# Основные тенденции развития вредоносного ПО в 2009 году (ботнет сети, фишинг, спам)

**Андрей Ярных**
Начальник отдела интернет-решений
Andrew_y@kaspersky.com

21-23 апреля 2010 г.

# Глобальные тенденции

- **Определились лидеры 2009 г.**
  Китай - лидер в создании вредоносного ПО
  Россия - «Законодатель моды», новые технологии
- **Ботнет сети совершенствуются**
  'Индивидуальное' заражение пользователей взломанных сайтов
  Использование технологии постоянной миграции серверов
- **Мода на альтернативные OS**
  эффективность распространения вредоносного кода в социальных сетях составляет около 10%,

# Зараженные интернет сайты

| Место | Страна | Количество атак | Процент от общего числа атак |
|---|---|---|---|
| 1 | CHINA | 18568923 | 78,990% |
| 2 | UNITED STATES | 1615247 | 6,871% |
| 3 | NETHERLANDS | 762506 | 3,244% |
| 4 | GERMANY | 446476 | 1,899% |
| 5 | RUSSIAN FEDERATION | 420233 | 1,788% |
| 6 | LATVIA | 369858 | 1,573% |
| 7 | UNITED KINGDOM | 272905 | 1,161% |
| 8 | UKRAINE | 232642 | 0,990% |
| 9 | CANADA | 141012 | 0,600% |
| 10 | ISRAEL | 116130 | 0,494% |

Почти 80% всех вредоносных программ и эксплойтов, действие которых было заблокировано в момент проникновения на компьютеры наших пользователей, находились именно на китайских серверах.

70% новых вредоносных программ имеют китайское происхождение

# Зараженные интернет сайты

| | |
|---|---|
| **Тройка стран, на территории которых обнаружено больше всего вредоносных URLs** | Первое место – Канада. Более 21% вредоносных ссылок от «общемировых запасов».<br>Второе – США – 16%.<br>Третье – Китай – 15% |
| **Тройка стран, на территории которых обнаружено больше всего сайтов, распространяющих вредоносные объекты** | Первое место – Китай – 26% от числа вредоносных сайтов во всем мире.<br>Второе – США – 18%.<br>Третье – Россия с – 12% |
| **Вредоносный сайт, от которого пострадало больше всего посетителей** | langlangXXX.com – 1,62% фактов заражения компьютеров от общего числа заражений по всему миру. Это китайский портал с порнографическими материалами. |

Данные за сентябрь 2009 г.
Лаборатория Касперского

# Зараженные компьютеры

| Место | Страна | Количество атак | Процент от общего числа атак |
|---|---|---|---|
| 1 | CHINA | 12708285 | 53,665% |
| 2 | EGYPT | 3615355 | 15,267% |
| 3 | TURKEY | 709499 | 2,996% |
| 4 | INDIA | 479429 | 2,025% |
| 5 | UNITED STATES | 416437 | 1,759% |
| 6 | VIETNAM | 346602 | 1,464% |
| 7 | RUSSIAN FEDERATION | 335656 | 1,417% |
| 8 | MEXICO | 308399 | 1,302% |
| 9 | SAUDI ARABIA | 287300 | 1,213% |
| 10 | GERMANY | 253097 | 1,069% |

По итогам работы KSN в 2009 году:
компьютеры жителей 215 стран и регионов мира подвергались угрозе заражения **23 680 646** раз.
Самые маленькие и отдаленные (Микронезия – 15 атак, Кирибати – 2 атаки, Каймановы острова – 13 атак)

