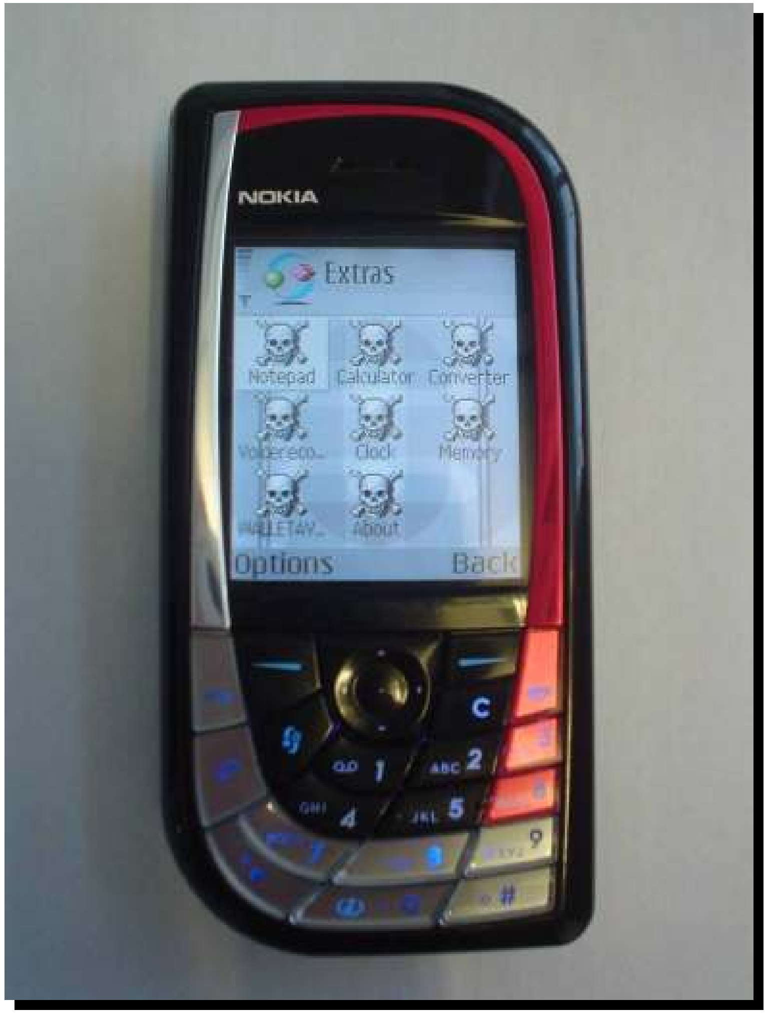
Enigma
Nokia 6600 128 MB

Case Skulls

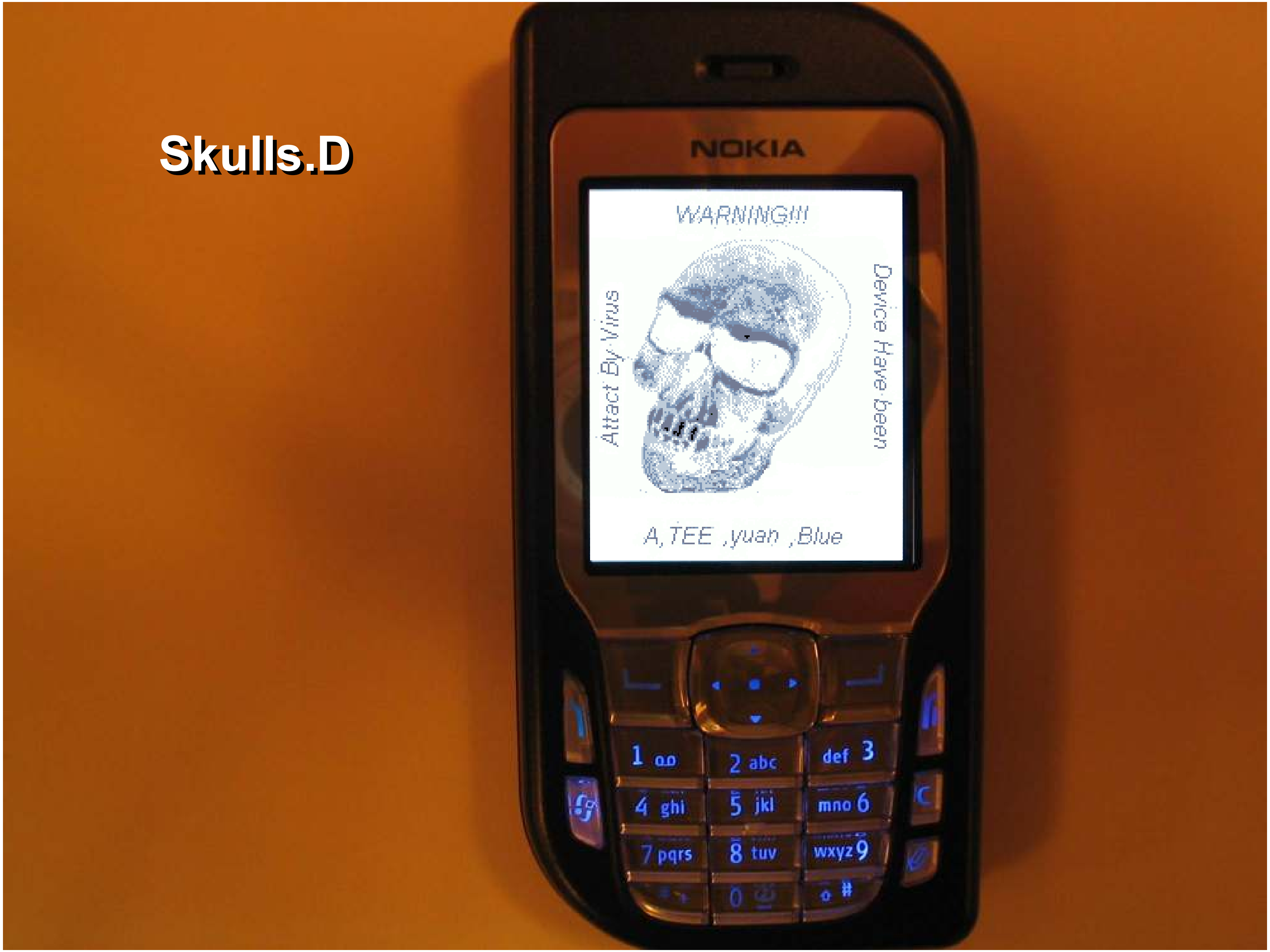
Trojan for Symbian

Kills your apps

Very hard to get rid of



Skulls.D



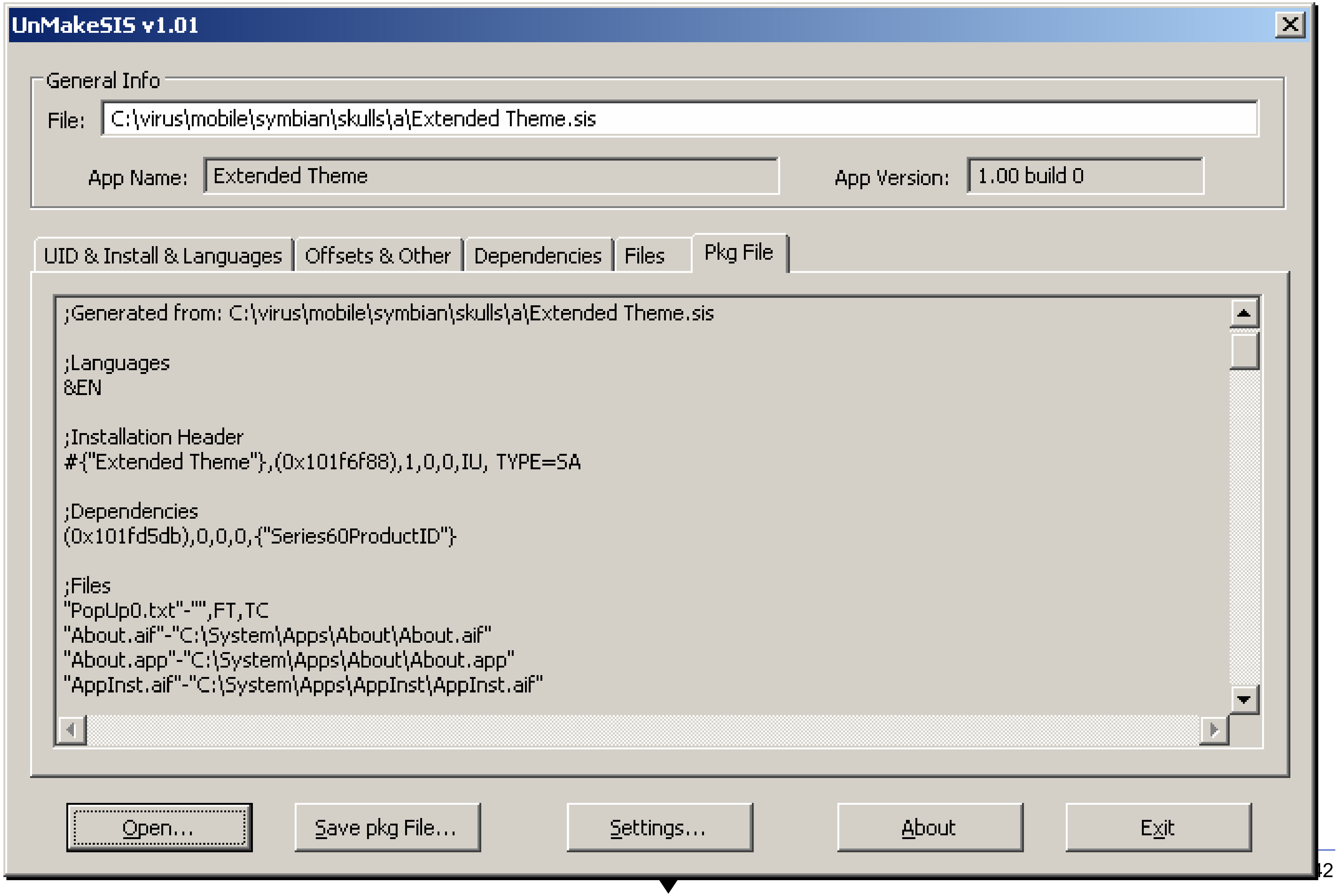
WARNING!!!

