KASPERSKY lab

Cell Phone Money Laundering

Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab

07.10.2011, Virus Bulletin Conference, Barcelona, Spain

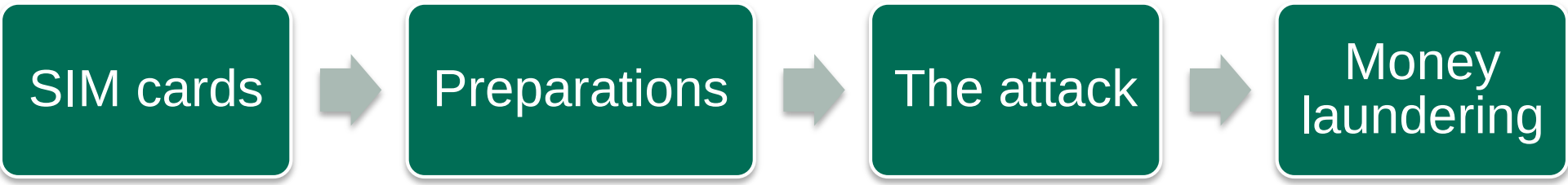
Agenda

- General scheme
- Three pillars:
  - Ransomware
  - Mobile malware
  - SMS scam campaigns
- Money laundering
- Cooperation