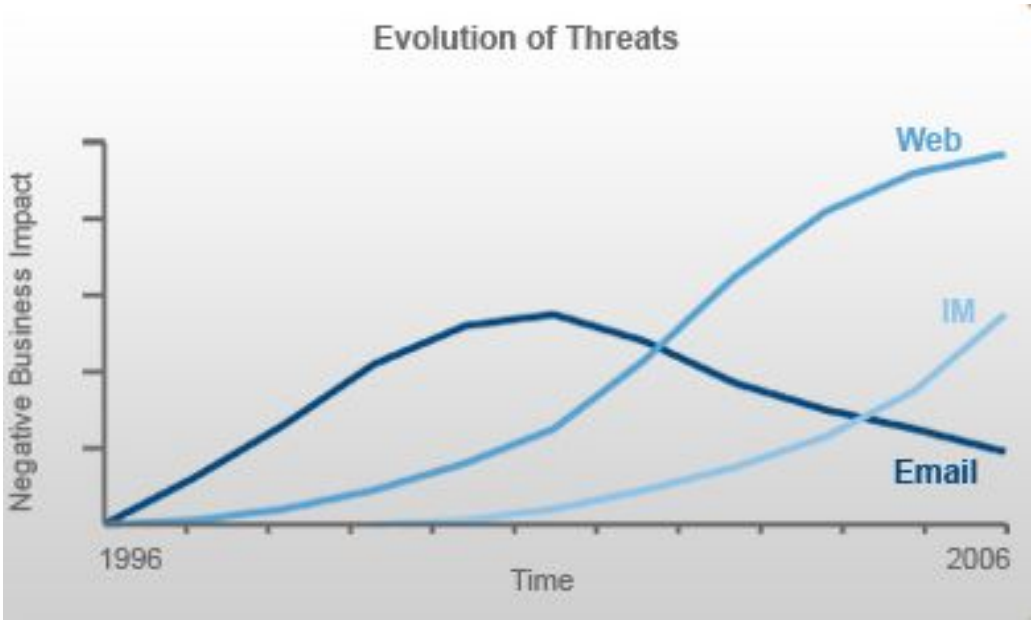
# Зараженные компьютеры

| | Страна | Регион | Среднее число уникальных зловредов на одного пользователя | Изменение позиции в рейтинге |
|---|---|---|---|---|
| 1 | Канада | Северная Америка | 2,03 | +1 |
| 2 | Великобритания | Европа | 1,92 | +1 |
| 3 | Малайзия | Азия | 1,82 | new |
| 4 | Россия | Европа | 1,68 | - |
| 5 | Китай | Азия | 1,51 | - |

пять стран, с веб-серверов которых вредоносный контент распространялся наиболее активно.
Источник: «Лаборатория Касперского»

# Веб атаки

**Веб-атака – загрузка и установка вредоносного ПО с заражённого веб-сайта без ведома пользователя.**




**Развитие методов доставки вредоносного ПО**

Данные ScanSafe

74% всего обнаруженного вредоносного ПО, было размещено на зараженных веб-сайтах

# Масштабы проблемы

*1,3% поисковых запросов в Google дает по меньшей мере один URL-адрес, помеченный как «опасный» на странице результатов поиска*