Attact By Virus

Device Have been

A,TEE ,yuan ,Blue

Studying Skulls

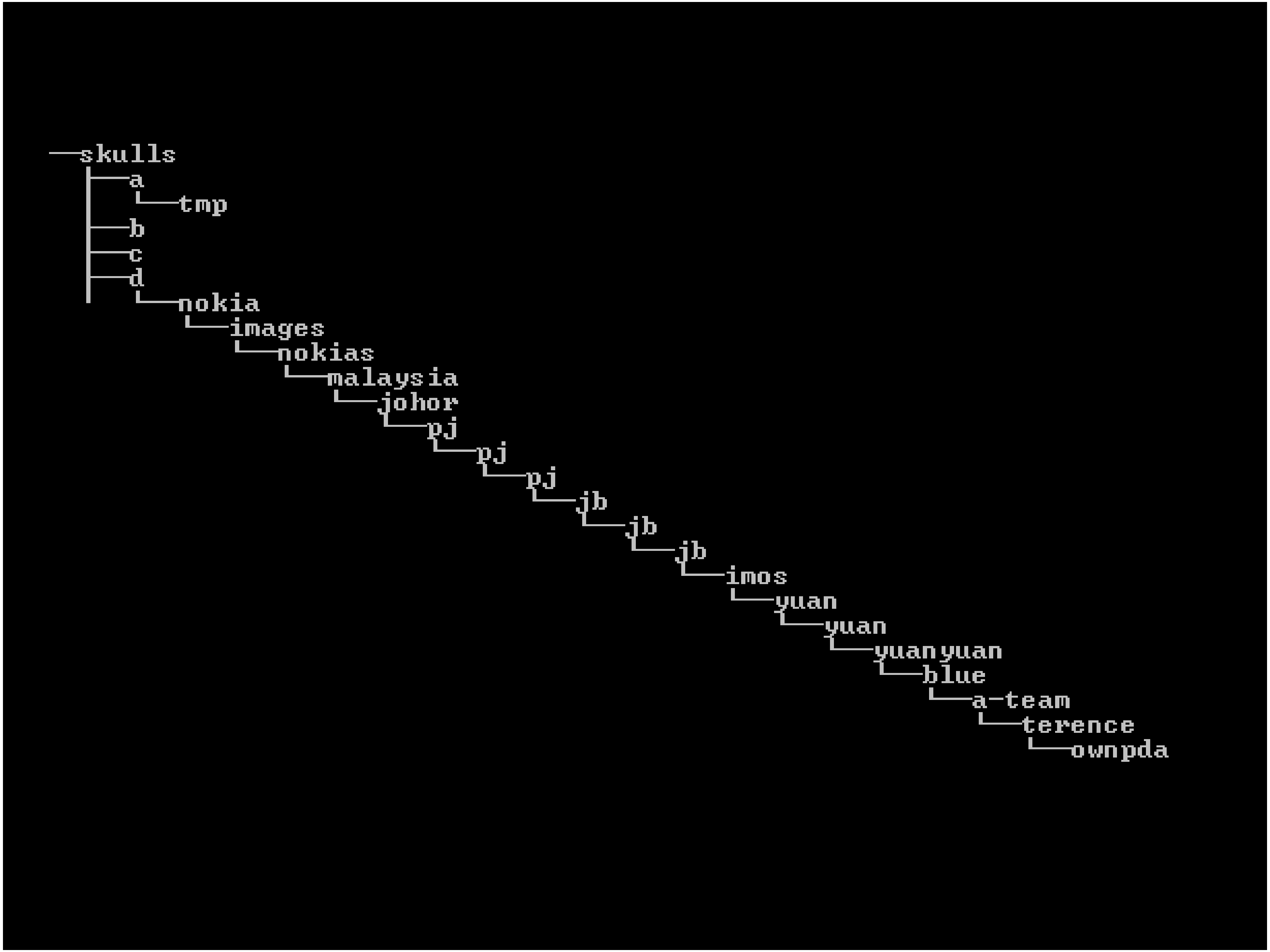


File: C:\virus\mobile\symbian\skulls\a\Extended Theme.sis

App Name: Extended Theme

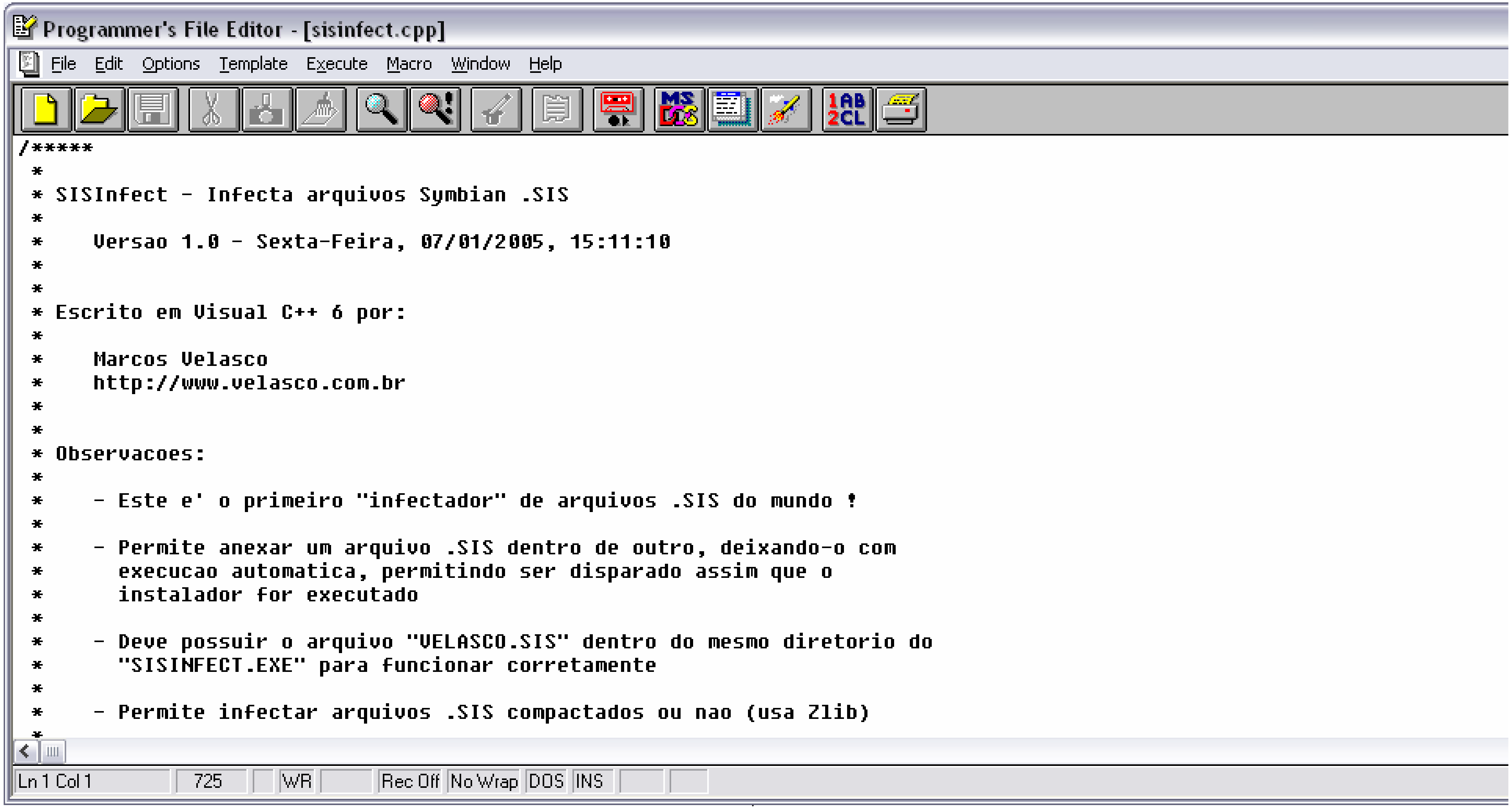
App Version: 1.00 build 0

```
;Generated from: C:\virus\mobile\symbian\skulls\a\Extended Theme.sis

;Languages
&EN

;Installation Header
#{"Extended Theme"},(0x101f6f88),1,0,0,IU, TYPE=SA

;Dependencies
(0x101fd5db),0,0,0,{"Series60ProductID"}

;Files
"PopUp0.txt"-"",FT,TC
"About.aif"-"C:\System\Apps\About\About.aif"
"About.app"-"C:\System\Apps\About\About.app"
"AppInst.aif"-"C:\System\Apps\AppInst\AppInst.aif"
```

