Russian cybercriminals on the move: profiting from mobile malware

Denis Maslennikov

Senior Malware Analyst, Mobile Research Group Manager
Kaspersky Lab

Virus Bulletin International Conference, September 29 – October 1
Westin Bayshore Hotel, Vancouver, BC, Canada

Agenda

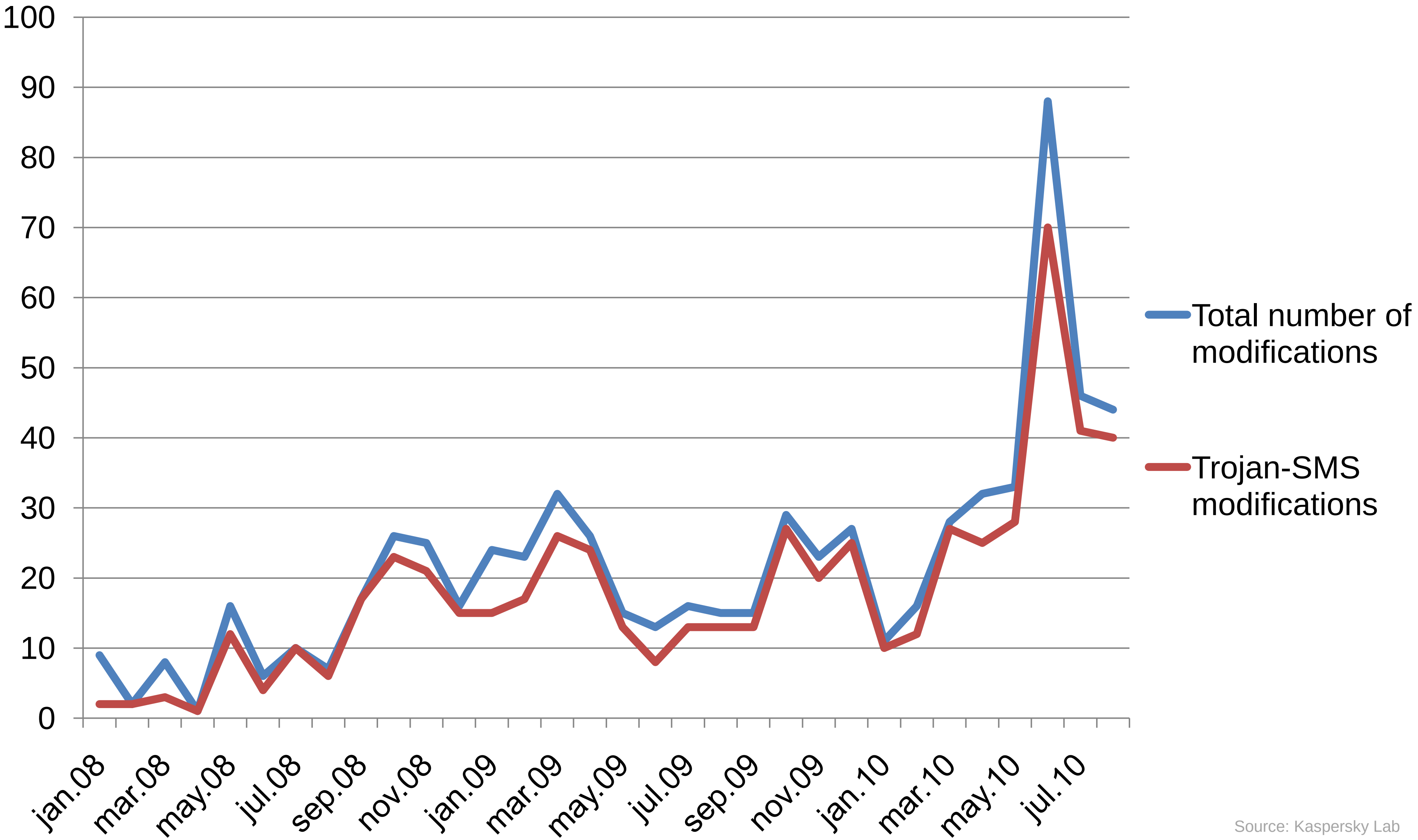
- Statistics
- Evolution of SMS Trojans:
  - J2ME Trojans
  - Symbian and Windows Mobile Trojans
- The root of all evil
  - Affiliate networks
  - Anonymity
- How much do they make?
- Today and tomorrow

‘A long time ago…’