General scheme

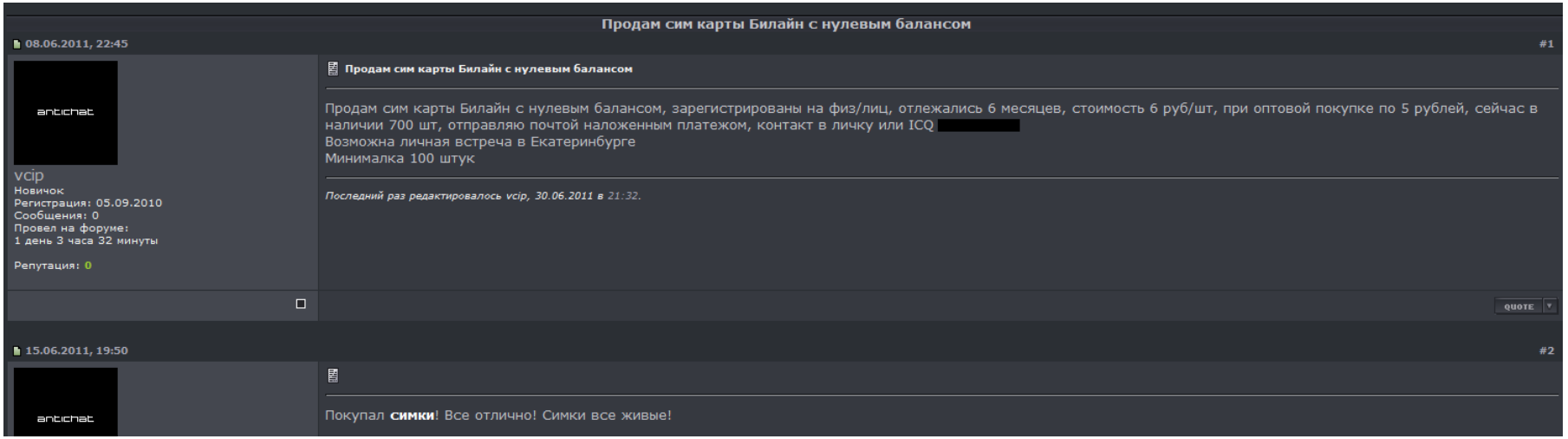
General scheme…

…in a nutshell



SIM cards

SIM cards



Beeline SIM cards… $0,15 per unit… 700 units… 100 SIM cards is minimum

SIM cards

Three pillars

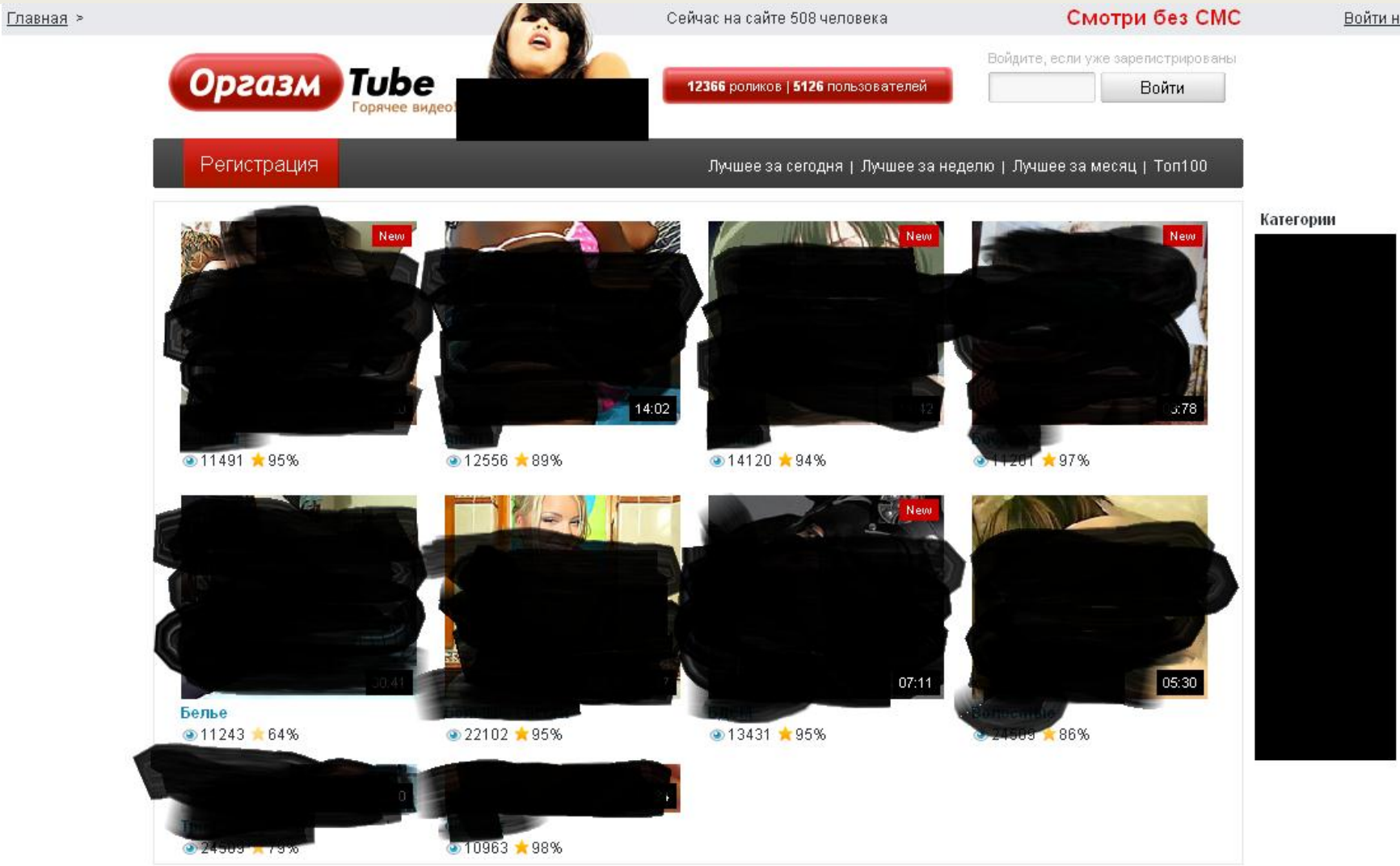
Ransomware, mobile malware, SMS scam campaigns