**Результаты поисков, содержащих вредоносный URL**

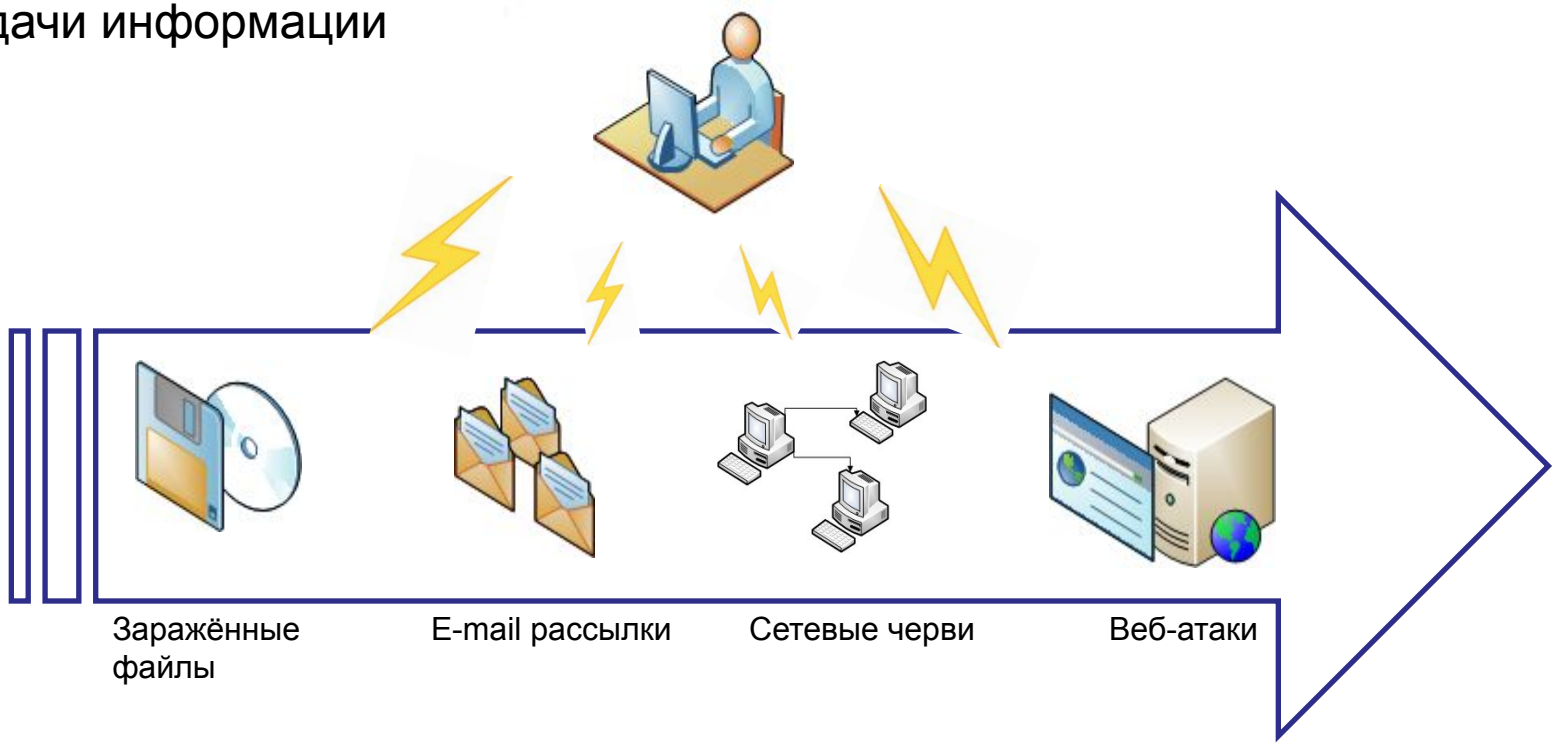
Данные Google Anti-Malware Team

## Объекты заражения

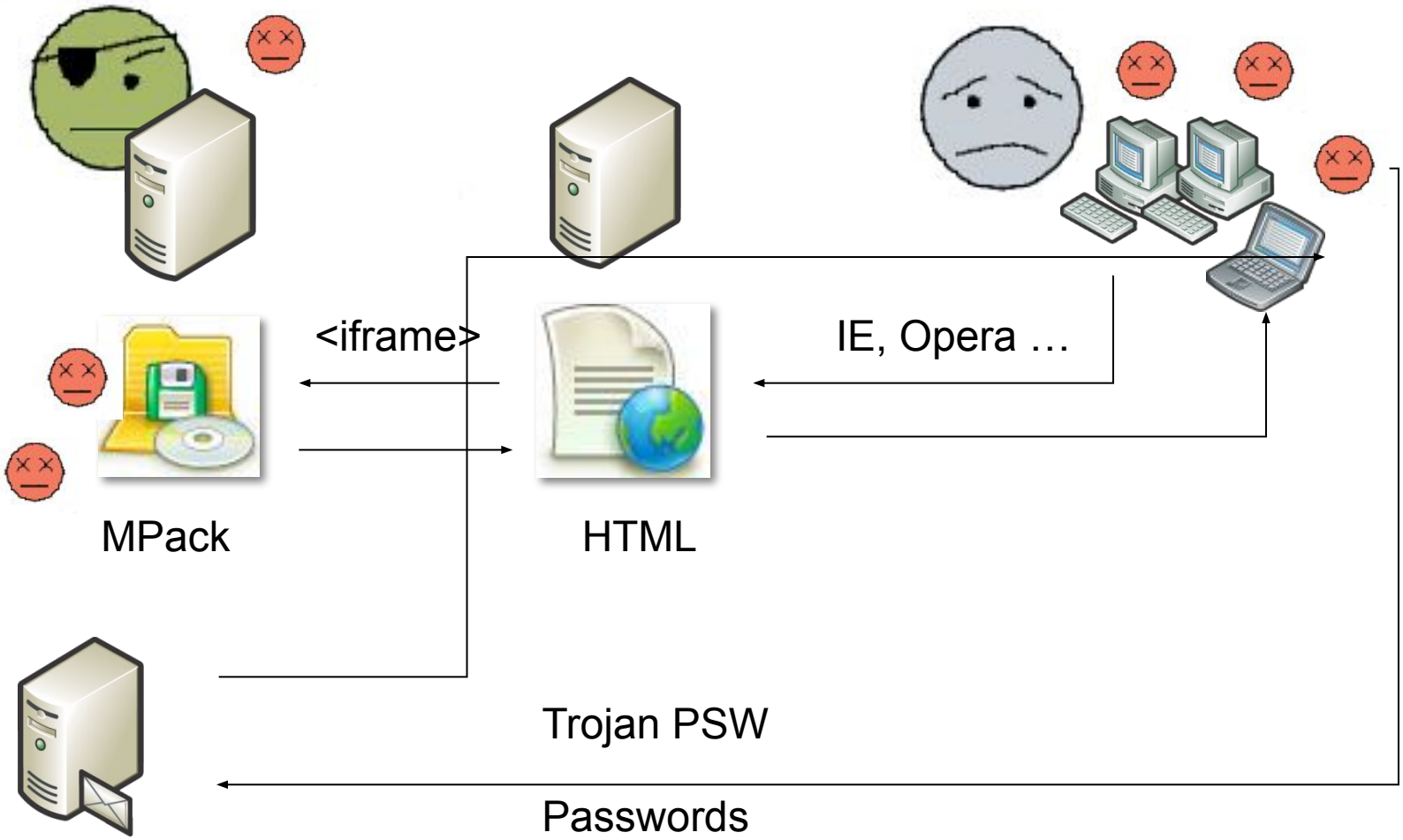
