



Deblocker

Практика противодействия вредоносным программам

Марина Еремина, Веб-аналитик, Лаборатория Касперского

Светлана Мушта, Веб-аналитик, Лаборатория Касперского

Эволюция баннеров-блокеров



министерство внутренних дел
информационная
безопасность

лаборатория
КА(ПЕР)КОГО

Microsoft®

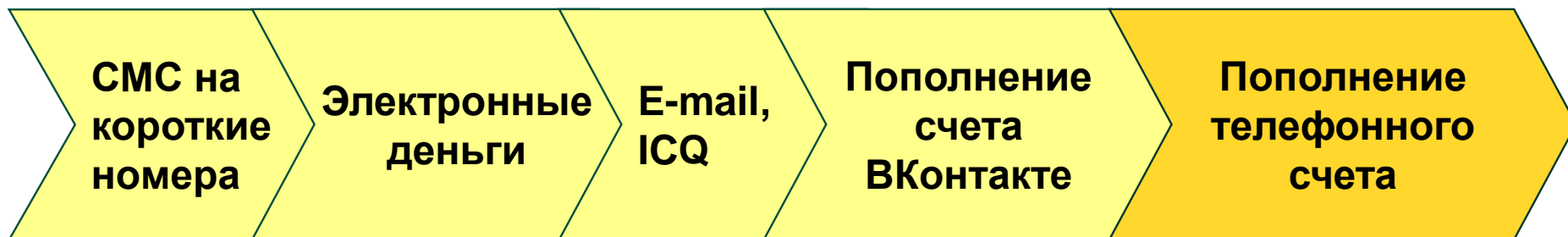
Январь 2011: PornoCodec

Динамика развития блокировщиков

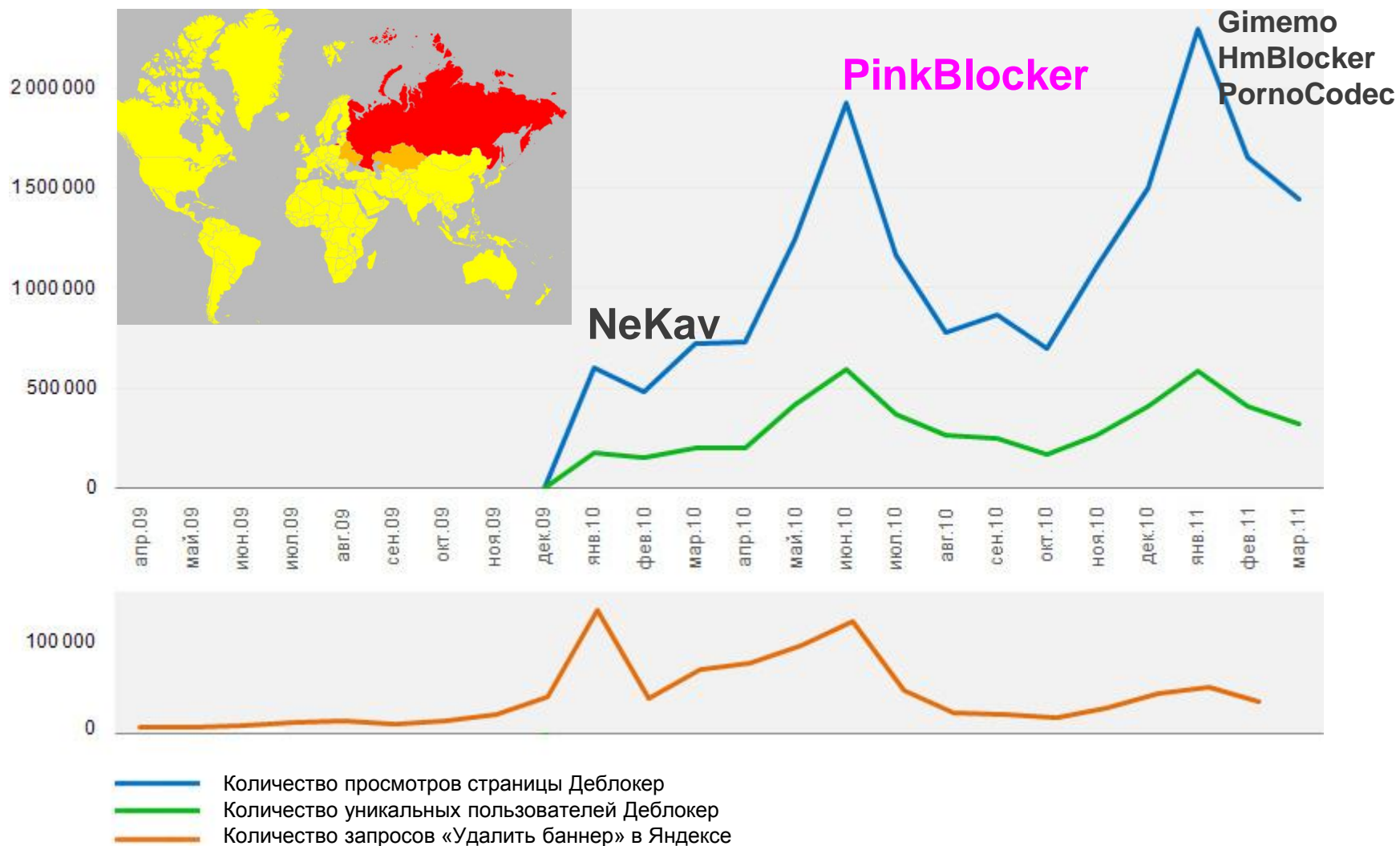
Социальная инженерия применительно к баннерам-блокировщикам:



Методы получения прибыли вымогателями:



Масштаб явления



Сервис Deblocker 1.0

Информация:

Номер SMS*

Ключевое слово

» Сгенерировать ключ деактивации «

Ключи деактивации:



3071

Я НЕ ПИСЕЦ, НО Я ПРИШЕЛ

Сервис Deblocker 2.0

Поиск алгоритма по SMS

SMS

Список всех алгоритмов [65]

| | | | | |
|--------------------------------|---------------------------------|----------------------------------|-----------------------------------|------------------------------------|
| <input type="checkbox"/> 1046 | <input type="checkbox"/> 1053 | <input type="checkbox"/> 1098 | <input type="checkbox"/> 1121 | <input type="checkbox"/> 1171 |
| <input type="checkbox"/> 1206 | <input type="checkbox"/> 1624 | <input type="checkbox"/> 1645 | <input type="checkbox"/> 1824 | <input type="checkbox"/> 1874 |
| <input type="checkbox"/> 1899 | <input type="checkbox"/> 1945 | <input type="checkbox"/> 2090 | <input type="checkbox"/> 2322 | <input type="checkbox"/> 2810 |
| <input type="checkbox"/> 2895 | <input type="checkbox"/> 3354 | <input type="checkbox"/> 3631 | <input type="checkbox"/> 3649 | <input type="checkbox"/> 4070 |
| <input type="checkbox"/> 4108 | <input type="checkbox"/> 4113 | <input type="checkbox"/> 4161 | <input type="checkbox"/> 4280 | <input type="checkbox"/> 4449 |
| <input type="checkbox"/> 4460 | <input type="checkbox"/> 4565 | <input type="checkbox"/> 4617 | <input type="checkbox"/> 5155 | <input type="checkbox"/> 5175 |
| <input type="checkbox"/> 5339 | <input type="checkbox"/> 5370 | <input type="checkbox"/> 5373 | <input type="checkbox"/> 5537 | <input type="checkbox"/> 6005 |
| <input type="checkbox"/> 6008 | <input type="checkbox"/> 7117 | <input type="checkbox"/> 7122 | <input type="checkbox"/> 7125 | <input type="checkbox"/> 7132 |
| <input type="checkbox"/> 7138 | <input type="checkbox"/> 7250 | <input type="checkbox"/> 7796 | <input type="checkbox"/> 7910 | <input type="checkbox"/> 7923 |
| <input type="checkbox"/> 8155 | <input type="checkbox"/> 8161 | <input type="checkbox"/> 8171 | <input type="checkbox"/> 8353 | <input type="checkbox"/> 8355 |
| <input type="checkbox"/> 8385 | <input type="checkbox"/> 8926 | <input type="checkbox"/> 9099 | <input type="checkbox"/> 9690 | <input type="checkbox"/> 9691 |
| <input type="checkbox"/> 9915 | <input type="checkbox"/> 17013 | <input type="checkbox"/> 72170 | <input type="checkbox"/> 80888 | <input type="checkbox"/> 82300 |
| <input type="checkbox"/> 83868 | <input type="checkbox"/> 179479 | <input type="checkbox"/> 9090199 | <input type="checkbox"/> 90645045 | <input type="checkbox"/> 590437534 |

