KASPERSKY lab

# The Underground Economy and Ecosystem of SMS Based Cybercrime

Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab

15.06.2011, 23rd Annual FIRST Conference, Vienna, Austria

# Agenda

- **SMS based threats**
  - Ransomware
  - SMS Trojans
- The **ecosystem**
- **Underground economy**
- **Threats round** the **globe**
- **What should we do?**

# Lottery

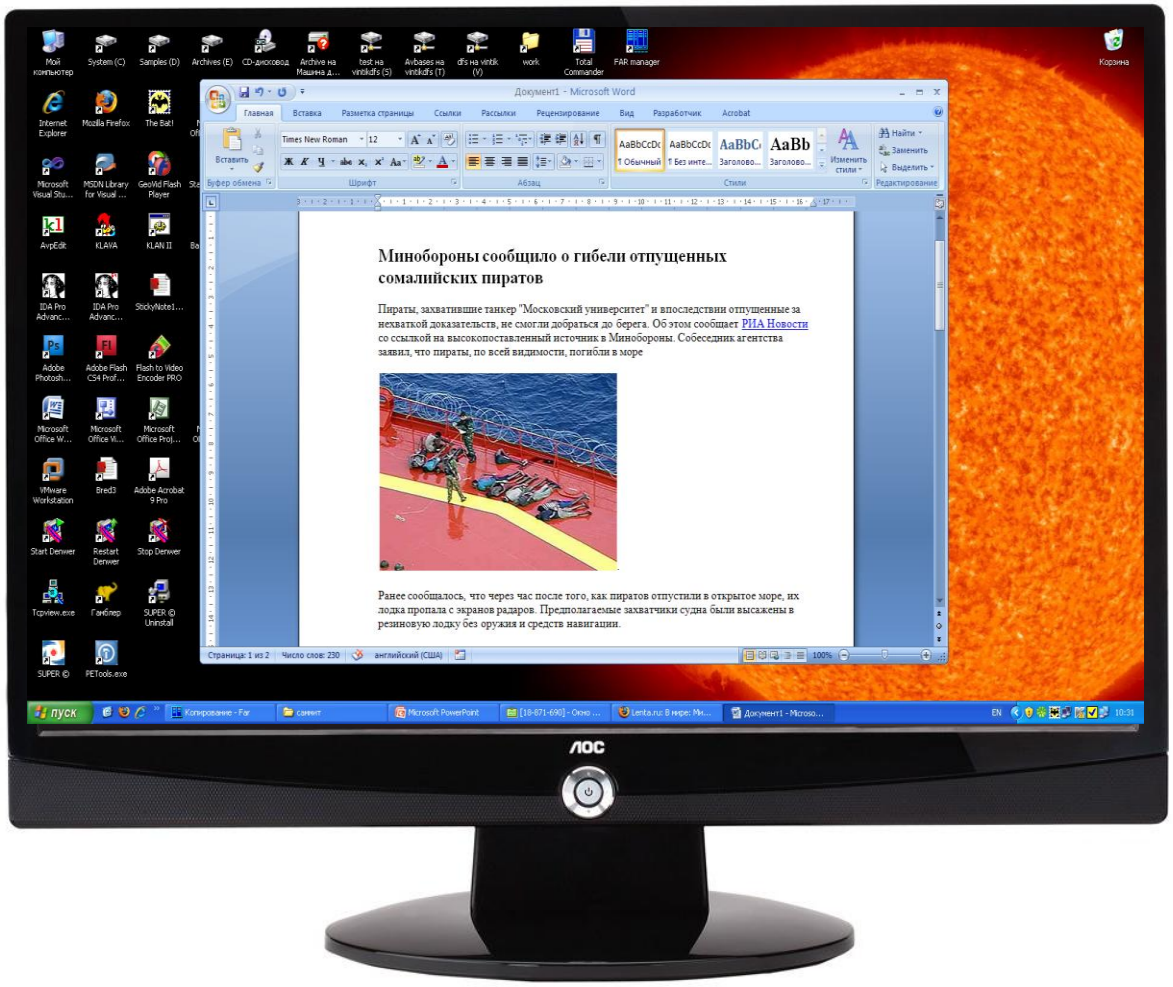
# How much have users lost?