- специальные вредоносные сайты
- законопослушные сайты-жертвы

# Почему веб?

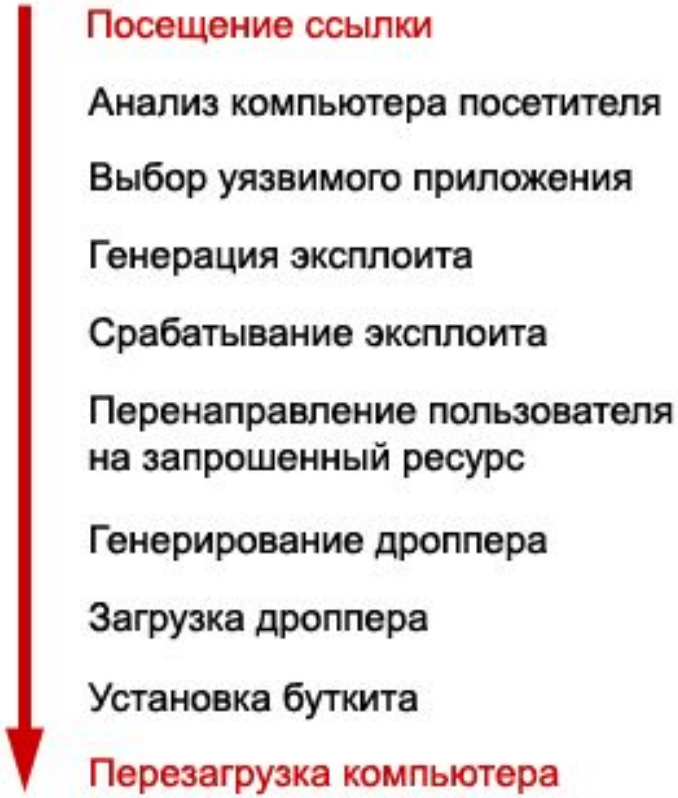
Транспортная среда вредоносного ПО развивается вместе со способами передачи информации