История модификации алгоритмов для ID = 2895

10.12.2009 16:00:58
текущий

Модификация алгоритма

SMS

```
// === 2895 ===  
function Generate($strKeyword)  
{  
    $pKeys = array();  
    // ключевое слово - код деактивации  
    $pDeactivateCodes = array(  
        "70+112701+now_algoritm" => "5748839",);  
    // получить код по ключевому слову  
    $strDeactivateCode = $pDeactivateCodes[$strKeyword];  
    if (strlen($strDeactivateCode) > 0)  
    {  
        array_push($pKeys, $strDeactivateCode);  
    }  
}
```

Сервис Deblocker 3.0

KASPERSKY Deblocker 3.0

[Генераторы](#)
[Алгоритмы](#)
[Функции](#)
[Скриншоты](#)
[Статистика](#)
[Проверка генераторов](#)
[Внешний сайт](#)
[Мобильная версия](#)
[Инструкция](#)

Топ 30 запросов за последние 24 часа

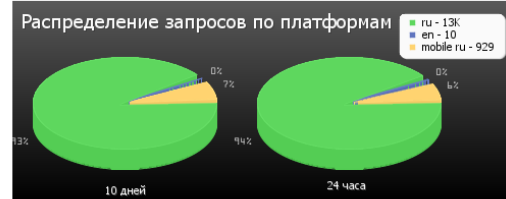
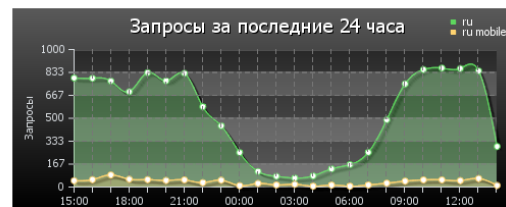
| SMS | Количество | %% |
|-----------------|------------|------|
| → 9879568116 | 810 | 5.75 |
| ↑ 5 9688919819 | 710 | 5.04 |
| ↑ 7 9879427424 | 372 | 2.64 |
| ↓ 3 9117219762 | 368 | 2.61 |
| ↓ 3 9879570169 | 365 | 2.52 |
| ↑ 3 9879210076 | 348 | 2.47 |
| → 9117222488 | 331 | 2.35 |
| → 9117222499 | 331 | 2.35 |
| ↓ 3 9879570913 | 321 | 2.28 |
| ↑ 1 9879196898 | 319 | 2.27 |
| ↑ 8 9879569398 | 299 | 2.12 |
| ↑ 1 9110133035 | 297 | 2.11 |
| ↓ 9 9117219915 | 294 | 2.09 |
| ↓ 11 9110943669 | 290 | 2.06 |
| → 9117219907 | 287 | 2.04 |
| ↓ 11 9117219785 | 280 | 1.99 |
| → 9110132987 | 247 | 1.75 |
| ↓ 10 3381 | 238 | 1.69 |
| → 9117222496 | 208 | 1.48 |
| → 9688919818 | 175 | 1.24 |
| ↓ 6 9670696942 | 173 | 1.23 |
| ↓ 1 8353 | 155 | 1.1 |
| ↓ 5 9879210255 | 129 | 0.92 |
| → 9879569578 | 122 | 0.87 |
| → 9179521861 | 114 | 0.81 |
| ↑ 4 9179517894 | 113 | 0.8 |
| ↓ 15 1121 | 113 | 0.8 |
| → 9688919860 | 112 | 0.8 |
| ↓ 1 9179522671 | 110 | 0.78 |
| → 9117282296 | 105 | 0.75 |