# Ransomware

KASPERSKY lab

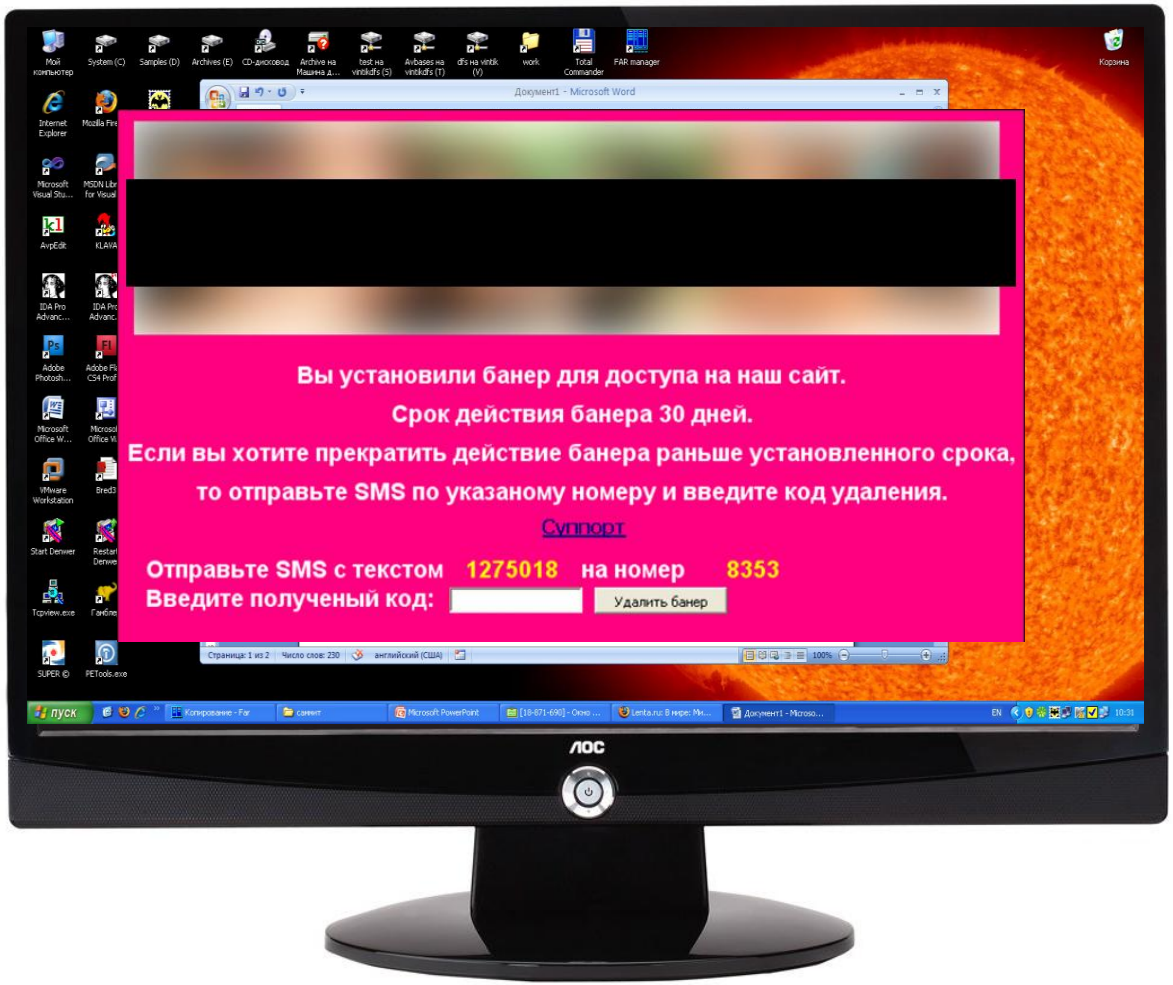
# Ransomware

## In a nutshell



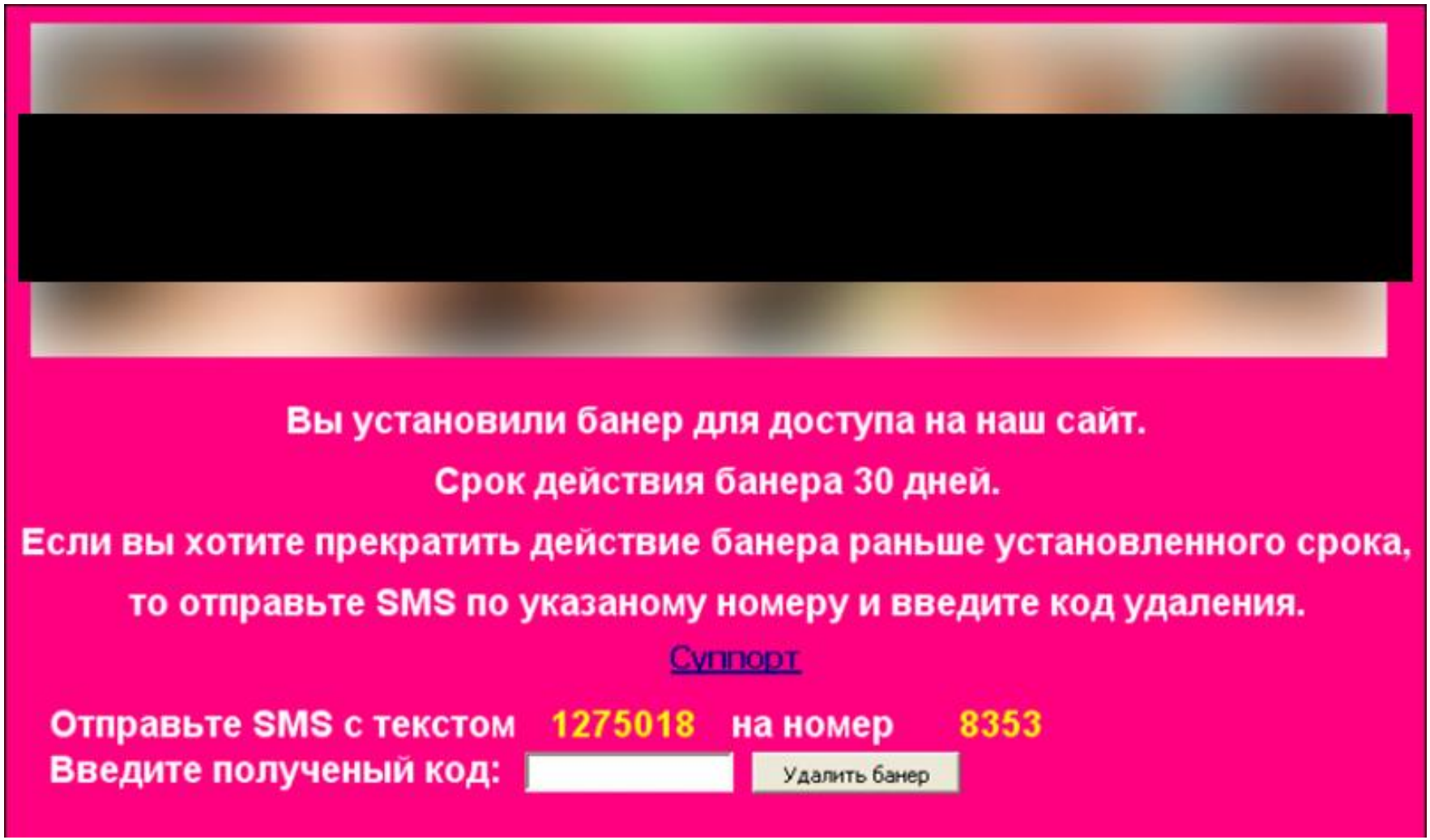
# Ransomware

## In a nutshell



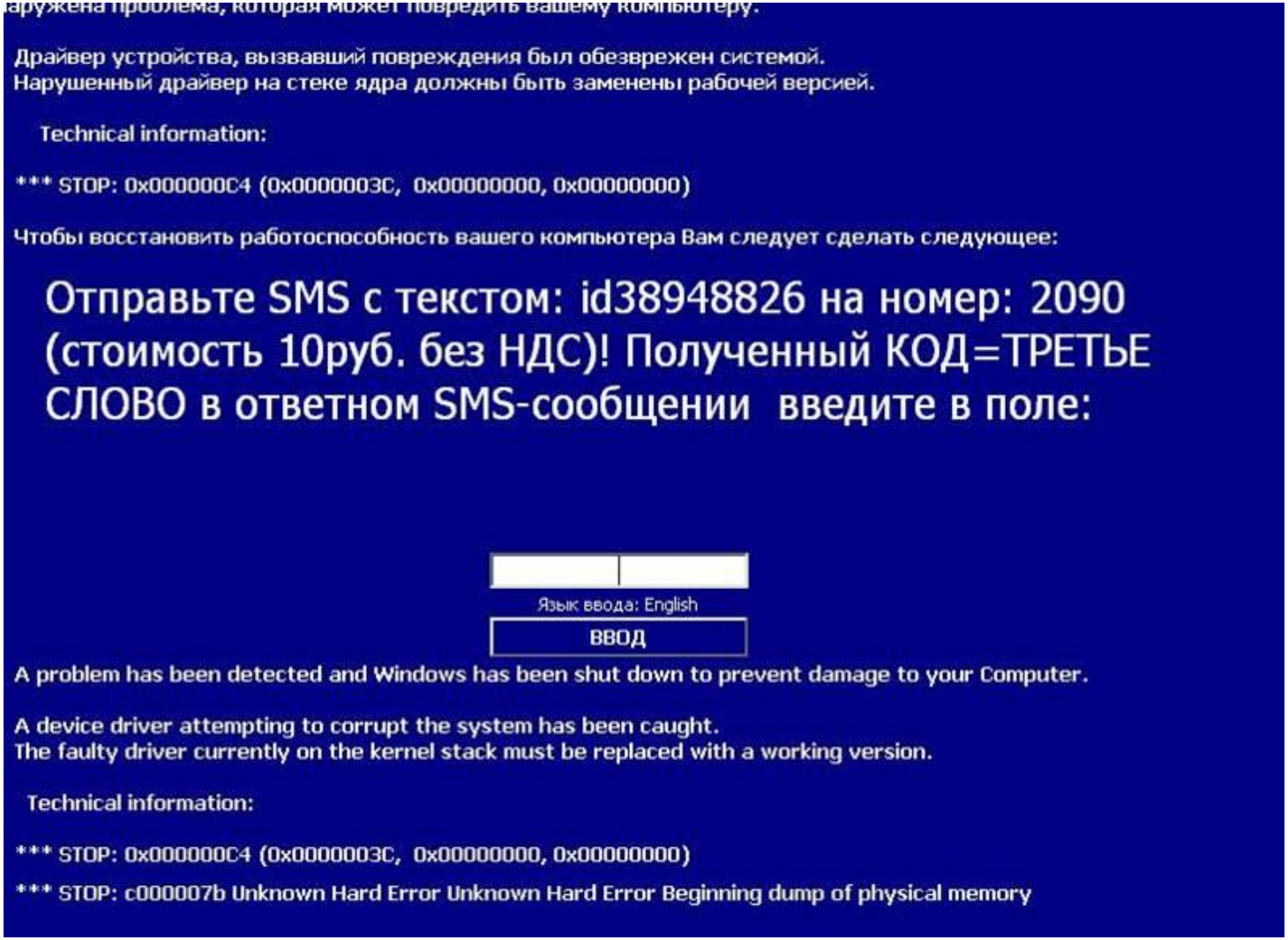
# Ransomware

## Variety



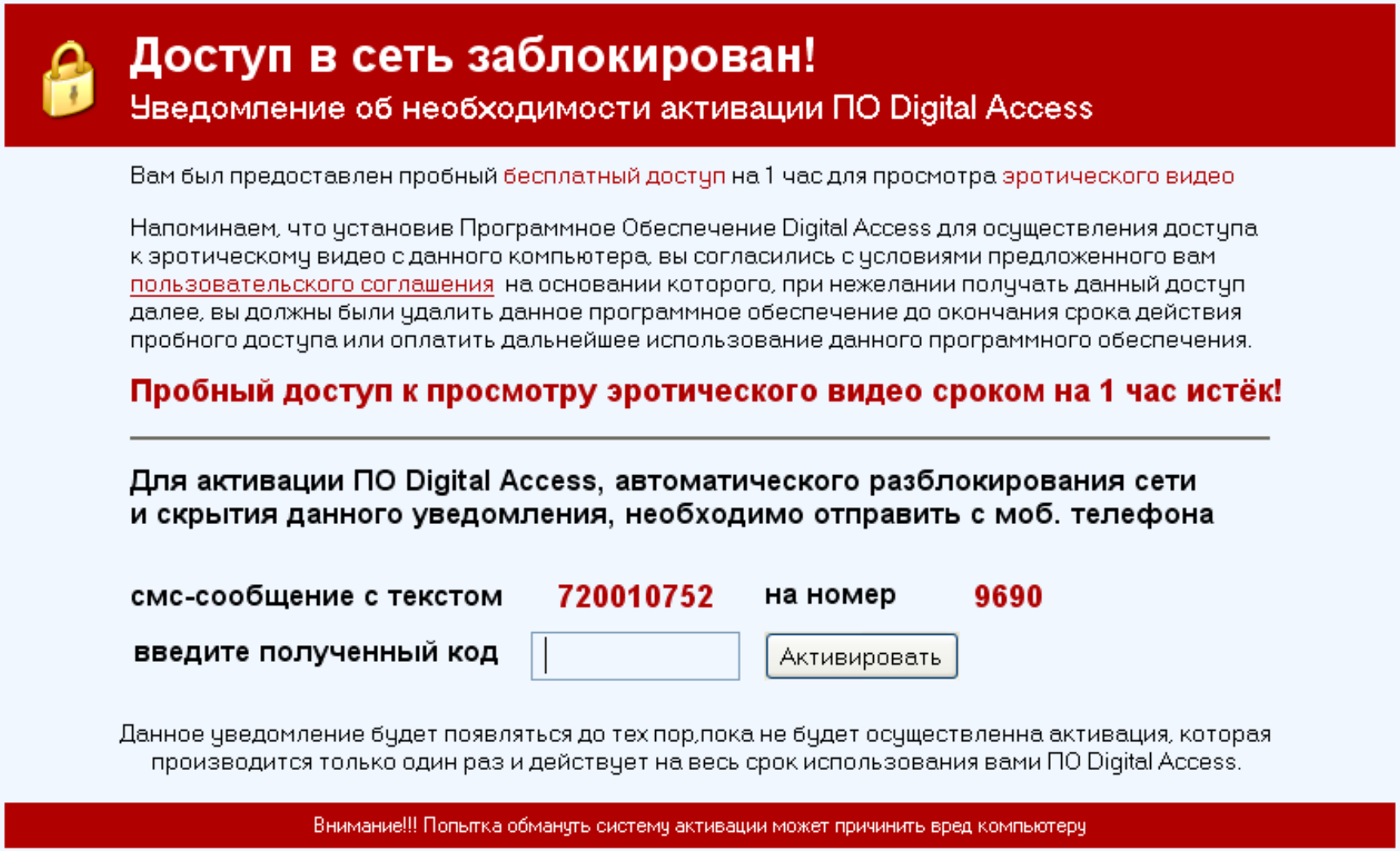
# Ransomware

## Variety



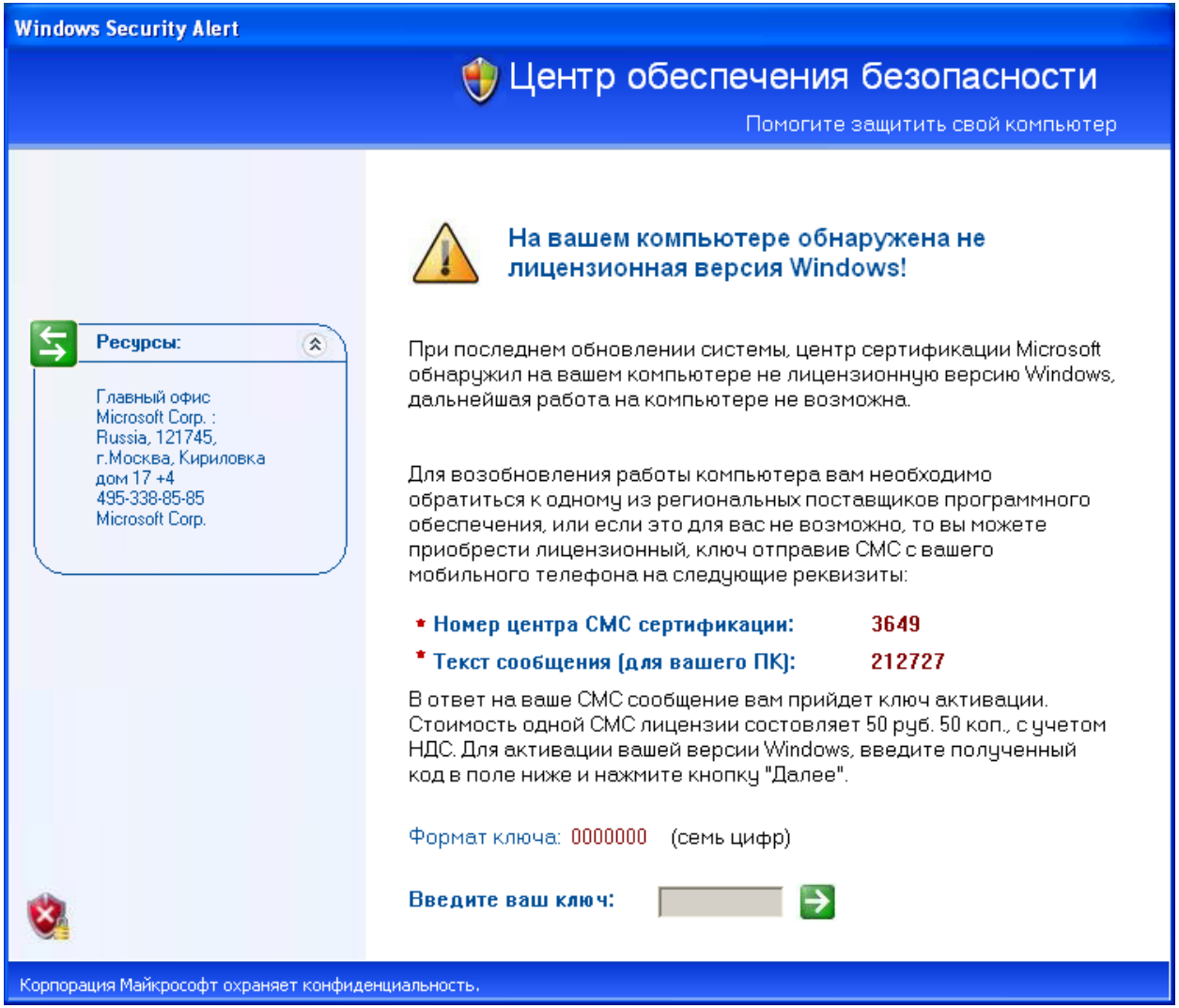
# Ransomware

## Variety



# Ransomware

## Variety

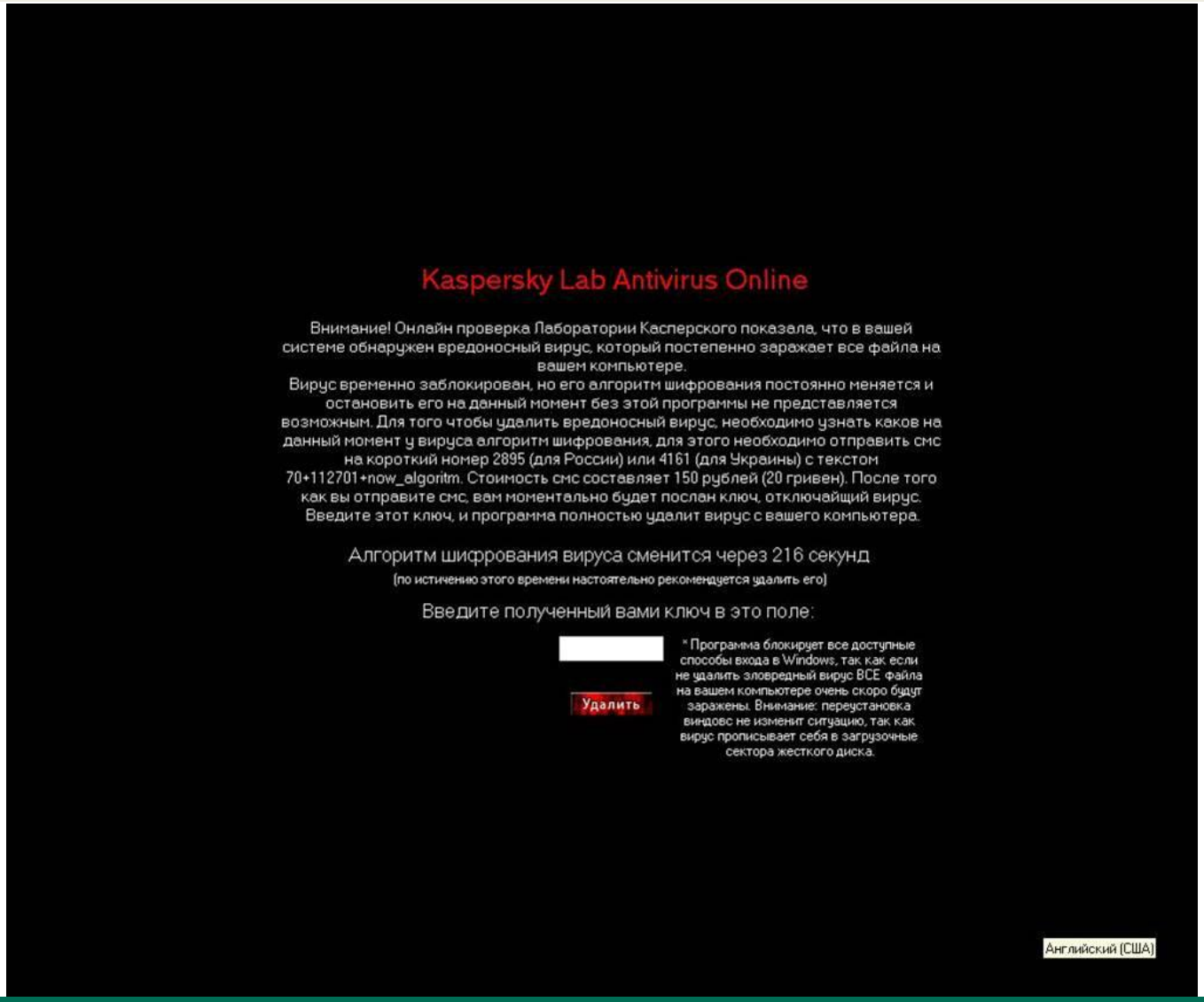


# Ransomware

## Variety

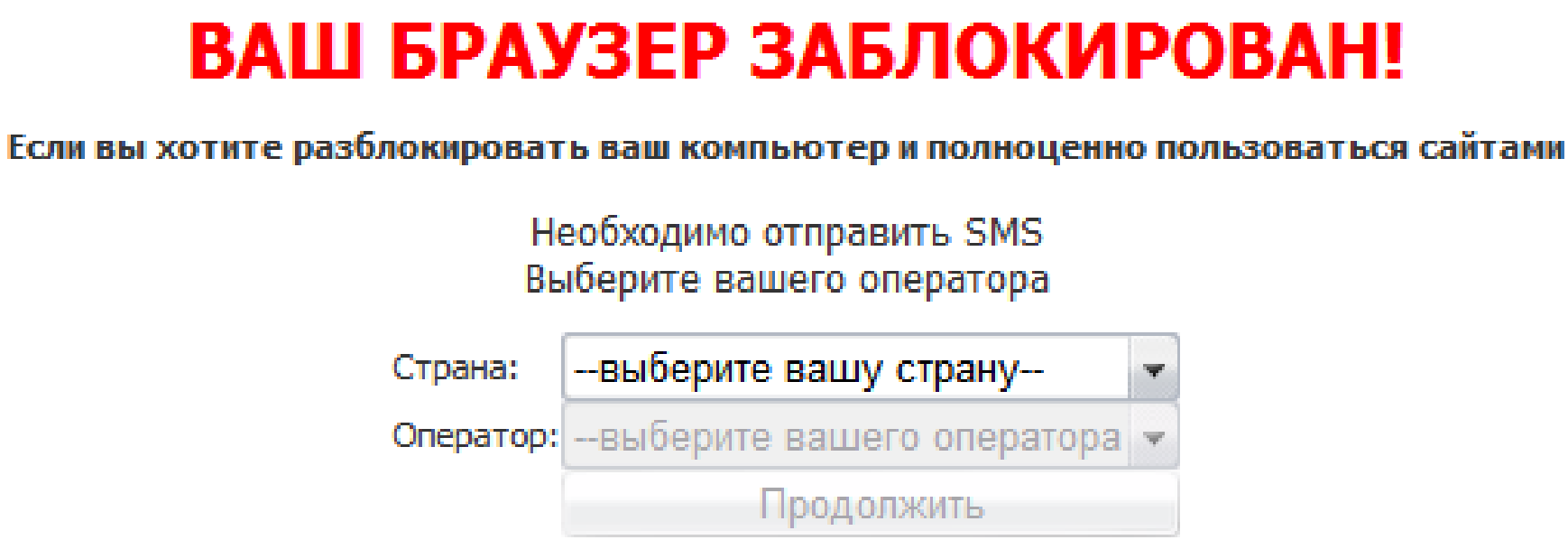
# Ransomware

## Variety



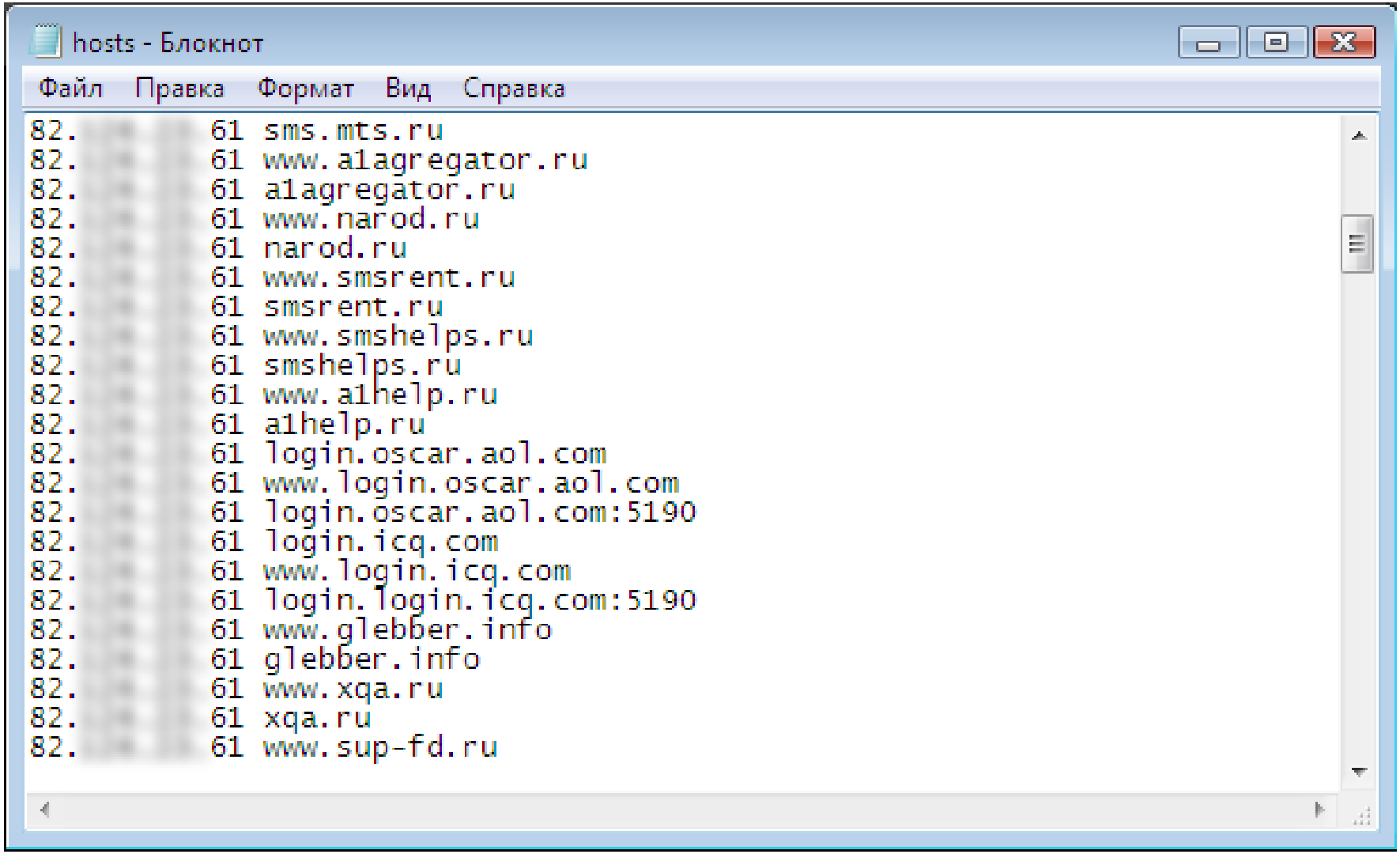
# Ransomware

## Variety



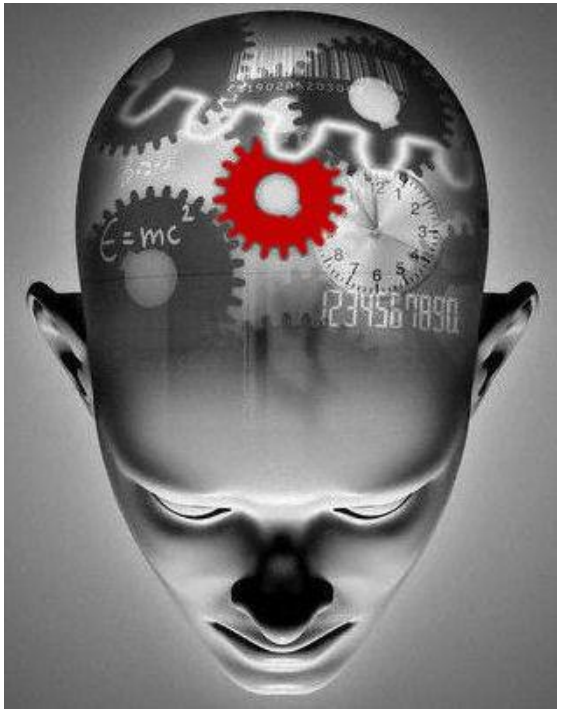
# Ransomware

## Variety



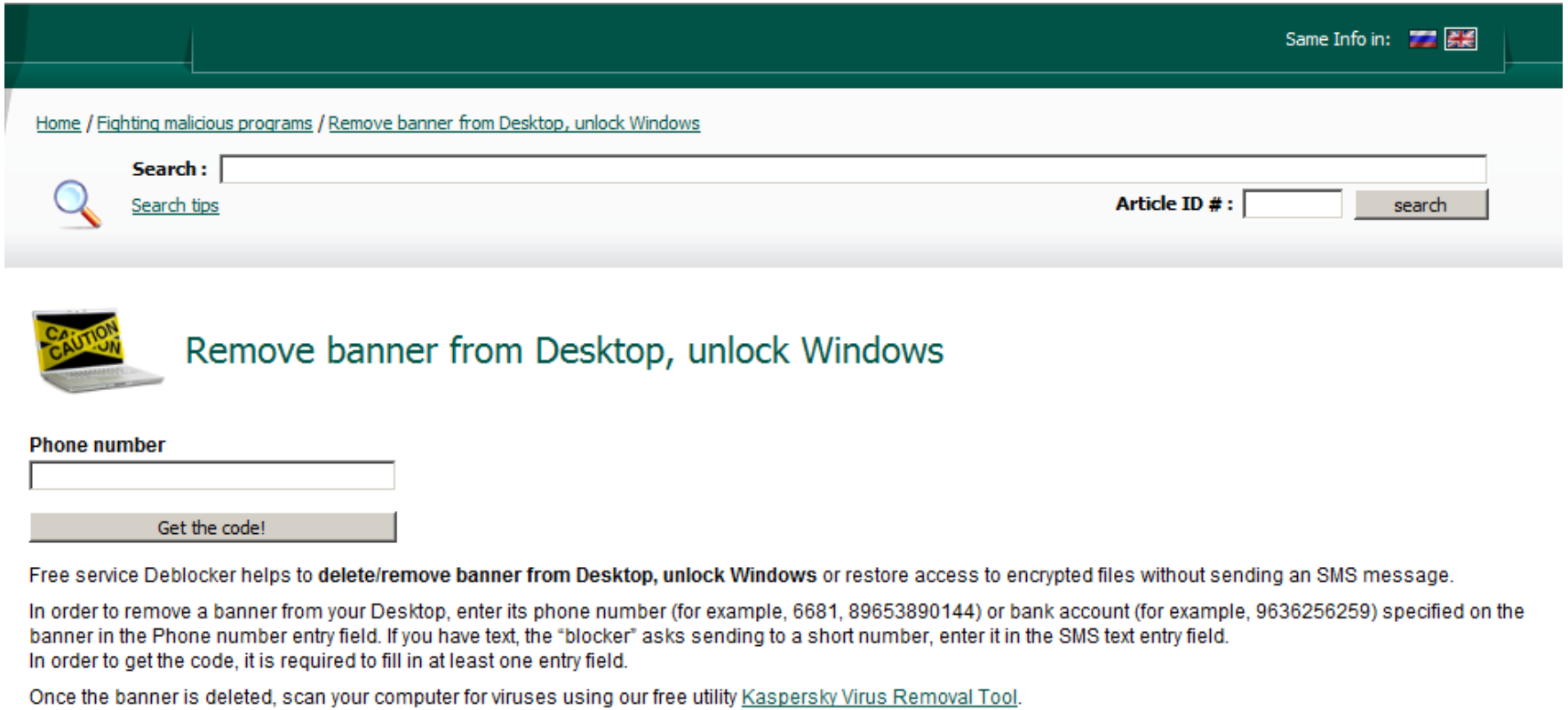
# Psychological tricks

- Legal prosecution threats
- Data corruption threats
- Malware infection (!) threats
- Annoying pop-ups

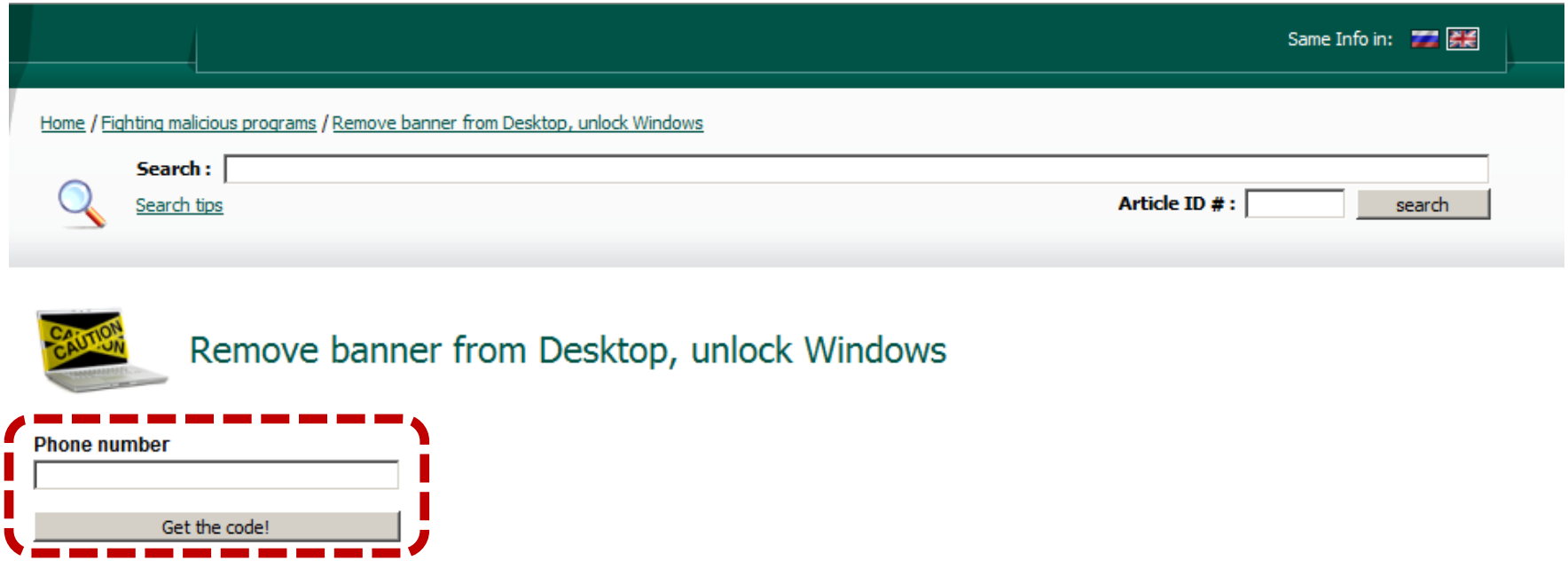


# What do they want?

# Deblocker


Same Info in:
Home / Fighting malicious programs / Remove banner from Desktop, unlock Windows
Search :
Search tips
Article ID # :
search
Remove banner from Desktop, unlock Windows
Phone number
Get the code!
Free service Deblocker helps to delete/remove banner from Desktop, unlock Windows or restore access to encrypted files without sending an SMS message.
In order to remove a banner from your Desktop, enter its phone number (for example, 6681, 89653890144) or bank account (for example, 9636256259) specified on the banner in the Phone number entry field. If you have text, the "blocker" asks sending to a short number, enter it in the SMS text entry field.
In order to get the code, it is required to fill in at least one entry field.