Веб-атака – наиболее незаметный и эффективный способ заражения пользовател


<iframe>
IE, Opera …
MPack
HTML
Trojan PSW
Passwords

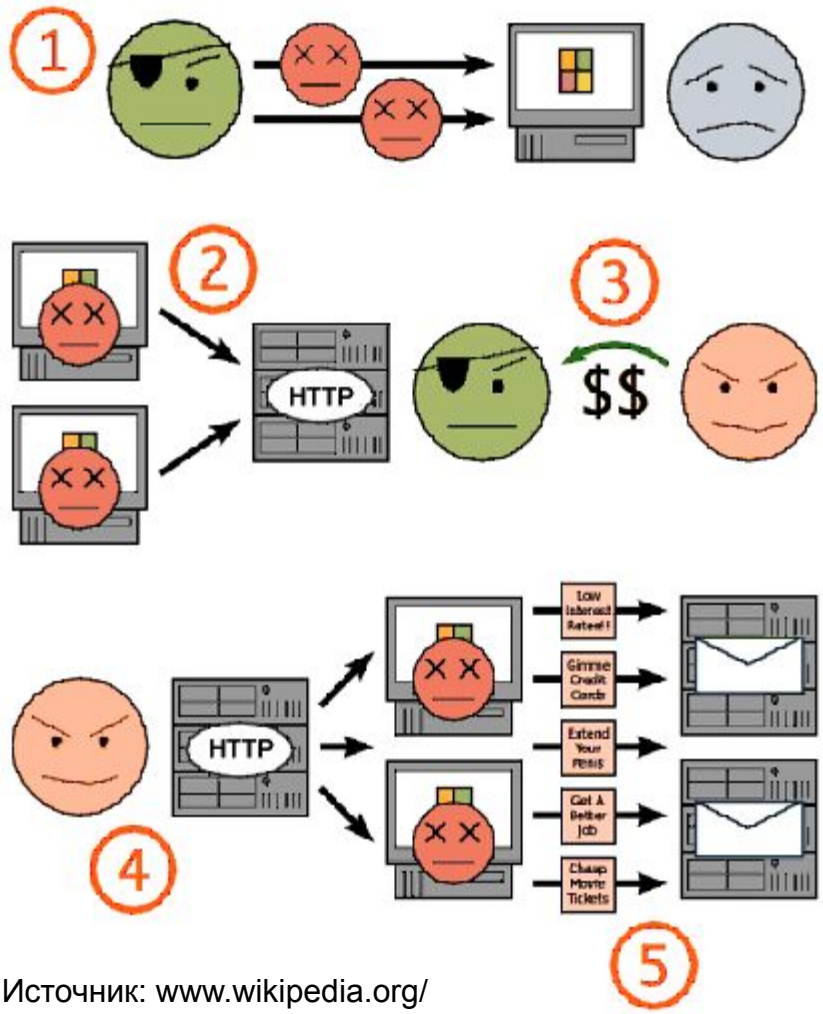
# Механизм создания ботнетсети




Самыми популярными являются следующие уязвимости:

CVE-2007-5659
CVE-2006-0003
CVE-2006-5820
CVE-2007-5779
CVE-2008-1472
CVE-2007-0018
CVE-2006-4777
CVE-2006-3730
CVE-2007-5779
CVE-2008-0624
CVE-2007-2222
CVE-2006-0005
CVE-2007-0015

# Механизм создания ботнетсети




1. Вирусописатель – заражение компьютеров пользователей с помощью троянский программ.
2. Объединение компьютеров в бот-нет сеть с единым управлением
3. Продажа или «аренда» машинного времени ботнет сети.
4. Использование централизованного управления, передача зловредной деятельности на зомби компьютеры.
5. Рассылка спама, Ddos атака, расширение ботнет сети (рассылка вирусов).

