



# The Underground Economy and Ecosystem of SMS Based Cybercrime

Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab

15.06.2011, 23<sup>rd</sup> 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



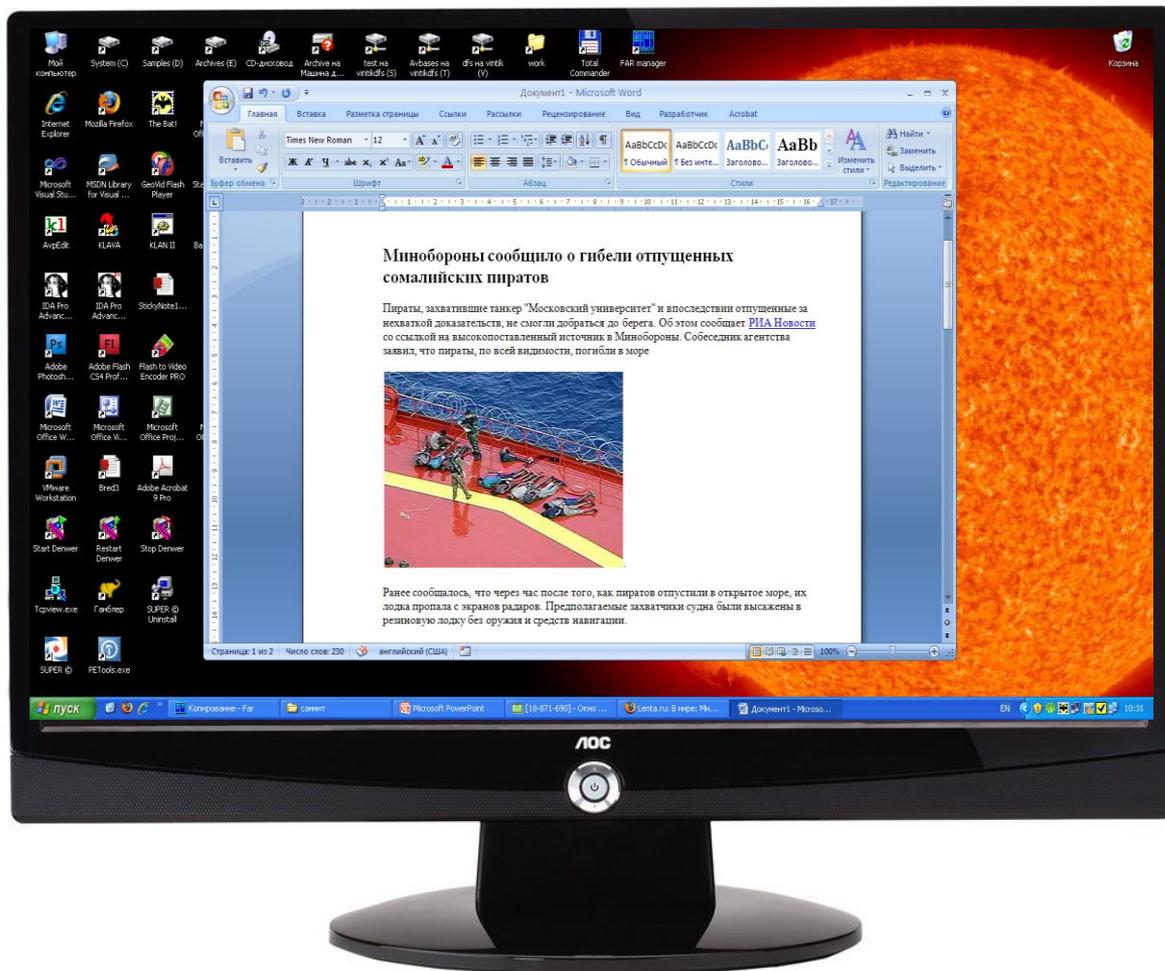
# How much have users lost?



# Ransomware

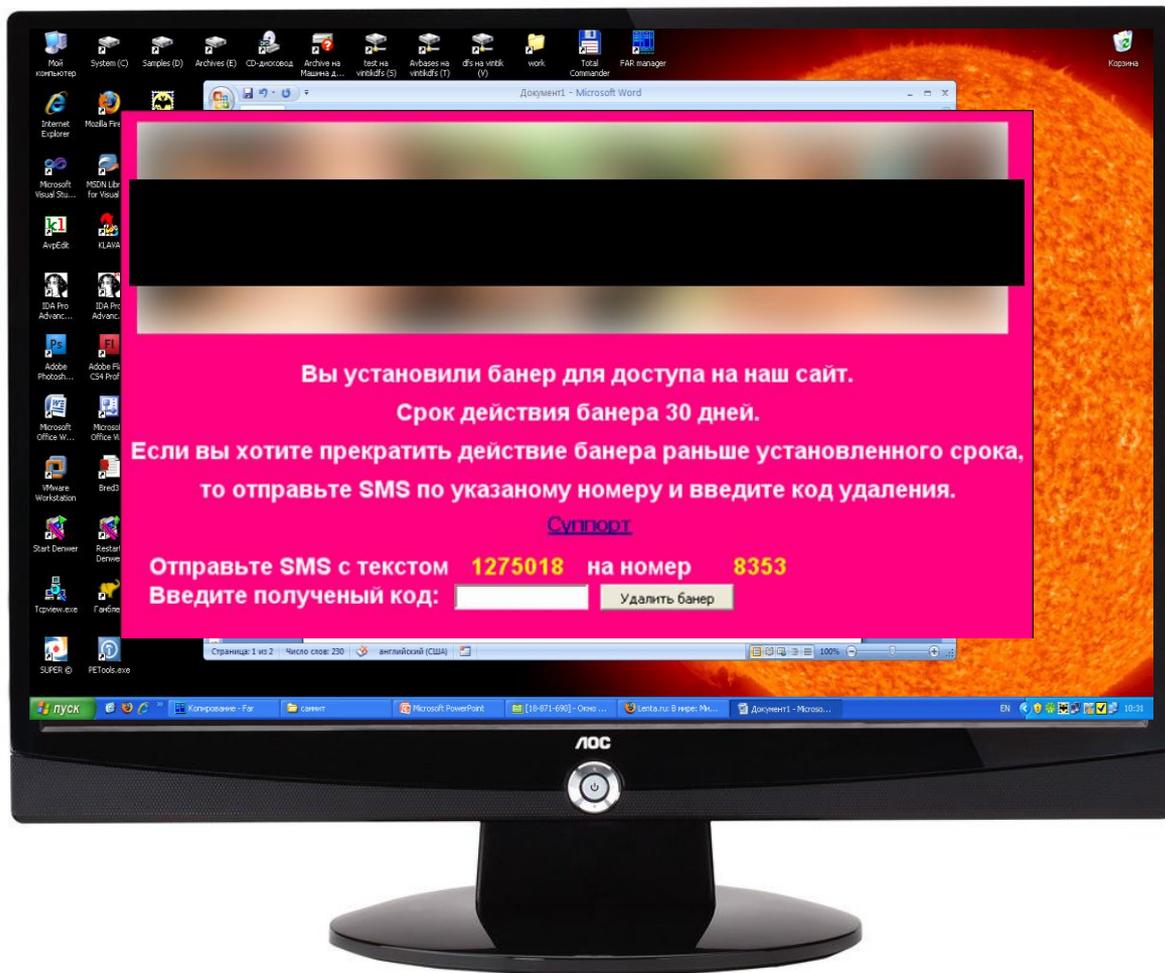
# Ransomware

## In a nutshell



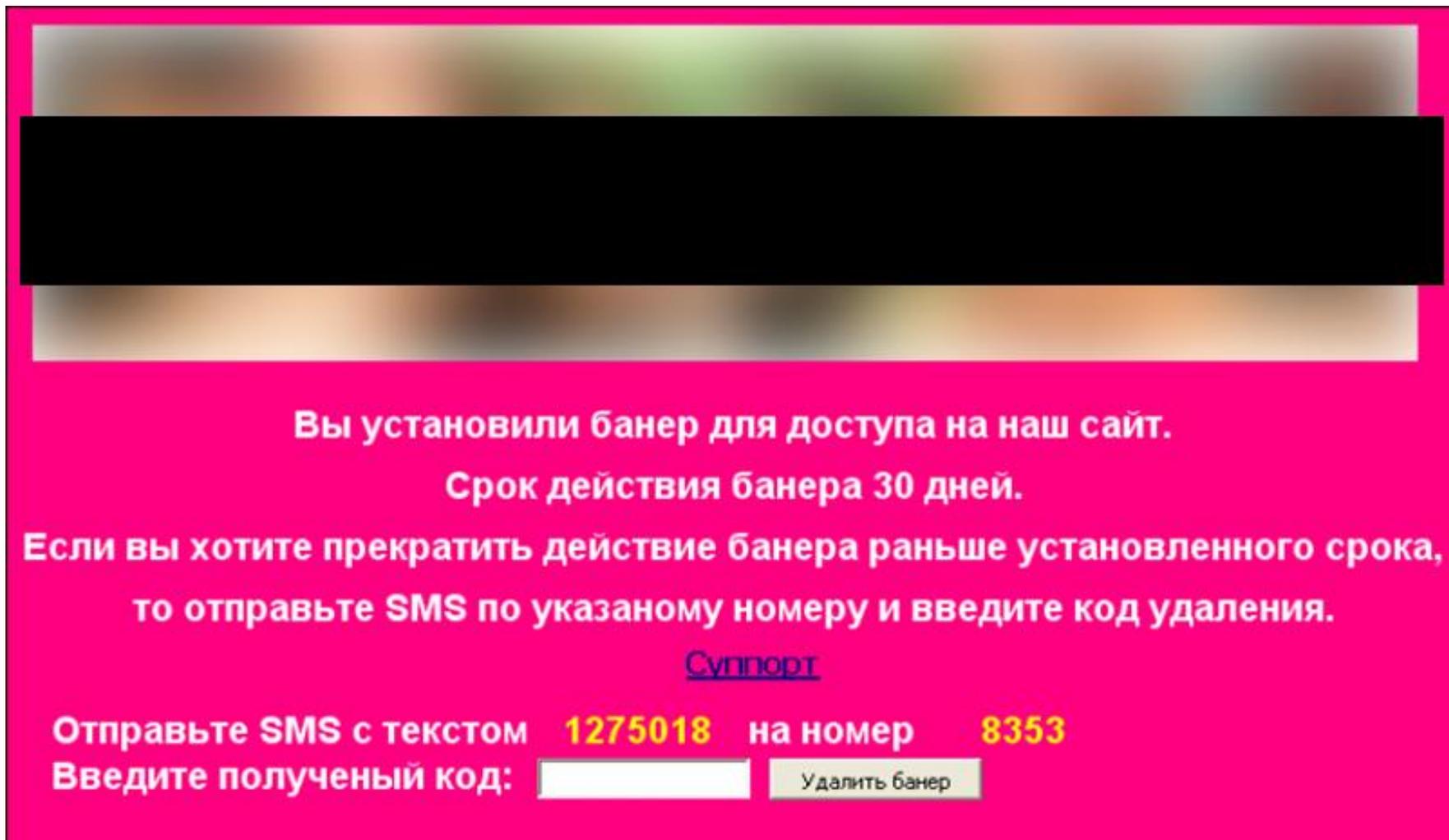
# Ransomware

## In a nutshell



# Ransomware

## Variety



Вы установили банер для доступа на наш сайт.  
Срок действия банера 30 дней.  
Если вы хотите прекратить действие банера раньше установленного срока,  
то отправьте SMS по указаному номеру и введите код удаления.