Once the banner is deleted, scan your computer for viruses using our free utility Kaspersky Virus Removal Tool.

# Deblocker


Same Info in:
Home / Fighting malicious programs / Remove banner from Desktop, unlock Windows
Search :
Search tips
Article ID # :
search
Remove banner from Desktop, unlock Windows
Phone number
Get the code!
Free service Deblocker helps to delete/remove banner from Desktop, unlock Windows or restore access to encrypted files without sending an SMS message.
In order to remove a banner from your Desktop, enter its phone number (for example, 6681, 89653890144) or bank account (for example, 9636256259) specified on the banner in the Phone number entry field. If you have text, the "blocker" asks sending to a short number, enter it in the SMS text entry field.
In order to get the code, it is required to fill in at least one entry field.
Once the banner is deleted, scan your computer for viruses using our free utility Kaspersky Virus Removal Tool.

# Deblocker service statistics

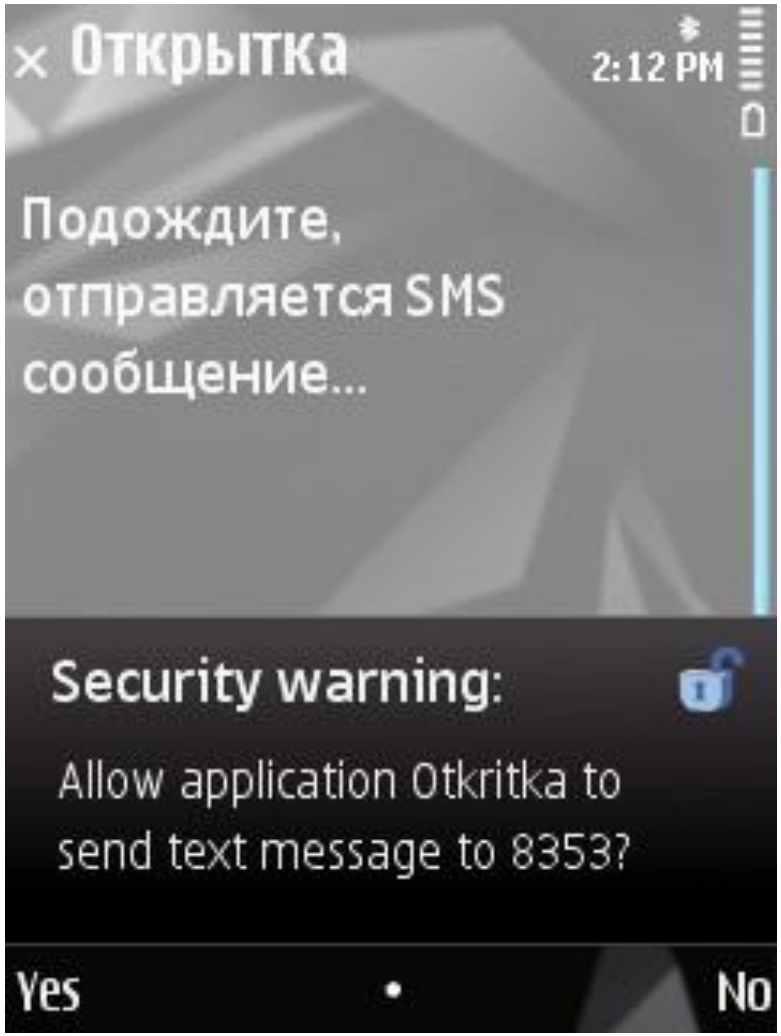
- **Launch: January 2010**
- **Current state:**
  - More than **5,100,000 unique visitors**
  - More than **19,500,000 requests**
  - **~60,000 unique visitors per day**
  - **~230,000 requests per day**

Source: Kaspersky Lab

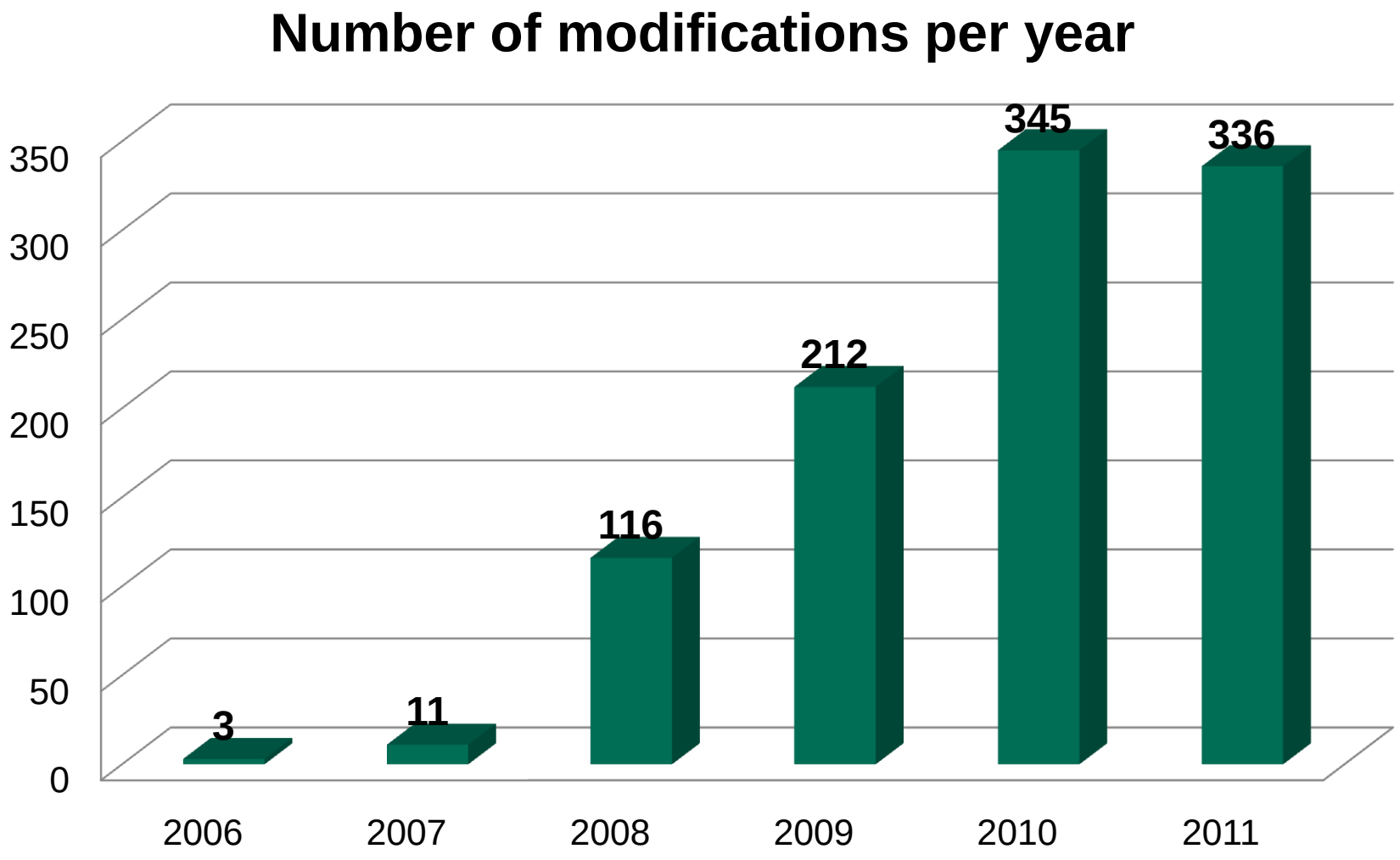
# SMS Trojans

# SMS Trojans

## In a nutshell



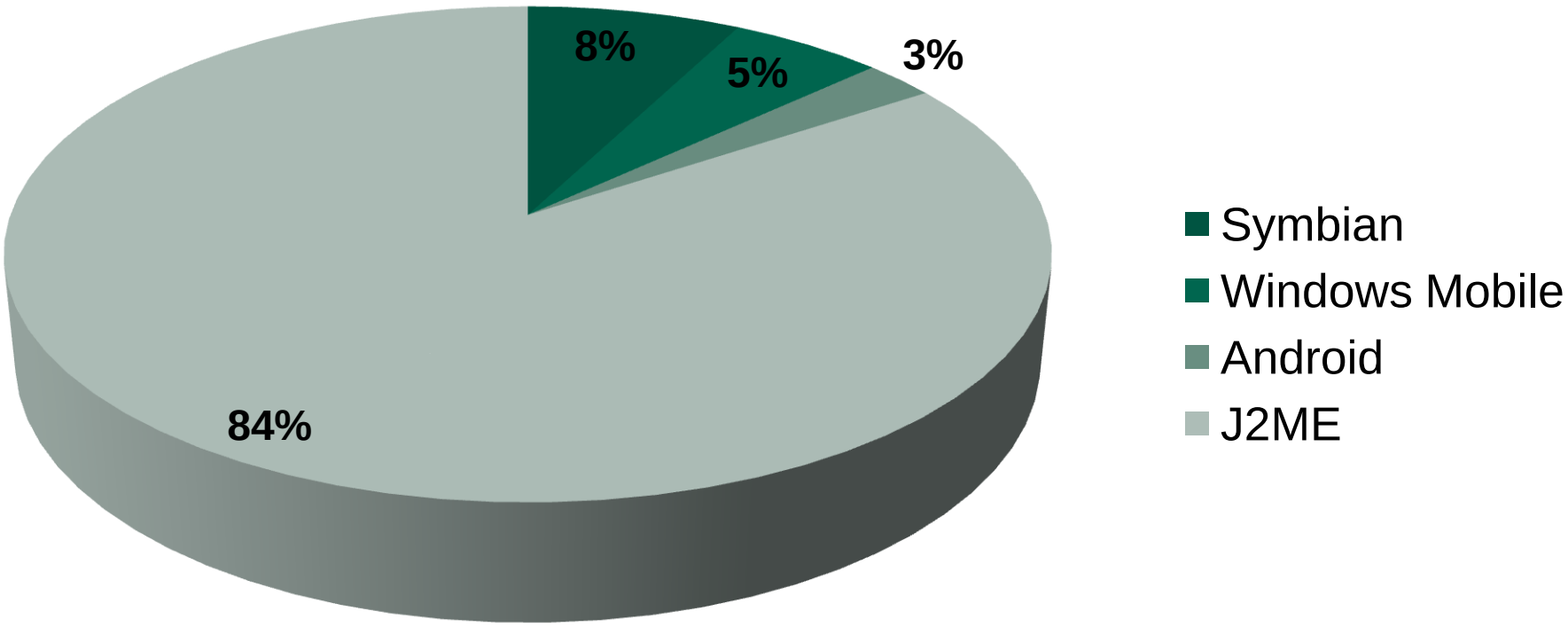
# Statistics




Source: Kaspersky Lab

# Statistics

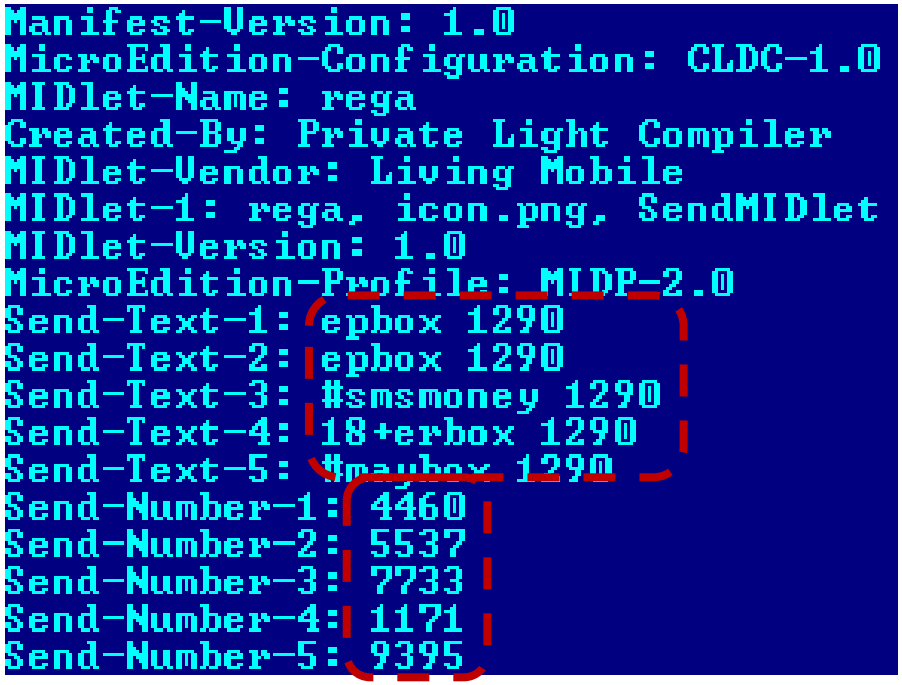
## Platform distribution




Source: Kaspersky Lab

# Primitive: Trojan-SMS.J2ME.Konov

- One of the first **widespread** SMS Trojans:
  - **Small** (1,5 – 8 kB)
  - **No encryption**
  - **No social engineering tricks**