Источник: www.wikipedia.org/

# Структура ботнета

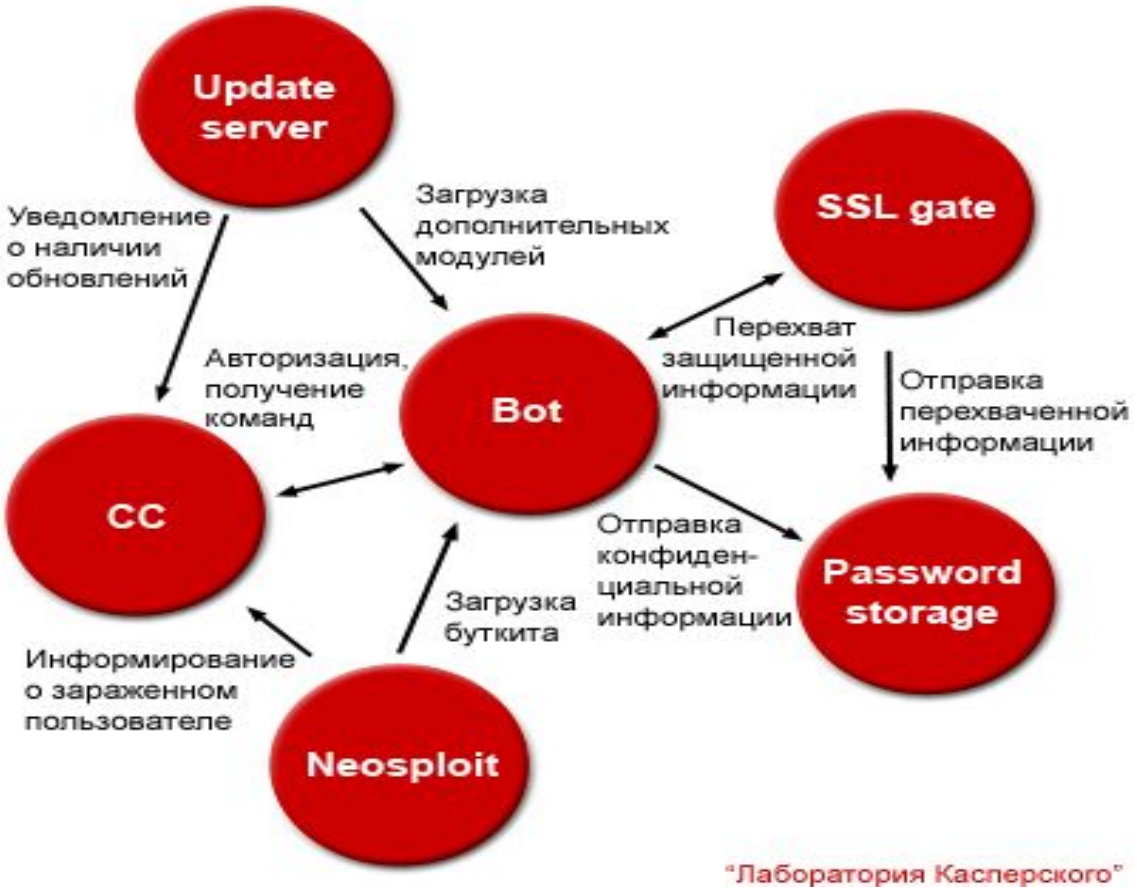