Топ 30 алгоритмов за последние 10 дней

| Алгоритм | Количество | %% |
|--------------------------------------|------------|-------|
| Gimemo_Blue_Phones_1 | 9027 | 23.02 |
| Gimemo_Blue_Phones_7 | 5779 | 14.74 |
| Chameleon_PirateSoftware_Phones | 3898 | 9.94 |
| Algorithm_XBlocker_White_3381 | 3104 | 7.92 |
| 1121 | 2884 | 7.36 |
| Algorithm_BrowHost | 1504 | 3.84 |
| FullScreen_RedText_WindowsBlocked | 1443 | 3.68 |
| Algorithm_PinkBlocker_LightPink_8353 | 874 | 2.23 |
| Losya_Blue_1 | 702 | 1.79 |
| 9800 | 637 | 1.62 |
| 3381 | 527 | 1.34 |
| PornoBlocker_MegaWarning | 448 | 1.14 |
| PornoBlocker_WinLicenseAndPorno | 405 | 1.03 |
| PornoCodec_Black | 391 | 1 |
| 3121 | 357 | 0.91 |
| Gimemo_Blue_Griva | 316 | 0.81 |
| Algorithm_XBlocker_Orange_5581 | 311 | 0.79 |
| PornoBlocker_FS_BlackBgmd | 289 | 0.74 |
| Algorithm_ArchSMS | 273 | 0.7 |
| PornoBlocker_PedoZoo_GrayBgmd | 262 | 0.67 |
| FakeFromSite_2 | 252 | 0.64 |
| HomoBlocker | 214 | 0.55 |
| 8353 | 210 | 0.54 |
| 7132 | 205 | 0.52 |
| PornoBlocker_GayFreeView_GrayBgmd | 204 | 0.52 |
| 3855 | 165 | 0.42 |
| 9395 | 142 | 0.36 |
| Gimemo_PornoCodec | 137 | 0.35 |
| Chameleon_WebCreds | 133 | 0.34 |
| 9697 | 129 | 0.33 |

Посещение

| IP | Имя | Количество | %% |
|--------------|--------------|------------|-----|
| 81.176.69.73 | 81.176.69.73 | 199699 | 100 |



Источники переходов

Февраль 2011 – Апрель 2011



Livejournal: пример работы ссылок

15 января 2011

Firefox

dolboeb: Не платите винлокерам

http://dolboeb.livejournal.com/1965911.html

Google

Создать аккаунт или войти через

username

Забывли имя пользователя или пароль?

Пример: [Блоги](#)

Заломнить

ГЛАВНАЯ | СОЗДАТЬ АККАУНТ | ИНТЕРЕСНОЕ | МАГАЗИН | ЕЩЁ | LJ.RU | LJTIMES

Мобильная версия | Мобильные возможности | Вся статистика ЖЖ

Пишет Anton Nossik ([dolboeb](#))
@ 2011-01-15 12:17:00

Местоположение: [Morjim, Goa](#)

Метки данной записи: [вирус](#), [криминал](#)