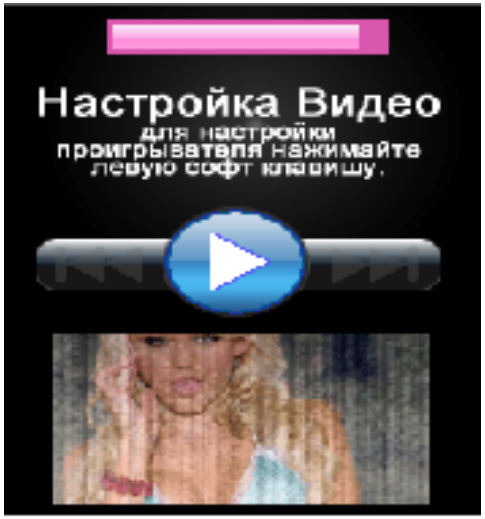


# Advanced: Trojan-SMS.J2ME.VScreener

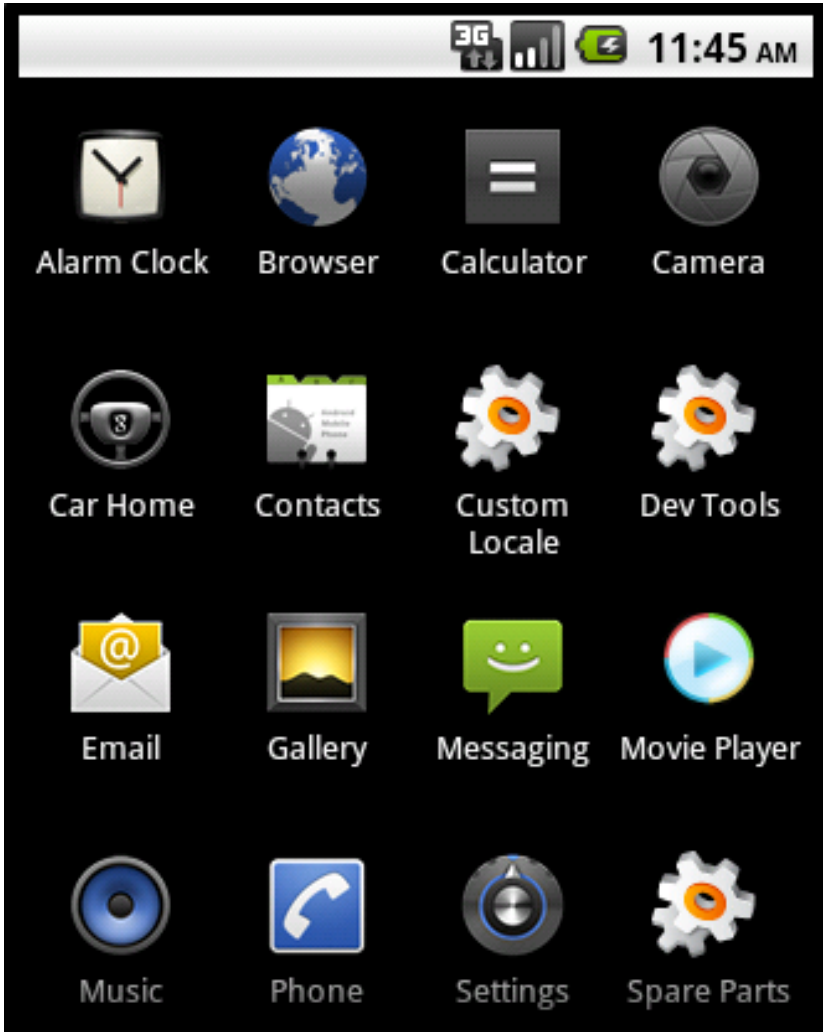
- **‘Faulty’ video player**

- Must be **‘tuned’ by user**
  - **Quick** left soft **key pressing**
- **SMS are sent during ‘tuning’**

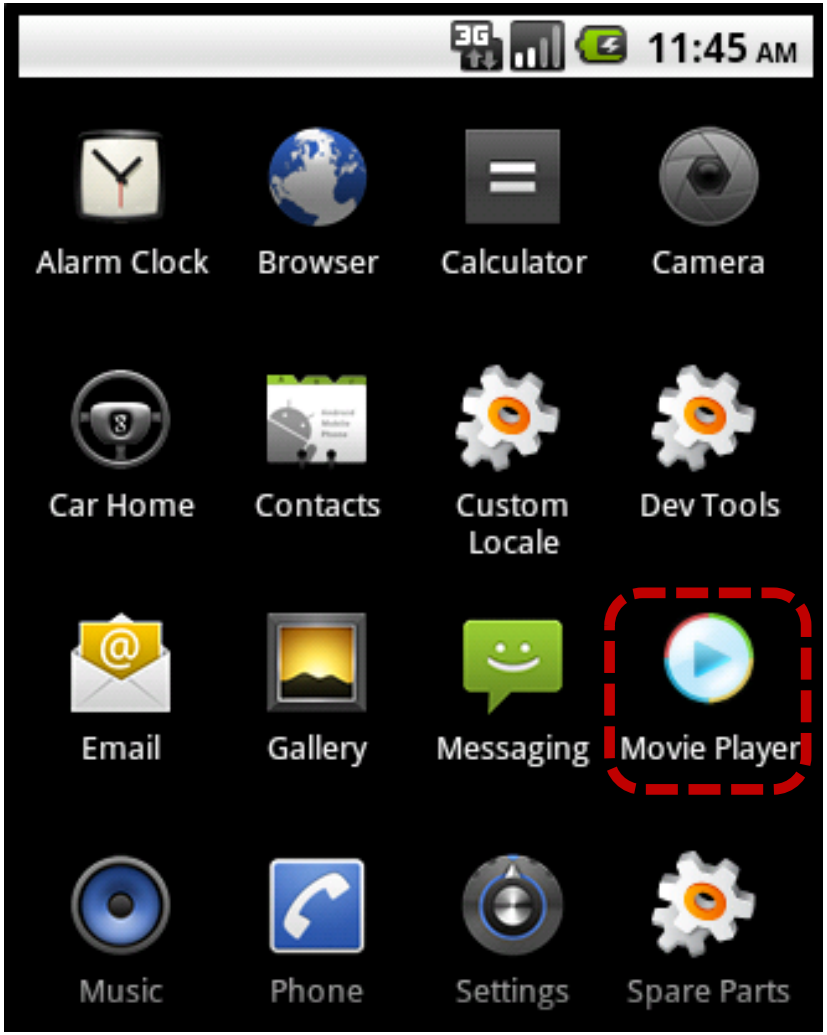
- Premium rate number and SMS text **are stored** in ‘load.bin’ file
- **File** ‘load.bin’ is **encoded** with ADD and ‘0xA’ key