[Суппорт](#)

Отправьте SMS с текстом **1275018** на номер **8353**  
Введите полученный код:

# Ransomware

## Variety

Обнаружена проблема, которая может повредить вашему компьютеру.

Драйвер устройства, вызвавший повреждения был обезврежен системой.  
Нарушенный драйвер на стеке ядра должны быть заменены рабочей версией.

Technical information:

\*\*\* STOP: 0x000000C4 (0x0000003C, 0x00000000, 0x00000000)

Чтобы восстановить работоспособность вашего компьютера Вам следует сделать следующее:

**Отправьте SMS с текстом: id38948826 на номер: 2090  
(стоимость 10руб. без НДС)! Полученный КОД=ТРЕТЬЕ  
СЛОВО в ответном SMS-сообщении введите в поле:**

|                      |                      |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |
| Язык ввода: English  |                      |
| <b>ВВОД</b>          |                      |

A problem has been detected and Windows has been shut down to prevent damage to your Computer.

A device driver attempting to corrupt the system has been caught.  
The faulty driver currently on the kernel stack must be replaced with a working version.

Technical information:

\*\*\* STOP: 0x000000C4 (0x0000003C, 0x00000000, 0x00000000)

\*\*\* STOP: c000007b Unknown Hard Error Unknown Hard Error Beginning dump of physical memory



## Доступ в сеть заблокирован!

### Уведомление об необходимости активации ПО Digital Access

Вам был предоставлен пробный **бесплатный доступ** на 1 час для просмотра **эротического видео**

Напоминаем, что установив Программное Обеспечение Digital Access для осуществления доступа к эротическому видео с данного компьютера, вы согласились с условиями предложенного вам **пользовательского соглашения** на основании которого, при нежелании получать данный доступ далее, вы должны были удалить данное программное обеспечение до окончания срока действия пробного доступа или оплатить дальнейшее использование данного программного обеспечения.

### Пробный доступ к просмотру эротического видео сроком на 1 час истёк!

Для активации ПО Digital Access, автоматического разблокирования сети и скрывтия данного уведомления, необходимо отправить с моб. телефона

смс-сообщение с текстом **720010752** на номер **9690**

введите полученный код

Активировать

Данное уведомление будет появляться до тех пор, пока не будет осуществлена активация, которая производится только один раз и действует на весь срок использования вами ПО Digital Access.

Внимание!!! Попытка обмануть систему активации может причинить вред компьютеру

# Ransomware

## Variety

Windows Security Alert

 Центр обеспечения безопасности

Помогите защитить свой компьютер

 **Ресурсы:**

Главный офис  
Microsoft Corp. :  
Russia, 121745,  
г. Москва, Кирилловка  
дом 17 +4  
495-338-85-85  
Microsoft Corp.

 **На вашем компьютере обнаружена не лицензионная версия Windows!**

При последнем обновлении системы, центр сертификации Microsoft обнаружил на вашем компьютере не лицензионную версию Windows, дальнейшая работа на компьютере не возможна.

Для возобновления работы компьютера вам необходимо обратиться к одному из региональных поставщиков программного обеспечения, или если это для вас не возможно, то вы можете приобрести лицензионный, ключ отправив СМС с вашего мобильного телефона на следующие реквизиты:

- **Номер центра СМС сертификации:** **3649**
- **Текст сообщения (для вашего ПК):** **212727**

В ответ на ваше СМС сообщение вам придет ключ активации. Стоимость одной СМС лицензии составляет 50 руб. 50 коп., с учетом НДС. Для активации вашей версии Windows, введите полученный код в поле ниже и нажмите кнопку "Далее".

Формат ключа: **0000000** (семь цифр)

**Введите ваш ключ:**  



Корпорация Майкрософт охраняет конфиденциальность.

# Ransomware

## Variety



**Ваш компьютер заражен вирусом!**  
**Теперь вы не сможете зайти на сайт [vkontakte.ru](http://vkontakte.ru)**  
**Сканирование любым антивирусом бессмысленно!**

Если вы все еще можете зайти на сайт ВКонтакте не беспокойтесь,  
после перезапуска браузера вы сможете про него забыть

**Для того чтобы избавиться от вируса**  
**и возобновить доступ к [vkontakte.ru](http://vkontakte.ru)**

**отправьте смс с кодом **id21683897** на номер **2090****

### Kaspersky Lab Antivirus Online

Внимание! Онлайн проверка Лаборатории Касперского показала, что в вашей системе обнаружен вредоносный вирус, который постепенно заражает все файлы на вашем компьютере.

Вирус временно заблокирован, но его алгоритм шифрования постоянно меняется и остановить его на данный момент без этой программы не представляется возможным. Для того чтобы удалить вредоносный вирус, необходимо узнать каков на данный момент у вируса алгоритм шифрования, для этого необходимо отправить sms на короткий номер 2895 (для России) или 4161 (для Украины) с текстом 70+112701+now\_algorithm. Стоимость sms составляет 150 рублей (20 гривен). После того как вы отправите sms, вам моментально будет послан ключ, отключающий вирус. Введите этот ключ, и программа полностью удалит вирус с вашего компьютера.

Алгоритм шифрования вируса сменится через 216 секунд

(по истечению этого времени настоятельно рекомендуется удалить его)

Введите полученный вами ключ в это поле:

Удалить

\* Программа блокирует все доступные способы входа в Windows, так как если не удалить зловерный вирус ВСЕ файла на вашем компьютере очень скоро будут заражены. Внимание: переустановка вивдовс не изменит ситуацию, так как вирус прописывает себя в загрузочные сектора жесткого диска.

Английский (США)

# ВАШ БРАУЗЕР ЗАБЛОКИРОВАН!

Если вы хотите разблокировать ваш компьютер и полноценно пользоваться сайтами

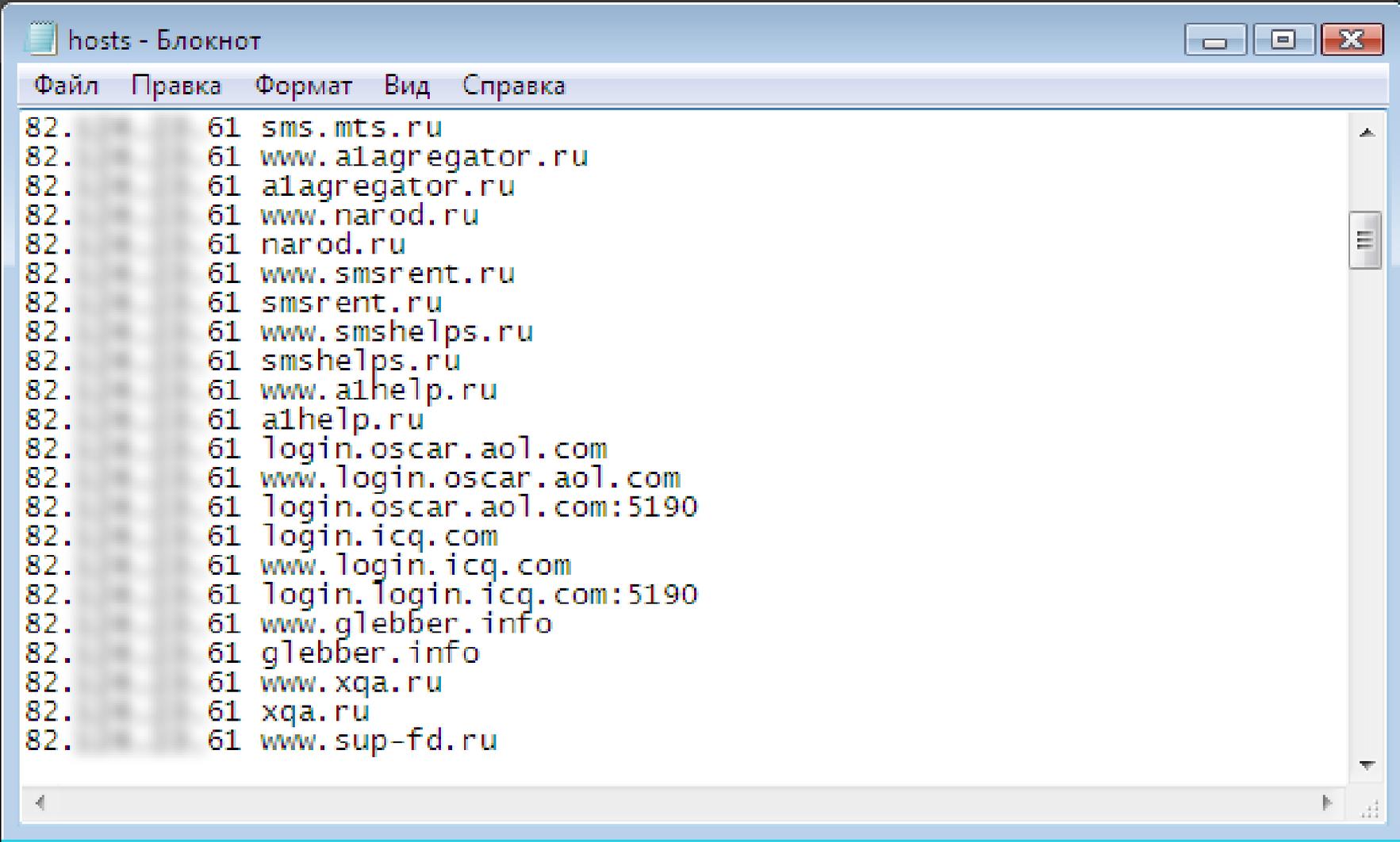
Необходимо отправить SMS  
Выберите вашего оператора