KASPERSKY lab

Ransomware

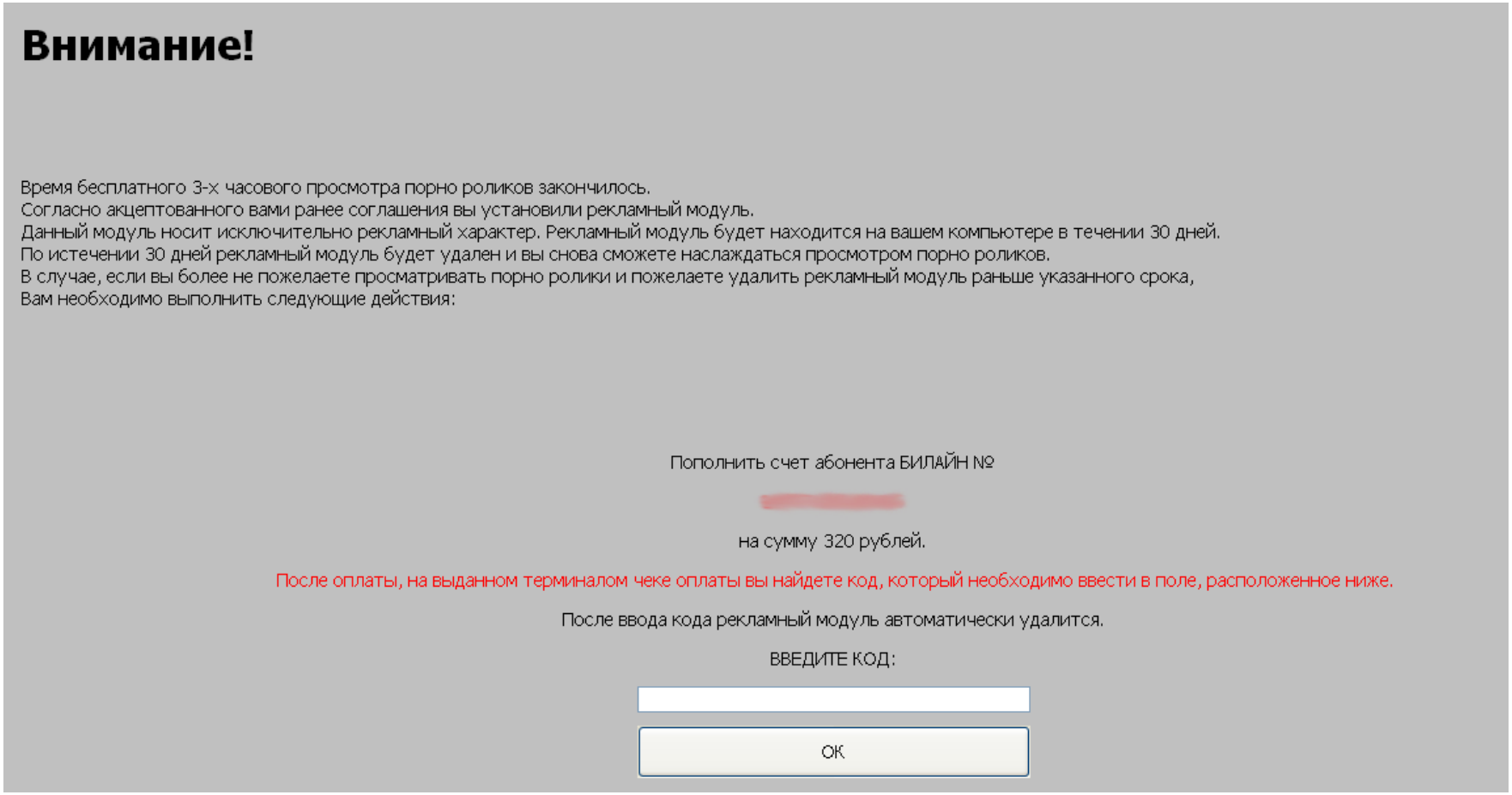

Windows заблокирован!
Microsoft Security обнаружил нарушения использования сети интернет.
Причина: Вы смотрели фильмы содержащие гей-порно.
Для разблокировки Windows необходимо:
Пополнить номер абонента BeeLine: 8 на сумму 600 рублей.
Оплатить можно через терминал для оплаты сотовой связи.
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш персональный код разблокировки, который необходимо ввести ниже.
0 1 2 3 4 5 6 7 8 9 ОЧИСТИТЬ
Ваш код:
ВХОД В СИСТЕМУ
Если в течении 12 часов с момента появления данного сообщения, не будет введён код, все данные, включая Windows и bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка переустановить систему приведёт к нарушениям работы компьютера.