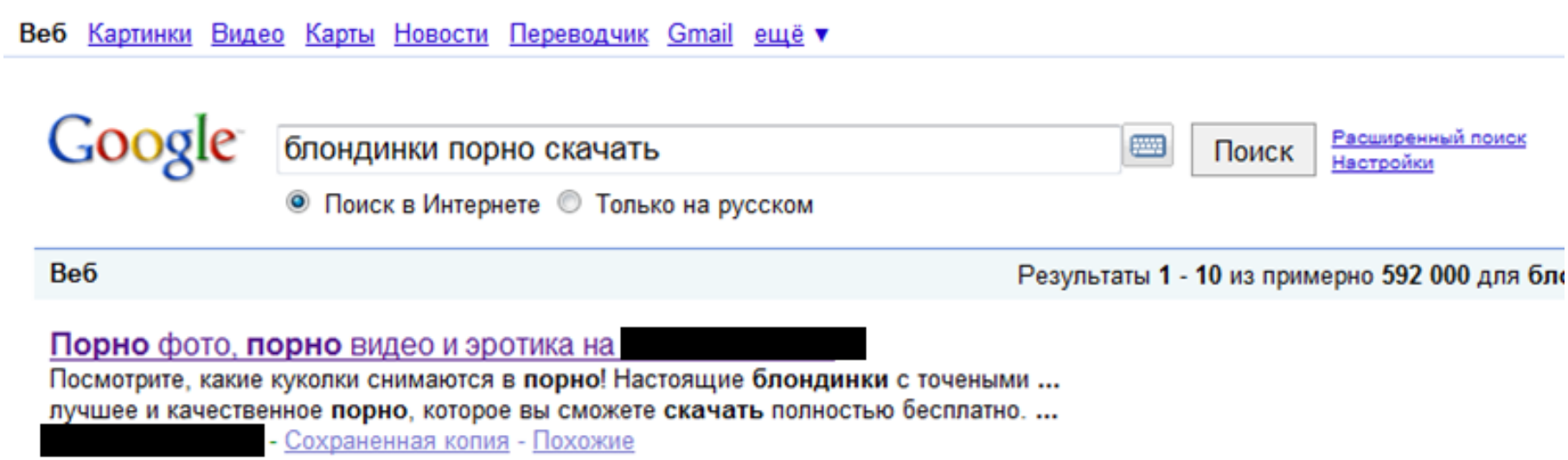
# ‘Video player’
## Again



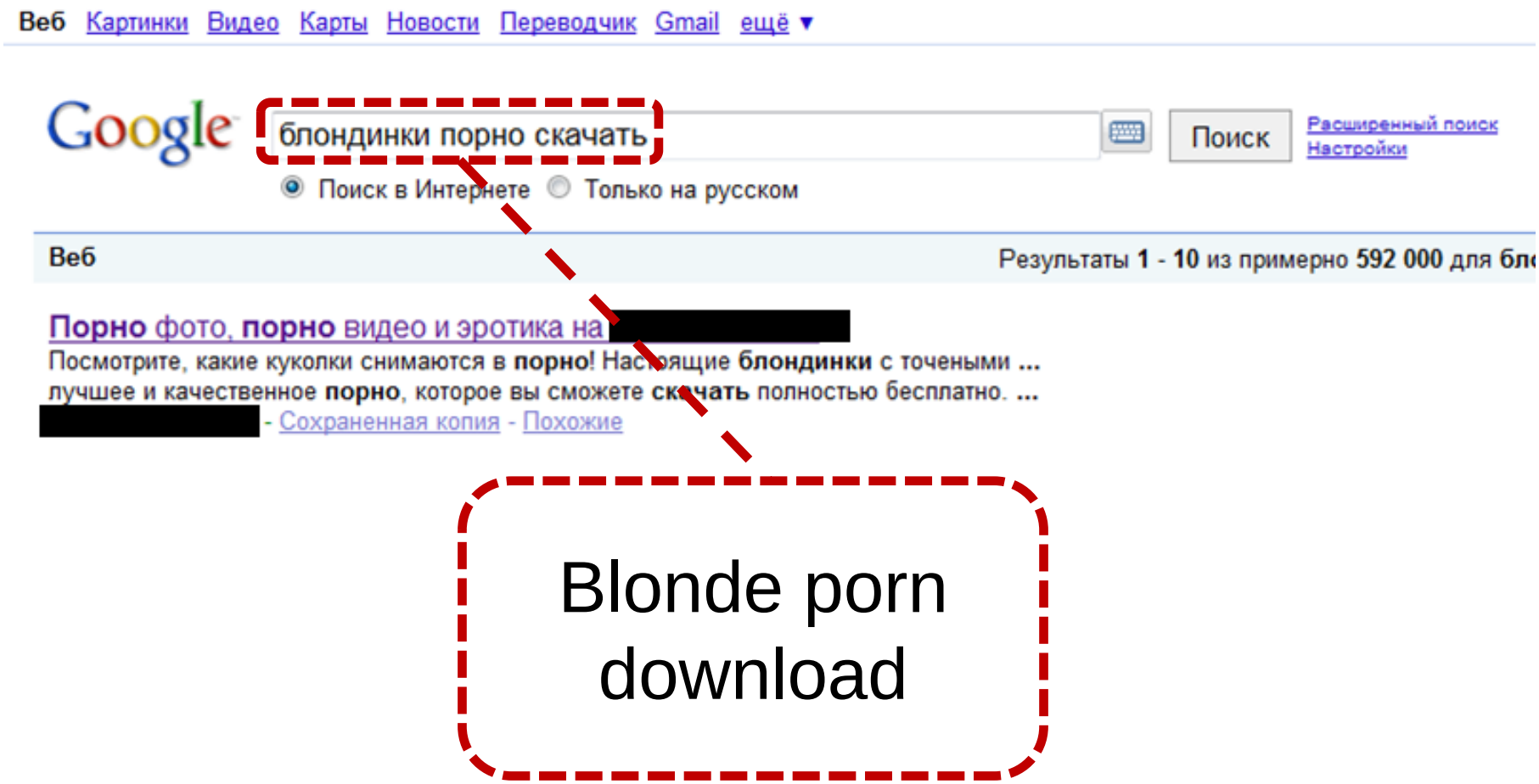
# ‘Video player’
## Again



# SEO and mobile malware



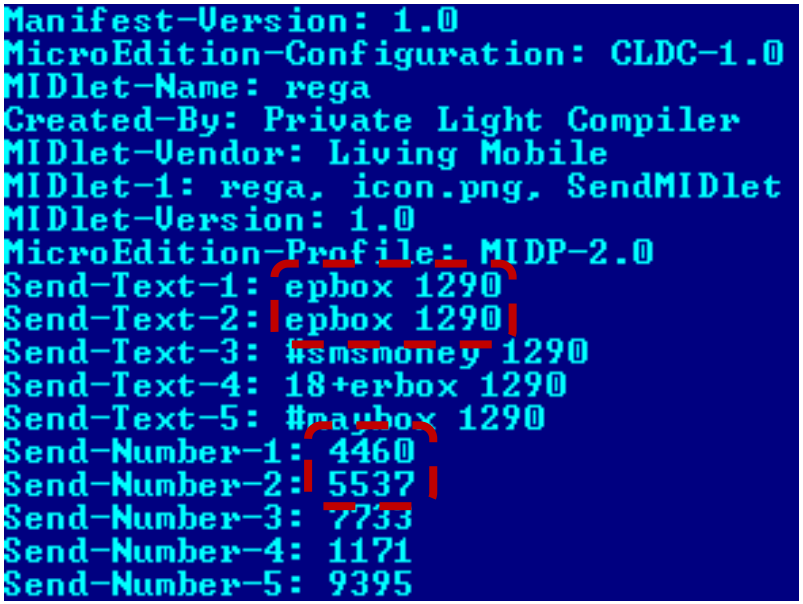
# SEO and mobile malware



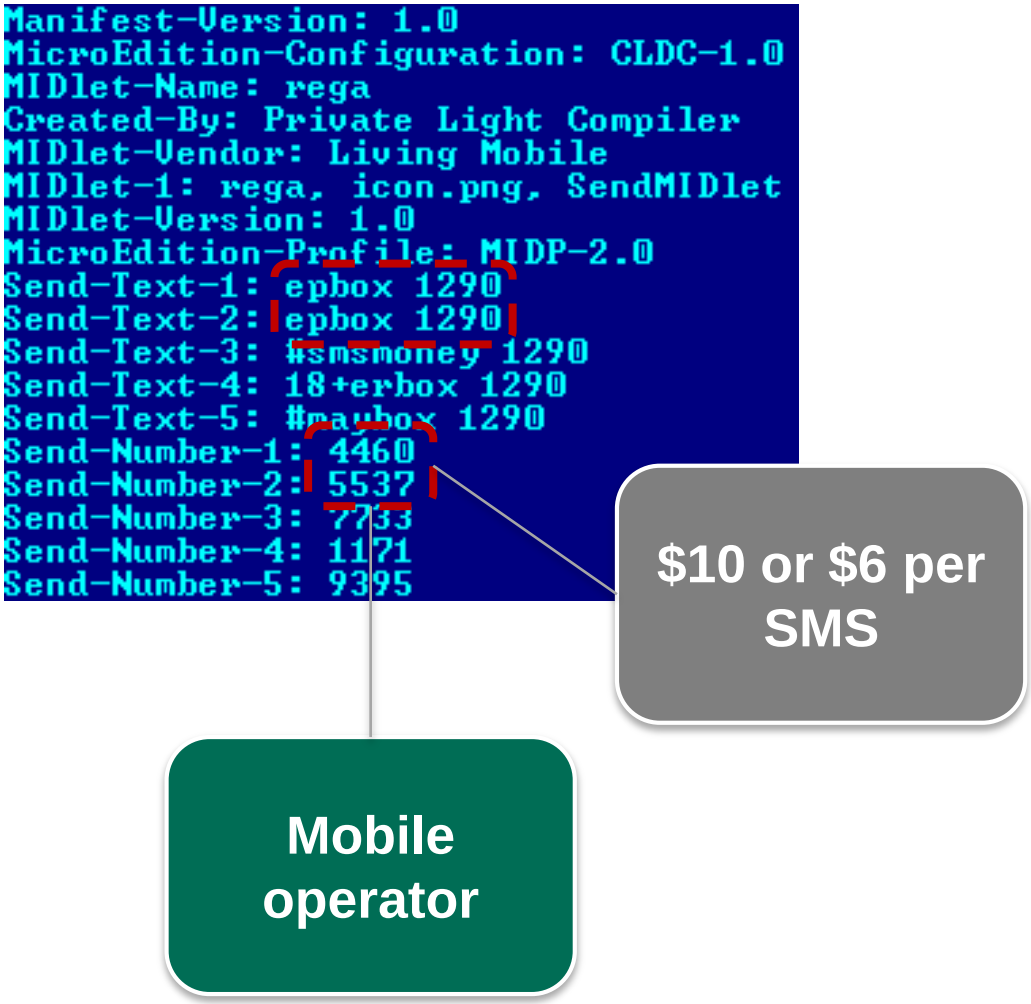
# The ecosystem

## The root of all evil

# Trojan-SMS.J2ME.Konov

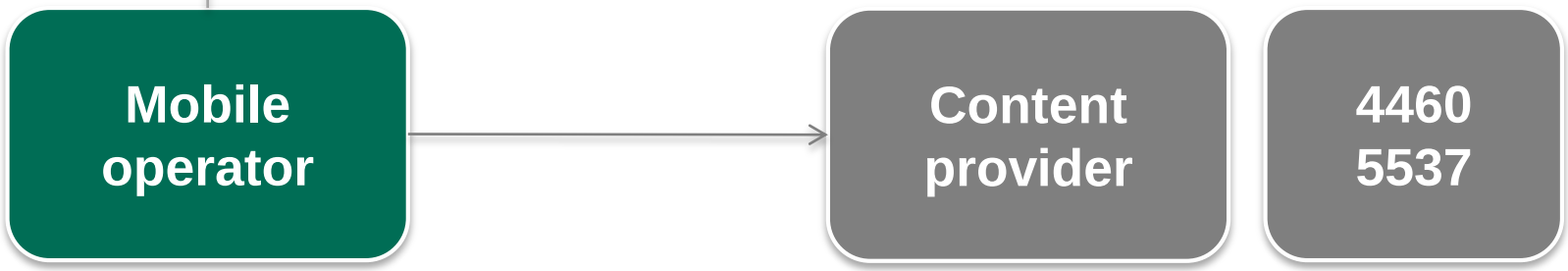


# Trojan-SMS.J2ME.Konov

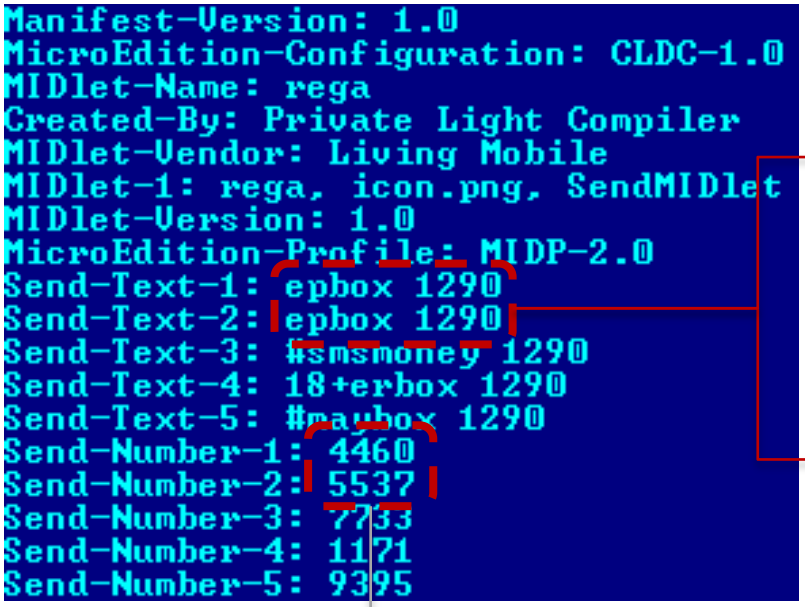


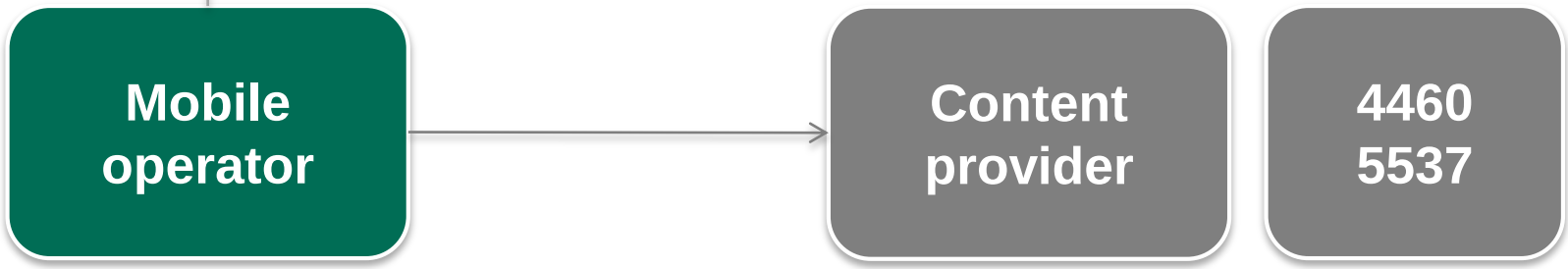
# Trojan-SMS.J2ME.Konov

```
Manifest-Version: 1.0
MicroEdition-Configuration: CLDC-1.0
MIDlet-Name: rega
Created-By: Private Light Compiler
MIDlet-Vendor: Living Mobile
MIDlet-1: rega, icon.png, SendMIDlet
MIDlet-Version: 1.0
MicroEdition-Profile: MIDP-2.0
Send-Text-1: epbox 1290
Send-Text-2: epbox 1290
Send-Text-3: #smsmoney 1290
Send-Text-4: 18+erbox 1290
Send-Text-5: #mybox 1290
Send-Number-1: 4460
Send-Number-2: 5537
Send-Number-3: 7733
Send-Number-4: 1171
Send-Number-5: 9395
```