Не платите винлокерам

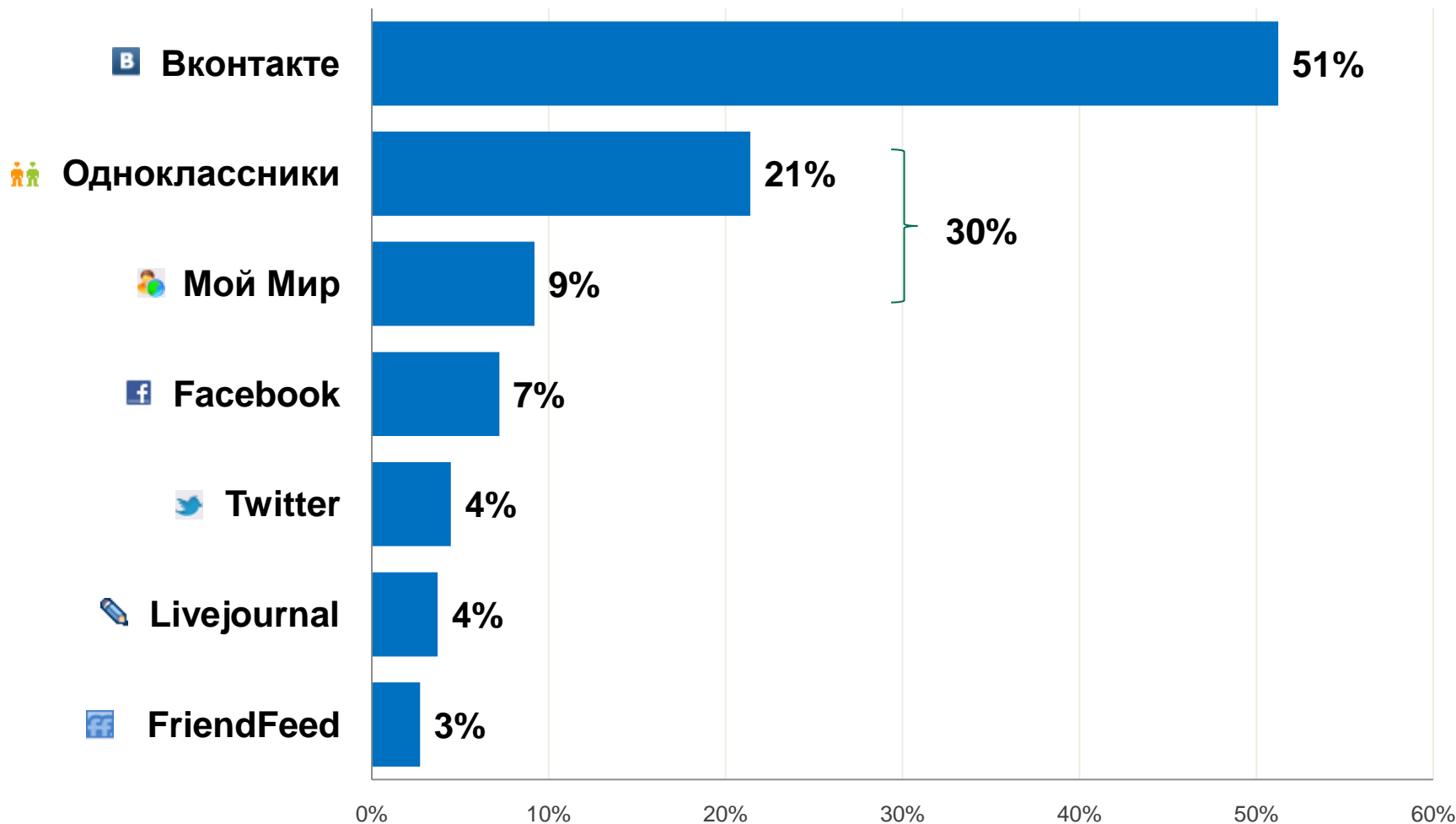
Выручка российских *винлокеров* (распространителей вируса, блокирующего систему Windows) оценивается специалистами TrendMicro в [100.000.000 рублей за 2010 год](#). Эти деньги злоумышленникам приносят те 2% владельцев заражённых компьютеров, которые послушно отправляют вымогателям платный SMS в обмен на обещание разблокировки.

Не будьте в числе этих 2% лохов, которые, вместе с коррумпированными ментами, тупыми законодателями и жуликоватыми связистами, помогают криминальному бизнесу цвести и развиваться. Никогда не отправляйте платные СМС мошенникам, которые об этом просят. Код, который злоумышленники предлагают прислать за 360 рублей, можно совершенно бесплатно [получить на сайте Касперского](#).