Страна:

Оператор:

# Ransomware

## Variety



```
82. 61 sms.mts.ru
82. 61 www.alagregator.ru
82. 61 alagregator.ru
82. 61 www.narod.ru
82. 61 narod.ru
82. 61 www.smsrent.ru
82. 61 smsrent.ru
82. 61 www.smshelps.ru
82. 61 smshelps.ru
82. 61 www.aihelp.ru
82. 61 aihelp.ru
82. 61 login.oscar.aol.com
82. 61 www.login.oscar.aol.com
82. 61 login.oscar.aol.com:5190
82. 61 login.icq.com
82. 61 www.login.icq.com
82. 61 login.login.icq.com:5190
82. 61 www.glebber.info
82. 61 glebber.info
82. 61 www.xqa.ru
82. 61 xqa.ru
82. 61 www.sup-fd.ru
```

# 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 #:



## Remove banner from Desktop, unlock Windows

Phone number

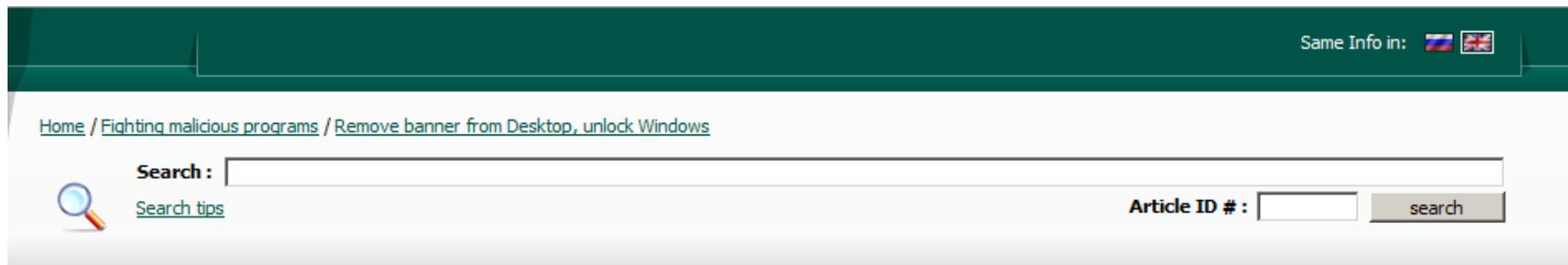
Free service Deblocker helps to **delete/remove banner from Desktop, unlock Windows** or restore access to encrypted files without sending an SMS message.