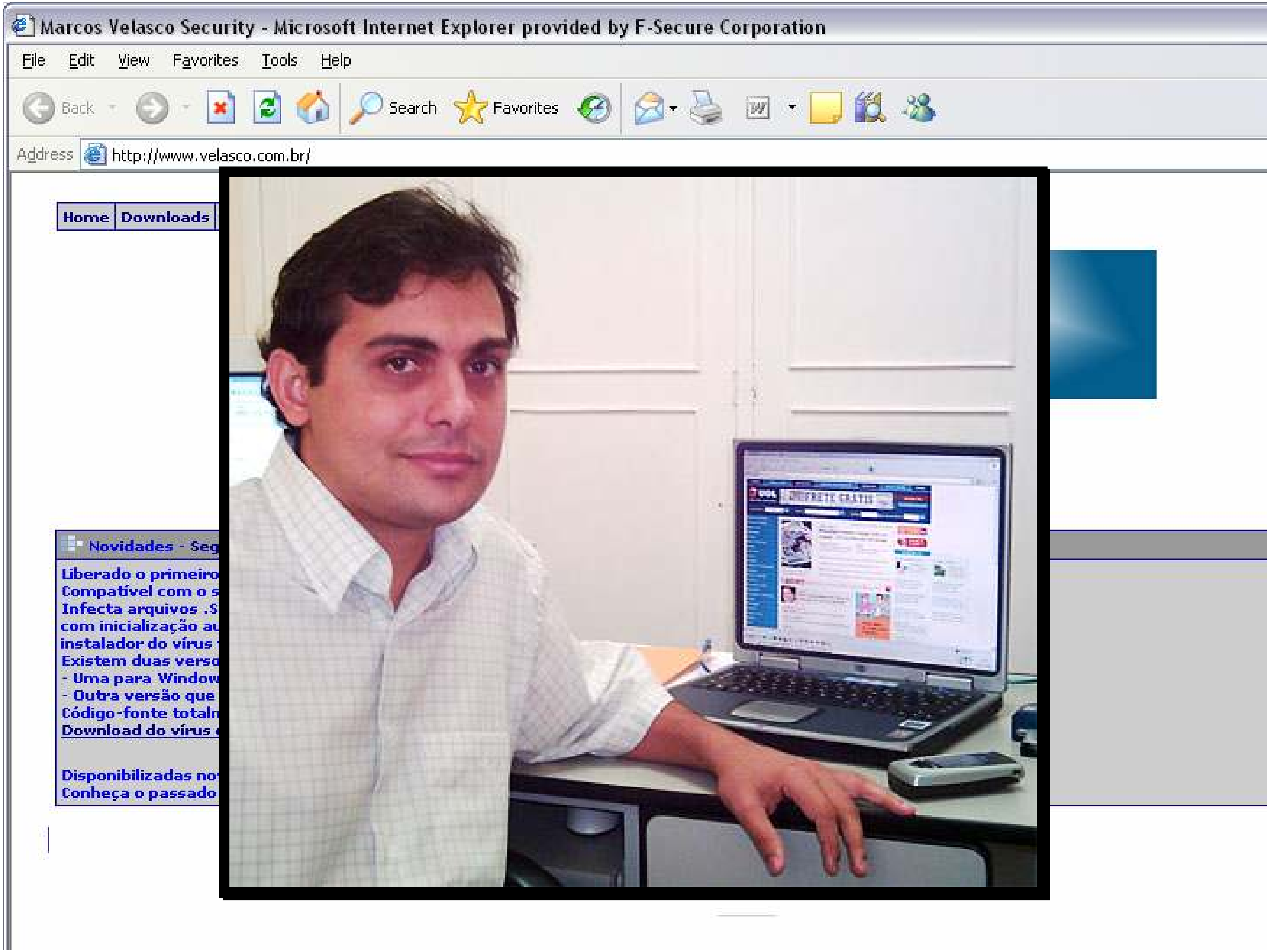


```
──skulls
  ├──a
  │  └──tmp
  ├──b
  ├──c
  ├──d
  │  └──nokia
        └──images
           └──nokias
              └──malaysia
                 └──johor
                    └──pj
                       └──pj
                          └──pj
                             └──jb
                                └──jb
                                   └──jb
                                      └──imos
                                         └──yuan
                                            └──yuan
                                               └──yuanyuan
                                                  └──blue
                                                     └──a-team
                                                        └──terence
                                                           └──ownpda
```

Lasco



```
/*****
 *
 * SISInfect - Infecta arquivos Symbian .SIS
 *
 *    Versao 1.0 - Sexta-Feira, 07/01/2005, 15:11:10
 *
 *
 * Escrito em Visual C++ 6 por:
 *
 *    Marcos Velasco
 *    http://www.velasco.com.br
 *
 *
 * Observacoes:
 *
 *    - Este e' o primeiro "infectador" de arquivos .SIS do mundo !
 *
 *    - Permite anexar um arquivo .SIS dentro de outro, deixando-o com
 *      execucao automatica, permitindo ser disparado assim que o
 *      instalador for executado
 *
 *    - Deve possuir o arquivo "VELASCO.SIS" dentro do mesmo diretorio do
 *      "SISINFECT.EXE" para funcionar corretamente
 *
 *    - Permite infectar arquivos .SIS compactados ou nao (usa Zlib)
 *
```



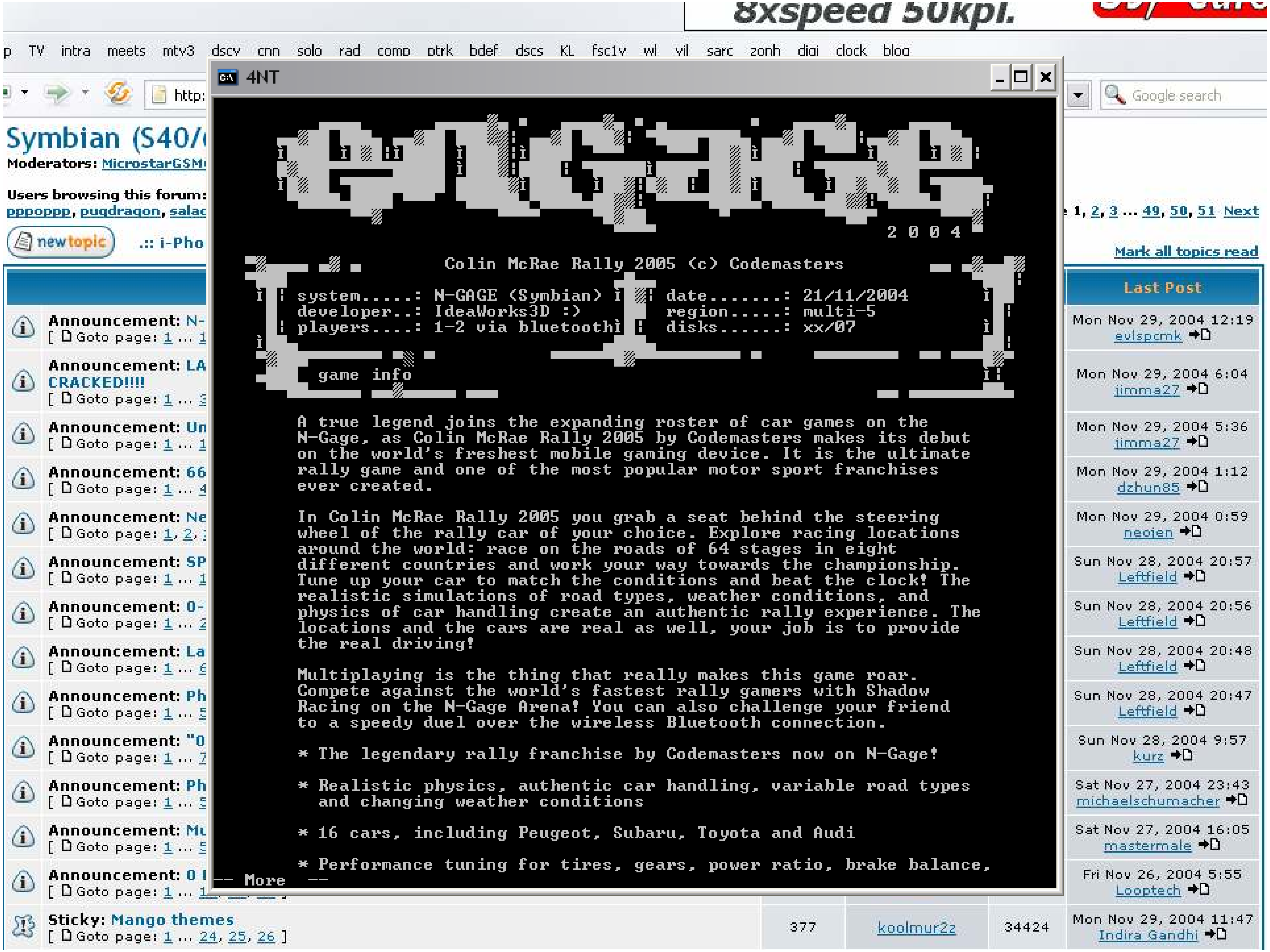
Marcos Velasco Security - Microsoft Internet Explorer provided by F-Secure Corporation

http://www.velasco.com.br/

Novidades - Seg

Liberado o primeiro
Compatível com o s
Infecta arquivos .S
com inicialização au
instalador do vírus
Existem duas versõ
- Uma para Window
- Outra versão que
Código-fonte totaln
Download do vírus

Disponibilizadas no
Conheça o passado



8xspeed 50kpi.
p TV intra meets mtv3 dscv cnn solo rad comp ptrk bdef dscs KL fsc1v wl vil sarc zonh digi clock blog
http:
Google search
4NT
newtopic
Last Post