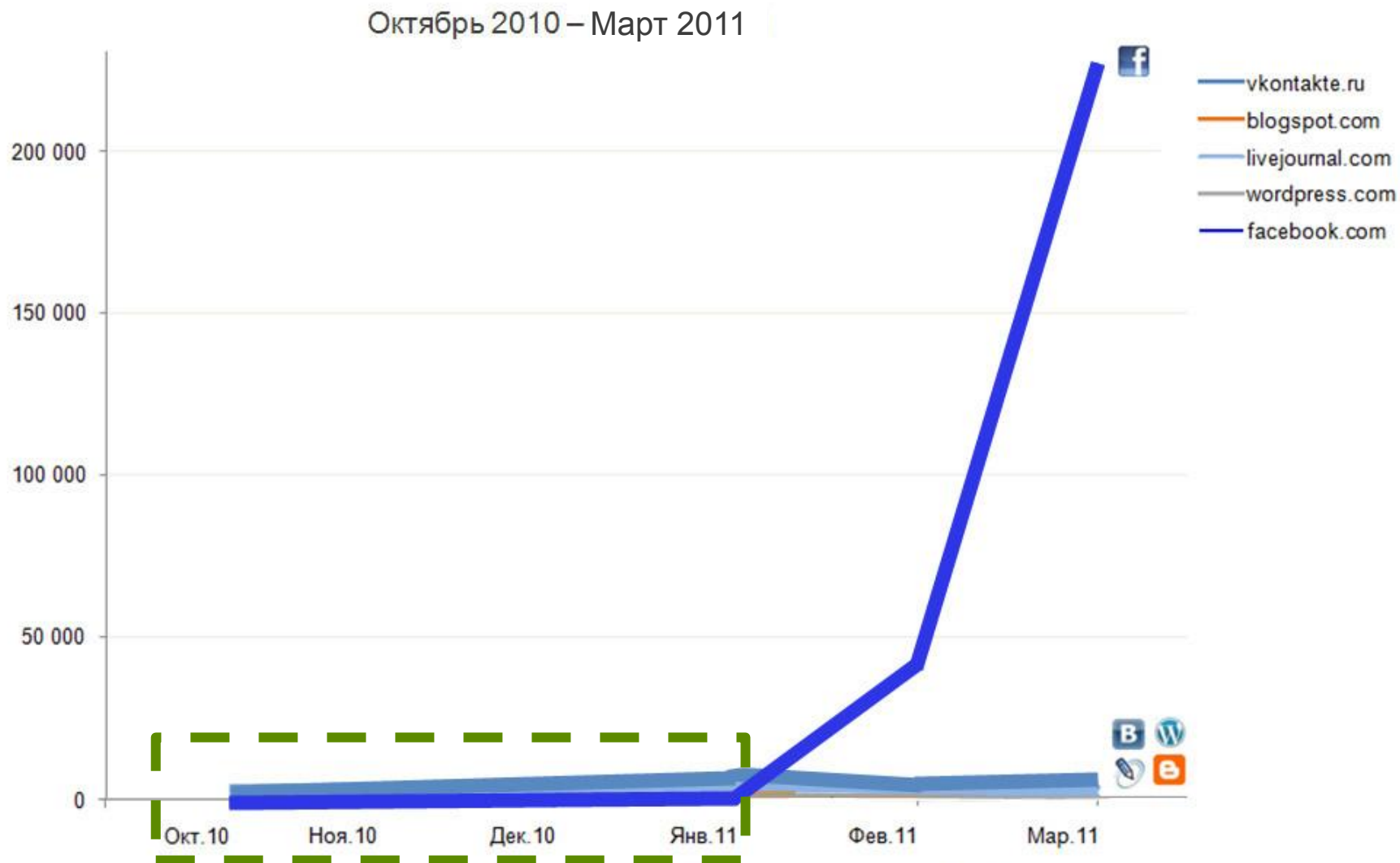
1 800 переходов

Ya.Share: Распределение по социальным сетям

26 марта 2011 – 17 апреля 2011



Переходы с социальных сетей



Демография: лояльные пользователи

Facebook: Мне нравится

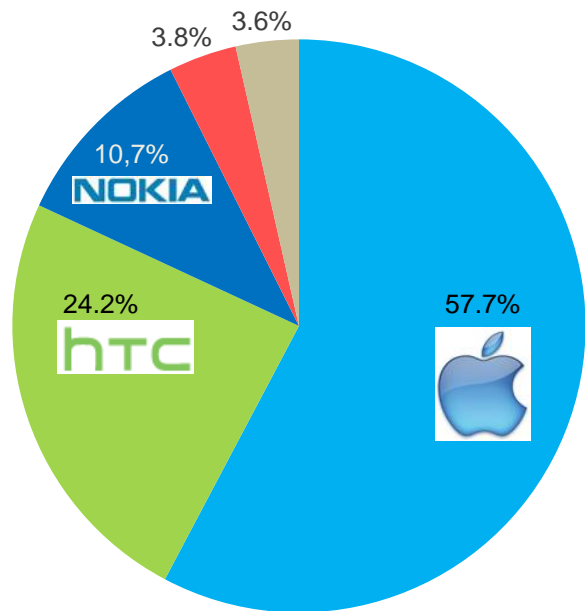
| Возраст | Женщины (27%) | | Мужчины (73%) | |
|---------|---------------|----|---------------|------|
| 13-17 | 1.8% | 6 | 49 | 15% |
| 18-24 | 4.9% | 16 | 60 | 18% |
| 25-34 | 18% | 59 | 81 | 25% |
| 35-44 | 0% | 0 | 28 | 8.6% |
| 45-54 | 1.2% | 4 | 16 | 4.9% |
| 55+ | 0.61% | 2 | 5 | 1.5% |