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



## Remove banner from Desktop, unlock Windows

Phone number

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

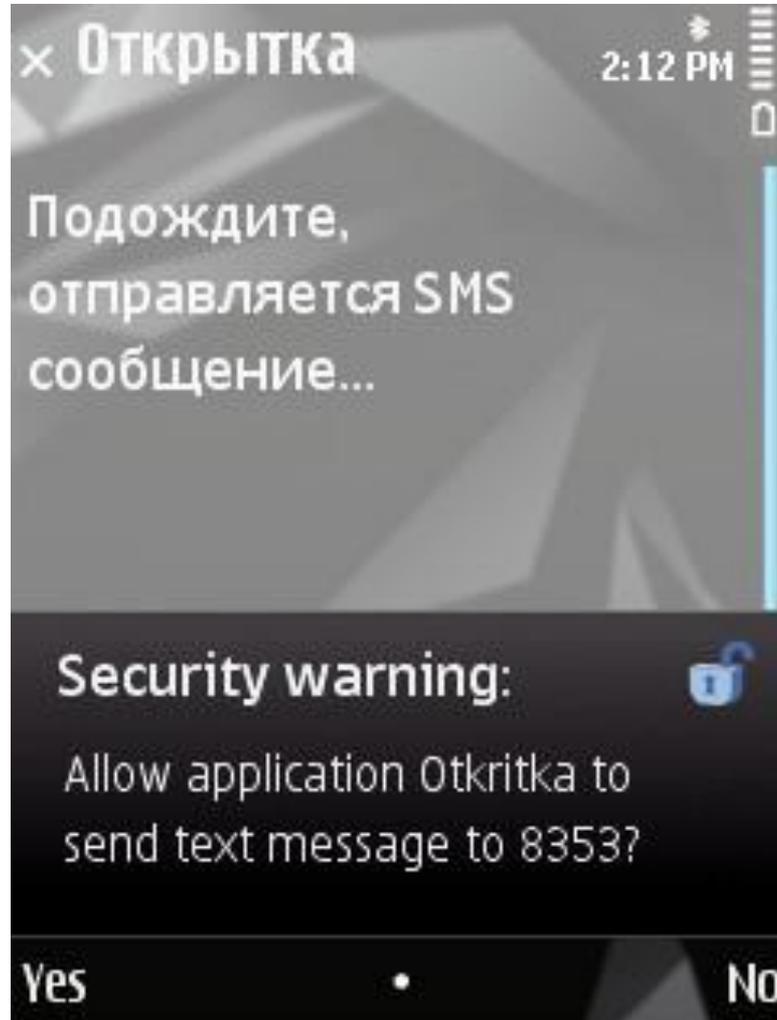


Source: Kaspersky Lab

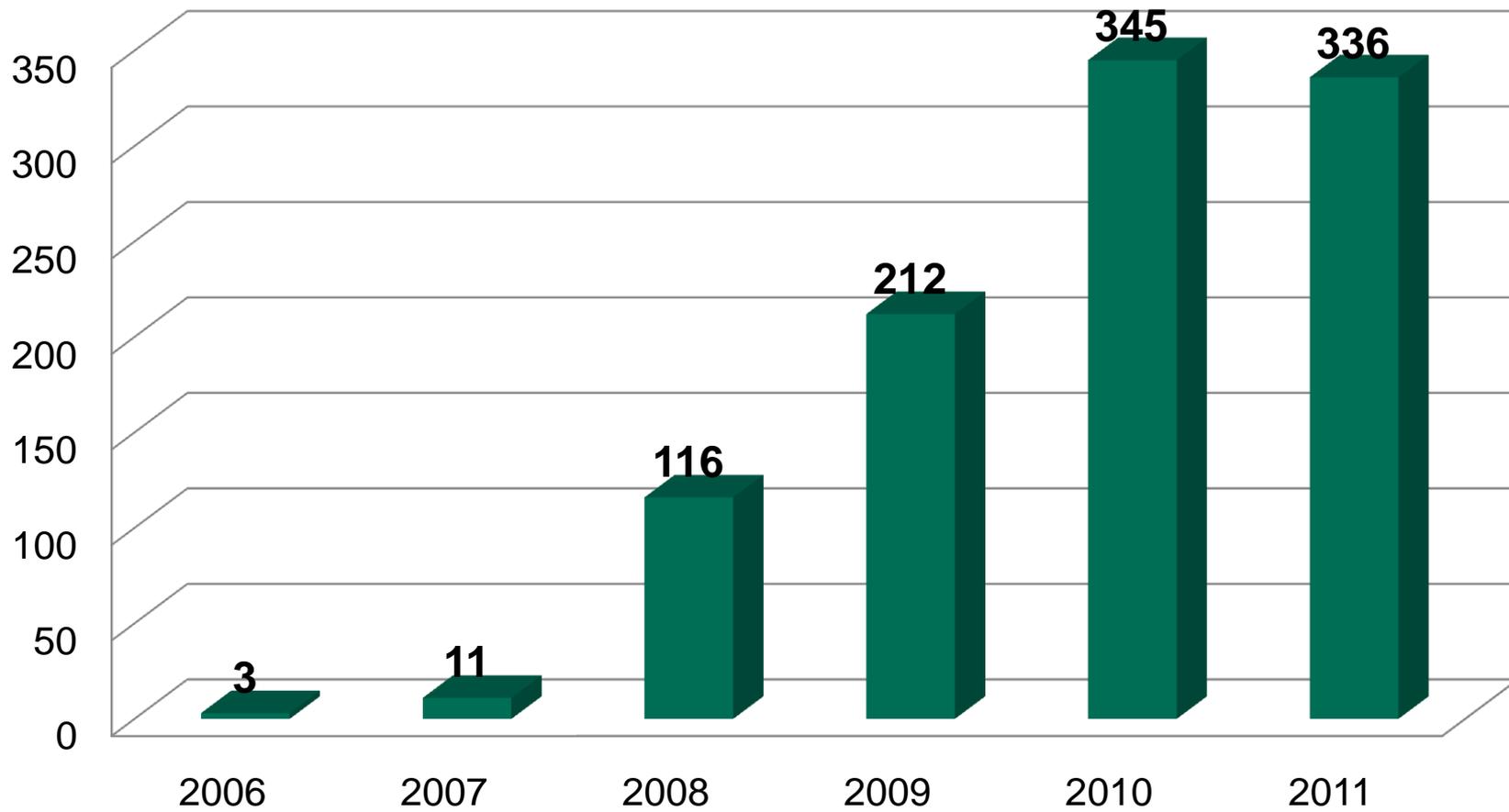
# SMS Trojans

# SMS Trojans

In a nutshell

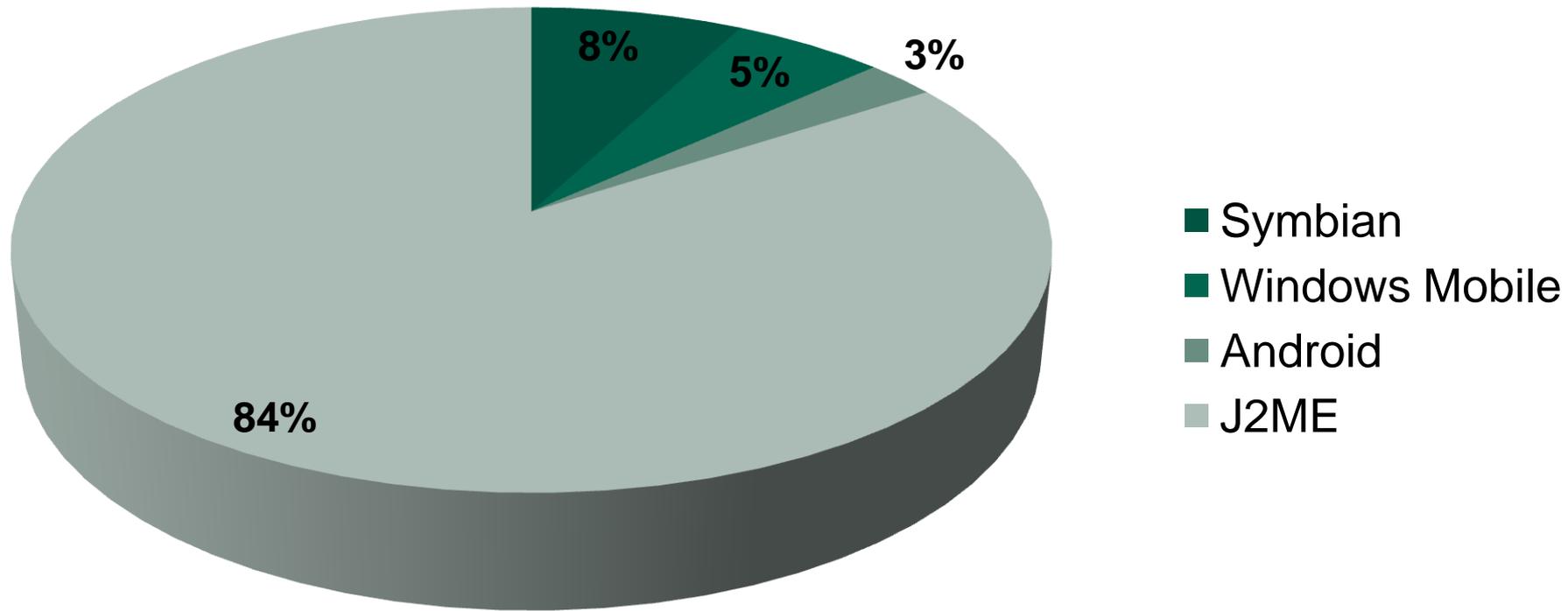


## Number of modifications per year



Source: Kaspersky Lab

## Platform distribution



Source: Kaspersky Lab

# Primitive: Trojan-SMS.J2ME.Konov

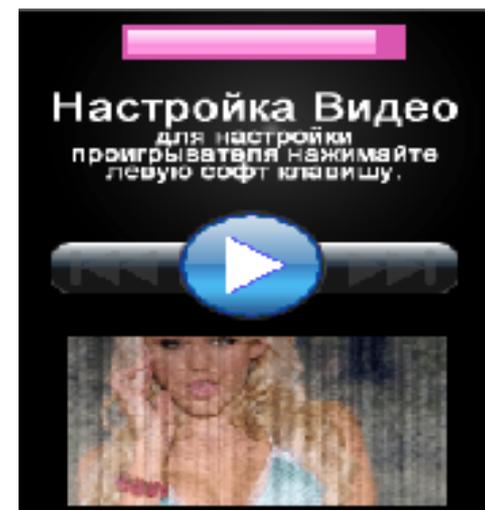
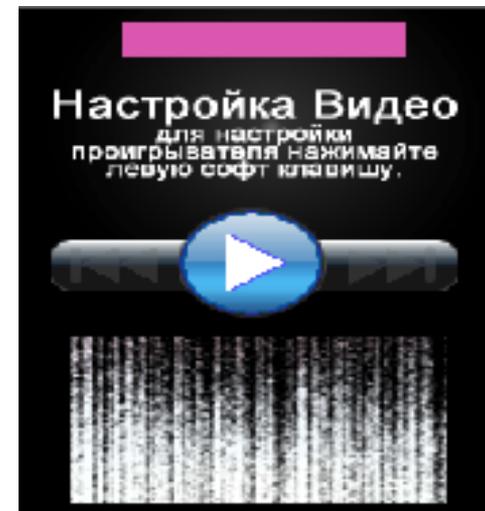
## ► One of the first **widespread** SMS Trojans:

- **Small** (1,5 – 8 kB)
- **No encryption**
- **No social engineering tricks**

```
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: #maibox 1290
Send-Number-1: 4460
Send-Number-2: 5537
Send-Number-3: 7733
Send-Number-4: 1171
Send-Number-5: 9395
```

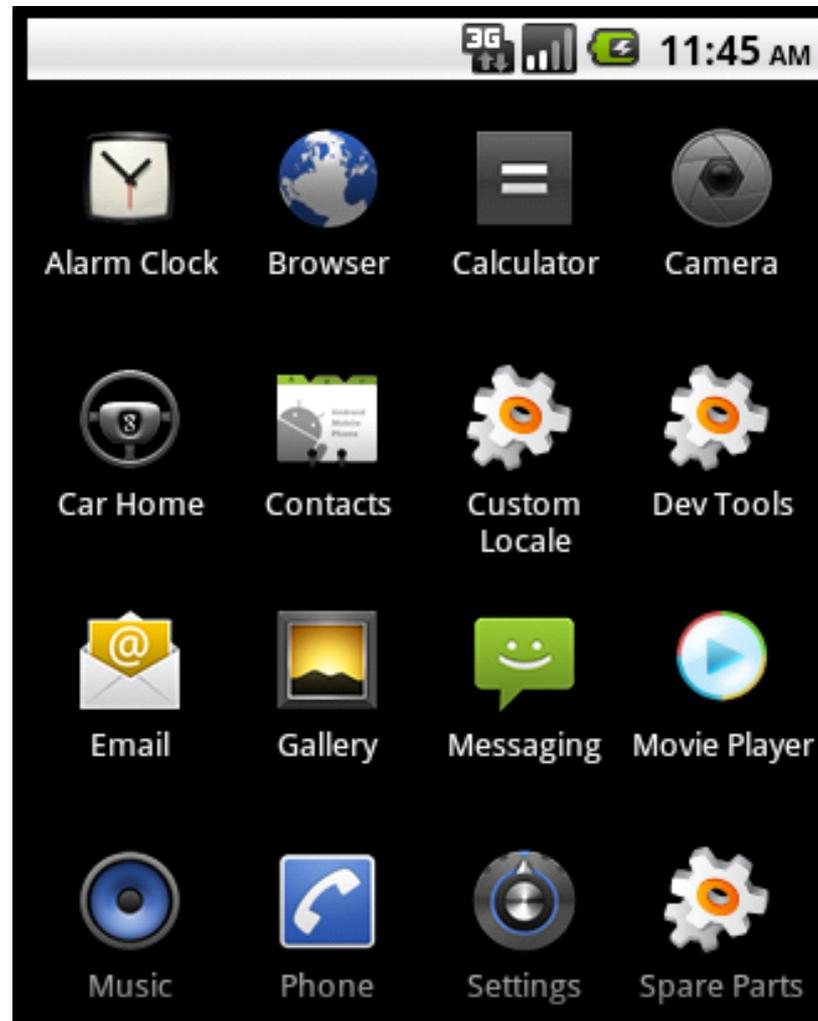
# Advanced: Trojan-SMS.J2ME.VScreener

- ▶ **'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



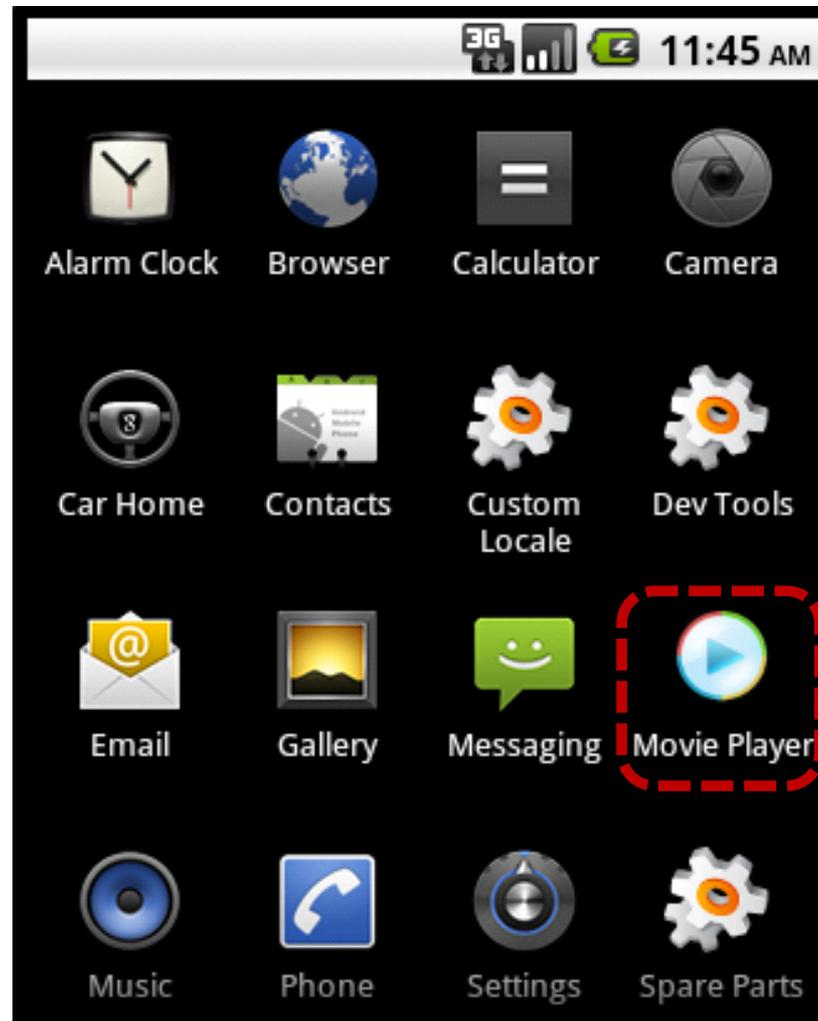
# 'Video player'

Again



# 'Video player'

Again



# SEO and mobile malware

Веб [Картинки](#) [Видео](#) [Карты](#) [Новости](#) [Переводчик](#) [Gmail](#) [ещё](#) ▼



блондинки порно скачать



Поиск

[Расширенный поиск](#)  
[Настройки](#)

Поиск в Интернете  Только на русском

Веб

Результаты 1 - 10 из примерно 592 000 для бл

[Порно фото, порно видео и эротика на \[REDACTED\]](#)

Посмотрите, какие куколки снимаются в **порно**! Настоящие **блондинки** с точеными ...  
лучшее и качественное **порно**, которое вы сможете **скачать** полностью бесплатно. ...

[REDACTED] - [Сохраненная копия](#) - [Похожие](#)

# SEO and mobile malware

Веб [Картинки](#) [Видео](#) [Карты](#) [Новости](#) [Переводчик](#) [Gmail](#) [ещё](#) ▼

Google

блондинки порно скачать



Поиск

[Расширенный поиск](#)  
[Настройки](#)

Поиск в Интернете  Только на русском

Веб

Результаты 1 - 10 из примерно 592 000 для бл

[Порно фото, порно видео и эротика на \[REDACTED\]](#)

Посмотрите, какие куколки снимаются в порно! Настоящие блондинки с точеными ...  
лучшее и качественное порно, которое вы сможете скачать полностью бесплатно. ...