Ransomware

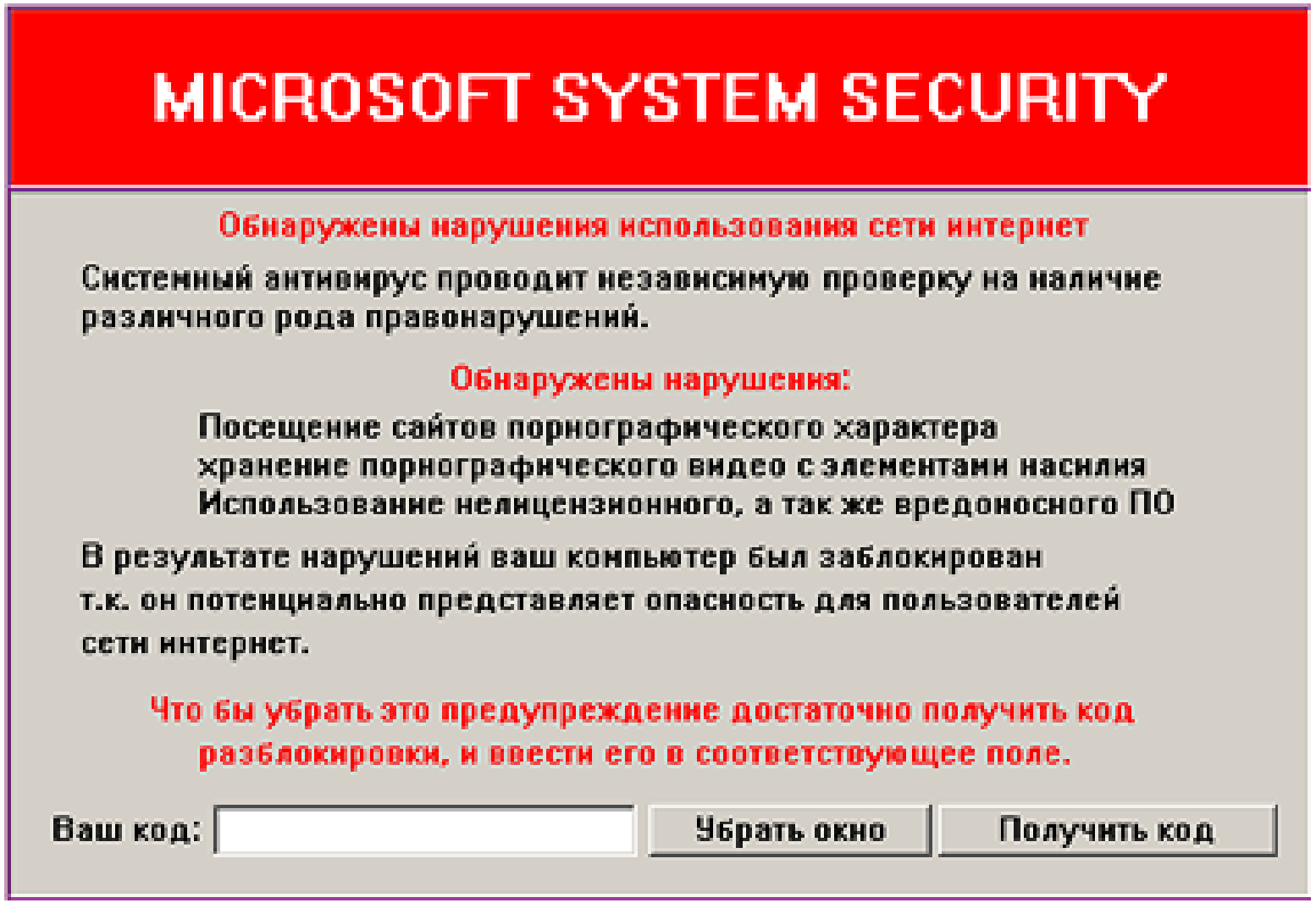


KASPERSKY

Ransomware


Внимание!
Время бесплатного 3-х часового просмотра порно роликов закончилось.
Согласно акцептованного вами ранее соглашения вы установили рекламный модуль.
Данный модуль носит исключительно рекламный характер. Рекламный модуль будет находится на вашем компьютере в течении 30 дней.
По истечении 30 дней рекламный модуль будет удален и вы снова сможете наслаждаться просмотром порно роликов.
В случае, если вы более не пожелаете просматривать порно ролики и пожелаете удалить рекламный модуль раньше указанного срока,
Вам необходимо выполнить следующие действия:
Пополнить счет абонента БИЛАЙН №
на сумму 320 рублей.
После оплаты, на выданном терминалом чеке оплаты вы найдете код, который необходимо ввести в поле, расположенное ниже.
После ввода кода рекламный модуль автоматически удалится.
ВВЕДИТЕ КОД:
OK

Ransomware


MICROSOFT SYSTEM SECURITY
Обнаружены нарушения использования сети интернет
Системный антивирус проводит независимую проверку на наличие различного рода правонарушений.
Обнаружены нарушения:
Посещение сайтов порнографического характера
хранение порнографического видео с элементами насилия
Использование нелицензионного, а так же вредоносного ПО
В результате нарушений ваш компьютер был заблокирован