Trojan-SMS.J2ME.RedBrowser.a

Statistics

Mobile malware vs. Trojan-SMS: the numbers

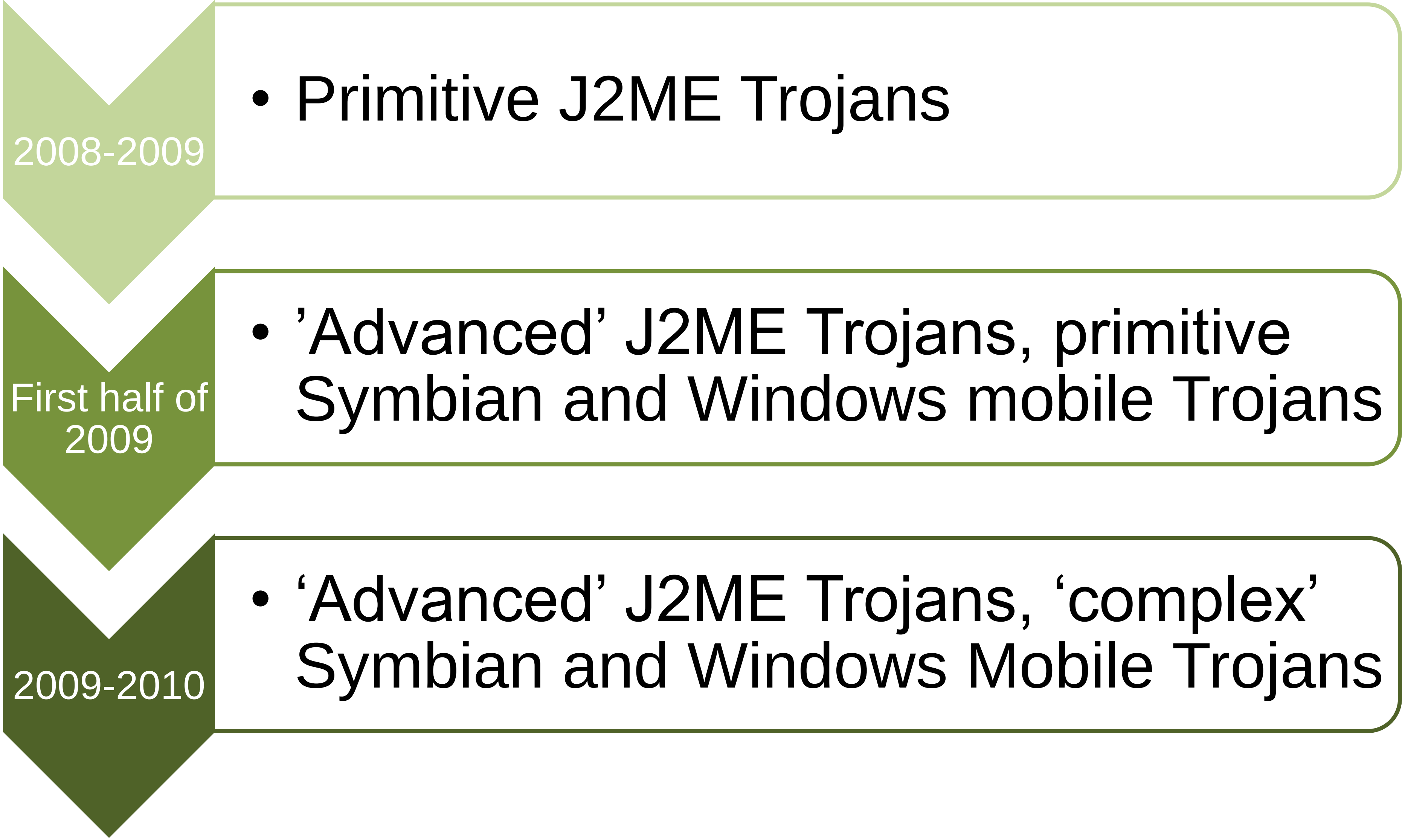


Source: Kaspersky Lab

Evolution of SMS Trojans

Notable examples

Evolution overview



2008-2009

- Primitive J2ME Trojans

First half of 2009

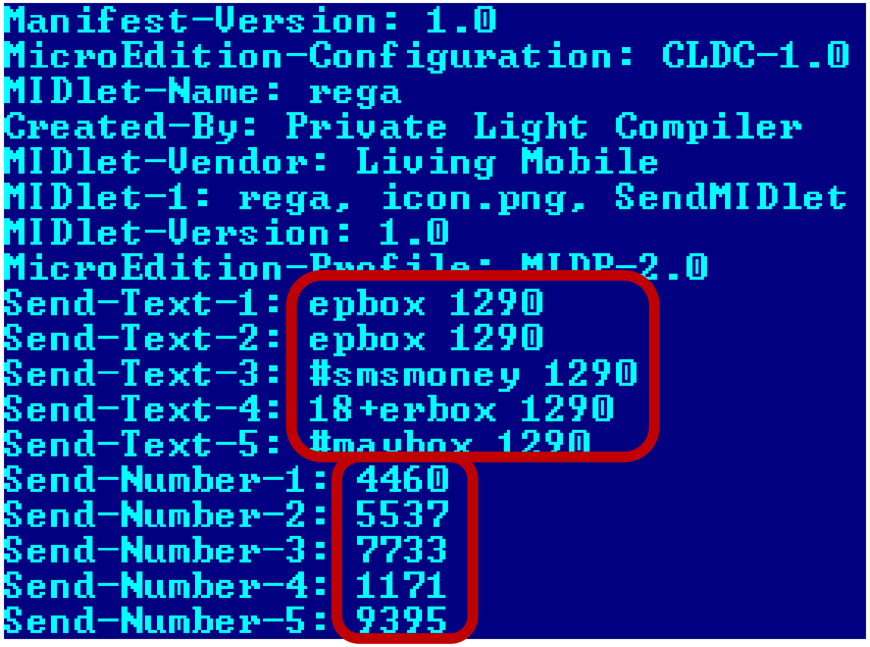
- ’Advanced’ J2ME Trojans, primitive Symbian and Windows mobile Trojans

2009-2010

- ‘Advanced’ J2ME Trojans, ‘complex’ Symbian and Windows Mobile Trojans

Primitive: Trojan-SMS.J2ME.Konov

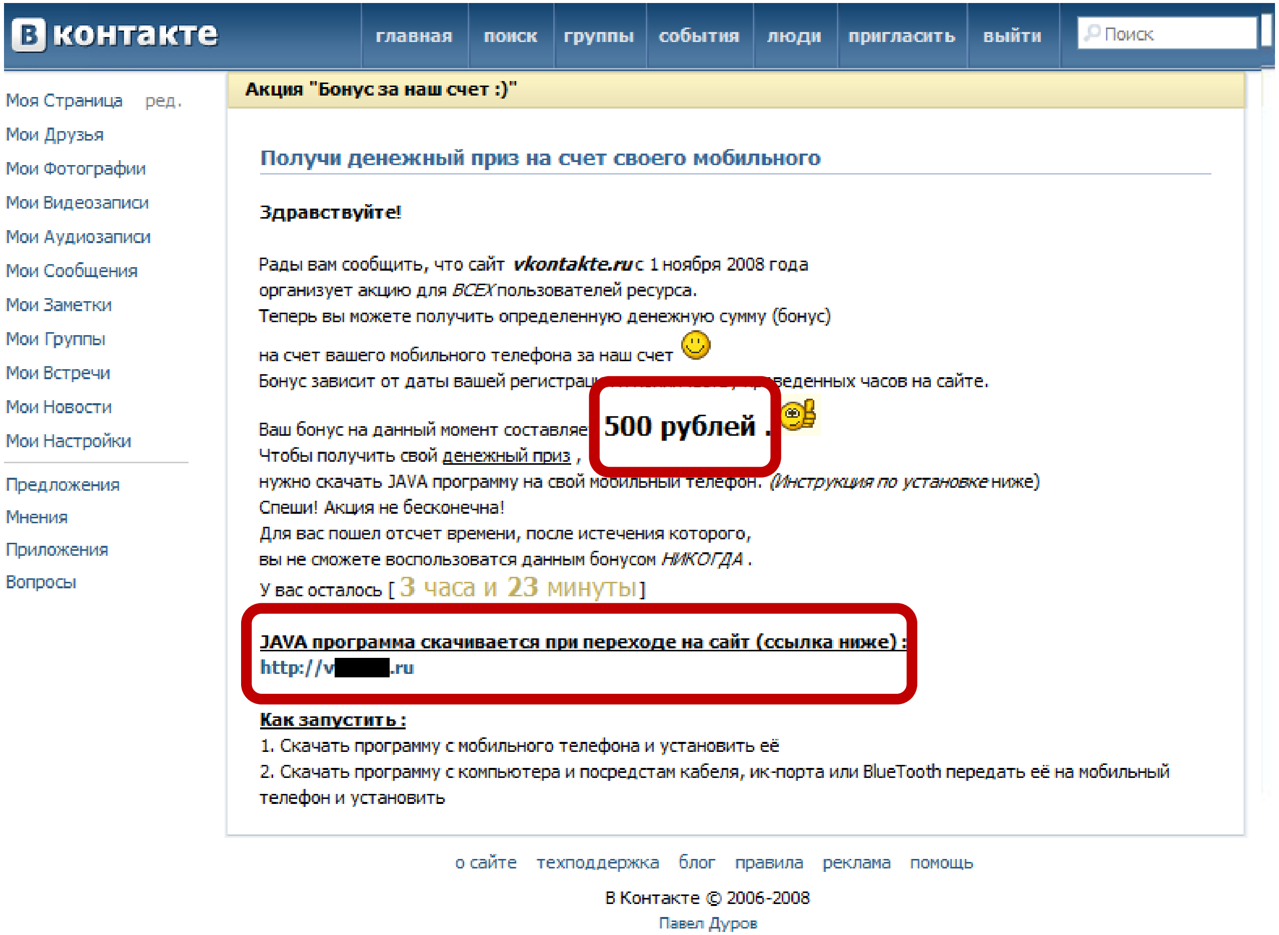
- One of the first widespread SMS Trojans:
  - Small (1.5 – 6 kB)
  - No encryption
  - No social engineering



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

Konov and VKontakte

- Spam in social networks



Акция "Бонус за наш счет :)"

Получи денежный приз на счет своего мобильного

Здравствуйте!

Рады вам сообщить, что сайт ***vkontakte.ru*** с 1 ноября 2008 года
организует акцию для *ВСЕХ* пользователей ресурса.
Теперь вы можете получить определенную денежную сумму (бонус)
на счет вашего мобильного телефона за наш счет
Бонус зависит от даты вашей регистраци веденных часов на сайте.

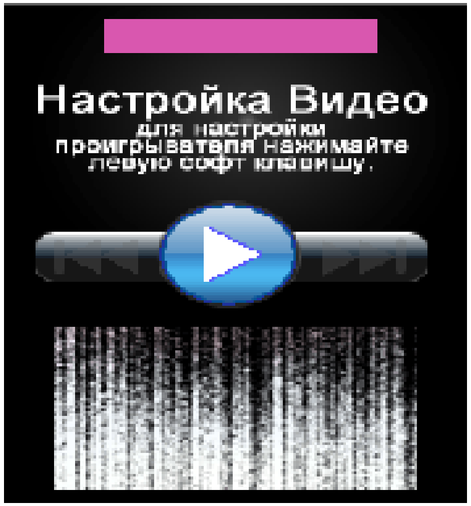
Ваш бонус на данный момент составляе **500 рублей .**
Чтобы получить свой денежный приз ,
нужно скачать JAVA программу на свой мобильный телефон. *(Инструкция по установке* ниже)
Спеши! Акция не бесконечна!
Для вас пошел отсчет времени, после истечения которого,
вы не сможете воспользоватся данным бонусом *НИКОГДА* .
У вас осталось [3 часа и 23 минуты]

JAVA программа скачивается при переходе на сайт (ссылка ниже) :
http://v[redacted].ru

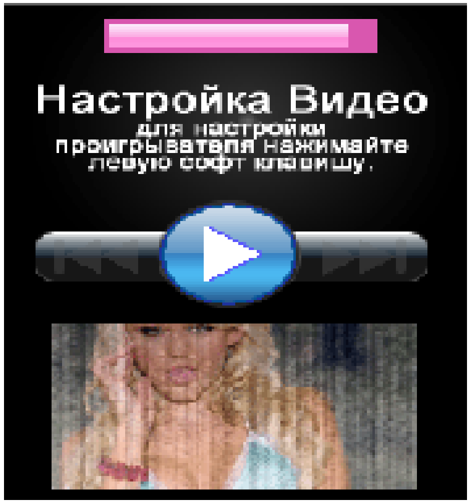
Как запустить :
1. Скачать программу с мобильного телефона и установить её
2. Скачать программу с компьютера и посредстам кабеля, ик-порта или BlueTooth передать её на мобильный телефон и установить