[REDACTED] - [Сохраненная копия](#) - [Похожие](#)

Blonde porn  
download

# The ecosystem

The root of all evil

# 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: #paybox 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

```
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: #maibox 1290
Send-Number-1: 4460
Send-Number-2: 5537
Send-Number-3: 7733
Send-Number-4: 1171
Send-Number-5: 9395
```

\$10 or \$6 per  
SMS

Mobile  
operator

# 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: #maibox 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

```
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: #maibox 1290
Send-Number-1: 4460
Send-Number-2: 5537
Send-Number-3: 7733
Send-Number-4: 1171
Send-Number-5: 9395
```

Mobile operator

Content provider

4460  
5537

# 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: #paybox 1290
Send-Number-1: 4460
Send-Number-2: 5537
Send-Number-3: 7733
Send-Number-4: 1171
Send-Number-5: 9395
```

Subtenant  
with ID 1290

'epbox  
1290' on  
4460 &  
5537

'epbox'  
renter

'epbox'  
on 4460  
& 5537

Mobile  
operator

Content  
provider

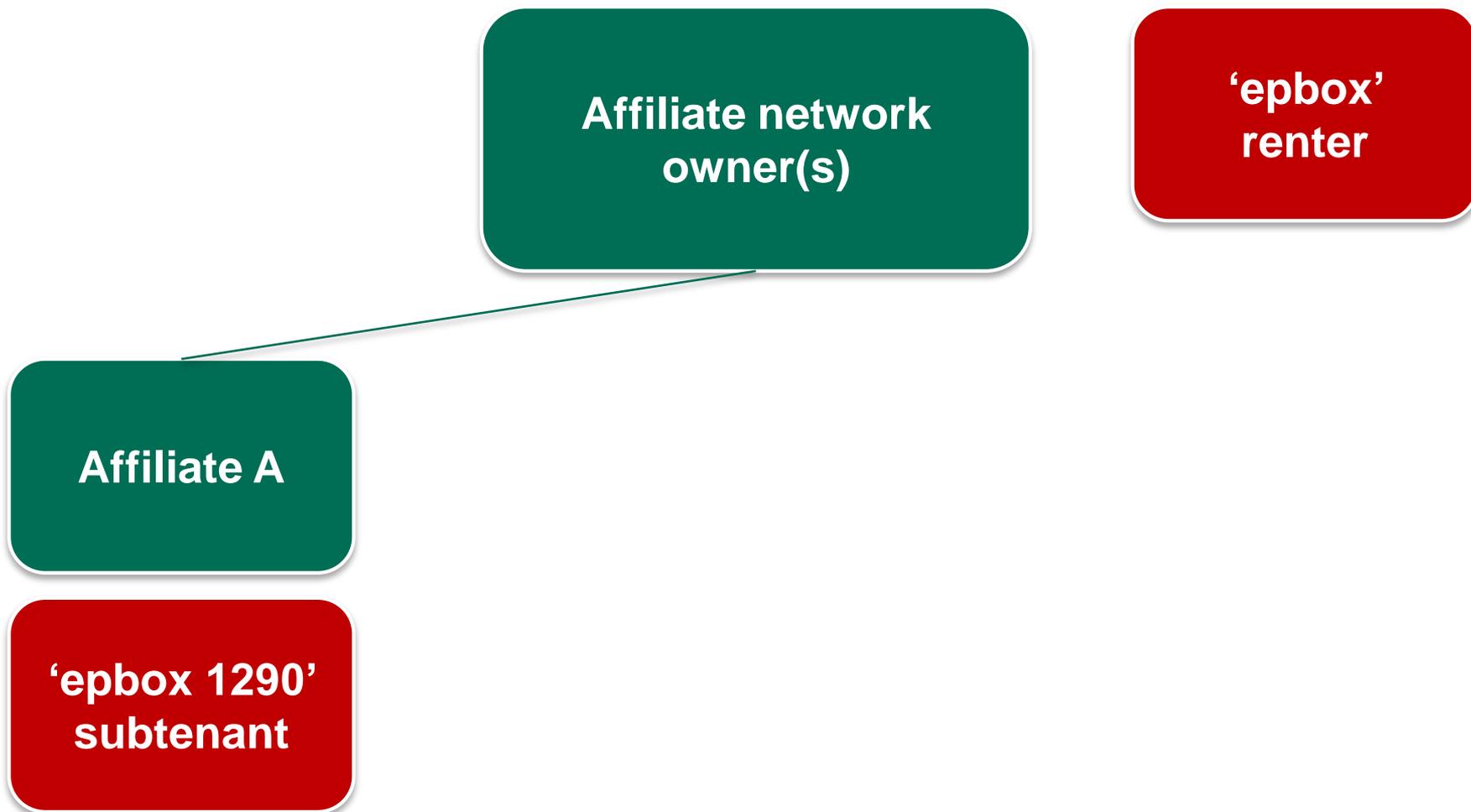
4460  
5537

# Who are 'epbox' and 'epbox 1290'

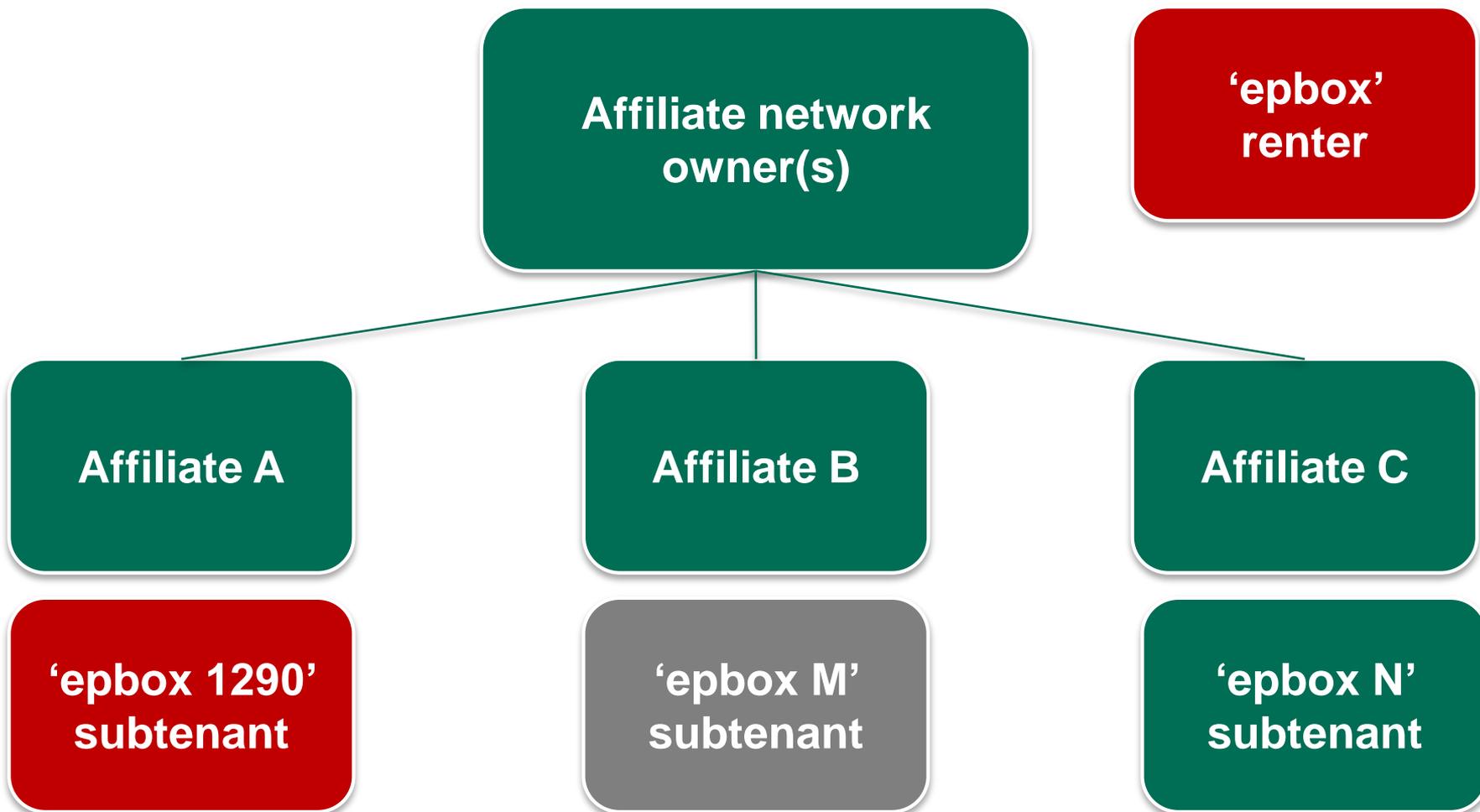
**'epbox'  
renter**

**'epbox 1290'  
subtenant**

# Who are 'epbox' and 'epbox 1290'



# Who are 'epbox' and 'epbox 1290'



# The root of all evil

## ► Affiliate network registration form



Регистрация...

Поля, выделенные **красным** обязательны к заполнению:

**Ваше имя:**

**Ваше e-mail:**

**Ваш сайт:**

**Название сайта:**

Выплаты WebMoney:

**WMZ:**

**WMR:**

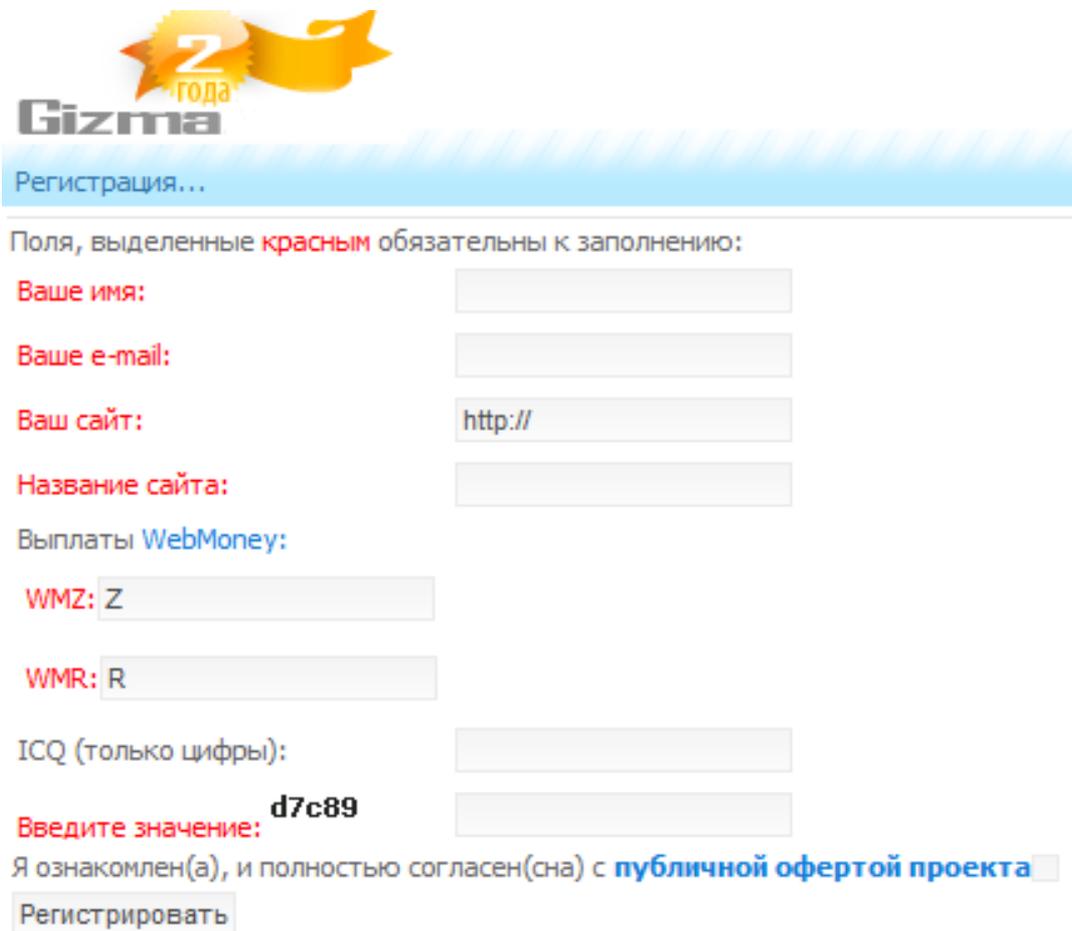
ICQ (только цифры):

**Введите значение:**

Я ознакомлен(а), и полностью согласен(сна) с **публичной офертой проекта**

# The root of all evil

## ► Affiliate network registration form



**Gizma**  
2 года

Регистрация...

Поля, выделенные **красным** обязательны к заполнению:

**Ваше имя:**

**Ваше e-mail:**

**Ваш сайт:**

**Название сайта:**

Выплаты **WebMoney:**

**WMZ:**

**WMR:**

**ICQ (только цифры):**

**Введите значение:**

Я ознакомлен(а), и полностью согласен(сна) с **публичной офертой проекта**

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

# The root of all evil

## ► Affiliate network registration form

**Gizma**  
2 года

Регистрация...

Поля, выделенные **красным** обязательны к заполнению:

**Ваше имя:**

**Ваше e-mail:**

**Ваш сайт:**

**Название сайта:**

Выплаты **WebMoney:**

**WMZ:**

**WMR:**

**ICQ (только цифры):**

**Введите значение:**

Я ознакомлен(а), и полностью согласен(сна) с **публичной офертой проекта**

**No sensitive data!**

**Affiliate ID  
'epbox 1290'**

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

# Typical affiliate website

Скачать сейчас!



[Скачать/3qr,mp4](#)



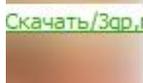
[Скачать/3qr,mp4](#)



[Скачать/3qr,mp4](#)



[Скачать/3qr,mp4](#)



[Скачать/3qr,mp4](#)



[Скачать/3qr,mp4](#)

[Скачать/3qr,mp4](#)

[Скачать/3qr,mp4](#)

Лучшее на сайте:

- [Джим с SEX смайлами](#)
- [ICQ шпион 5.2! NEW](#)

# Typical affiliate website

Скачать сейчас!



[Скачать/3qr,mp4](#)



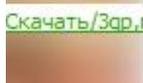
[Скачать/3qr,mp4](#)



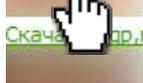
[Скачать/3qr,mp4](#)



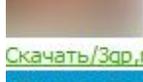
[Скачать/3qr,mp4](#)



[Скачать/3qr,mp4](#)



[Скачать/3qr,mp4](#)



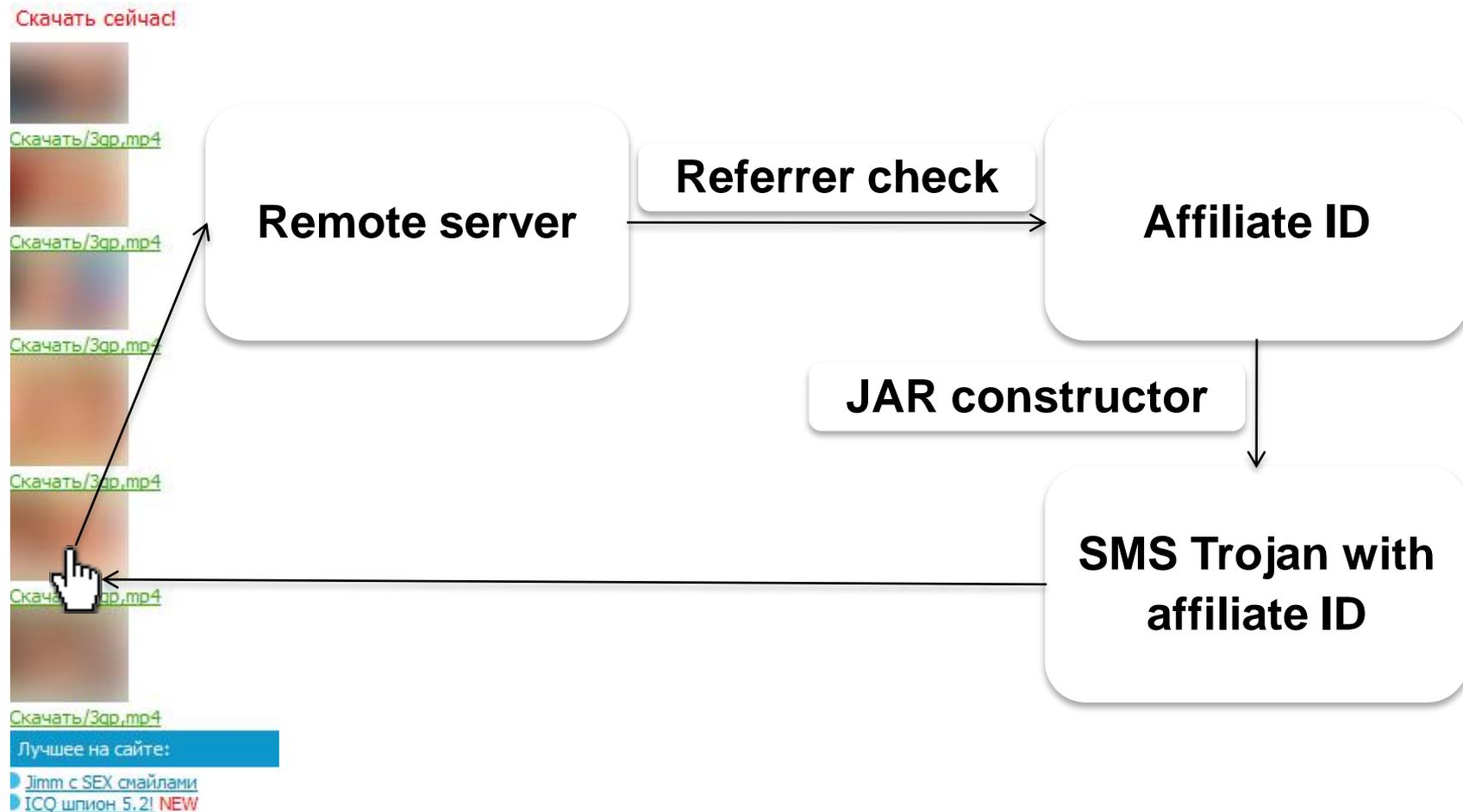
[Скачать/3qr,mp4](#)

Лучшее на сайте:

- [Джмм с SEX смайлами](#)
- [ICQ шпион 5.2! NEW](#)



# Typical affiliate website





# Ransomware

## Same situation

Главная > Сейчас на сайте 508 человека Смотри без СМС Войти на сайт | Регистрация

Горячее видео

12366 роликов | 5126 пользователей

РегистрацияЛучшее за сегодня | Лучшее за неделю | Лучшее за месяц | Топ100

Категории

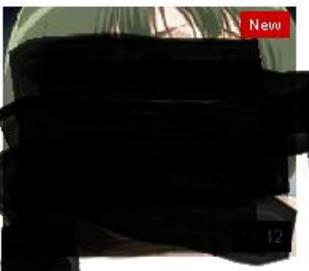
New

14:02

11491★ 95%



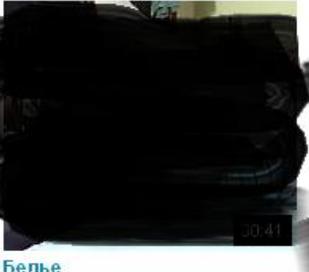
12556★ 89%

New

14120★ 94%

New

11201★ 97%



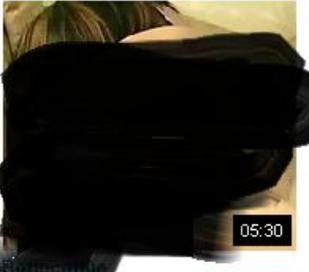
11243★ 64%



22102★ 95%

New

13431★ 95%



24503★ 86%



24503★ 73%



10963★ 98%

PAGE 48 |

23<sup>rd</sup> Annual FIRST Conference

| June 15, 2011



# Ransomware

Same situation



vr\_media\_player3.1\_inst.exe...  
Microsoft



vr\_codecpackage.exe\_.exe  
Microsoft



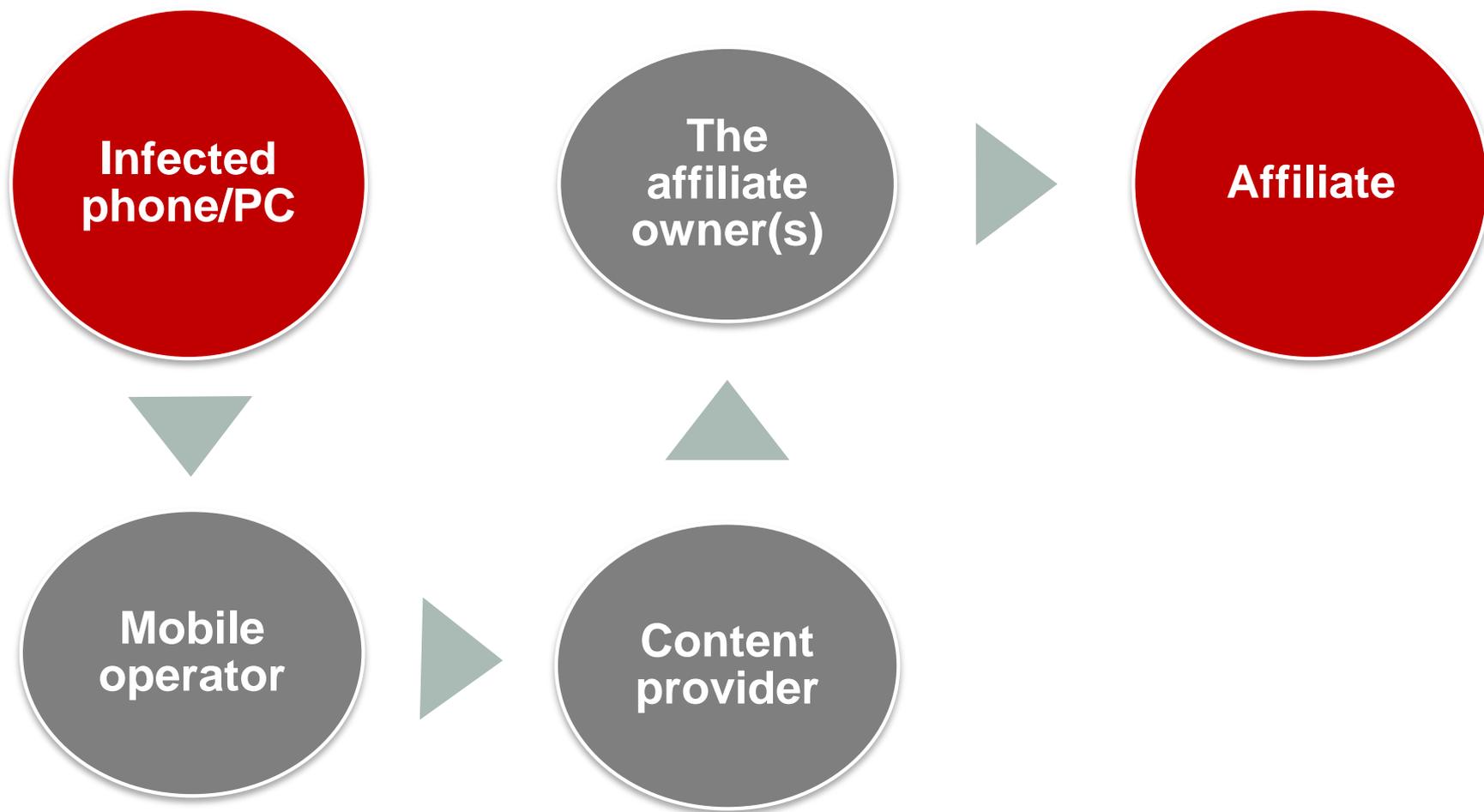
vr\_update\_player\_x90.exe\_....  
XlbOwO  
zOyvNN

# Underground economy

...and lottery results :)

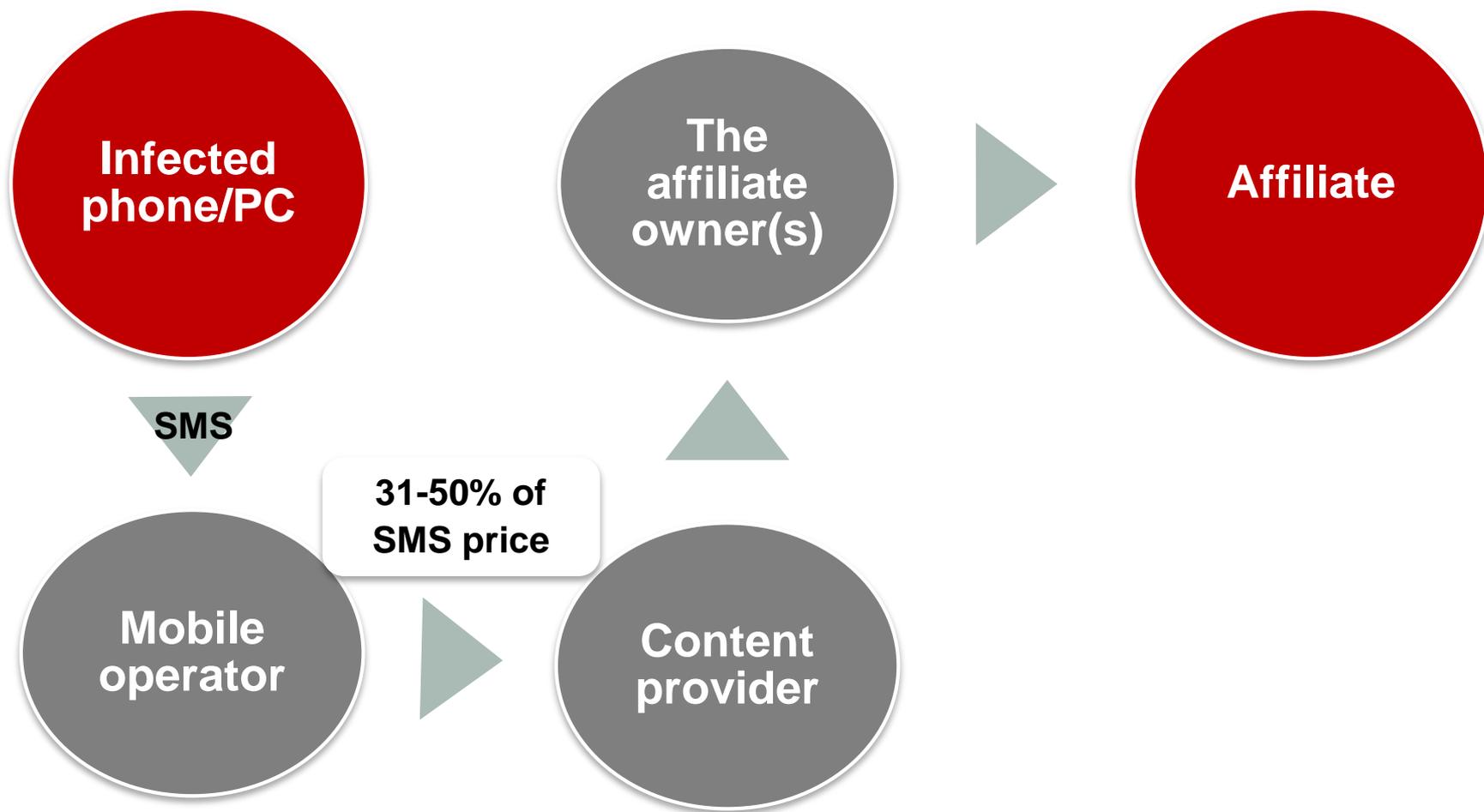
# Underground economy

## Revenue sharing



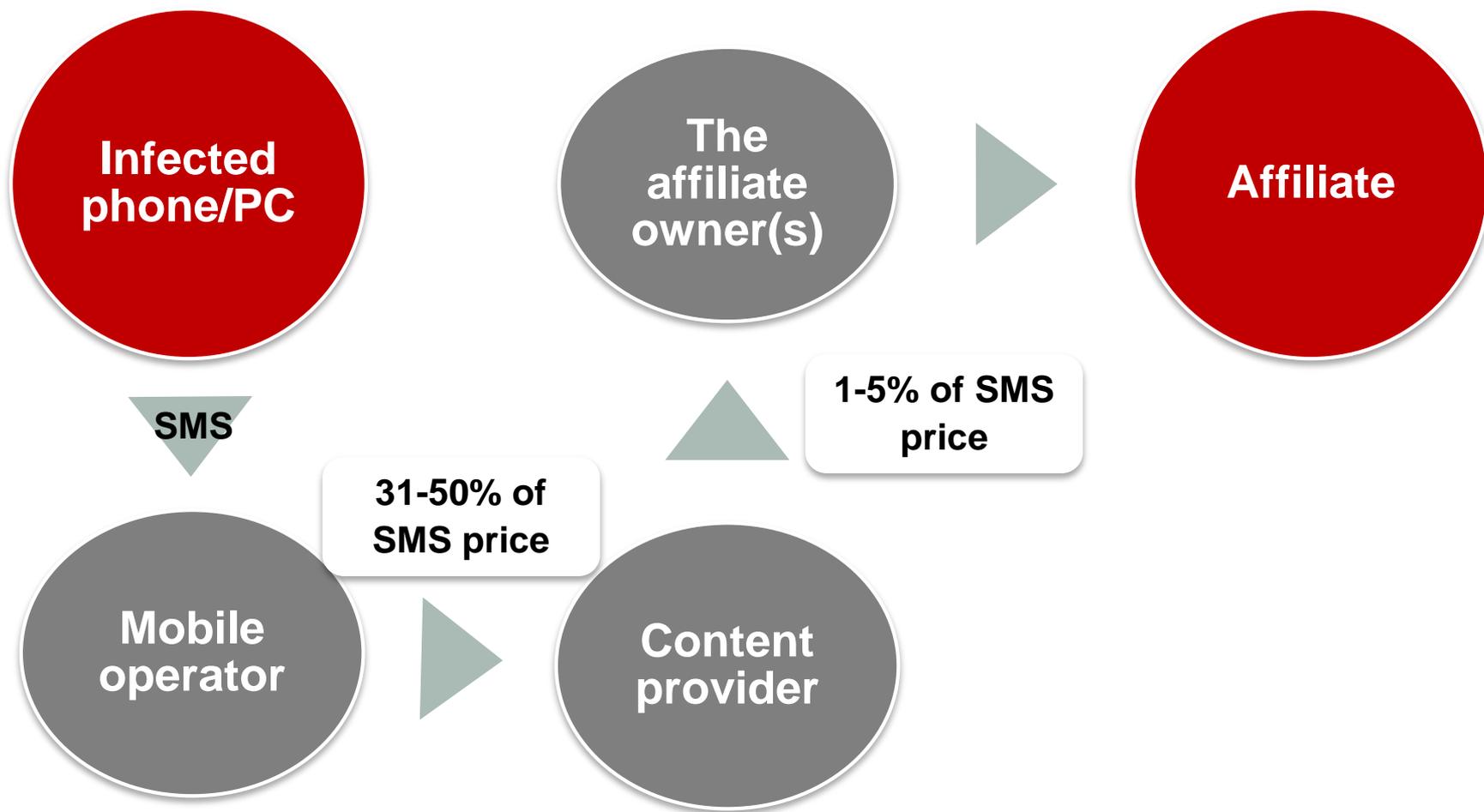
# Underground economy

## Revenue sharing



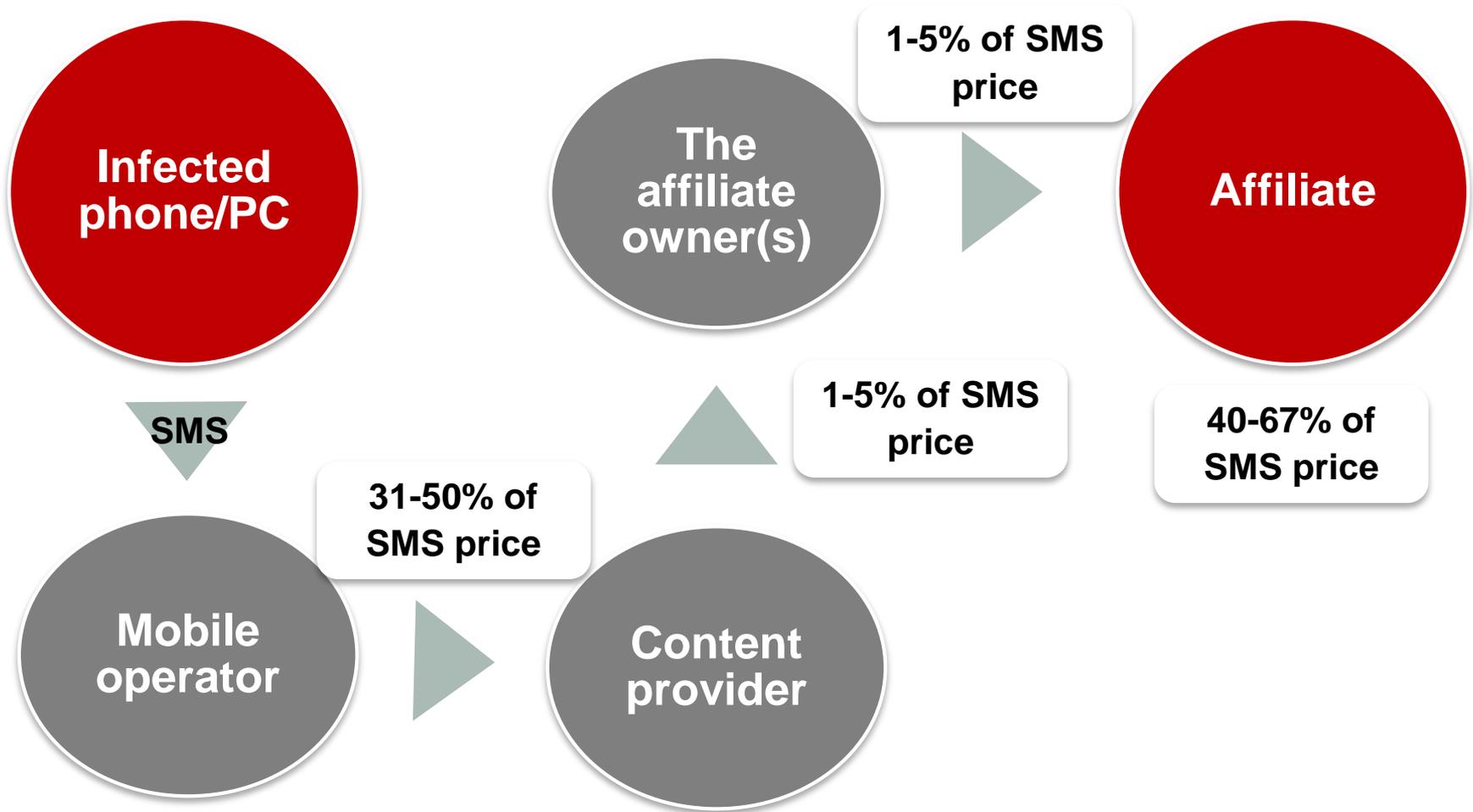
# Underground economy

## 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

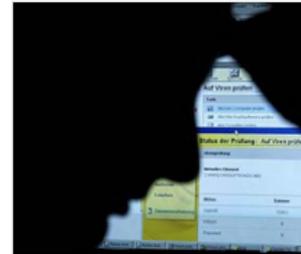
**Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали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

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

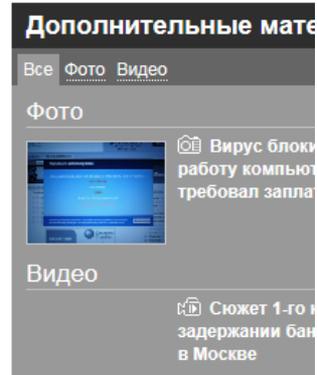
### Нечестные вымогатели

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



Жертвами кибер-мошенников стали тысячи пользователей интернета



## 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

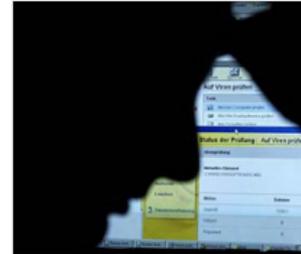
Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали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

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

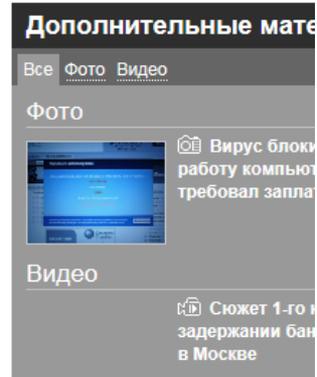
### Нечестные вымогатели

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



Жертвами кибер-мошенников стали тысячи пользователей интернета



‘...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

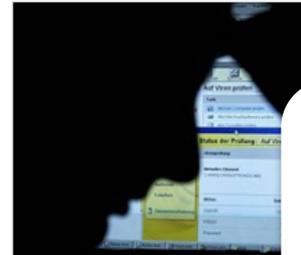
Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали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

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

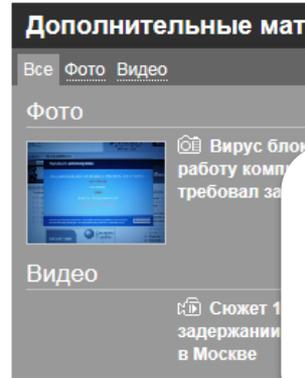
### Нечестные вымогатели

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



Жертвами кибер-мошенников пользователей интернета



‘...10 people were arrested...’

‘...half a year...’

‘...malware which blocks PC...’

‘...SMS as ransom...’

## 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

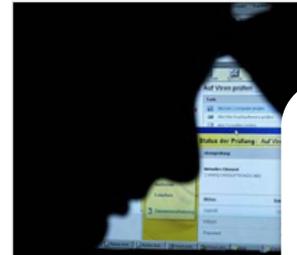
Оперативники столичного УБЭПа совместно с коллегами из отдела «К» ГУВД Москвы обезвредили группу хакеров, распространявшую вирусы, которые выводили из строя персональные компьютеры пользователей. Чтобы «оживить» технику, аферисты требовали отправить им платное SMS. От действий злоумышленников пострадали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

Как рассказали [GZT.RU](#) в столичном УБЭПе, фигурантами уголовного дела являются 10 человек, организаторы преступления, а также программисты, написавшие вирусы. Вирус блокировал работу компьютера, а для восстановления работоспособности требовалось отправить платное SMS-сообщение. По словам милиции, в основном жертвами становились молодые люди, пользователи интернета.

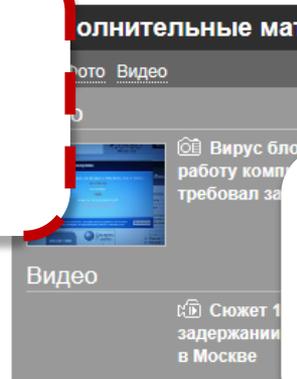
### Нечестные вымыслы

Орудовали хакеры, 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