т.к. он потенциально представляет опасность для пользователей сети интернет.
Что бы убрать это предупреждение достаточно получить код разблокировки, и ввести его в соответствующее поле.
Ваш код:
Убрать окно
Получить код

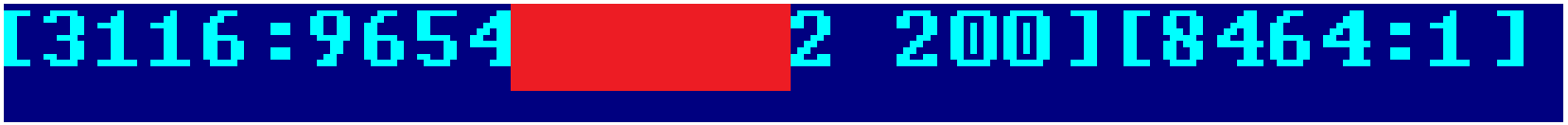
SMS Trojans

- **Transferring money** via **free SMS**
- **SMS #1:**
  - **3116** with **text** ‘Recipient_cell_phone_number Amount_of_money_to_transfer’

SMS Trojans

- **Transferring money** via **free SMS**
- **SMS #1:**
  - **3116** with **text** ‘Recipient_cell_phone_number Amount_of_money_to_transfer’
- **SMS #2:**
  - **8464** with **text ‘1’**
- **Trojan-SMS.J2ME.Smmer:**
  - **SMS spam** campaigns

SMS Trojans



200 rubles ~ $7

SMS scam campaigns

- **Appeared in 2008**
- ‘Mom, I’m in trouble, please replenish +7905XXXXXXX for 500 rubles. I’ll call you back later’

SMS scam campaigns

- **Appeared in 2008**
- ‘Mom, I’m in trouble, please replenish +7905XXXXXXX for 500 rubles. I’ll call you back later’
- **Terrorist attack** in **Moscow underground**
  - ‘Help me, I’m in underground, please replenish +7905XXXXXXX for 900 rubles’
- **Explosion** in **‘Domodedovo’ airport**
  - ‘It’s urgent, I’m in airport but have no money on my mobile account. Can you please replenish +7905XXXXXXX for 1000 rubles?’