‘Advanced’: Trojan-SMS.J2ME.VScreener

- ‘Faulty’ video player
- Must be ‘tuned’ by user:
  - Quick press left soft key
- SMSs are sent during ‘tuning’
- Premium rate number and SMS text are stored in ‘load.bin’ file and encoded with ADD and ‘0xA’ key



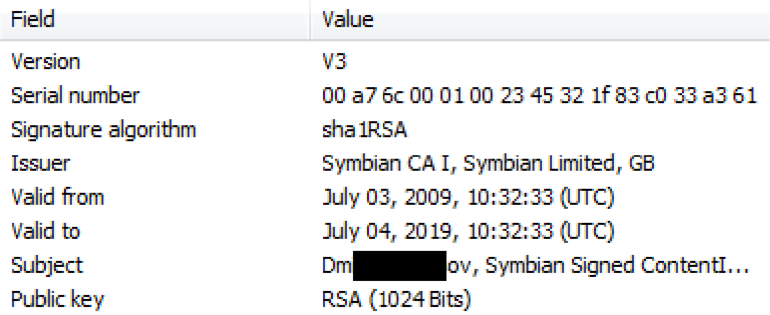
Настройка Видео
для настройки проигрывателя нажимайте левую софт клавишу.



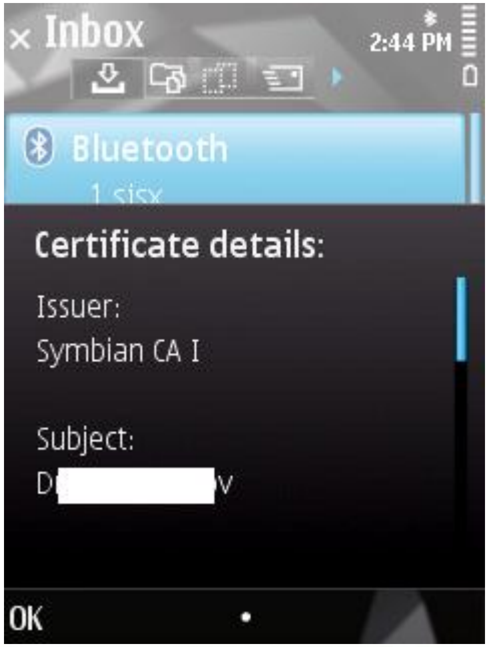
Настройка Видео
для настройки проигрывателя нажимайте левую софт клавишу.

‘Complex’: Trojan-SMS.SymbOS.Lopsoy

- Signed SMS Trojan for Symbian S60 3rd edition devices



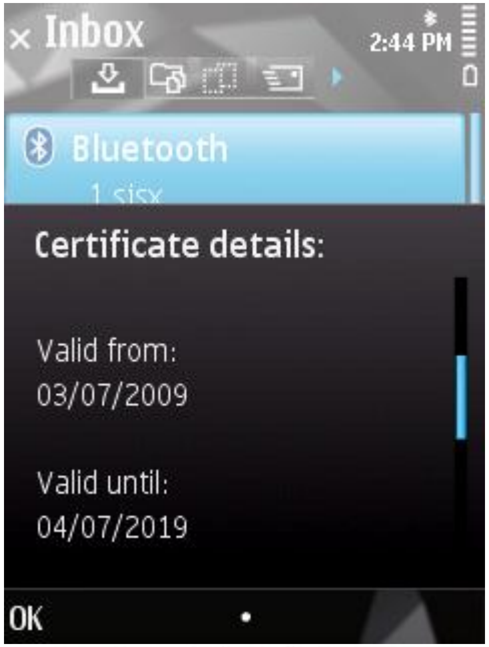
Field	Value
Version	V3
Serial number	00 a7 6c 00 01 00 23 45 32 1f 83 c0 33 a3 61
Signature algorithm	sha1RSA
Issuer	Symbian CA I, Symbian Limited, GB
Valid from	July 03, 2009, 10:32:33 (UTC)
Valid to	July 04, 2019, 10:32:33 (UTC)
Subject	Dm[redacted]ov, Symbian Signed ContentI...
Public key	RSA (1024 Bits)



Certificate details:

Issuer:
Symbian CA I

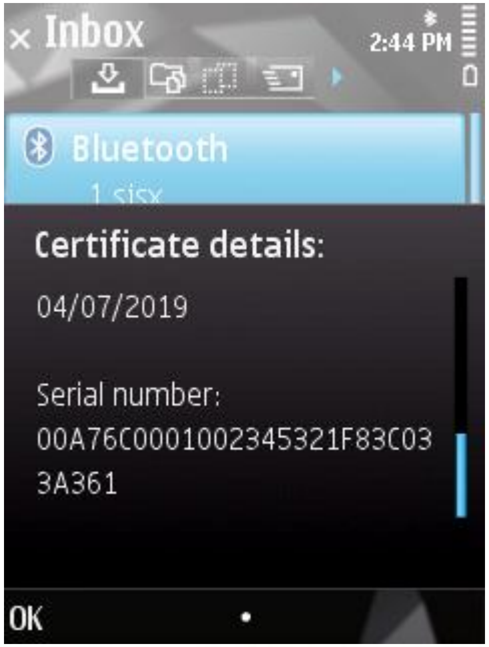
Subject:
D[redacted]v



Certificate details:

Valid from:
03/07/2009

Valid until:
04/07/2019



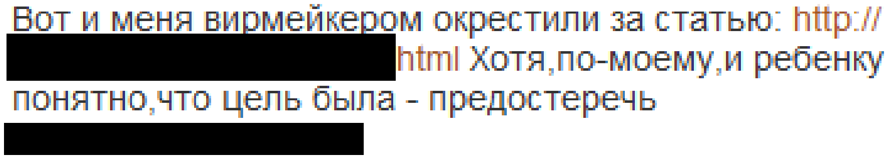
Certificate details:

04/07/2019

Serial number:
00A76C0001002345321F83C03
3A361

Lopsoy ‘source’

- Article on the website:
  - Description of how the Trojan works
  - Instructions on ‘How to sign your Trojan’

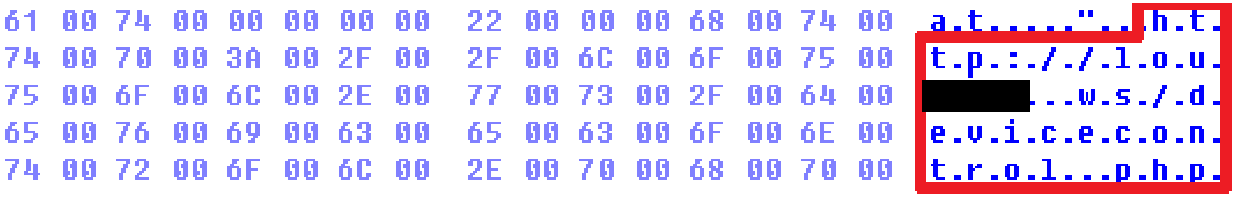


Вот и меня вирмейкером окрестили за статью: http:// [redacted] html Хотя,по-моему,и ребенку понятно,что цель была - предостеречь
[redacted]

‘Because of this article <url> they’re saying I’m a virus writer. Even though anyone could see that my goal was only to warn people’