Жертвами кибер-мошенников пользователи интернета



‘...10 people were arrested...’

‘...half a year...’

‘...1 billion rubles...’

‘...malware which blocks PC...’

‘...SMS as ransom...’

**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:

-1,588,999.54 Штраф 25% за использование ява регистрации без указания стоимост и отправкой множественных смс запросов.

### ▶ 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

# 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 deaktivieren,Windows

zu starten und dann sofort das Virus zu loeschen. Andernfalls wird diser Virus activ und loescht komplett 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



# A long time ago...



# Porn SMS senders

'Nooit spijt' case



# Porn SMS senders

## 'Nooit spijt' case



### Disclaimer

Abonneer je nu Krazymob! Type in de RELEASE ON -en versturen naar 6343, wordt u de Krazymob lid en krijg 3-gehalte per week. Dit is een abonnementsdienst van € 4.50/week abonnement voor 3-gehalte tot de tekst STOP naar 6343. Standaard carrier & datasnelheden toe te passen en abonnementskosten zullen worden gefactureerd op uw mobiele telefoon of afgetrokken van uw vooruitbetaalde saldo. Tekst HELP naar 6343 voor hulp. Om te annuleren, stuur STOP naar 6343. CS Help: 0-800-022-4671. By het verzenden van dit SMS, bent u akkoord met de voorwaarden. Voor meer info kunt u terecht op <http://nl.krazymob.com>.

# 'Dating' apps

If you are from UK

**Babe Finder**

 Emily, 23, Liverpool

 Jessica, 22, London

 Ivy, 20, Bradford

 Samantha, 25, Coventry

---

Exit

Select

# 'Dating' apps

## If you are from UK

### Babe Finder

 Emily, 23, Liverpool

 Jessica, 22, London

 Ivy, 20, Bradford

 Samantha, 25, Coventry

---

Exit

Select

## If you are from US

### BabeFinder

 Stefani, 23, LA

 Angela, 22, NY

 Lydia, 20, DC

 Joanne, 25, CA

---

Exit

Select

# 'Dating' apps

## If you are from UK

### Babe Finder

 Emily, 23, Liverpool

 Jessica, 22, London

 Ivy, 20, Bradford

 Samantha, 25, Coventry

## If you are from US

### BabeFinder

 Stefani, 23, LA

 Angela, 22, NY

 Lydia, 20, DC

 Joanne, 25, CA

Emily, 23, Liverpool



Tease Me

Exit

Select

**Name:** Emily, 23, Liverpool

**Age:** 23

**Height:** 168cm

**Weight:** 45kg

**BWH:** 36-24-38

Back



Menu

Exit

Select

## '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, 23<sup>rd</sup> Annual FIRST Conference, Vienna, Austria