Money laundering

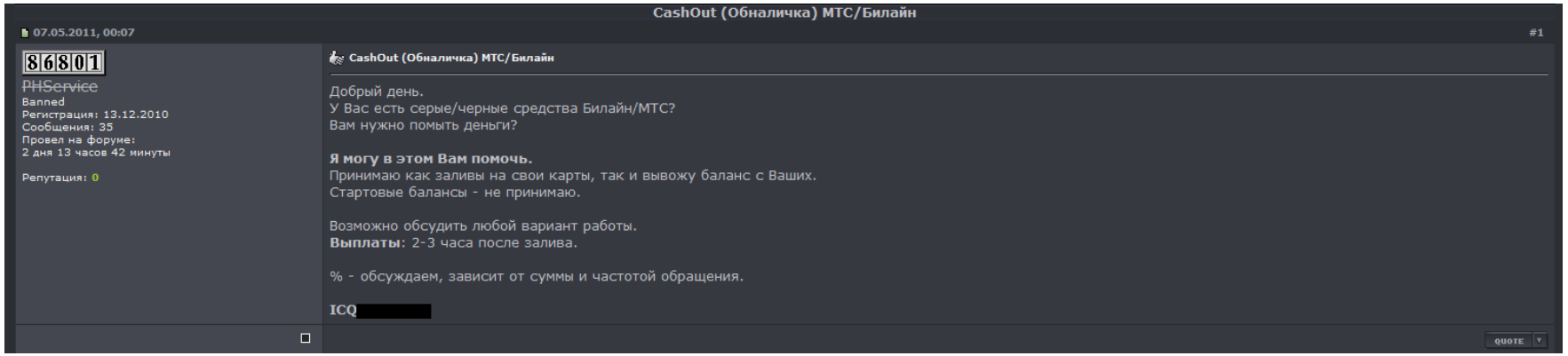
Money laundering

- Credit card
- Bank account
- Unistream
- Another cell phone number

Money laundering

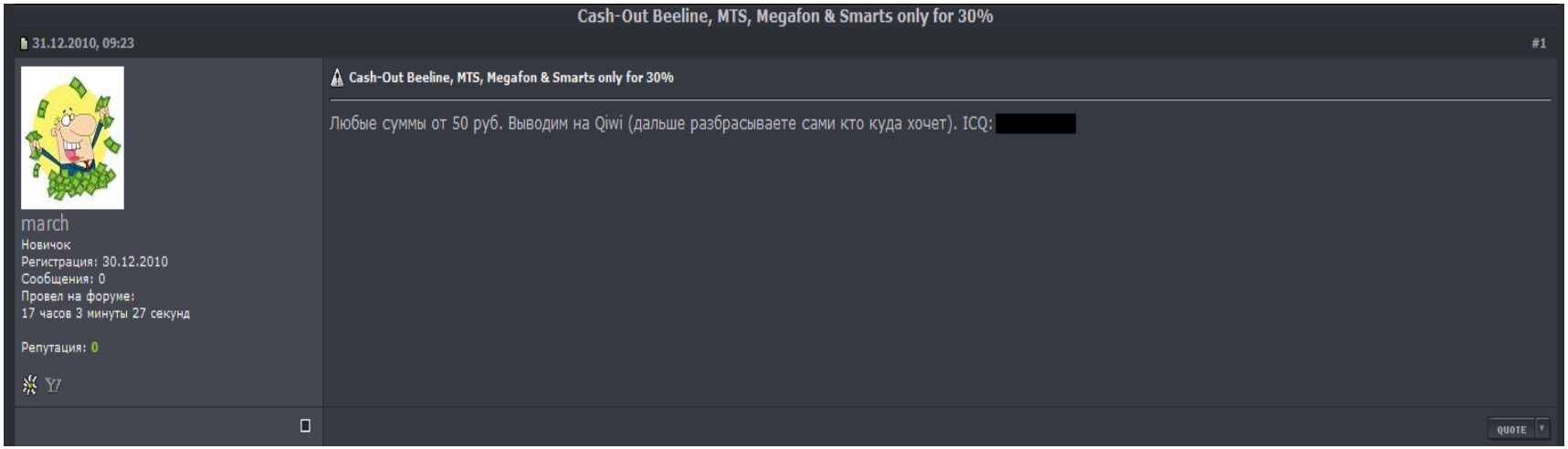
- **Premium rate SMS messages**
  - **Yes,** but what about **antifraud systems?**
  - **Yes,** but it's **not an immediate cash**
- **So,** there is a **demand** on **money laundering**