Symbian (S40/

Moderators: MicrostarGSM

Users browsing this forum: pppoppp, pugdragon, salac

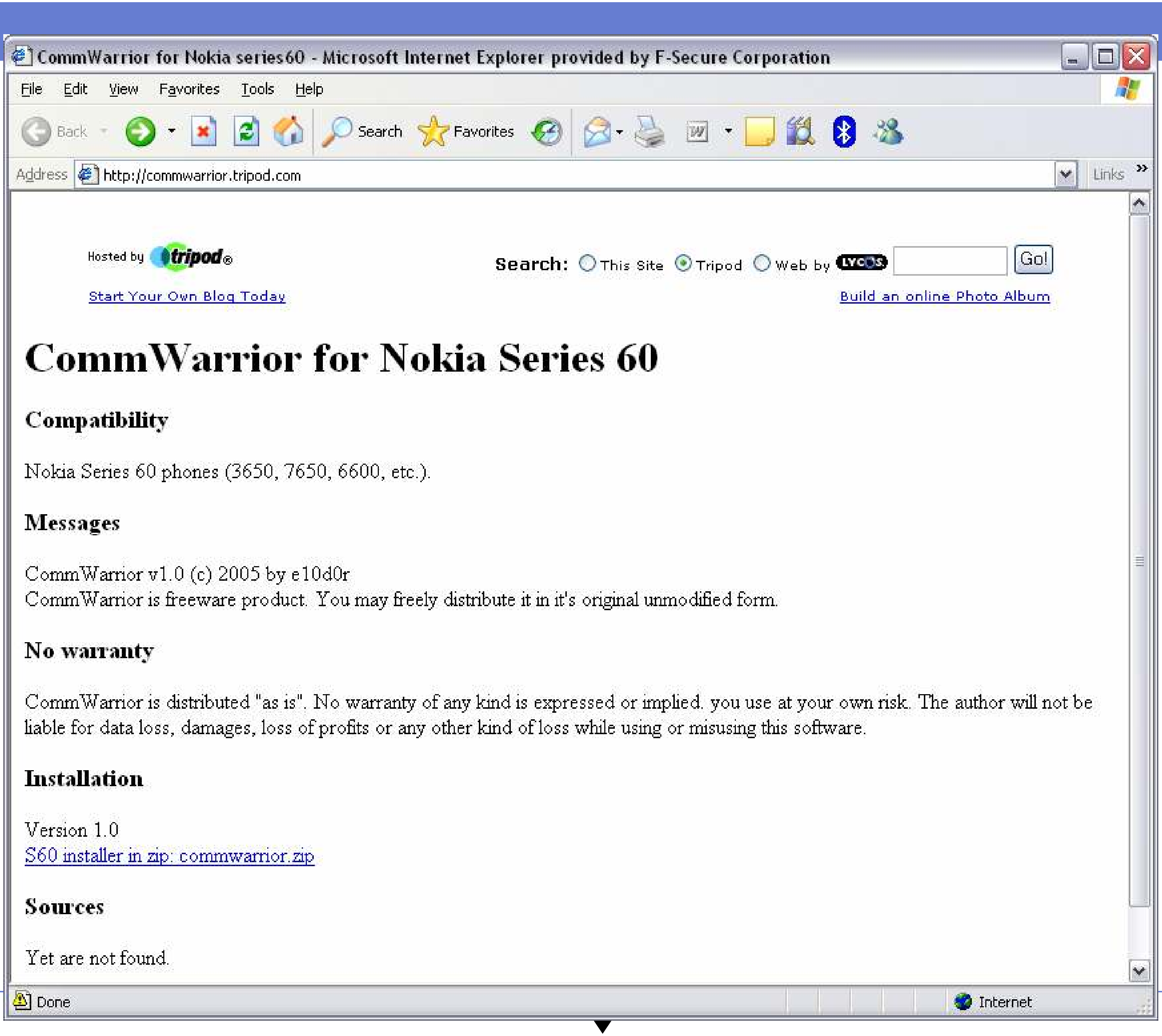
.:: i-Pho

1, 2, 3 ... 49, 50, 51 Next

Mark all topics read

```
                                                  2 0 0 4

                  Colin McRae Rally 2005 (c) Codemasters

   system.....: N-GAGE (Symbian)     date.......: 21/11/2004
   developer..: IdeaWorks3D :)       region.....: multi-5
   players....: 1-2 via bluetooth    disks......: xx/07

     game info

   A true legend joins the expanding roster of car games on the
   N-Gage, as Colin McRae Rally 2005 by Codemasters makes its debut
   on the world's freshest mobile gaming device. It is the ultimate
   rally game and one of the most popular motor sport franchises
   ever created.

   In Colin McRae Rally 2005 you grab a seat behind the steering
   wheel of the rally car of your choice. Explore racing locations
   around the world: race on the roads of 64 stages in eight
   different countries and work your way towards the championship.
   Tune up your car to match the conditions and beat the clock! The
   realistic simulations of road types, weather conditions, and
   physics of car handling create an authentic rally experience. The
   locations and the cars are real as well, your job is to provide
   the real driving!

   Multiplaying is the thing that really makes this game roar.
   Compete against the world's fastest rally gamers with Shadow
   Racing on the N-Gage Arena! You can also challenge your friend
   to a speedy duel over the wireless Bluetooth connection.

   * The legendary rally franchise by Codemasters now on N-Gage!

   * Realistic physics, authentic car handling, variable road types
     and changing weather conditions

   * 16 cars, including Peugeot, Subaru, Toyota and Audi

   * Performance tuning for tires, gears, power ratio, brake balance,
-- More --
```

Announcement: N- [Goto page: 1 ... 1				Mon Nov 29, 2004 12:19 evlspcmk
Announcement: LA CRACKED!!!! [Goto page: 1 ... 3				Mon Nov 29, 2004 6:04 jimma27
Announcement: Un [Goto page: 1 ... 1				Mon Nov 29, 2004 5:36 jimma27
Announcement: 66 [Goto page: 1 ... 4				Mon Nov 29, 2004 1:12 dzhun85
Announcement: Ne [Goto page: 1, 2,				Mon Nov 29, 2004 0:59 neojen
Announcement: SP [Goto page: 1 ... 1				Sun Nov 28, 2004 20:57 Leftfield
Announcement: 0- [Goto page: 1 ... 2				Sun Nov 28, 2004 20:56 Leftfield
Announcement: La [Goto page: 1 ... 6				Sun Nov 28, 2004 20:48 Leftfield
Announcement: Ph [Goto page: 1 ... 5				Sun Nov 28, 2004 20:47 Leftfield
Announcement: "0 [Goto page: 1 ... 7				Sun Nov 28, 2004 9:57 kurz
Announcement: Ph [Goto page: 1 ... 5				Sat Nov 27, 2004 23:43 michaelschumacher
Announcement: Mu [Goto page: 1 ... 5				Sat Nov 27, 2004 16:05 mastermale
Announcement: 0 I [Goto page: 1 ... 1				Fri Nov 26, 2004 5:55 Looptech
Sticky: Mango themes [Goto page: 1 ... 24, 25, 26]	377	koolmur2z	34424	Mon Nov 29, 2004 11:47 Indira Gandhi


CommWarrior for Nokia series60 - Microsoft Internet Explorer provided by F-Secure Corporation
File Edit View Favorites Tools Help
Back Search Favorites
Address http://commwarrior.tripod.com
Links
Hosted by tripod
Search: ○ This Site ● Tripod ○ Web by LYCOS Go!
Start Your Own Blog Today
Build an online Photo Album
Done
Internet

CommWarrior for Nokia Series 60

Compatibility

Nokia Series 60 phones (3650, 7650, 6600, etc.).

Messages

CommWarrior v1.0 (c) 2005 by e10d0r
CommWarrior is freeware product. You may freely distribute it in it's original unmodified form.

No warranty

CommWarrior is distributed "as is". No warranty of any kind is expressed or implied. you use at your own risk. The author will not be liable for data loss, damages, loss of profits or any other kind of loss while using or misusing this software.

Installation

Version 1.0
S60 installer in zip: commwarrior.zip

Sources

Yet are not found.

Commwarrior

By "e10d0r"

Symbian Series 60 virus

First virus to spread over MMS messages

Could potentially go global in just minutes

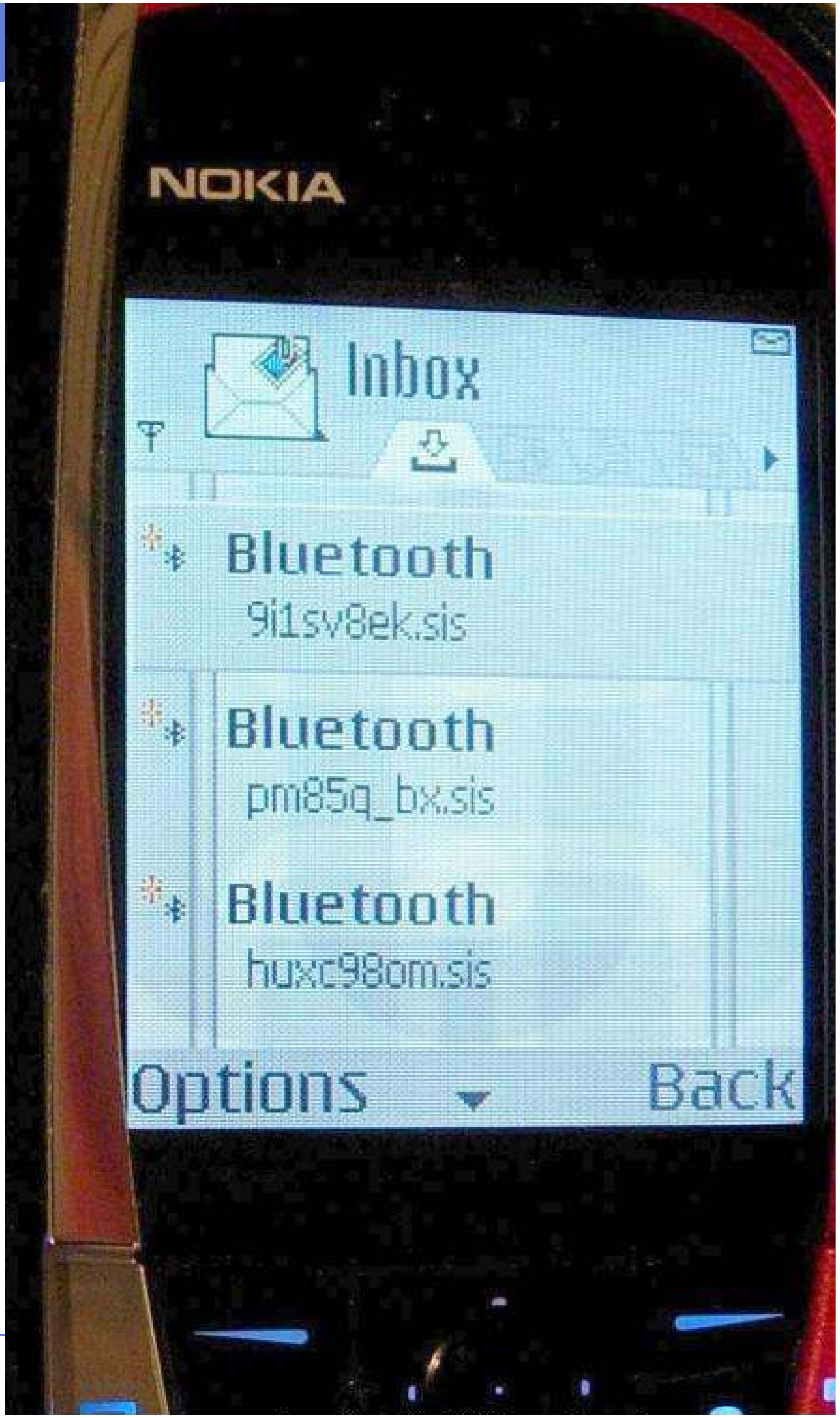
Also spreads over Bluetooth

Worst we've seen so far

But spreads surprisingly slow!

Could be really expensive

"OTMOP03KAM HET!"



Confirmed Commwarrior sightings

1. Ireland
2. India
3. Oman
4. Italy
5. Philippines
6. Finland
7. Greece
8. South Africa
9. Malaysia
10. Austria
11. Brunei
12. Germany
13. USA
14. Canada
15. UK
16. Romania
17. Poland
18. Russia

Receive message via Bluetooth from Nokia 6630?