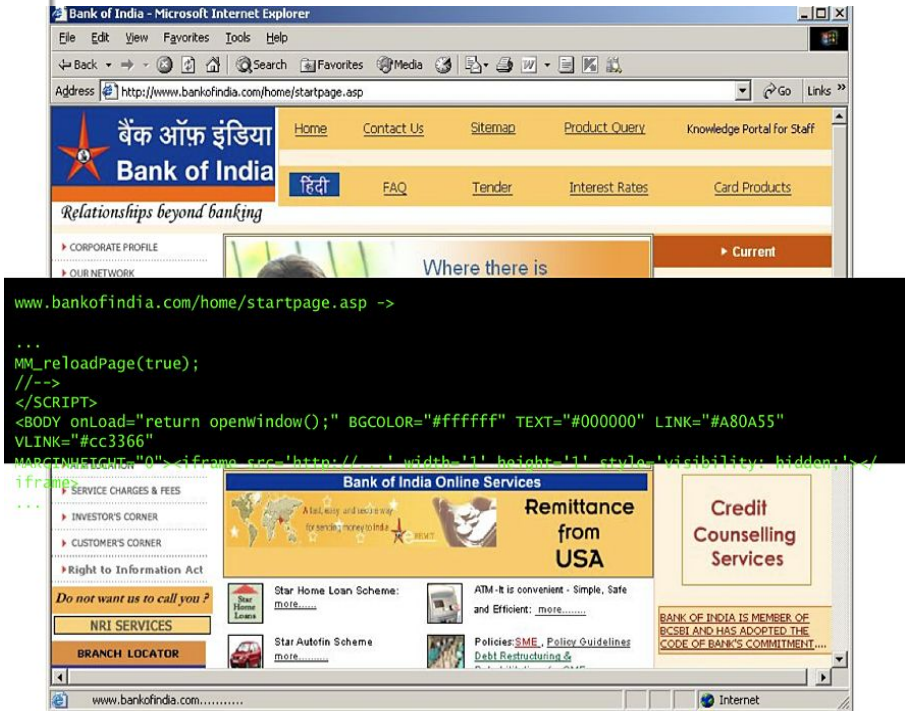
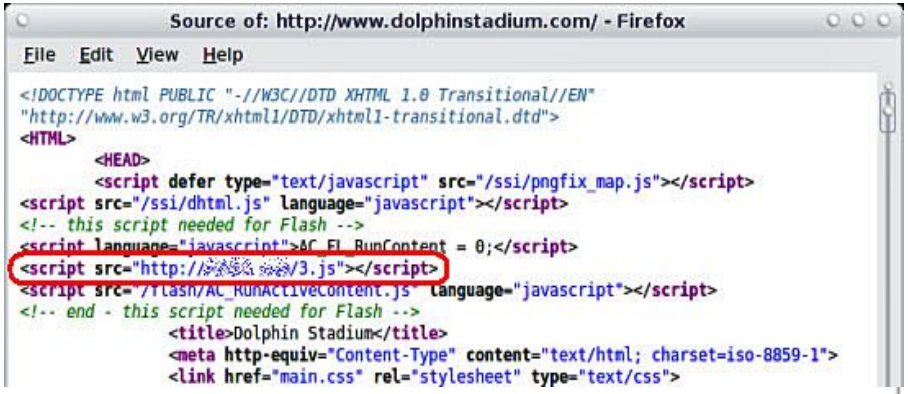