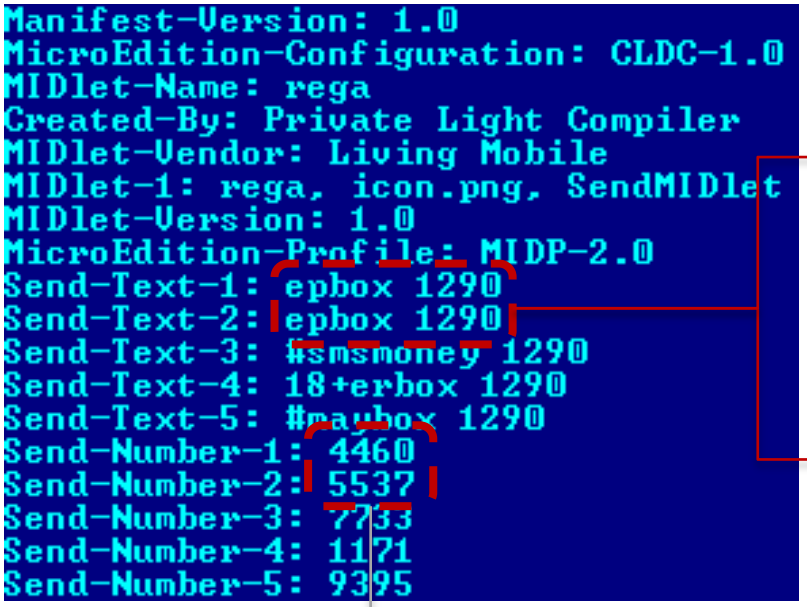


# Trojan-SMS.J2ME.Konov



# Trojan-SMS.J2ME.Konov




Subtenant with ID 1290

'epbox 1290' on 4460 & 5537

'epbox' renter

'epbox' on 4460 & 5537

Mobile operator

Content provider

4460
5537



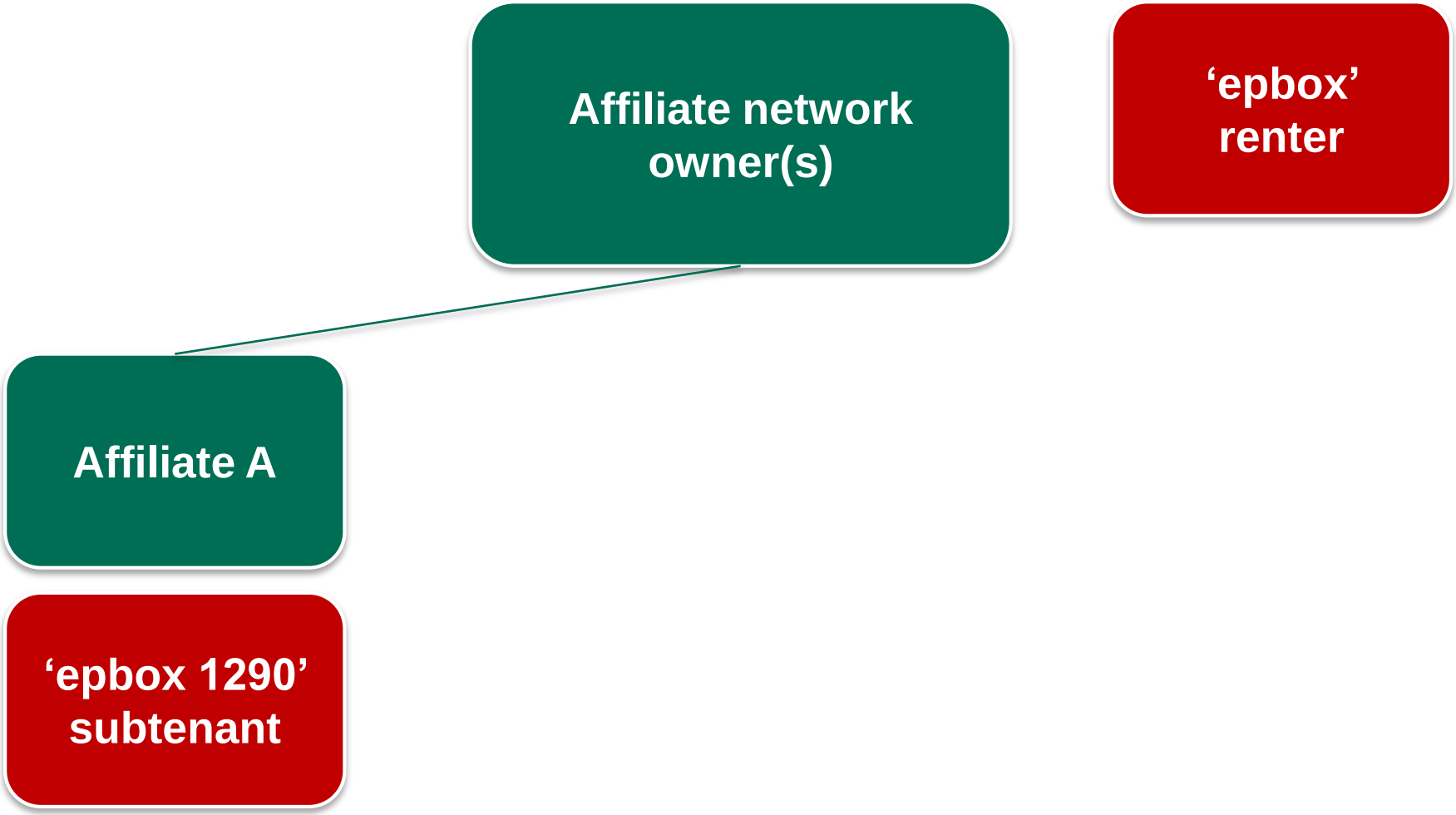
KASPERSKY lab

# Who are ‘epbox’ and ‘epbox 1290’

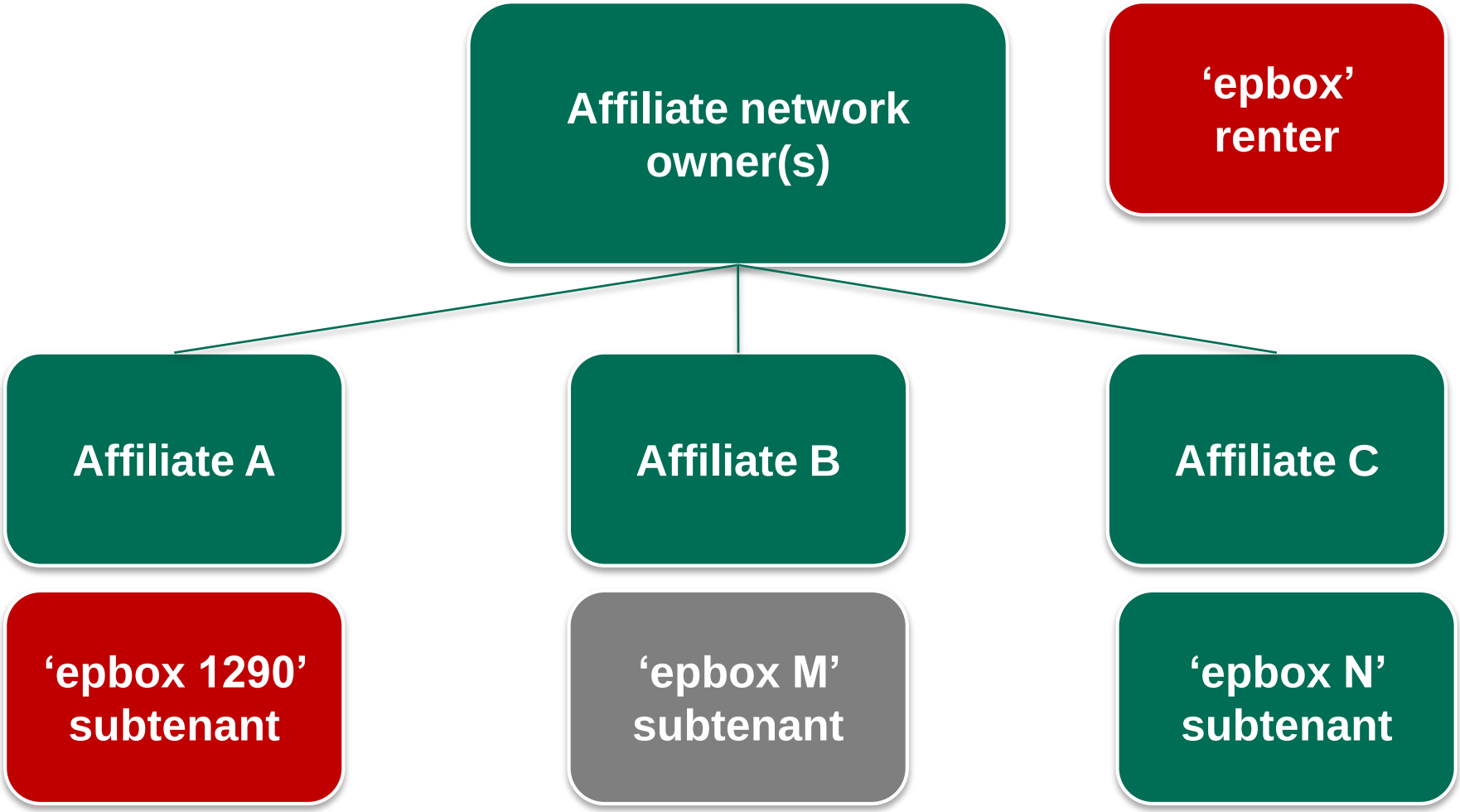
‘epbox’ renter

‘epbox 1290’ subtenant

# Who are ‘epbox’ and ‘epbox 1290’

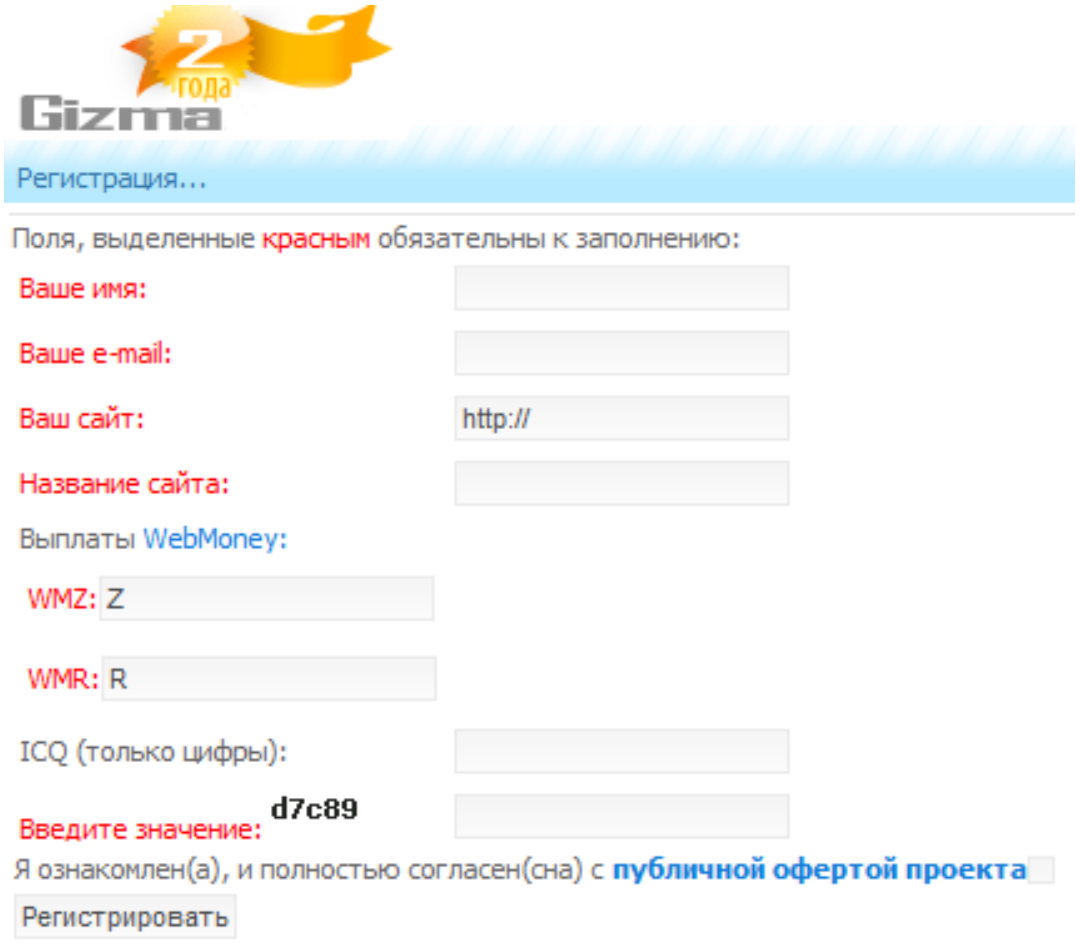


# Who are ‘epbox’ and ‘epbox 1290’



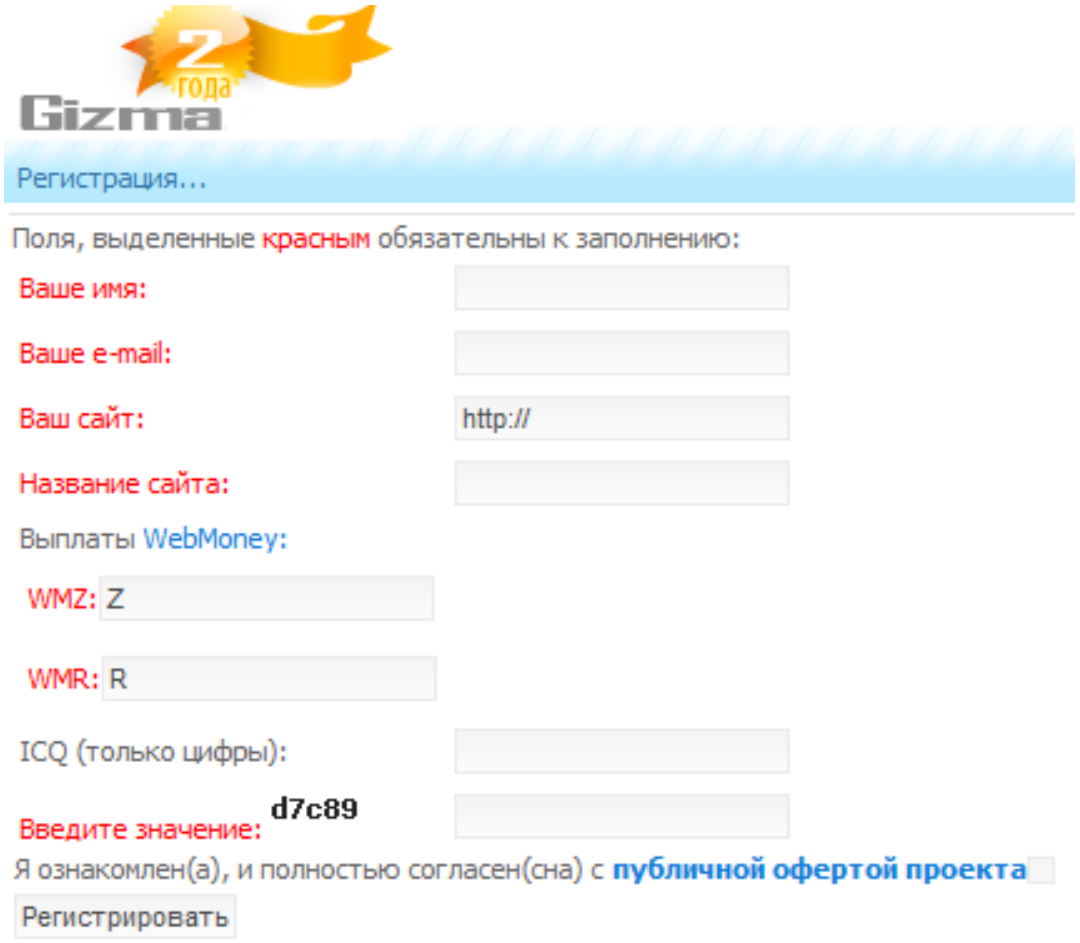
# The root of all evil

- **Affiliate network registration form**



# The root of all evil

- **Affiliate network registration form**




**Name**
**Email**
**Website URL**
**Website name**
**WMZ and WMR**
**ICQ (optional)**

# The root of all evil

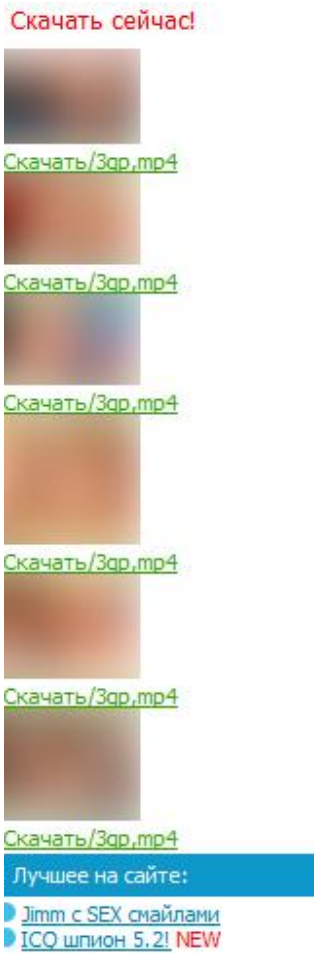
- **Affiliate network registration form**


**Affiliate ID 'epbox 1290'**

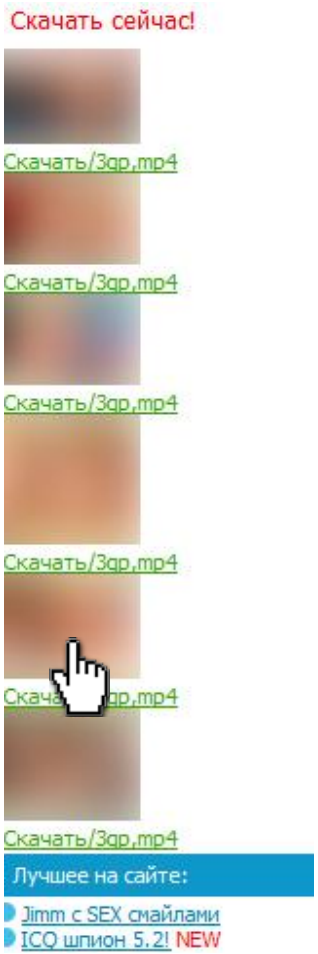
**No sensitive data!**

**Name**
**Email**
**Website URL**
**Website name**
**WMZ and WMR**
**ICQ (optional)**

# Typical affiliate website



# Typical affiliate website



# Typical affiliate website


**Remote server** → **Referrer check** → **Affiliate ID**

# Typical affiliate website


Remote server

Referrer check

Affiliate ID

JAR constructor

SMS Trojan with affiliate ID

# Typical affiliate website


Remote server

Referrer check

Affiliate ID

JAR constructor

SMS Trojan with affiliate ID

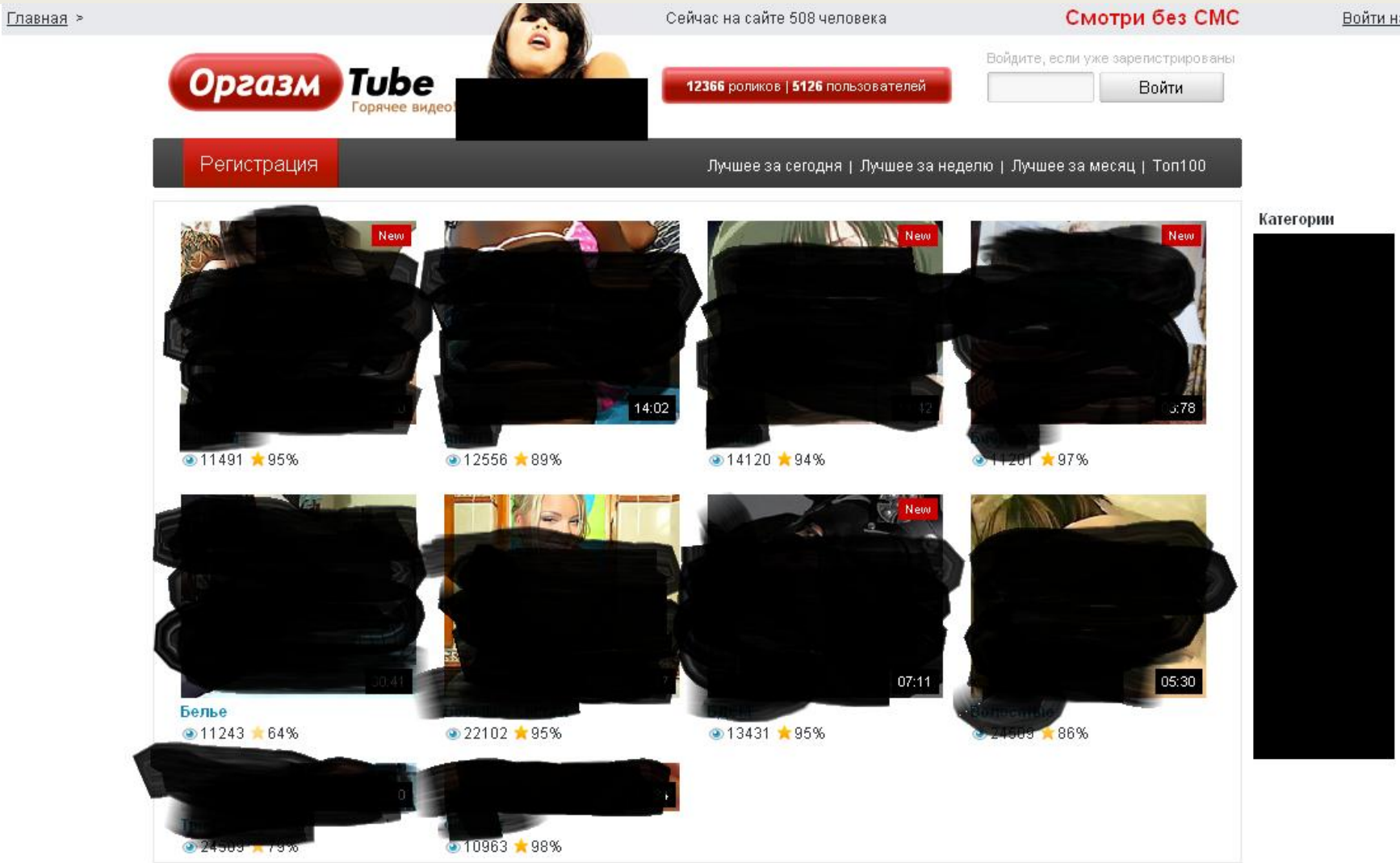
**Thousands of websites!**



KASPERSKY lab

# Ransomware

## Same situation



# Ransomware

## Same situation

vr_media_player3.1_inst.exe...
Microsoft

vr_codecpackage.exe_.exe
Microsoft

vr_update_player_x90.exe_....
XlbOwO
zOyvNN

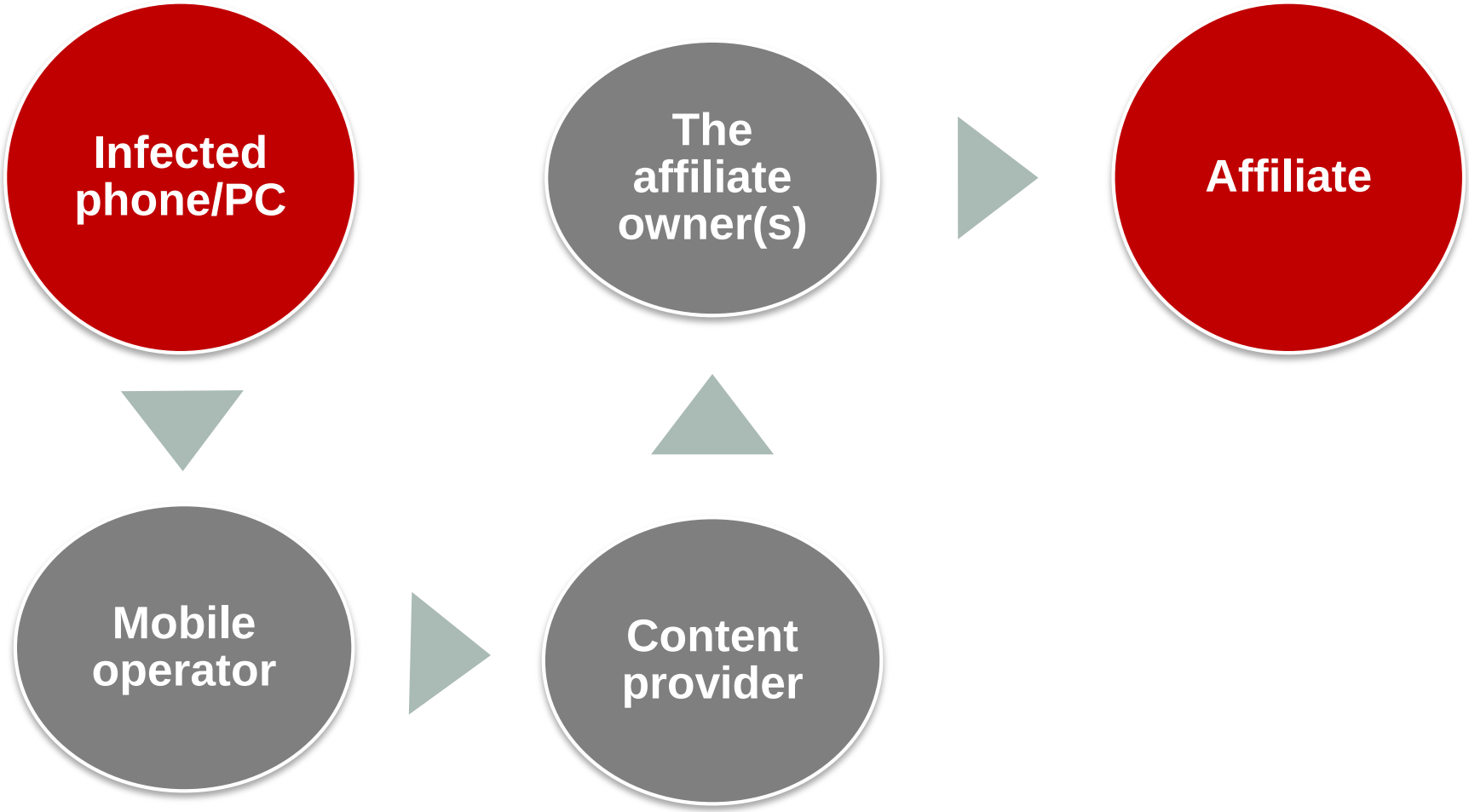
# Underground economy

…and lottery results :)