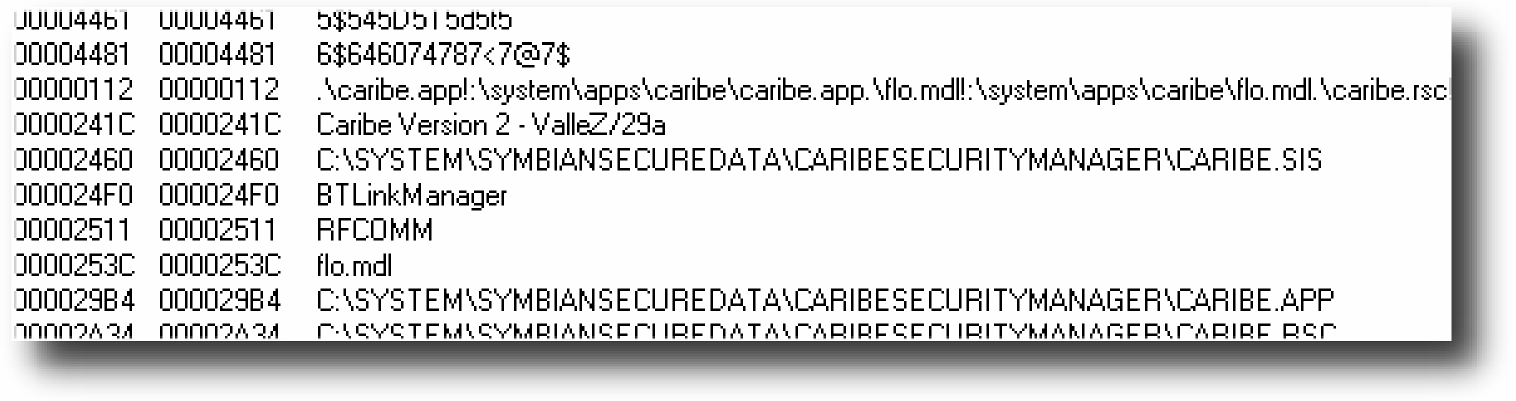
Commwarrior spreads very fast

Mabir

Written by "Vallez" of 29A

Spreads through both Bluetooth and MMS

Only sends itself to numbers which have sent MMS messages before



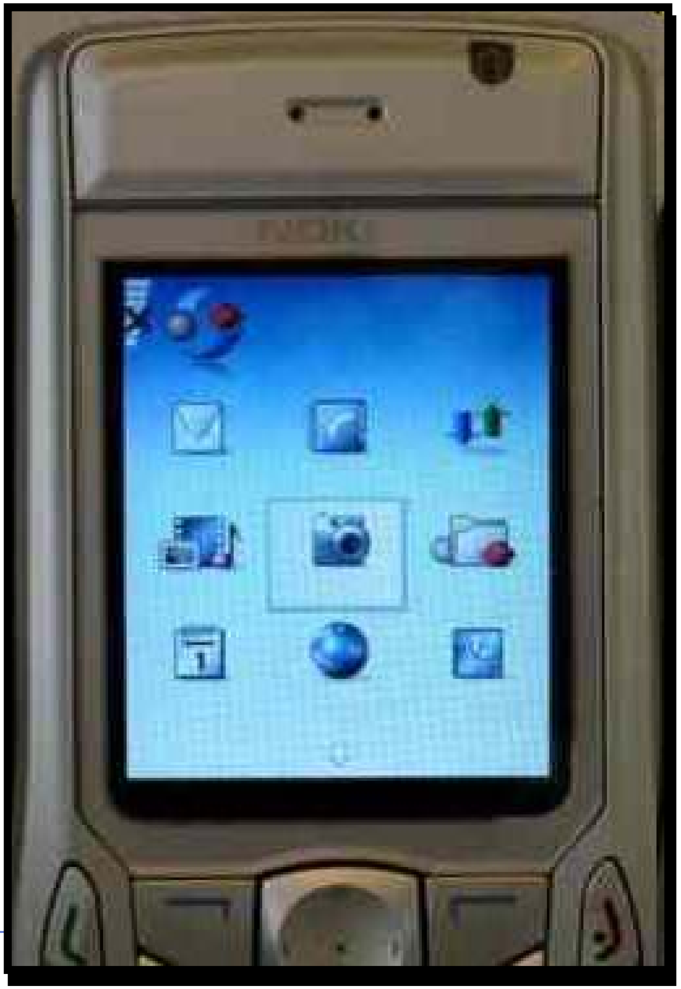
```
00004461  00004461   5$545D515d5f5
00004481  00004481   6$646074787<7@7$
00000112  00000112   .\caribe.app!:\system\apps\caribe\caribe.app.\flo.mdl!:\system\apps\caribe\flo.mdl.\caribe.rsc
0000241C  0000241C   Caribe Version 2 - ValleZ/29a
00002460  00002460   C:\SYSTEM\SYMBIANSECUREDATA\CARIBESECURITYMANAGER\CARIBE.SIS
000024F0  000024F0   BTLinkManager
00002511  00002511   RFCOMM
0000253C  0000253C   flo.mdl
000029B4  000029B4   C:\SYSTEM\SYMBIANSECUREDATA\CARIBESECURITYMANAGER\CARIBE.APP
00002A34  00002A34   C:\SYSTEM\SYMBIANSECUREDATA\CARIBESECURITYMANAGER\CARIBE.RSC
```

Blankfont

Found in August 2005

Makes all texts on the phone disappear

Tricky to clean



Doomboot

Claims to create phone ”skins” with pictures of pretty girls

Actually does what it claims

Also prevents the phone from booting up

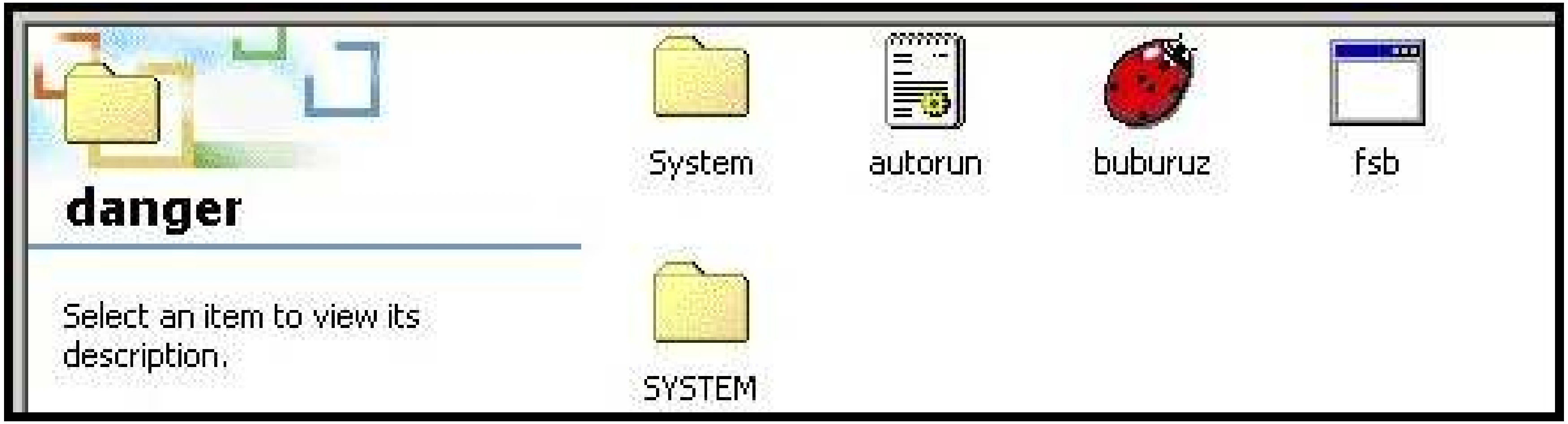
Several variants found

Cardtrap

Found last week

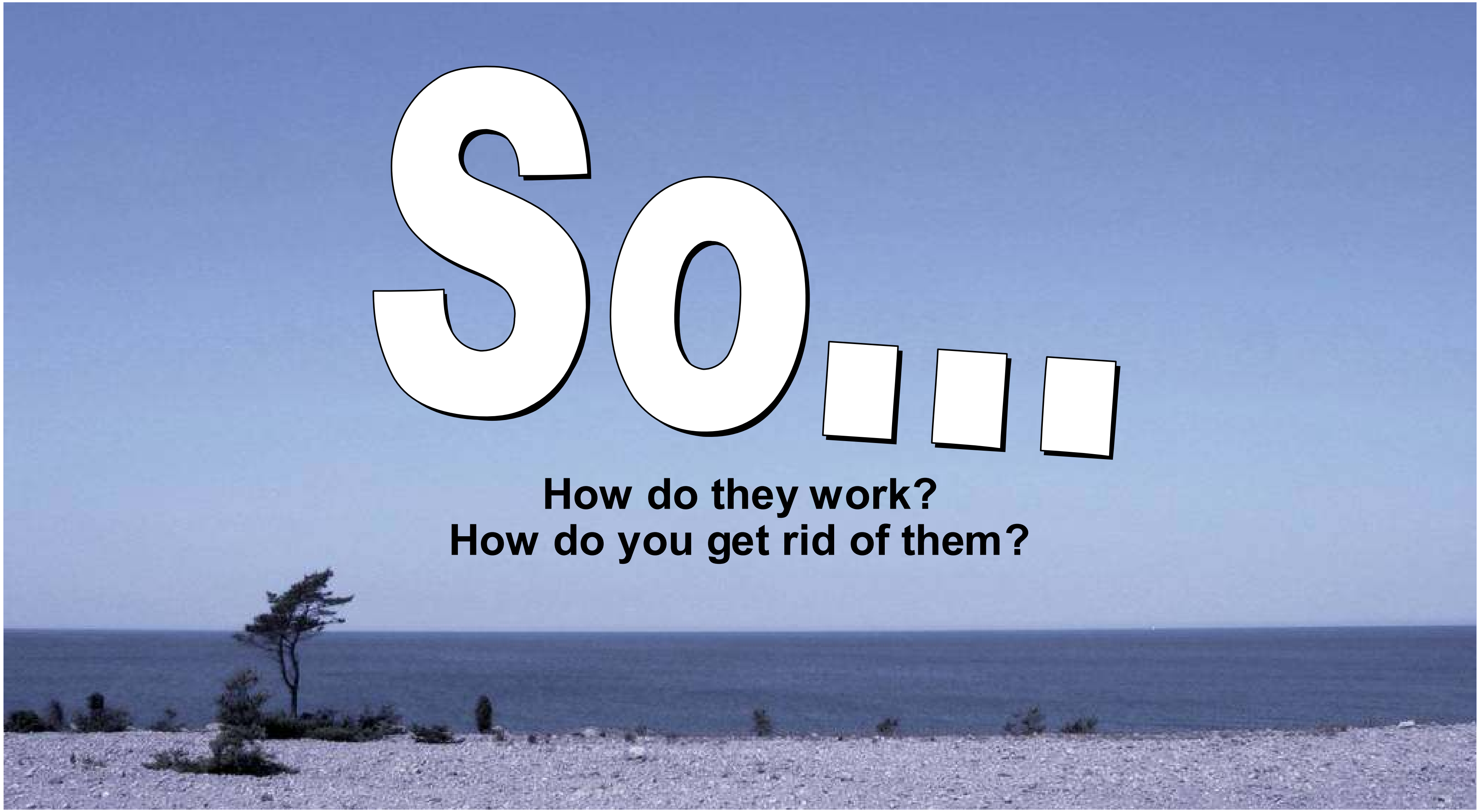
First mobile phone virus that tries to infect Windows PCs too

Drops two Windows viruses to phone’s memory card



Autostart.inf

A Korean manufacturer making USB sticks that claim to be a CD-ROM drive:
http://www.udrw.com/



So...