How Lopsoy gets SMS information

- Connects to author’s URL



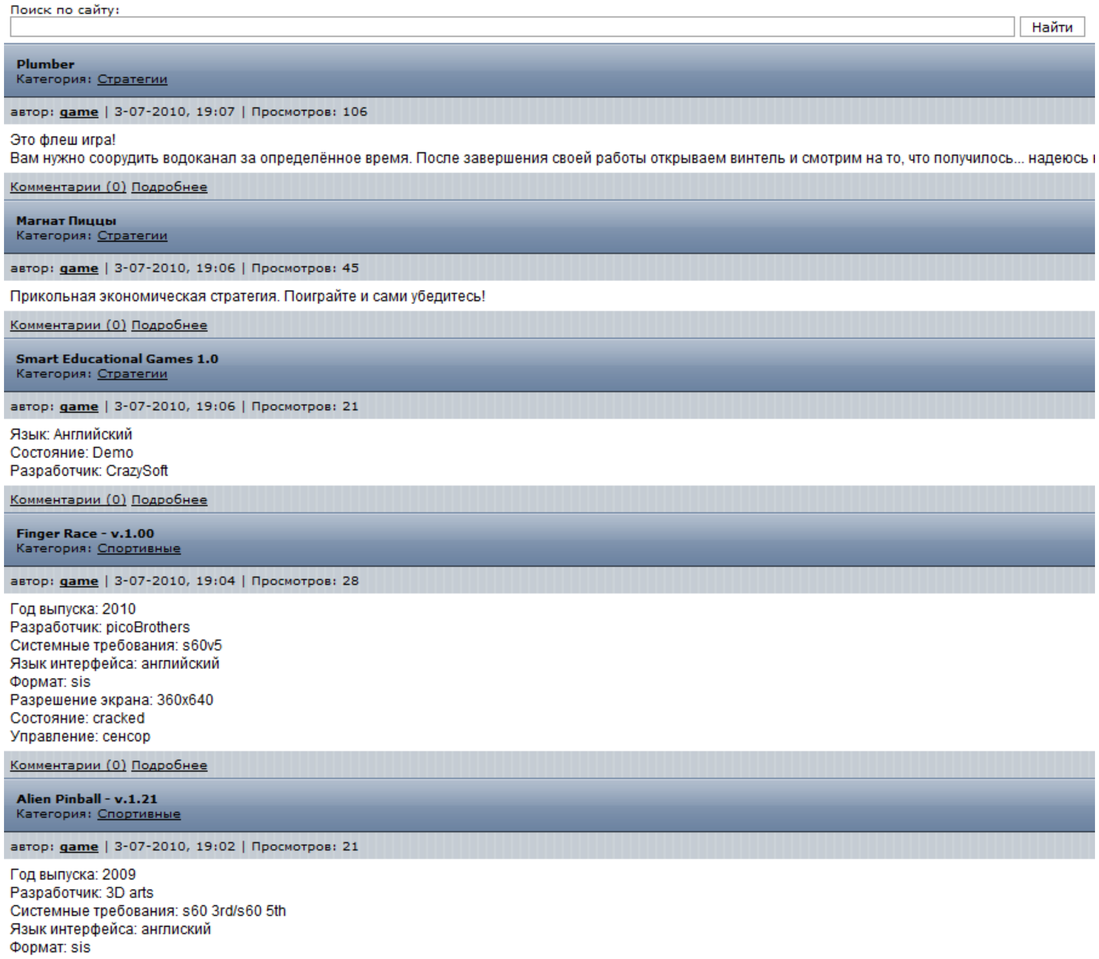
```
61 00 74 00 00 00 00 00  22 00 00 00 68 00 74 00  a.t....."...h.t.
74 00 70 00 3A 00 2F 00  2F 00 6C 00 6F 00 75 00  t.p.:././.l.o.u.
75 00 6F 00 6C 00 2E 00  77 00 73 00 2F 00 64 00  [redacted]..w.s./.d.
65 00 76 00 69 00 63 00  65 00 63 00 6F 00 6E 00  e.v.i.c.e.c.o.n.
74 00 72 00 6F 00 6C 00  2E 00 70 00 68 00 70 00  t.r.o.l...p.h.p.
```

http://lou***.ws/devicecontrol.php

- Gets SMS text and premium rate number

How Lopsoy spreads

- Various ‘smartphone games’ websites



Поиск по сайту:

Найти

Plumber
Категория: Стратегии

автор: **game** | 3-07-2010, 19:07 | Просмотров: 106

Это флеш игра!
Вам нужно соорудить водоканал за определённое время. После завершения своей работы открываем винтель и смотрим на то, что получилось... надеюсь

Комментарии (0) Подробнее

Магнат Пиццы
Категория: Стратегии

автор: **game** | 3-07-2010, 19:06 | Просмотров: 45

Прикольная экономическая стратегия. Поиграйте и сами убедитесь!

Комментарии (0) Подробнее

Smart Educational Games 1.0
Категория: Стратегии

автор: **game** | 3-07-2010, 19:06 | Просмотров: 21

Язык: Английский
Состояние: Demo
Разработчик: CrazySoft

Комментарии (0) Подробнее

Finger Race - v.1.00
Категория: Спортивные

автор: **game** | 3-07-2010, 19:04 | Просмотров: 28

Год выпуска: 2010
Разработчик: picoBrothers
Системные требования: s60v5
Язык интерфейса: английский
Формат: sis
Разрешение экрана: 360x640
Состояние: cracked
Управление: сенсор

Комментарии (0) Подробнее

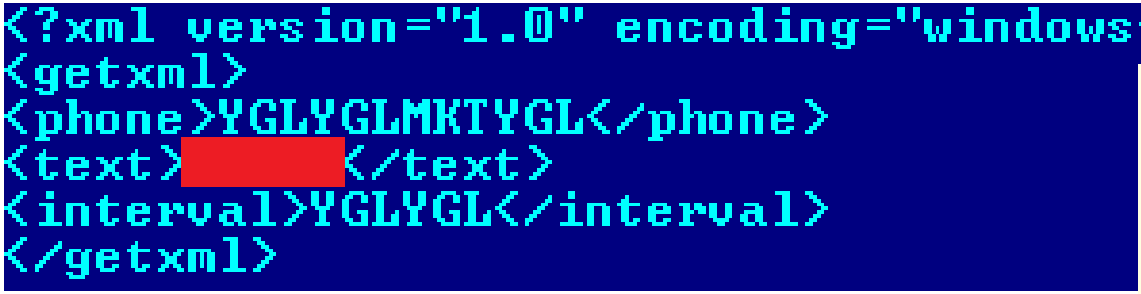
Alien Pinball - v.1.21
Категория: Спортивные

автор: **game** | 3-07-2010, 19:02 | Просмотров: 21

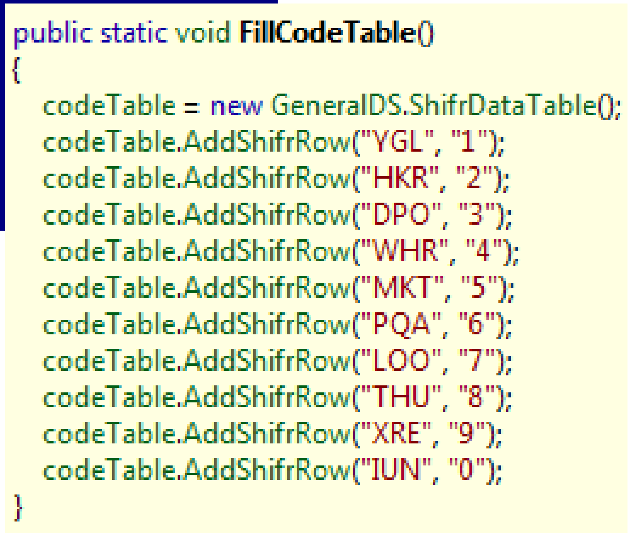
Год выпуска: 2009
Разработчик: 3D arts
Системные требования: s60 3rd/s60 5th
Язык интерфейса: англиский
Формат: sis

‘Complex’: Trojan-SMS.WinCE.Sejweek

- Connects to web server
- Downloads XML configuration file



```
<?xml version="1.0" encoding="windows-1251"?>
<getxml>
<phone>YGLYGLMKTYGL</phone>
<text>[redacted]</text>
<interval>YGLYGL</interval>
</getxml>
```