Вконтакте: Мне нравится

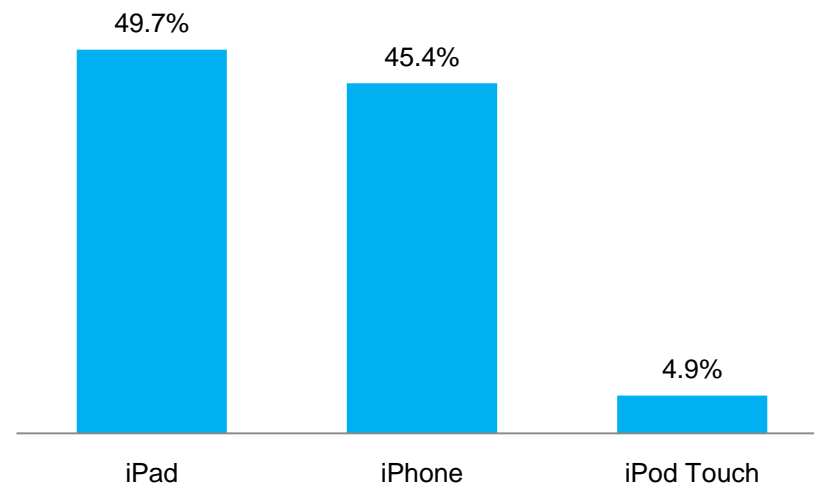


Мобильные пользователи

Октябрь 2010 – Апрель 2011



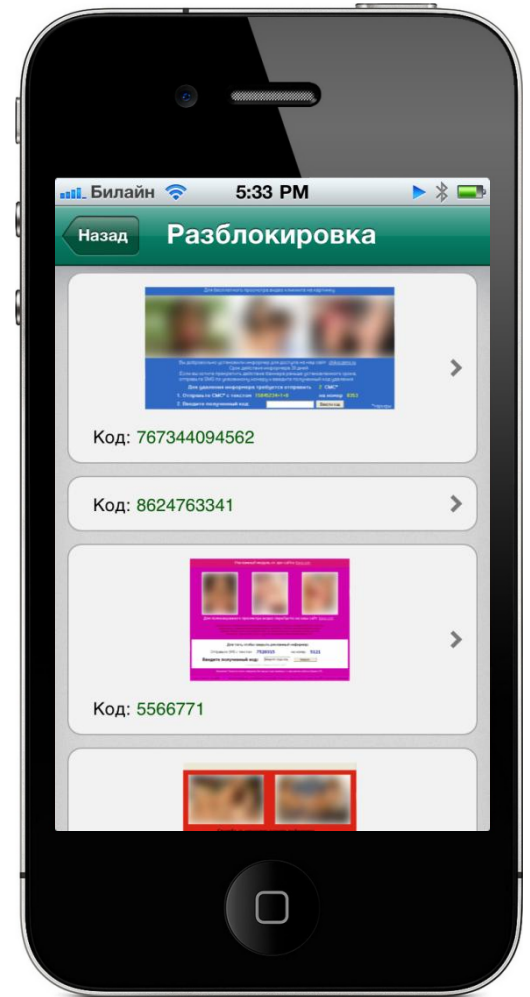
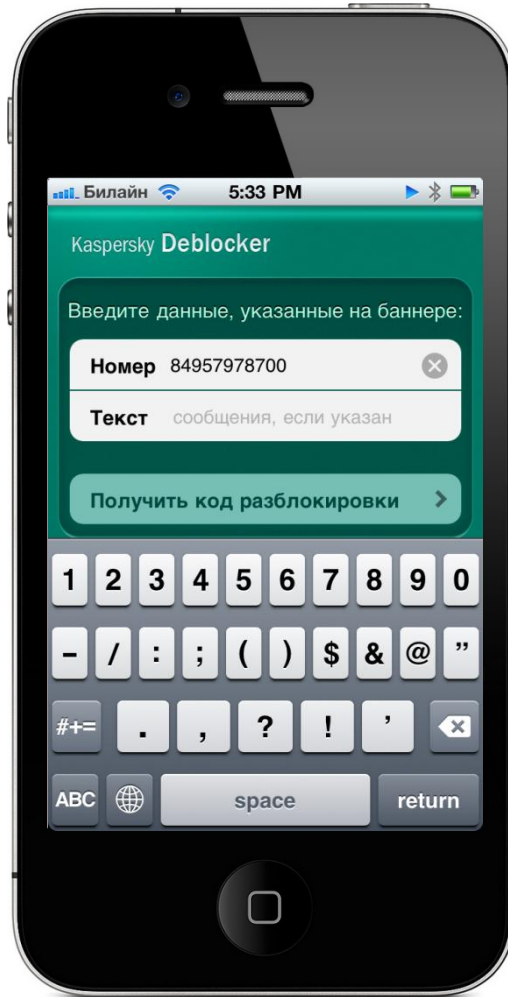
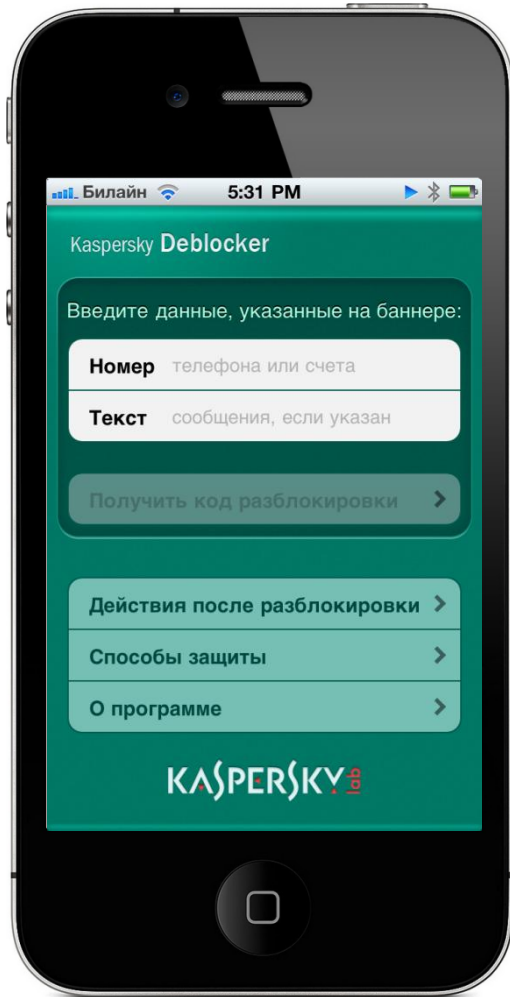
- Apple
- HTC
- Nokia
- Samsung
- Другие





Приложение для iPhone

Скоро в App Store



5% пострадавших заплатили блокерам
500 000 000* рублей за 2010 год
100 000 баннеров-блокеров
1 000 алгоритмов
100 блокерописателей
6 человек – команда Deblocker



* По различным оценкам от 100 000 000 до 500 000 000 рублей



<http://support.kaspersky.ru/sms>

Вопросы? Комментарии?

deblocker@kaspersky.com

Марина Еремина, Веб-аналитик, Лаборатория Касперского

Светлана Мушта, Веб-аналитик, Лаборатория Касперского

21 апреля 2011 / РИФ + КИБ 2011