How do they work?
How do you get rid of them?

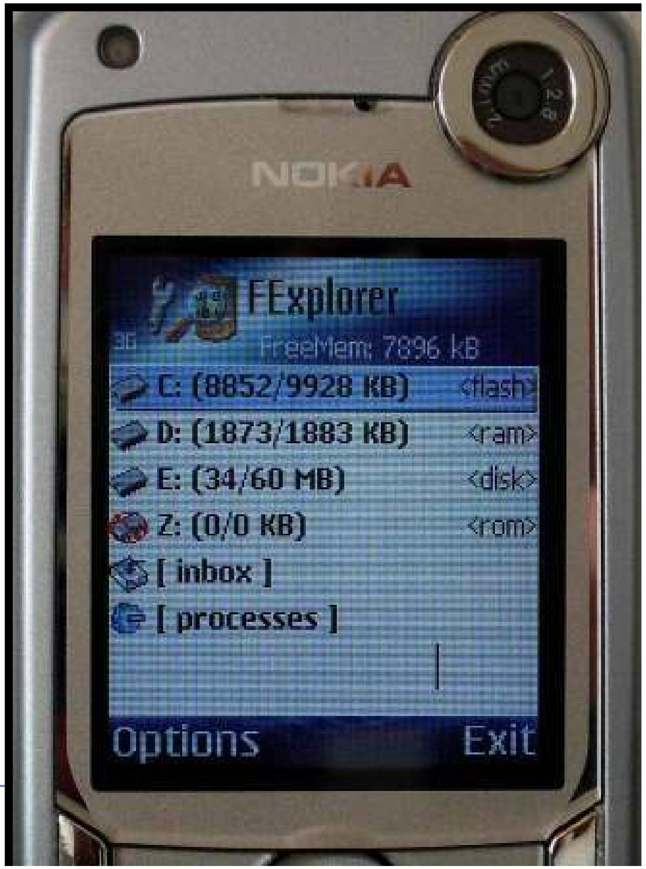
F-SECURE®

BE SURE.

Symbian filesystem

Default drives on Symbian phones:

C: FLASH RAM	User data and user installed applications
D: TEMP RAM	Temporary file storage for applications
E: MMC CARD	Removable disk / data & apps
Z: OS ROM	Flash drive / OS files



```
FreeMem: 7896 kB
C: (8852/9928 KB)   <flash>
D: (1873/1883 KB)   <ram>
E: (34/60 MB)       <disk>
Z: (0/0 KB)         <rom>
[ inbox ]
[ processes ]
```

Symbian Directory Architecture

All drives except D: have a “SYSTEM” directory

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

Most important directories

System\Apps	Applications that are visible to user
System\Recogs	Recognizer components
System\Install	Uninstall data
System\Libs	System and third party libraries

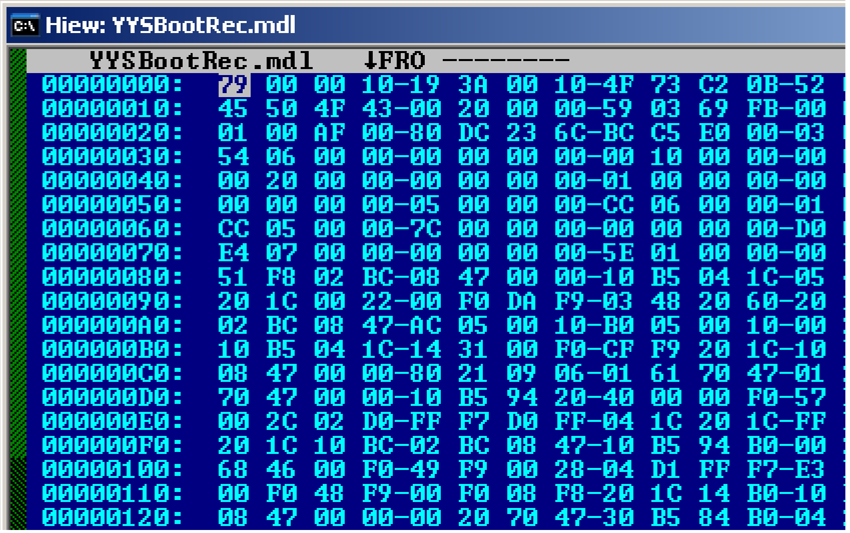
Symbian Executables

Symbian executables use unique identifiers

- Each application has unique 32-bit UID
- 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
- Foo.EXE Command line applications and servers
  - Cannot be accessed by user
- Foo.MDL Recognizer components
  - Provide file association services
  - Start automatically



Hiew: YYSBootRec.mdl

```
    YYSBootRec.mdl    ↓FRO ---------
00000000:  79 00 00 10-19 3A 00 10-4F 73 C2 0B-52
00000010:  45 50 4F 43-00 20 00 00-59 03 69 FB-00
00000020:  01 00 AF 00-80 DC 23 6C-BC C5 E0 00-03
00000030:  54 06 00 00-00 00 00 00-00 10 00 00-00
00000040:  00 20 00 00-00 00 00 00-01 00 00 00-00
00000050:  00 00 00 00-05 00 00 00-CC 06 00 00-01
00000060:  CC 05 00 00-7C 00 00 00-00 00 00 00-D0
00000070:  E4 07 00 00-00 00 00 00-5E 01 00 00-00
00000080:  51 F8 02 BC-08 47 00 00-10 B5 04 1C-05
00000090:  20 1C 00 22-00 F0 DA F9-03 48 20 60-20
000000A0:  02 BC 08 47-AC 05 00 10-B0 05 00 10-00
000000B0:  10 B5 04 1C-14 31 00 F0-CF F9 20 1C-10
000000C0:  08 47 00 00-80 21 09 06-01 61 70 47-01
000000D0:  70 47 00 00-10 B5 94 20-40 00 00 F0-57
000000E0:  00 2C 02 D0-FF F7 D0 FF-04 1C 20 1C-FF
000000F0:  20 1C 10 BC-02 BC 08 47-10 B5 94 B0-00
00000100:  68 46 00 F0-49 F9 00 28-04 D1 FF F7-E3
00000110:  00 F0 48 F9-00 F0 08 F8-20 1C 14 B0-10
00000120:  08 47 00 00-00 20 70 47-30 B5 84 B0-04
```

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
- Etc

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 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

Extended Theme.sis
Nokia Application Installer file
1,165 KB

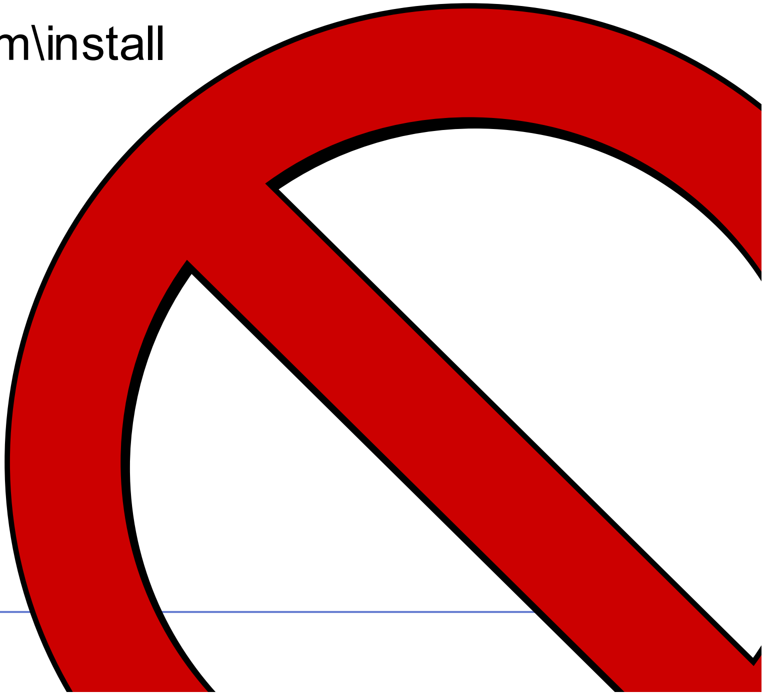
SIS contents of Doomboot.F

```
"About0.txt"-"",FT,TC
"ETel.dll"-"C:\ETel.dll"
"Part 2.sis"-"C:\Part 2.sis"
"Speed Overclock v3.41.sis"-"C:\Speed Overclock v3.41.sis"
"Your Welcome.gif"-"C:\Your Welcome.gif"
"Hat.mbm"-"C:\system\skins\b27724821b7e1846\Hat.mbm"
"Hat.skn"-"C:\system\skins\b27724821b7e1846\Hat.skn"
```

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
- Deleting it’s own uninstall SIS from system\install



Symbian Application Loading

Symbian uses a weird way of launching applications

- 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

<u>If an application in C: has the same name and path as one in Z: it will replace application in ROM</u>

- 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

How to work with an infected phone?