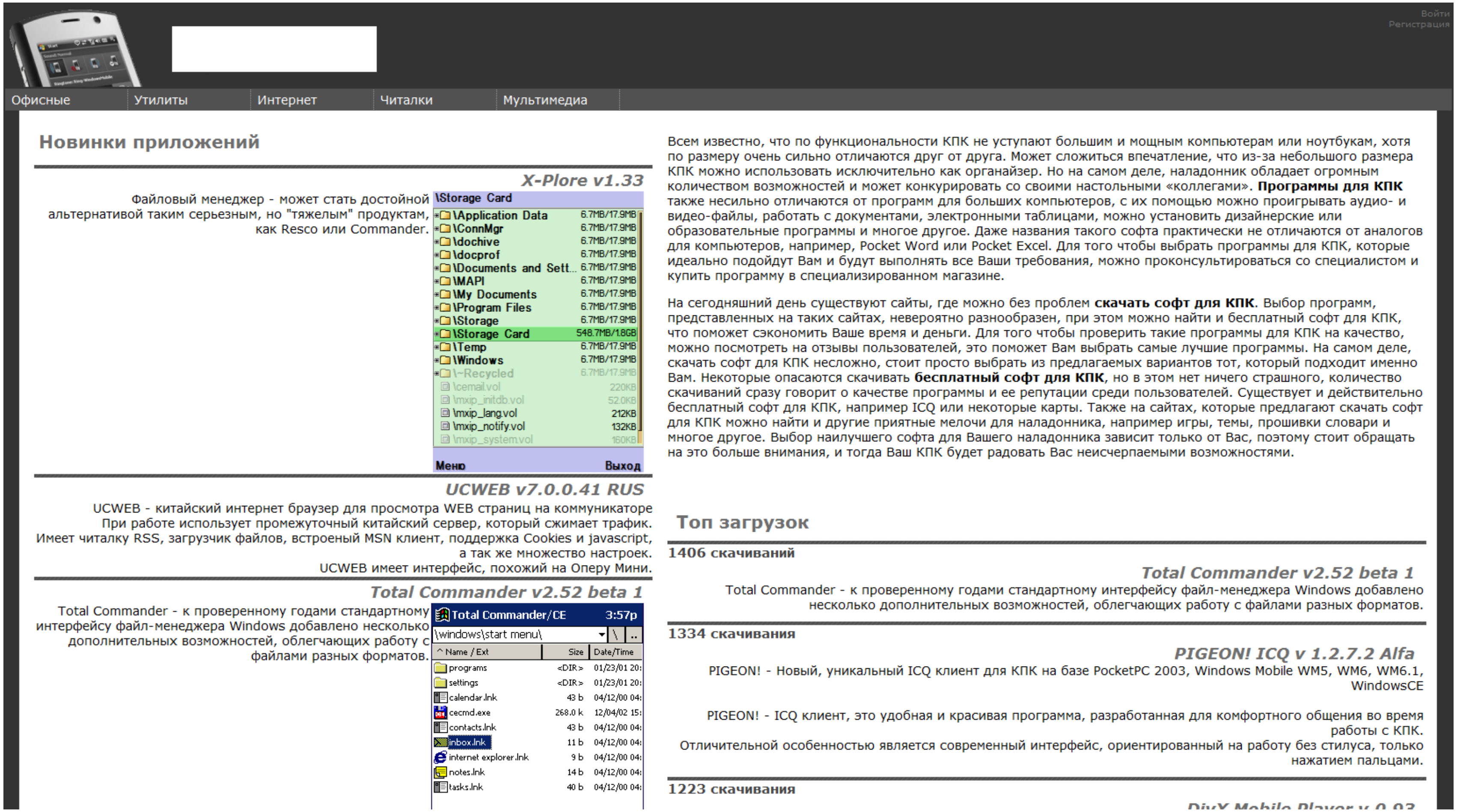


```
public static void FillCodeTable()
{
    codeTable = new GeneralDS.ShifrDataTable();
    codeTable.AddShifrRow("YGL", "1");
    codeTable.AddShifrRow("HKR", "2");
    codeTable.AddShifrRow("DPO", "3");
    codeTable.AddShifrRow("WHR", "4");
    codeTable.AddShifrRow("MKT", "5");
    codeTable.AddShifrRow("PQA", "6");
    codeTable.AddShifrRow("LOO", "7");
    codeTable.AddShifrRow("THU", "8");
    codeTable.AddShifrRow("XRE", "9");
    codeTable.AddShifrRow("IUN", "0");
}
```

- Decodes phone number and interval
- Regularly updates XML file

How Sejweek spreads

- Various ‘PDA application’ websites



Новинки приложений

X-Plore v1.33

Файловый менеджер - может стать достойной альтернативой таким серьезным, но "тяжелым" продуктам, как Resco или Commander.

```
\Storage Card
\Application Data      6.7MB/17.9MB
\ConnMgr               6.7MB/17.9MB
\dochive               6.7MB/17.9MB
\docprof               6.7MB/17.9MB
\Documents and Sett... 6.7MB/17.9MB
\MAPI                  6.7MB/17.9MB
\My Documents          6.7MB/17.9MB
\Program Files         6.7MB/17.9MB
\Storage               6.7MB/17.9MB
\Storage Card          548.7MB/1.8GB
\Temp                  6.7MB/17.9MB
\Windows               6.7MB/17.9MB
\~Recycled             6.7MB/17.9MB
\cemail.vol                   220KB
\mxip_initdb.vol             52.0KB
\mxip_lang.vol                212KB
\mxip_notify.vol              132KB
\mxip_system.vol              160KB
```

UCWEB v7.0.0.41 RUS

UCWEB - китайский интернет браузер для просмотра WEB страниц на коммуникаторе При работе использует промежуточный китайский сервер, который сжимает трафик. Имеет читалку RSS, загрузчик файлов, встроеный MSN клиент, поддержка Cookies и javascript, а так же множество настроек. UCWEB имеет интерфейс, похожий на Оперу Мини.

Total Commander v2.52 beta 1

Total Commander - к проверенному годами стандартному интерфейсу файл-менеджера Windows добавлено несколько дополнительных возможностей, облегчающих работу с файлами разных форматов.

```
Total Commander/CE                  3:57p
\windows\start menu\
^ Name / Ext              Size   Date/Time
programs                 <DIR>   01/23/01 20:
settings                 <DIR>   01/23/01 20:
calendar.lnk              43 b   04/12/00 04:
cecmd.exe              268.0 k   12/04/02 15:
contacts.lnk              43 b   04/12/00 04:
inbox.lnk                 11 b   04/12/00 04:
internet explorer.lnk      9 b   04/12/00 04:
notes.lnk                 14 b   04/12/00 04:
tasks.lnk                 40 b   04/12/00 04:
```

Всем известно, что по функциональности КПК не уступают большим и мощным компьютерам или ноутбукам, хотя по размеру очень сильно отличаются друг от друга. Может сложиться впечатление, что из-за небольшого размера КПК можно использовать исключительно как органайзер. Но на самом деле, наладонник обладает огромным количеством возможностей и может конкурировать со своими настольными «коллегами». **Программы для КПК** также несильно отличаются от программ для больших компьютеров, с их помощью можно проигрывать аудио- и видео-файлы, работать с документами, электронными таблицами, можно установить дизайнерские или образовательные программы и многое другое. Даже названия такого софта практически не отличаются от аналогов для компьютеров, например, Pocket Word или Pocket Excel. Для того чтобы выбрать программы для КПК, которые идеально подойдут Вам и будут выполнять все Ваши требования, можно проконсультироваться со специалистом и купить программу в специализированном магазине.

На сегодняшний день существуют сайты, где можно без проблем **скачать софт для КПК**. Выбор программ, представленных на таких сайтах, невероятно разнообразен, при этом можно найти и бесплатный софт для КПК, что поможет сэкономить Ваше время и деньги. Для того чтобы проверить такие программы для КПК на качество, можно посмотреть на отзывы пользователей, это поможет Вам выбрать самые лучшие программы. На самом деле, скачать софт для КПК несложно, стоит просто выбрать из предлагаемых вариантов тот, который подходит именно Вам. Некоторые опасаются скачивать **бесплатный софт для КПК**, но в этом нет ничего страшного, количество скачиваний сразу говорит о качестве программы и ее репутации среди пользователей. Существует и действительно бесплатный софт для КПК, например ICQ или некоторые карты. Также на сайтах, которые предлагают скачать софт для КПК можно найти и другие приятные мелочи для наладонника, например игры, темы, прошивки словари и многое другое. Выбор наилучшего софта для Вашего наладонника зависит только от Вас, поэтому стоит обращать на это больше внимания, и тогда Ваш КПК будет радовать Вас неисчерпаемыми возможностями.

Топ загрузок

1406 скачиваний

Total Commander v2.52 beta 1

Total Commander - к проверенному годами стандартному интерфейсу файл-менеджера Windows добавлено несколько дополнительных возможностей, облегчающих работу с файлами разных форматов.