KASPERSKY lab

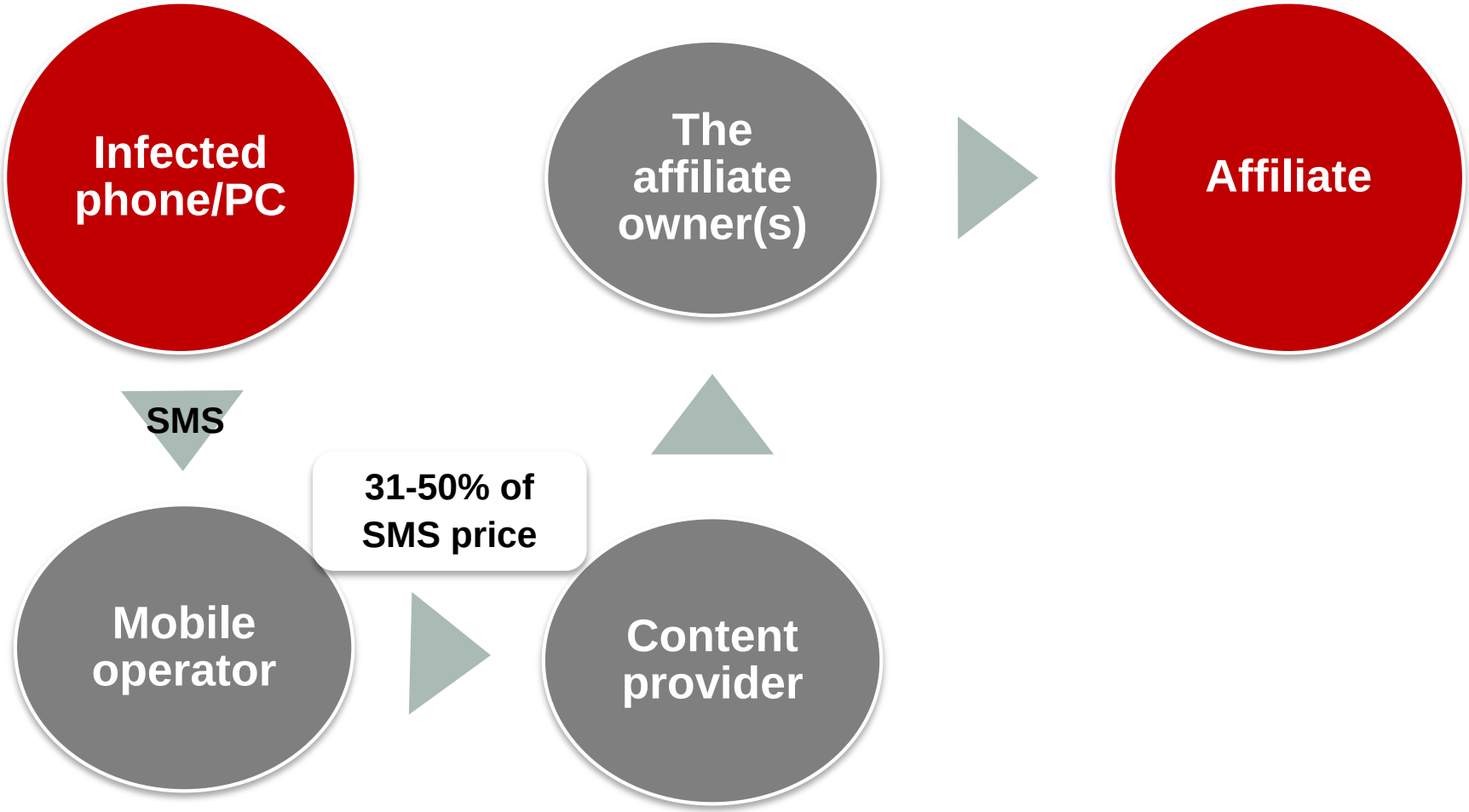
# Underground economy

## Revenue sharing



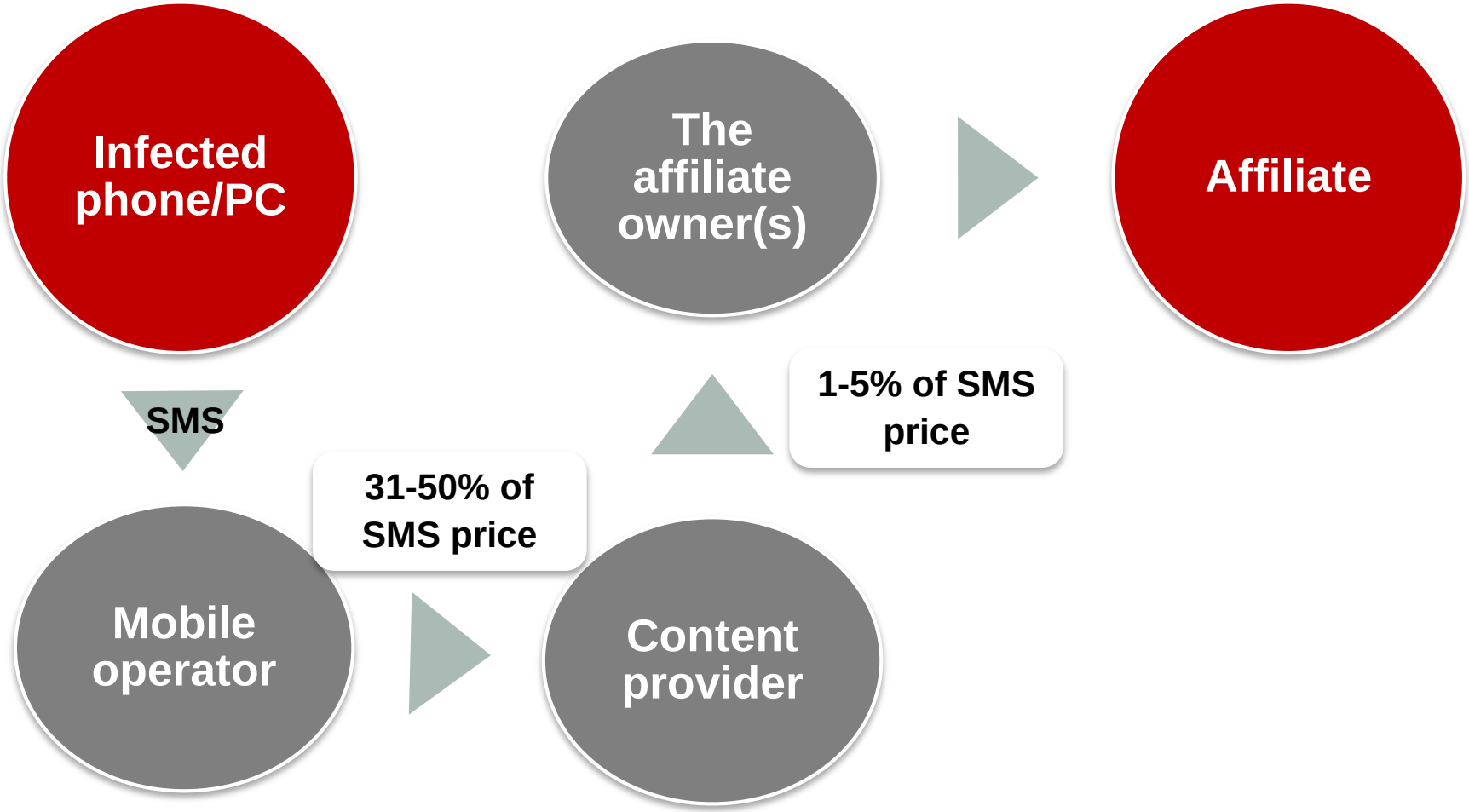
# Underground economy

## Revenue sharing



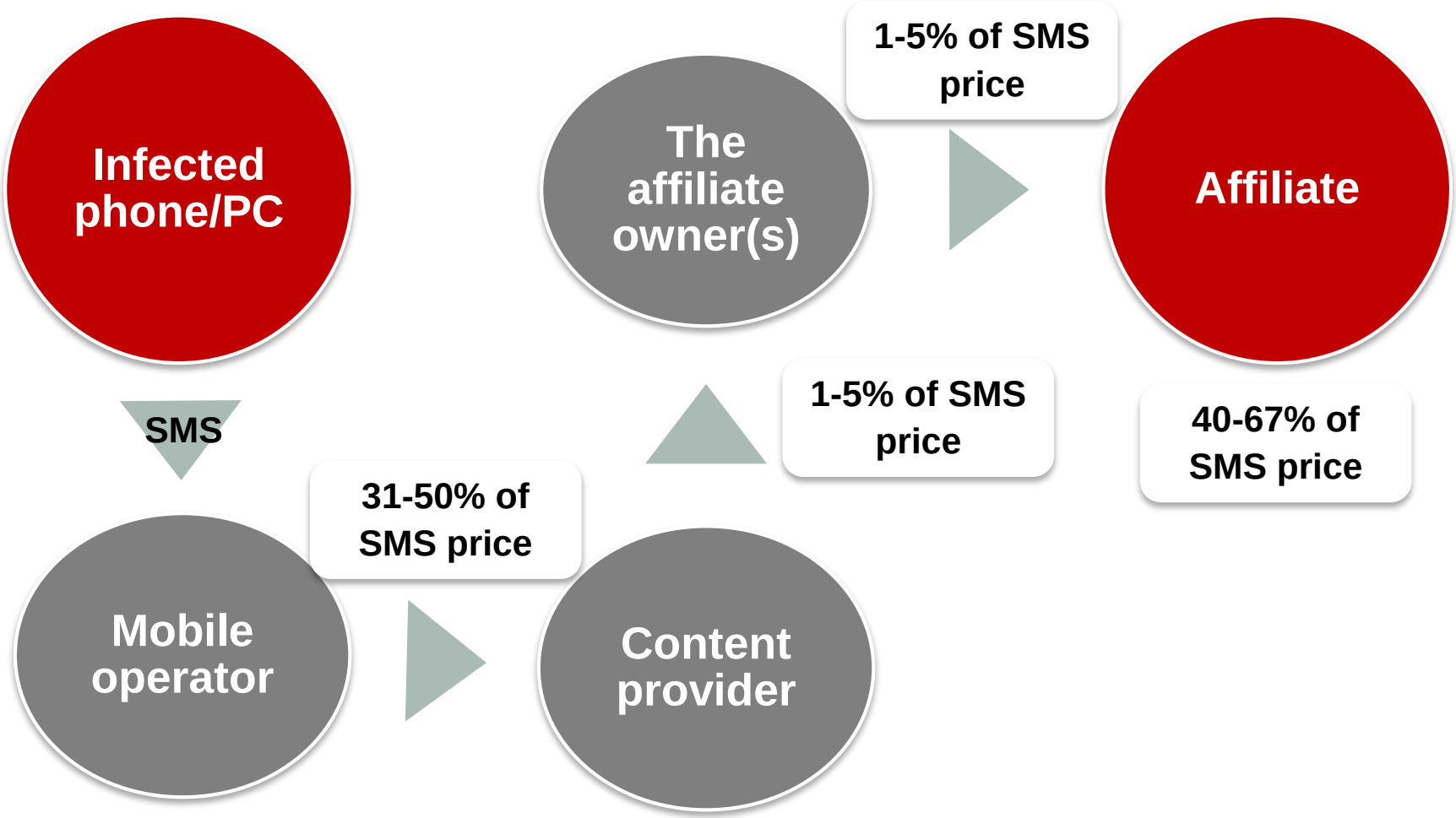
# Underground economy

## Revenue sharing



# Underground economy

## Revenue sharing

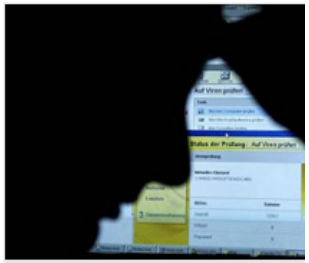


# $$$

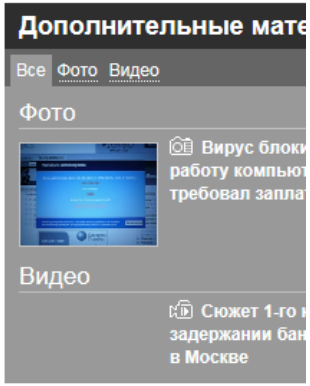
## За полгода пользователи интернета отправили мошенникам SMS на миллиард рублей

31.08.2010 в 14:59, обновлено 01.09.2010 в 12:46 | Рустам Такташев

**Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали тысячи пользователей интернета в разных странах.**



Жертвами кибер-мошенников ст
пользователей интернета




Как рассказали GZT.RU в столичном УБЭПе, фигурантами уголовного дела являются 10 человек— организаторы преступного бизнеса, программисты, написавшие вирус, лица, отвечавшие за обналичивание средств, и другие члены группировки. По словам милиционеров, все они жители Москвы, молодые люди, профессиональные программисты.

### Нечестные вымогатели

Орудовали хакеры около полугода. За это время их жертвами стали тысячи пользователей интернета. Причем не только в России. Оперативники установили, что от их действий пострадали также жители Украины, Белоруссии, Молдавии и стран Балтии.

Злоумышленники распространяли вирус, получивший название Winlock. Он блокировал работу компьютера. На экране монитора появлялась надпись, оповещающая, что операционная система заблокирована и для восстановления работы компьютера необходимо отправить SMS-сообщение на короткий четырехзначный номер. Один из номеров был 1350. Надпись также

# $$$

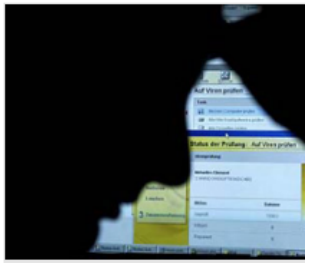
‘…10 people were arrested…’

‘…malware which blocks PC…’

## За полгода пользователи интернета отправили мошенникам SMS на миллиард рублей

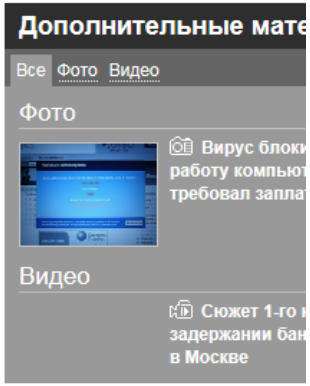
31.08.2010 в 14:59, обновлено 01.09.2010 в 12:46 | Рустам Такташев

**Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали тысячи пользователей интернета в разных странах.**



Жертвами кибер-мошенников ст
пользователей интернета

Как рассказали GZT.RU в столичном УБЭПе, фигурантами уголовного дела являются 10 человек— организаторы преступного бизнеса, программисты, написавшие вирус, лица, отвечавшие за обналичивание средств, и другие члены группировки. По словам милиционеров, все они жители Москвы, молодые люди, профессиональные программисты.




**Нечестные вымогатели**

Орудовали хакеры около полугода. За это время их жертвами стали тысячи пользователей интернета. Причем не только в России. Оперативники установили, что от их действий пострадали также жители Украины, Белоруссии, Молдавии и стран Балтии.

Злоумышленники распространяли вирус, получивший название Winlock. Он блокировал работу компьютера. На экране монитора появлялась надпись, оповещающая, что операционная система заблокирована и для восстановления работы компьютера необходимо отправить SMS-сообщение на короткий четырехзначный номер. Один из номеров был 1350. Надпись также

# $$$

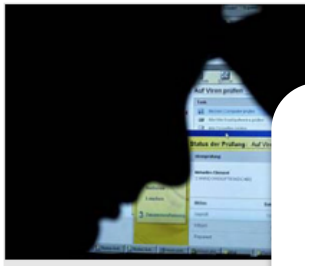
‘…10 people were arrested…’

‘…malware which blocks PC…’

## За полгода пользователи интернета отправили мошенникам SMS на миллиард рублей

31.08.2010 в 14:59, обновлено 01.09.2010 в 12:46 | Рустам Такташев

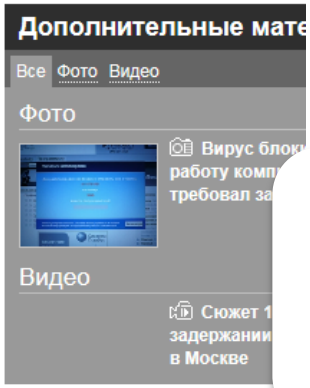
**Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали тысячи пользователей интернета в разных странах.**



Жертвами кибер-мошенников пользователей интернета

‘…half a year…’

Как рассказали GZT.RU в столичном УБЭПе, фигурантами уголовного дела являются 10 человек—организаторы преступного бизнеса, программисты, написавшие вирус, лица, отвечавшие за обналичивание средств, и другие члены группировки. По словам милиционеров, все они жители Москвы, молодые люди, профессиональные программисты.




‘…SMS as ransom…’

**Нечестные вымогатели**

Орудовали хакеры около полугода. За это время их жертвами стали тысячи пользователей интернета. Причем не только в России. Оперативники установили, что от их действий пострадали также жители Украины, Белоруссии, Молдавии и стран Балтии.