Built-in process list

- Keep ”Menu” down for a while
- You’ll get a list showing GUI processes. Cabir is visible, Commwarrior isn’t
- Kill processes by pressing ”C”

Process viewer

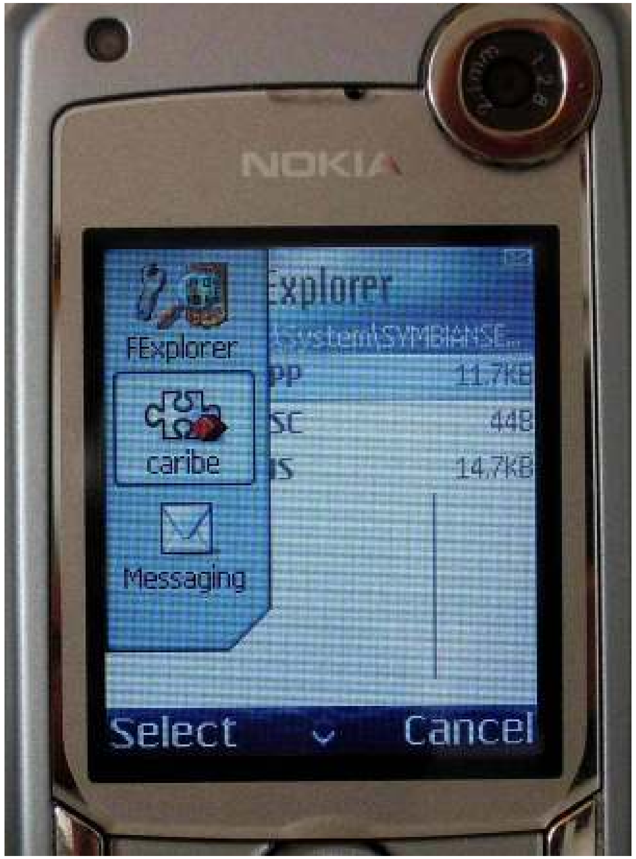
- Shows all processes http://www.microdene.com/

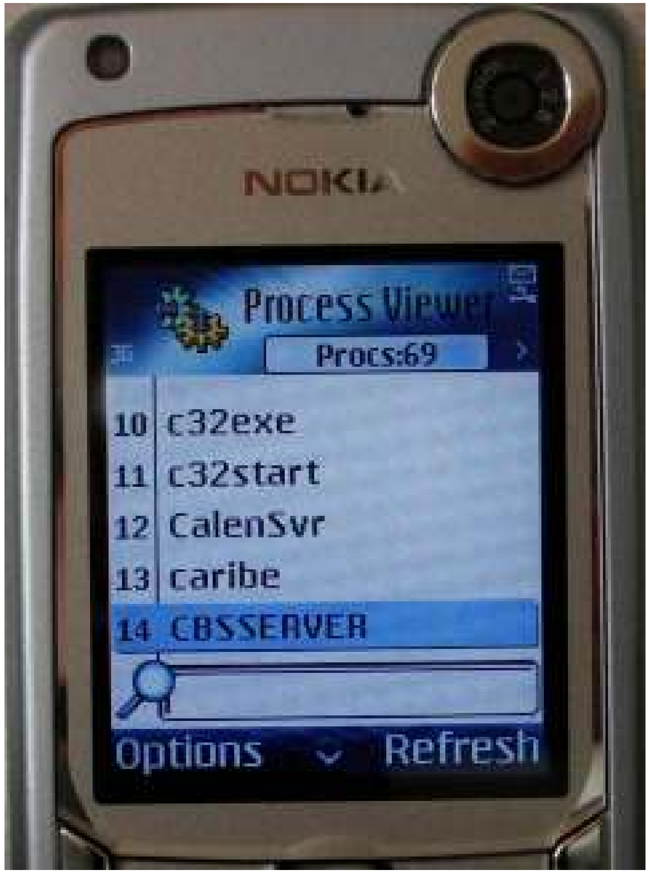
File Managers

- Fexplorer http://users.skynet.be/domi/
  - Simple & fast.
- EFileManager http://www.psiloc.com/
  - Takes a full image of the phone

F-SECURE

Process list





```
10 c32exe
11 c32start
12 CalenSvr
13 caribe
14 CBSSERVER
```

What to do to an infected phone?

Don’t Panic!

Move away from crowds

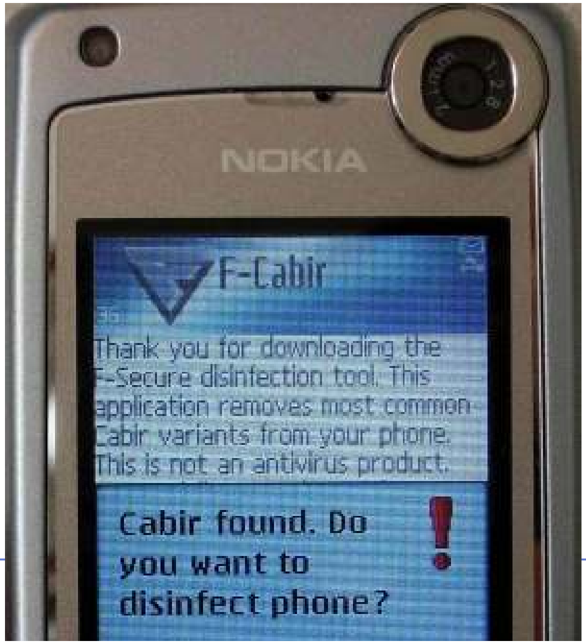
Check Symbian process list

Kill unknown processes (free$8, Caribe, Tee222)

Scan the phone with anti-virus tools

Available for free from http://mobile.f-secure.com (or phoneav.com)

- F-Secure Mobile Anti-Virus
- F-Cabir
- F-Commwarrior
- F-Skulls
- F-Locknut



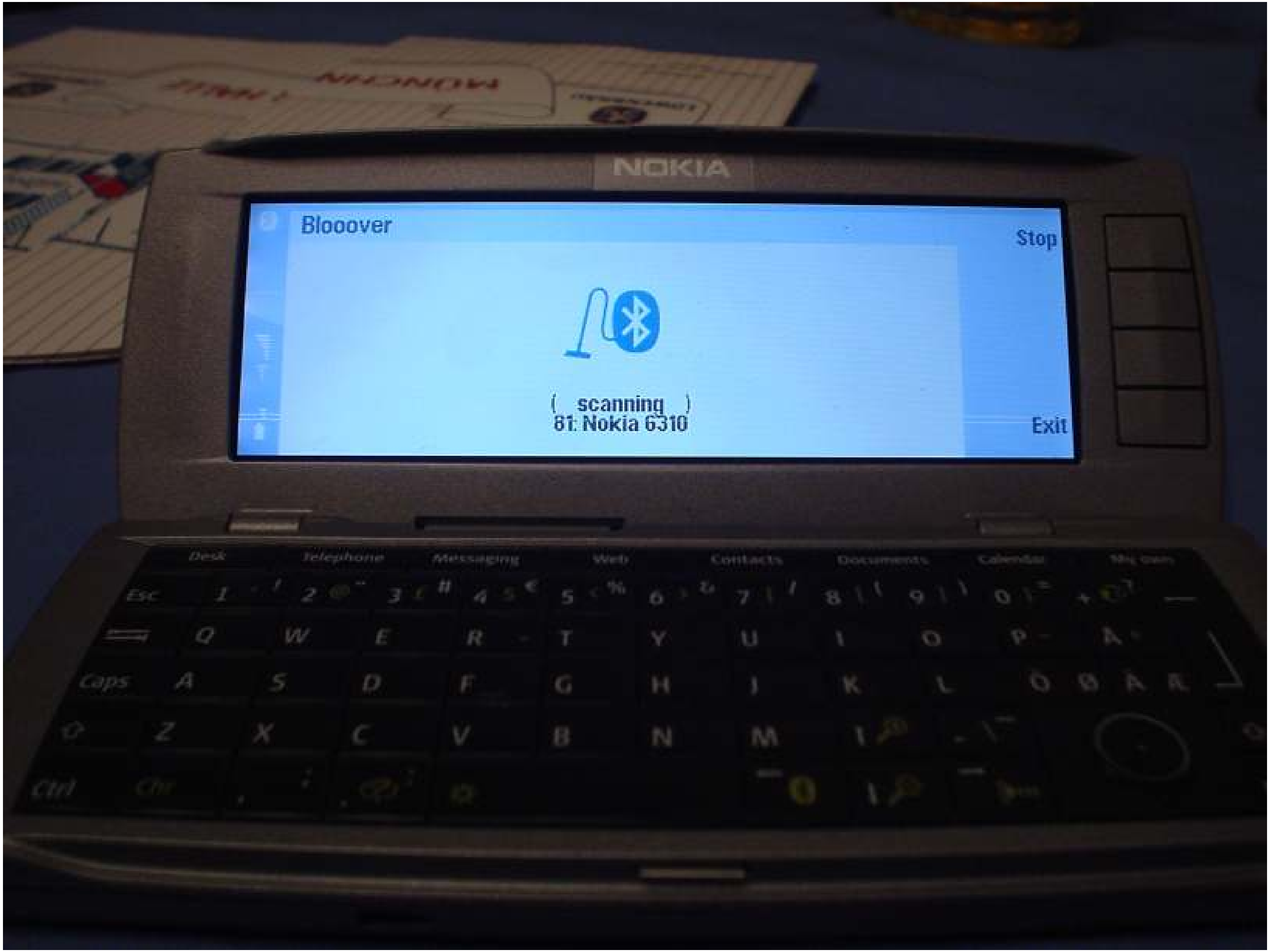
F-Cabir

Thank you for downloading the F-Secure disinfection tool. This application removes most common Cabir variants from your phone. This is not an antivirus product.