1334 скачивания

PIGEON! ICQ v 1.2.7.2 Alfa

PIGEON! - Новый, уникальный ICQ клиент для КПК на базе PocketPC 2003, Windows Mobile WM5, WM6, WM6.1, WindowsCE

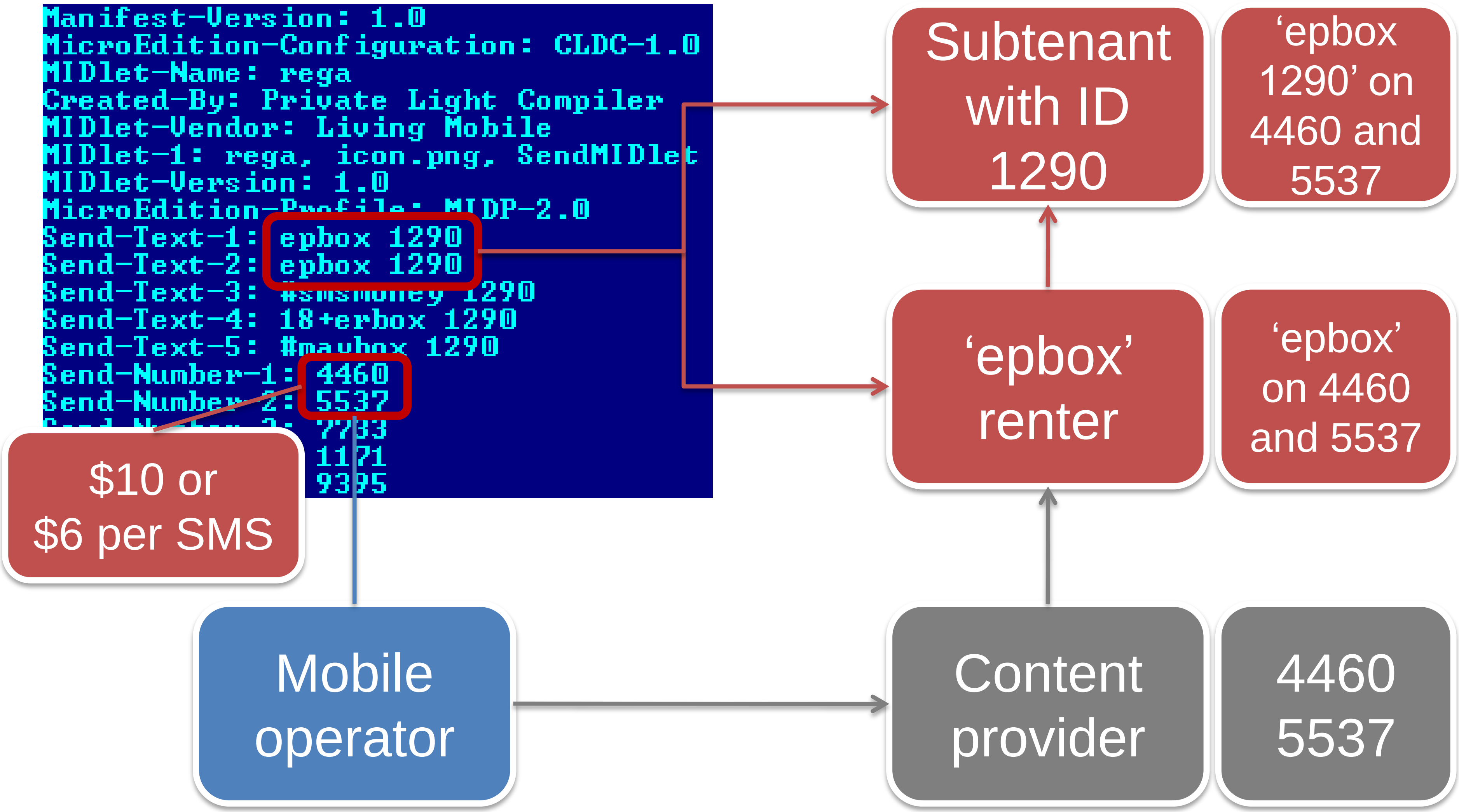
PIGEON! - ICQ клиент, это удобная и красивая программа, разработанная для комфортного общения во время работы с КПК. Отличительной особенностью является современный интерфейс, ориентированный на работу без стилуса, только нажатием пальцами.