Money laundering



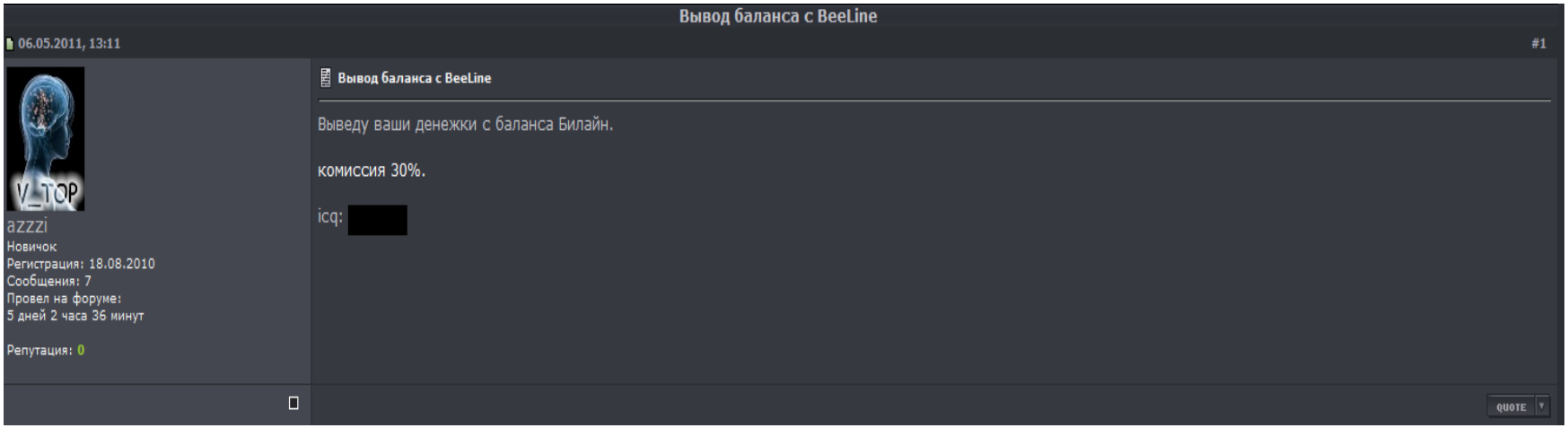
- ‘Hello. Do you have black/grey money in Beeline SIM cards? Do you need to launder money? I can help you. I accept all SIM cards. All variants are discussable. Payments: within 2-3 hours. Commission is also discussable and depends on amounts of money and request periodicity.’