Злоумышленники распространяли вирус, получивший название Winlock. Он блокировал работу компьютера. На экране монитора появлялась надпись, оповещающая, что операционная система заблокирована и для восстановления работы компьютера необходимо отправить SMS-сообщение на короткий четырехзначный номер. Один из номеров был 1350. Надпись также

# $$$

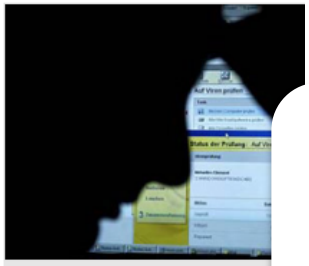
‘…10 people were arrested…’

‘…malware which blocks PC…’

## За полгода пользователи интернета отправили мошенникам SMS на миллиард рублей

31.08.2010 в 14:59, обновлено 01.09.2010 в 12:46 | Рустам Такташев

**Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали тысячи пользователей интернета в разных странах.**



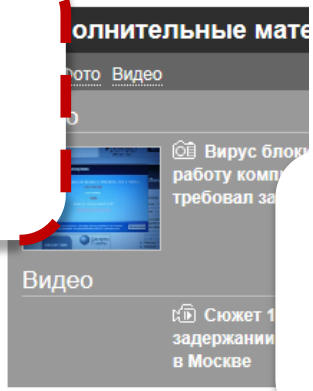
Жертвами кибер-мошенников пользователей интернета

Как рассказали GZT.RU в столичном УБЭПе, фигурантами уголов… организаторы пр… написавшие вир… обналичивание с… По словам мили… молодые люди, …

‘…1 billion rubles…’

**Нечестные вым…**

Орудовали хакер… жертвами стали тысячи пользователей интернета. Причем не только в России. Оперативники установили, что от их действий пострадали также жители Украины, Белоруссии, Молдавии и стран Балтии.




Злоумышленники распространяли вирус, получивший название Winlock. Он блокировал работу компьютера. На экране монитора появлялась надпись, оповещающая, что операционная система заблокирована и для восстановления работы компьютера необходимо отправить SMS-сообщение на короткий четырехзначный номер. Один из номеров был 1350. Надпись также

‘…half a year…’

‘…SMS as ransom…’

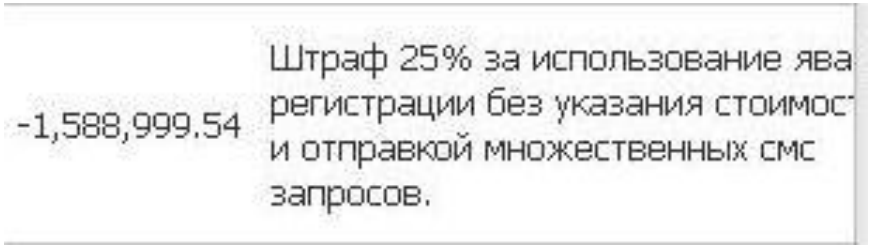
# Calculations

**1,000,000,000 rubles ~ $30,000,000**

**$30,000,000/6 ~ $5,000,000 per month**

# ‘Death penalty’

- Largest mobile **affiliate network was fined:**




- The fine was equal to **25% of the affiliate network weekly income:**
  - **1,590,000 rubles ~ $53,000**
  - **Weekly income ~ $212,000**
  - **Monthly income ~ $850,000**
- People **were losing at least** $1,200,000 per month

# Final score

# $6,200,000 per month

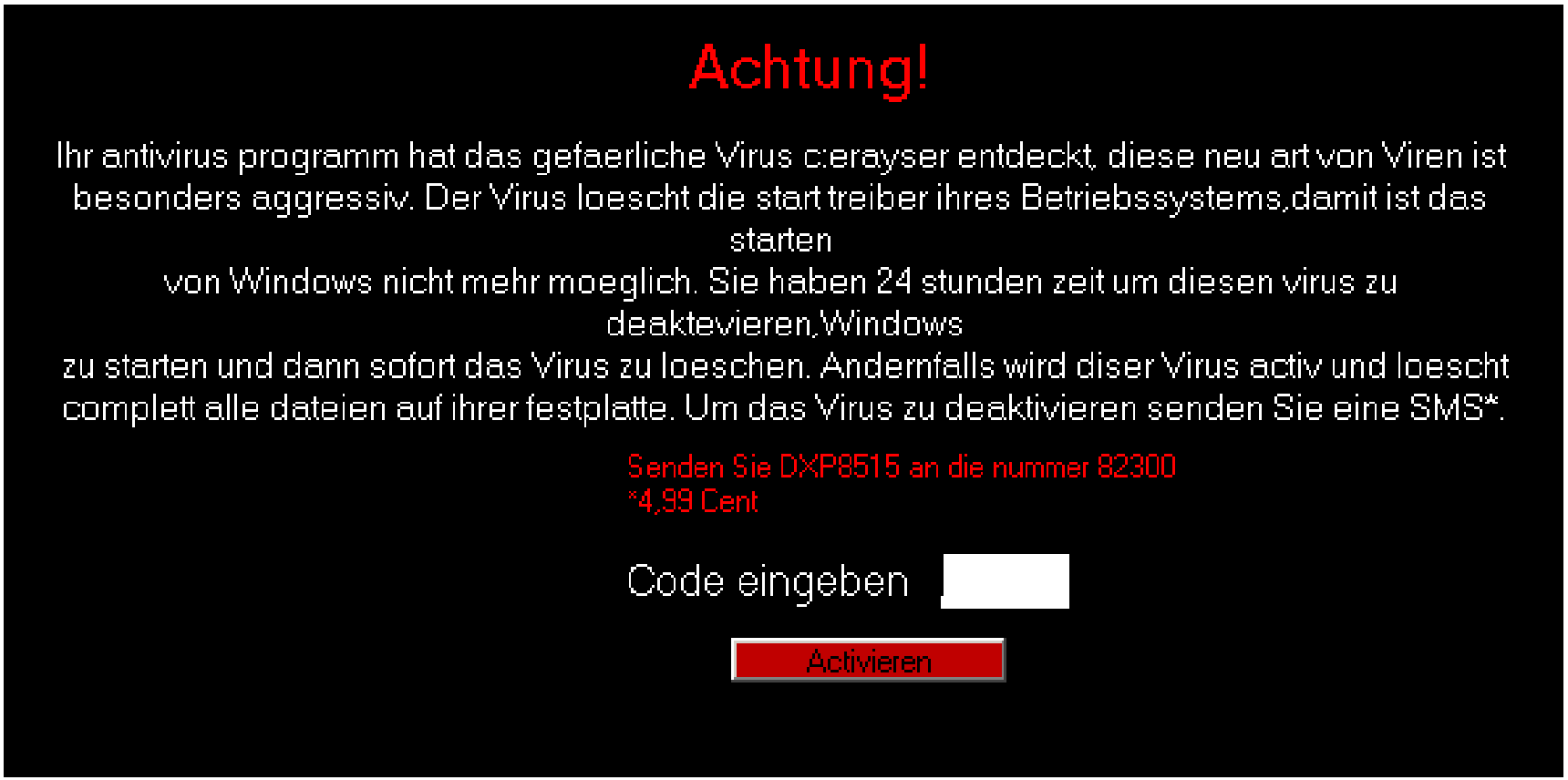
# Threats round the globe

KASPERSKY lab

# Ransomware


Warning
Warning!
This computer has been locked!
You must to receive a key
for unlocking and continuations
of use of this computer.
Step 1
Your country:
Step 2
Send SMS with the
to the nu
Step 3
Enter the key:
Protected by sms.zamok
Russia
Ukraine
Ukraine(Life)
Belarus
Azerbaijan
Latvia(Lmt)
Latvia(TELE2)
Poland
Lietuva
Estonia
Czechia
Hungary
Belgium
Israel
Kazakhstan
Tajikistan
Kirghizia
Great Britain
France

# Ransomware


Achtung!
Ihr antivirus programm hat das gefaerliche Virus c:erayser entdeckt, diese neu art von Viren ist besonders aggressiv. Der Virus loescht die start treiber ihres Betriebssystems,damit ist das starten
von Windows nicht mehr moeglich. Sie haben 24 stunden zeit um diesen virus zu deaktevieren,Windows
zu starten und dann sofort das Virus zu loeschen. Andernfalls wird diser Virus activ und loescht complett alle dateien auf ihrer festplatte. Um das Virus zu deaktivieren senden Sie eine SMS*.
Senden Sie DXP8515 an die nummer 82300
*4,99 Cent
Code eingeben
Activieren

# Ransomware


Activation de Windows
ACTIVATION DE WINDOWS
Code du PC :
Clé d'activation :
Activer
Email
OK
Pour recevoir votre clé d'activation envoyez 2 ALLOPASS et le code de votre PC à l'email :
[redacted]@gmail.com
Pour recevoir des codes ALLOPASS il vous suffit d'envoyer CODE par SMS au 81 038.
Un email/sms vous sera envoyée avec la clé d'activation.
Cet application supprimera toutes vos données 24h aprés son premier lancement.
Bonne chance.

# A long time ago…

# Porn SMS senders

## ‘Nooit spijt’ case

# Porn SMS senders

## ‘Nooit spijt’ case

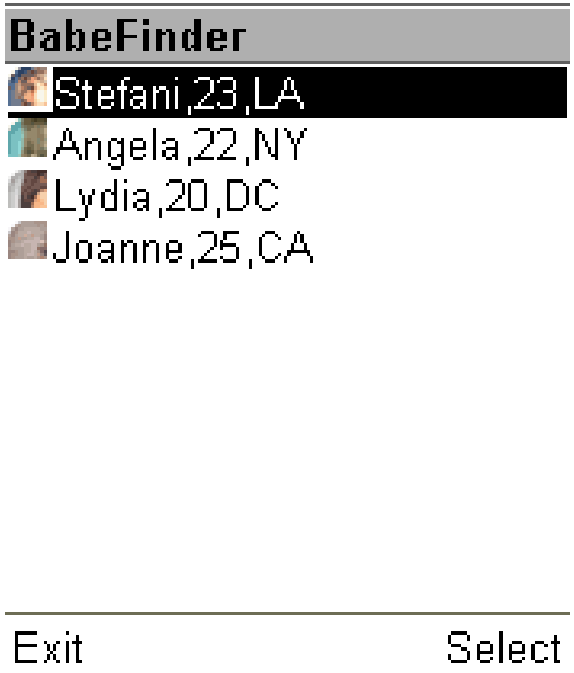
# ‘Dating’ apps

If you are from UK

# ‘Dating’ apps

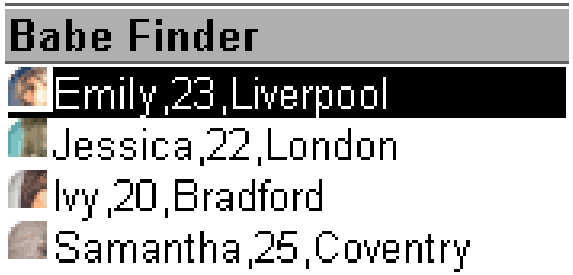
If you are from UK

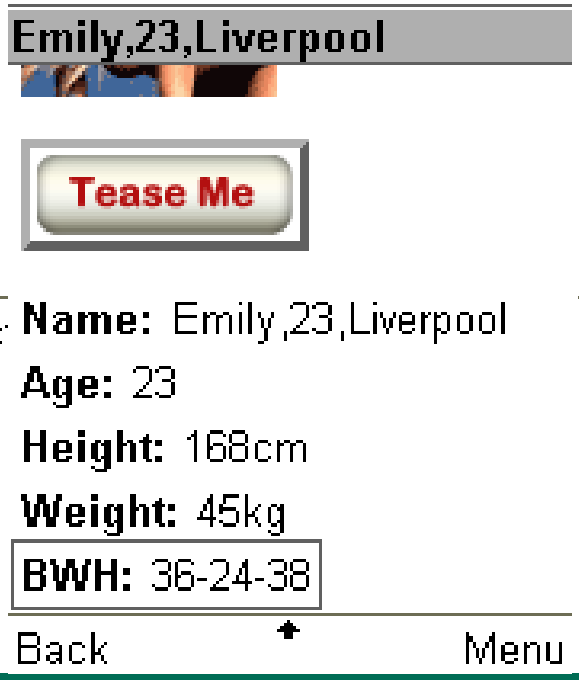

If you are from US



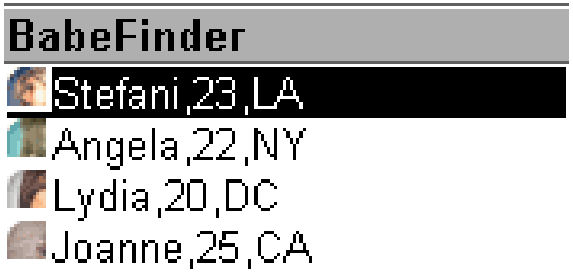
# ‘Dating’ apps

## If you are from UK

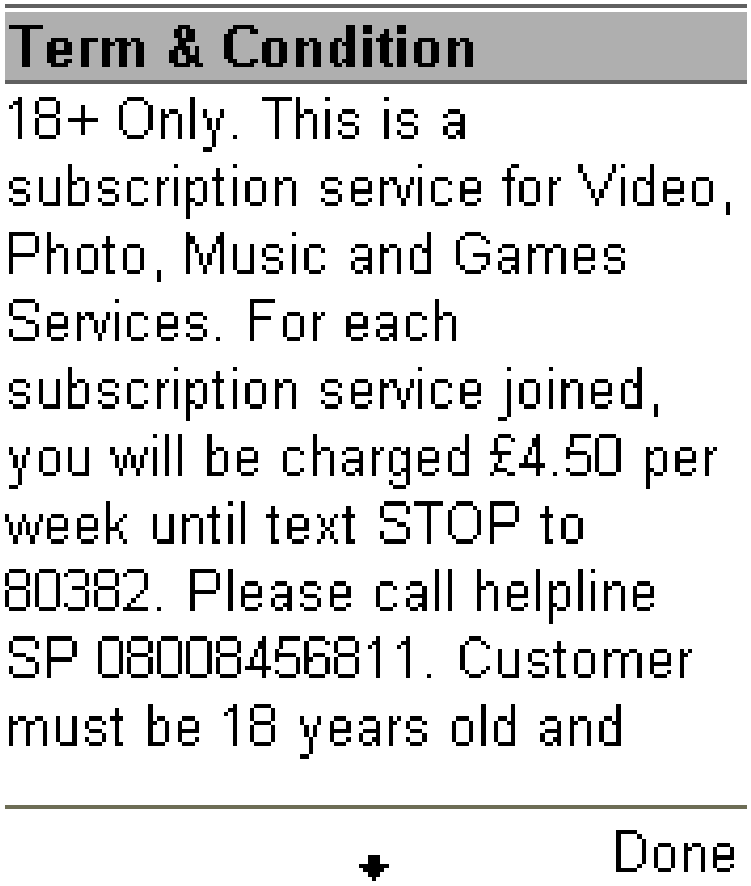


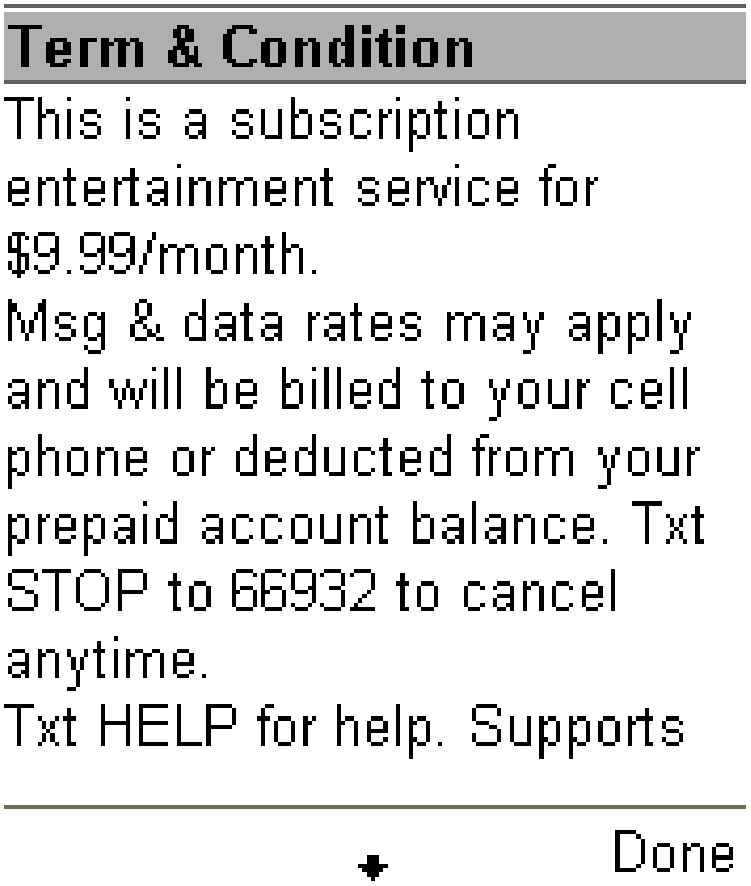




## If you are from US



# ‘Dating’ apps


Term & Condition
18+ Only. This is a subscription service for Video, Photo, Music and Games Services. For each subscription service joined, you will be charged £4.50 per week until text STOP to 80382. Please call helpline SP 08008456811. Customer must be 18 years old and
Done


Term & Condition
This is a subscription entertainment service for $9.99/month.
Msg & data rates may apply and will be billed to your cell phone or deducted from your prepaid account balance. Txt STOP to 66932 to cancel anytime.
Txt HELP for help. Supports
Done

# Countries

- 6343, **1,5 EUR** per SMS 
- 66932, **$9,99/month**, subscription number 
- 80382, **4,5 pounds/week**, subscription number 
- 39633, **RM3.00** per SMS 
- 8335, **30KES** per SMS 
- 41647, **R5** per SMS 

# What should we do?

# What should we do?

- Force **legislation changes** in certain countries
- **Cybercriminals** must be **punished**
- Provide **education** and **user's awareness**

# Thank You

## The Underground Economy and Ecosystem of SMS Based Cybercrime

Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab

Denis.Maslennikov@kaspersky.com, @hEx63

15.06.2011, 23rd Annual FIRST Conference, Vienna, Austria

KASPERSKY lab