1223 скачивания

DivX Mobile Player v 0.93

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: #maybox 1290
Send-Number-1: 4460
Send-Number-2: 5537
Send-Number-3: 7733
               1171
               9395
```

Subtenant with ID 1290

‘epbox 1290’ on 4460 and 5537

‘epbox’ renter

‘epbox’ on 4460 and 5537

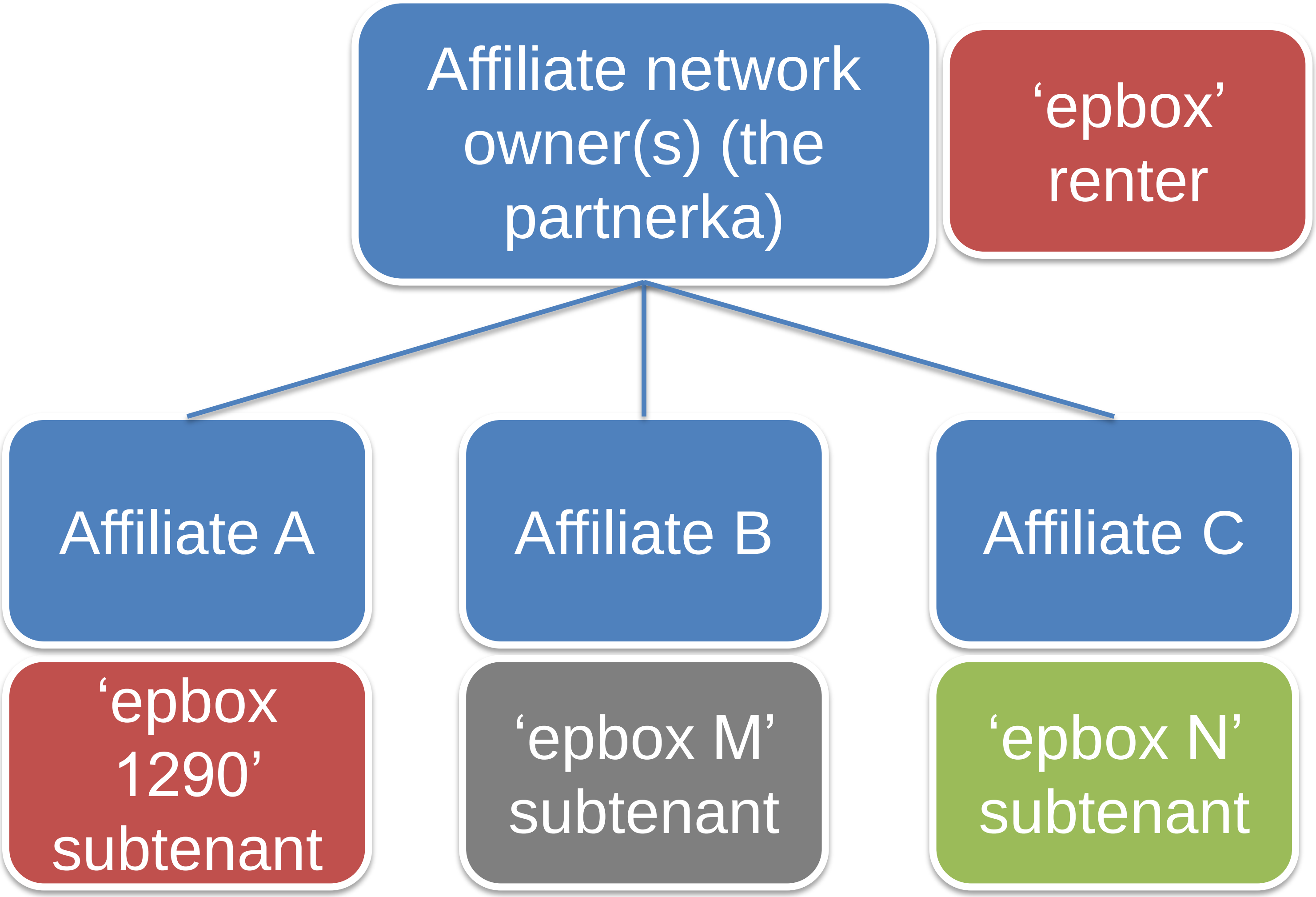
$10 or $6 per SMS

Mobile operator

Content provider

4460 5537

Who are 'epbox' and 'epbox 1290'?



Affiliate network owner(s) (the partnerka)

'epbox' renter

Affiliate A

Affiliate B

Affiliate C

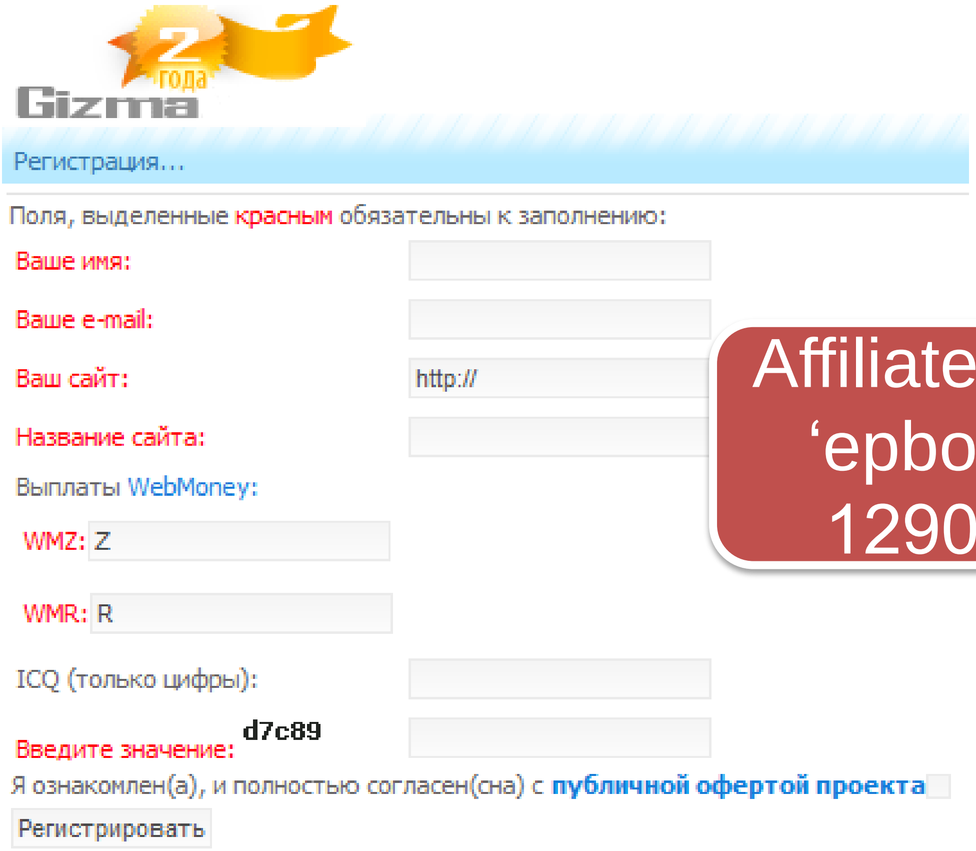
'epbox 1290' subtenant

'epbox M' subtenant

'epbox N' subtenant

The root of all evil

- Affiliate network registration form



Регистрация...

Поля, выделенные красным обязательны к заполнению:

Ваше имя:	
Ваше e-mail:	
Ваш сайт:	http://
Название сайта:	

Выплаты WebMoney:

WMZ:	Z
WMR:	R
ICQ (только цифры):	
Введите значение: d7c89	

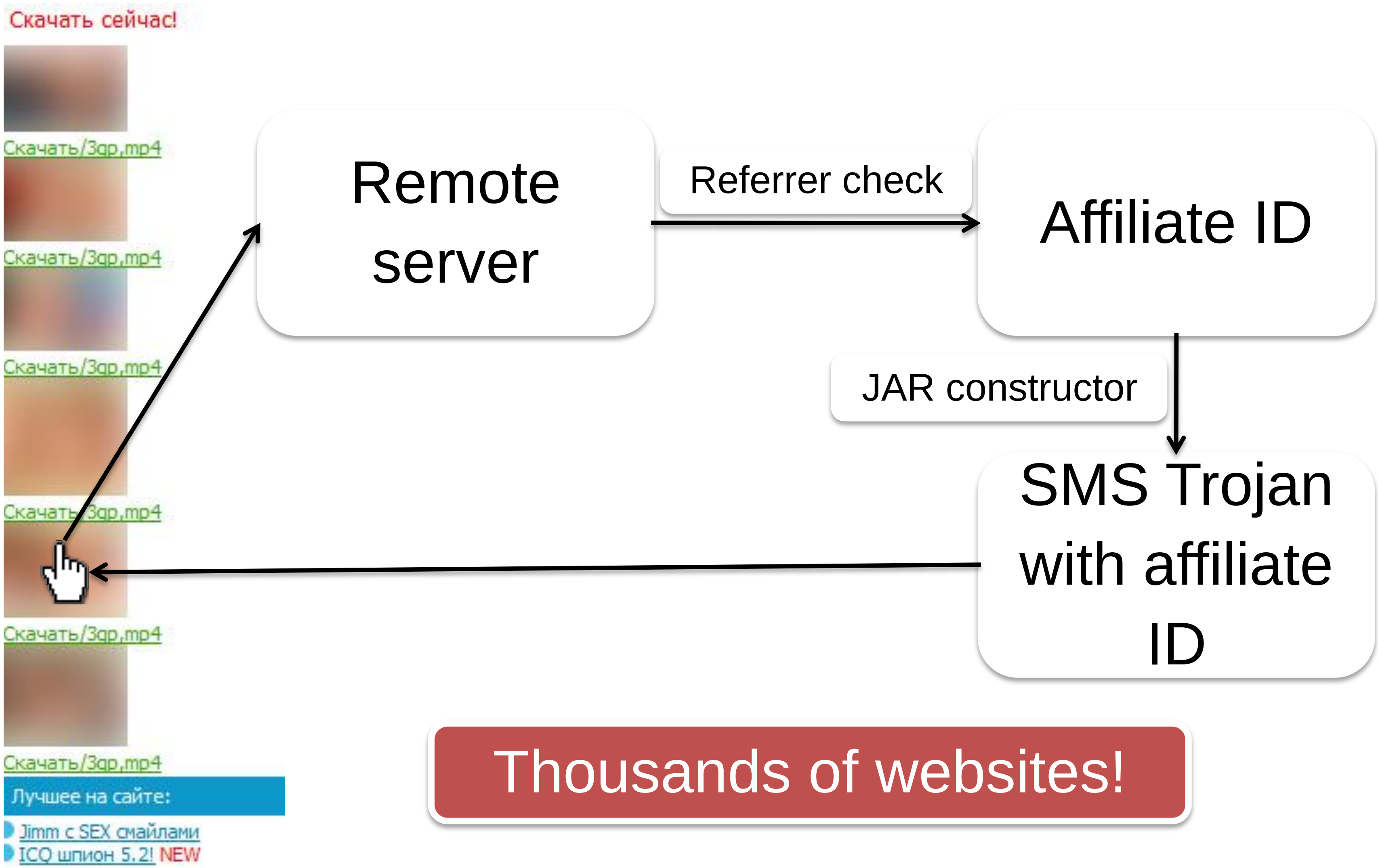
Я ознакомлен(а), и полностью согласен(сна) с публичной офертой проекта □

Affiliate ID ‘epbox 1290’

No sensitive data!

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

Typical affiliate website



Скачать сейчас!

Скачать/3gp,mp4

Скачать/3gp,mp4

Скачать/3gp,mp4

Скачать/3gp,mp4

Скачать/3gp,mp4

Скачать/3gp,mp4

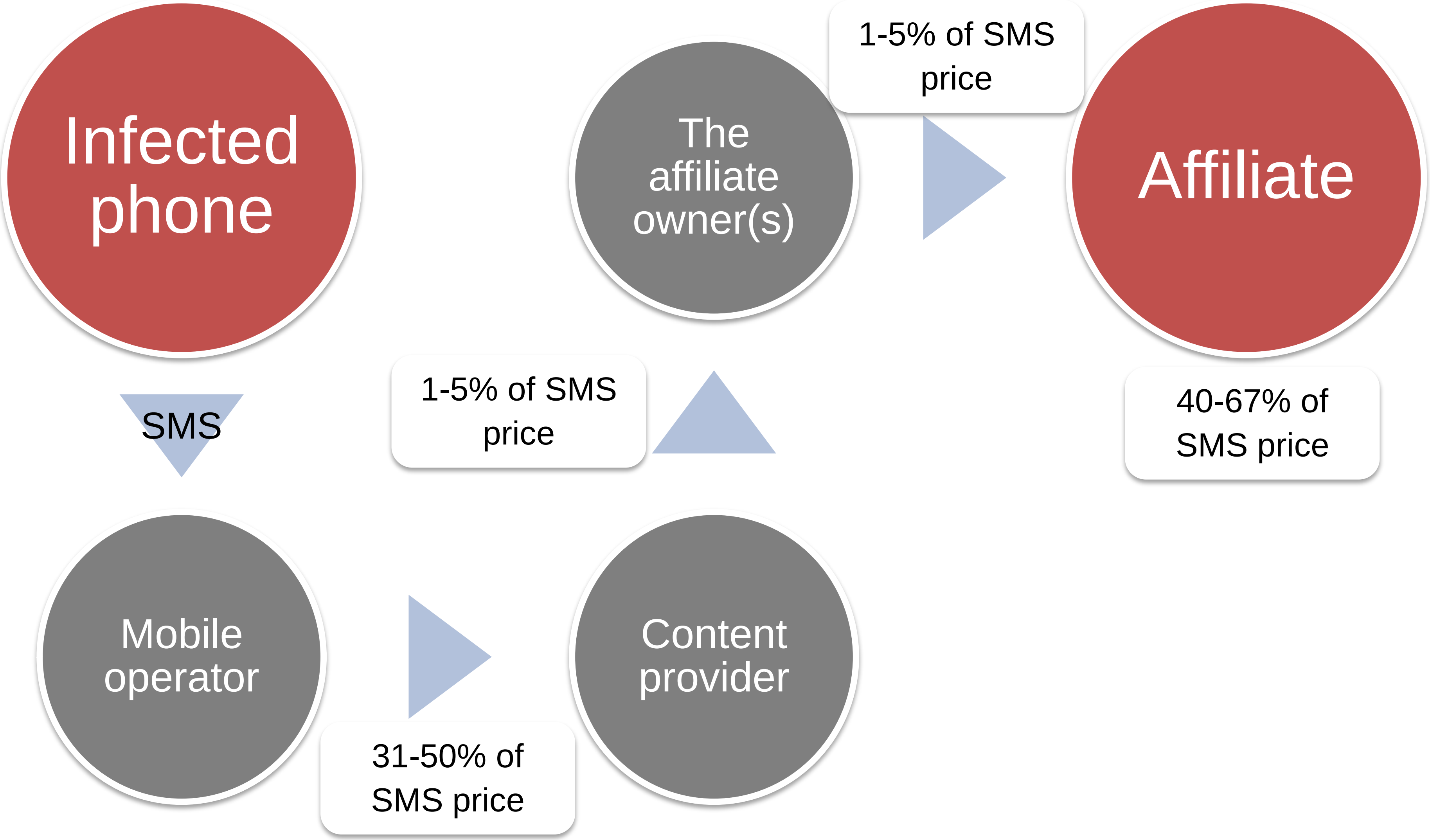
Лучшее на сайте:

- Jimm с SEX смайлами
- ICQ шпион 5.2! NEW

Thousands of websites!

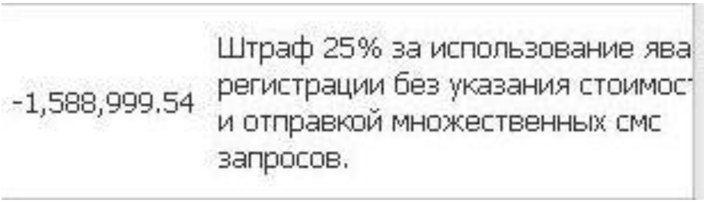
How much do they make?

Revenue sharing



‘Death penalty’

- Largest mobile affiliate network ‘Perlag’ was fined:



-1,588,999.54

Штраф 25% за использование ява регистрации без указания стоимос и отправкой множественных смс запросов.