Money laundering



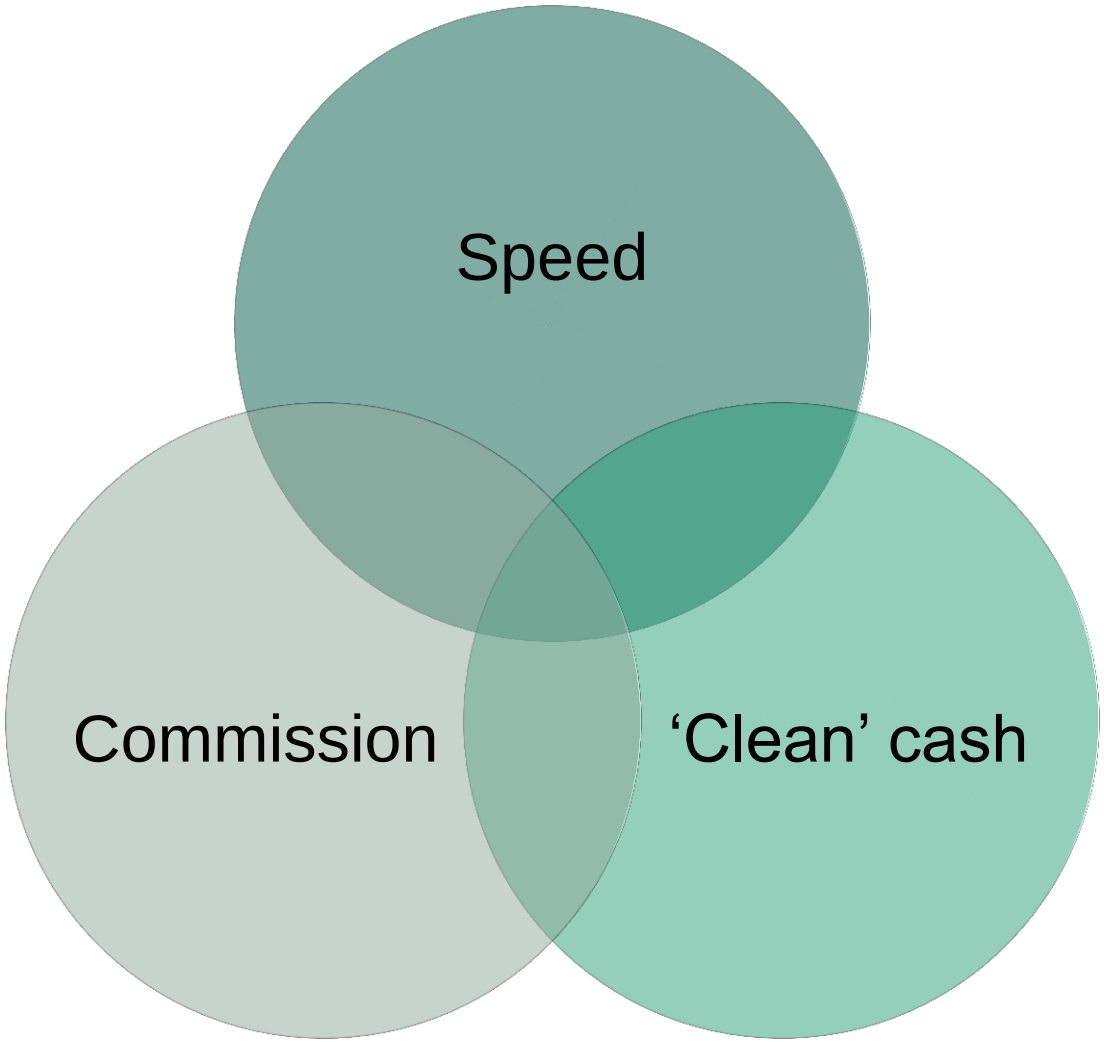
- ‘All amounts starting from 50 rubles (1,5 USD). Money will be transferred to Qiwi. Commission: 30%’.

Money laundering



- ‘Will launder you money from Beeline SIM cards. Commission: 30%’

Money laundering



Conclusion

KASPERSKY lab

Conclusion

- **Exploitation** of **legal service**
- **Various types** of **attacks**
  - **Ransomware**
  - **SMS Trojans**
  - **SMS scam**
- One more **cybercrime lifecycle**
- **Easy** to stay **unnoticed**
- **Legislation problems: again**

Thank You

Cell Phone Money Laundering

Denis Maslennikov, Senior Malware Analyst, Kaspersky Lab

Denis.Maslennikov@kaspersky.com, @hEx63

07.10.2011, Virus Bulletin Conference, Barcelona, Spain

KASPERSKY lab