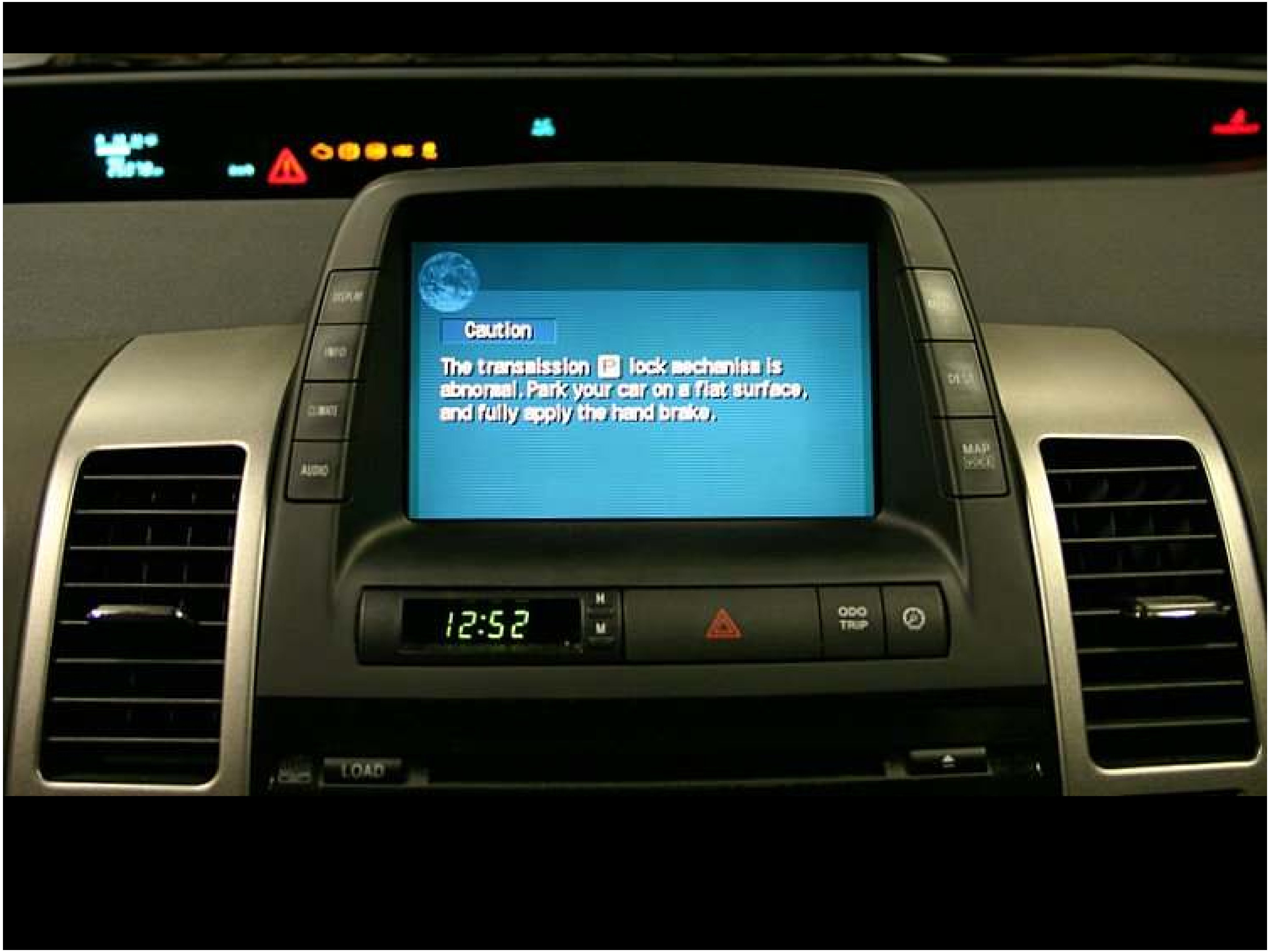
Cabir found. Do you want to disinfect phone?

DÈMÖ

Image Copyright (c) Flexilis


NOKIA
Blooover
Stop
(scanning)
81: Nokia 6310
Exit

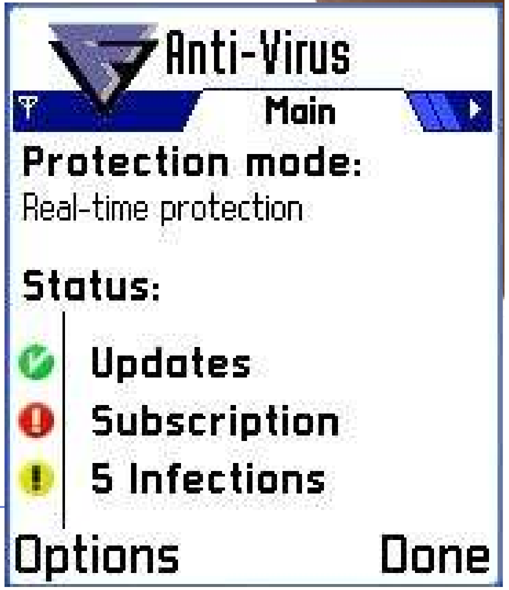
yota Prius.
Vuoden Auto 2005
Vuoden A
Toyota Prius.
CAR
YEAR
2005
Toyota Prius.
Vuoden Auto 2005.
OPG-454



Caution

The transmission P lock mechanism is abnormal. Park your car on a flat surface, and fully apply the hand brake.

F-Secure antivirus system for phones

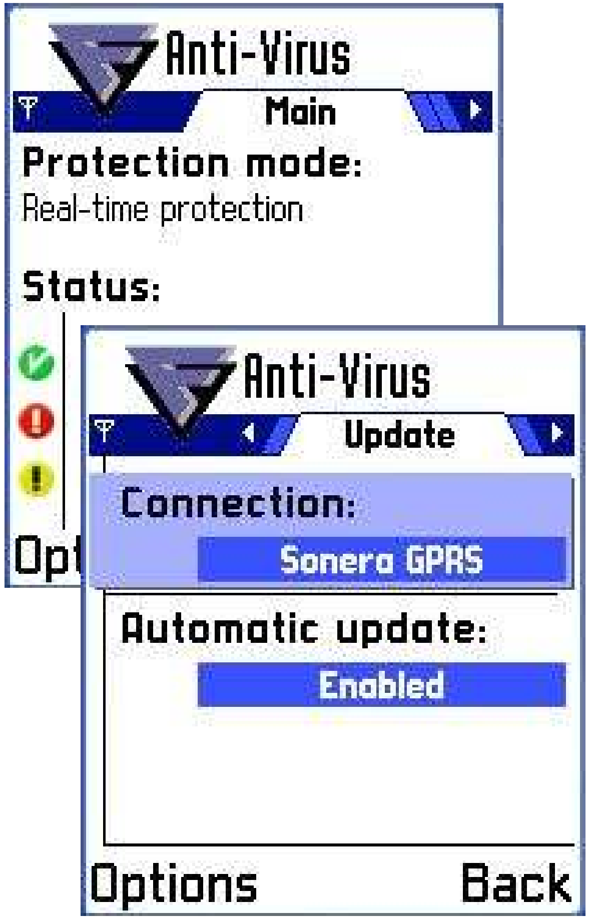


Protection mode:
Real-time protection

Status:

- ✓ Updates
- ! Subscription
- ! 5 Infections

Mobile antivirus solutions



Protection mode:
Real-time protection

Connection:
Sonera GPRS

Automatic update:
Enabled

Real-time scanning is the only way to ensure protection at all times

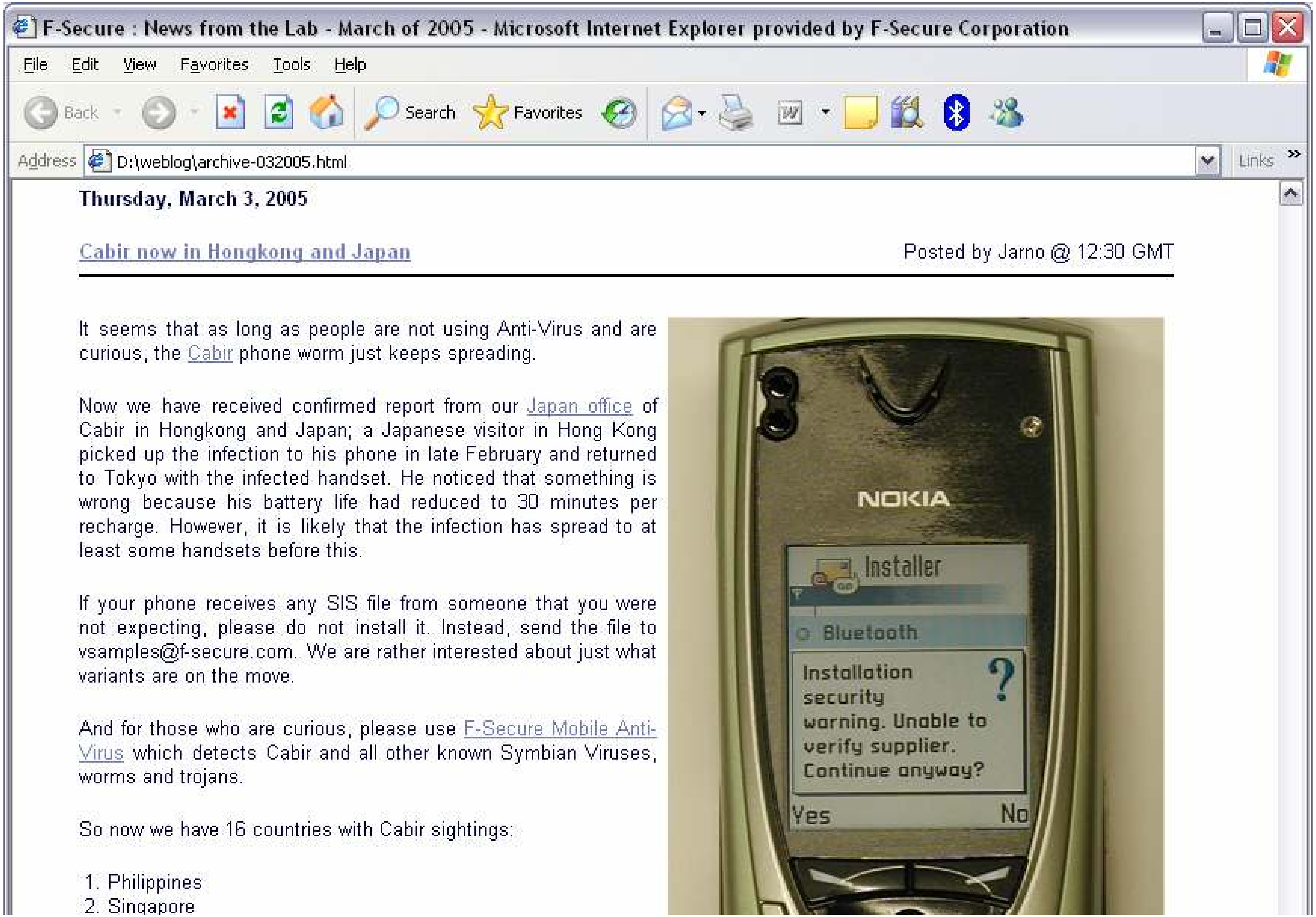
For mobile devices with a multitude of connectivity options, antivirus updates need to distributed over-the-air, directly to the device

MMS viruses can be scanned by the operator – Bluetooth viruses can't

Protection that relies on user interaction is never up-to-date

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

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

NOKIA
Installer
Bluetooth
Installation security warning. Unable to verify supplier. Continue anyway?
Yes
No

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