- The fine was equal to 25% of the affiliate network’s weekly revenue

1,590,000 rubles or $53,000

Weekly income ~$212,000

Monthly income ~$850,000

People were losing at least $1,200,000/month

Today and tomorrow

Today

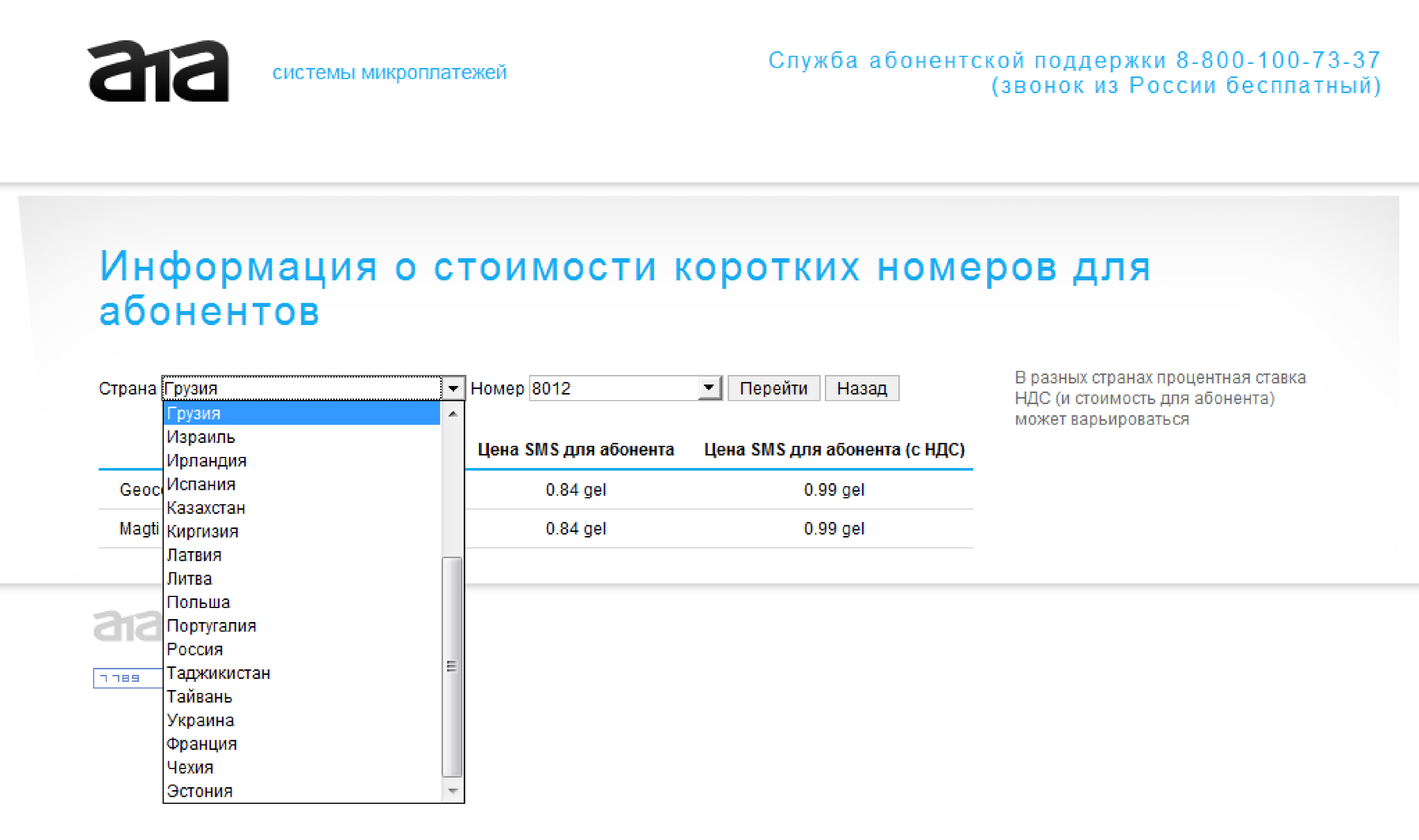
- Various SMS Trojans for different platforms
- Increasingly sophisticated techniques
- Hundreds of criminalized mobile affiliate networks
- Multi-million dollar losses
- Cybercriminals go unpunished
- Detection problems on simple mobile phones
- Targets: Russian and CIS users

- Reason: legislation loopholes

Tomorrow (with legislation loopholes)

- Various SMS Trojans for different platforms
- Increasingly sophisticated techniques
- Hundreds of criminalized mobile affiliate networks
- Multi-million dollar losses
- Cybercriminals go unpunished
- Detection problems on simple mobile phones
- Targets: ?

New targets



системы микроплатежей

Служба абонентской поддержки 8-800-100-73-37
(звонок из России бесплатный)

Информация о стоимости коротких номеров для абонентов

Страна Грузия ▾ Номер 8012 ▾ Перейти Назад

- Грузия
- Израиль
- Ирландия
- Испания
- Казахстан
- Киргизия
- Латвия
- Литва
- Польша
- Португалия
- Россия
- Таджикистан
- Тайвань
- Украина
- Франция
- Чехия
- Эстония

В разных странах процентная ставка НДС (и стоимость для абонента) может варьироваться

	Цена SMS для абонента	Цена SMS для абонента (с НДС)
Geoc	0.84 gel	0.99 gel
Magti	0.84 gel	0.99 gel

Thank you! Questions?

Denis Maslennikov

Senior Malware Analyst, Mobile Research Group Manager
Kaspersky Lab
Denis.Maslennikov@kaspersky.com
http://twitter.com/hEx63