**Схема работы буткита с серверами**

# Технология веб-атаки - заражение сайта

Внедрение в код веб-страниц вызова вредоносного ПО с внешнего ресурса



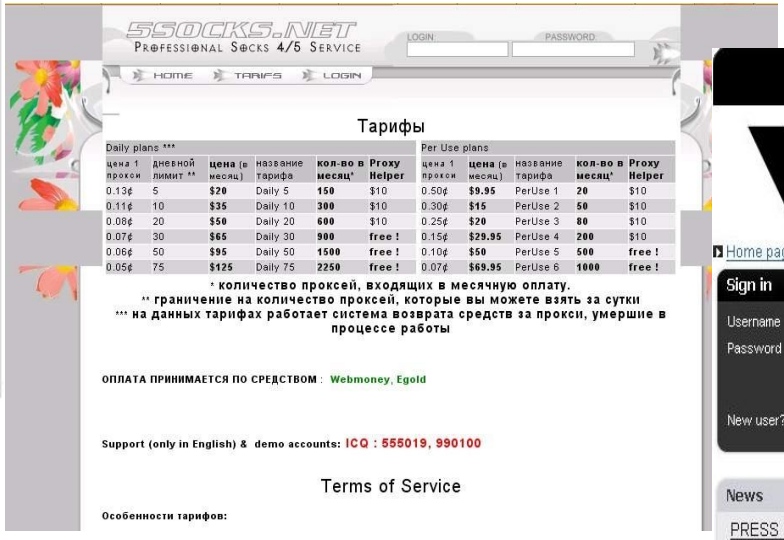



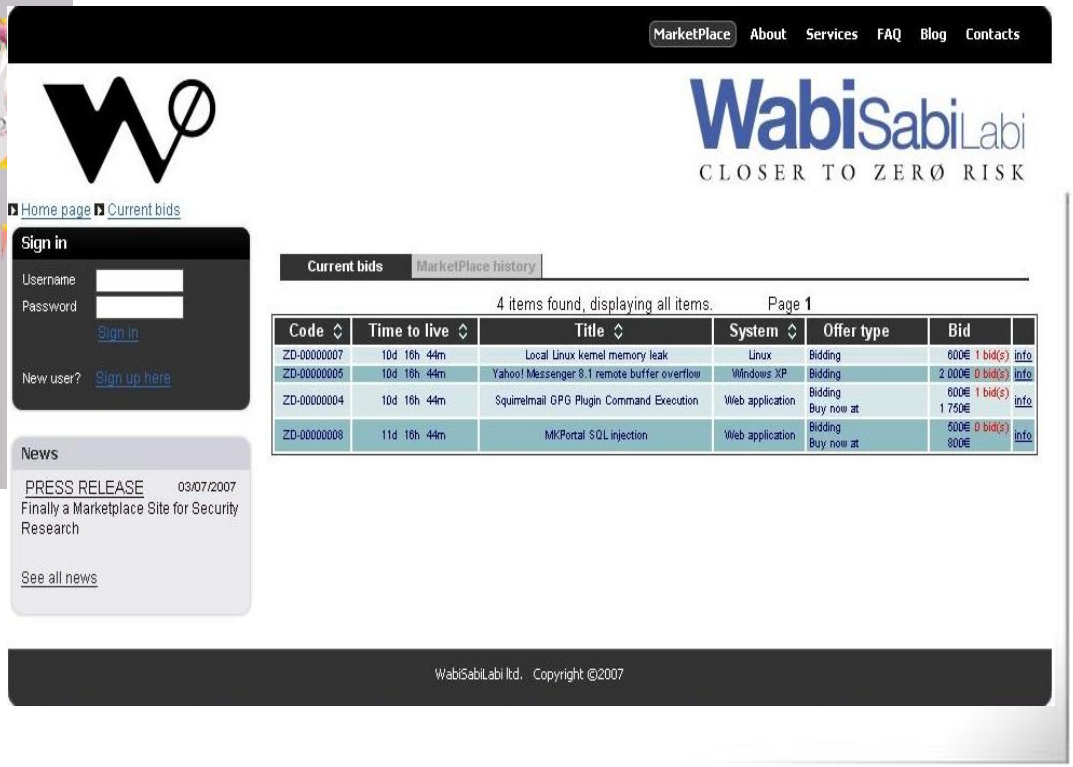

**Примеры:**

- Сайт стадиона Miami's Dolphin
- Сайт Bank of India
- Сайт Альфастрахования
- Сайт Минсвязи Бразилии
- Баннерообменная сеть utro.ru
- …

# Инструменты заражения

Инструментарий, использующий уязвимости QuickTime, Adobe Flash Player, Adobe Reader, RealPlayer, WinZip и пр. ПО, свободно продаётся в Интернет



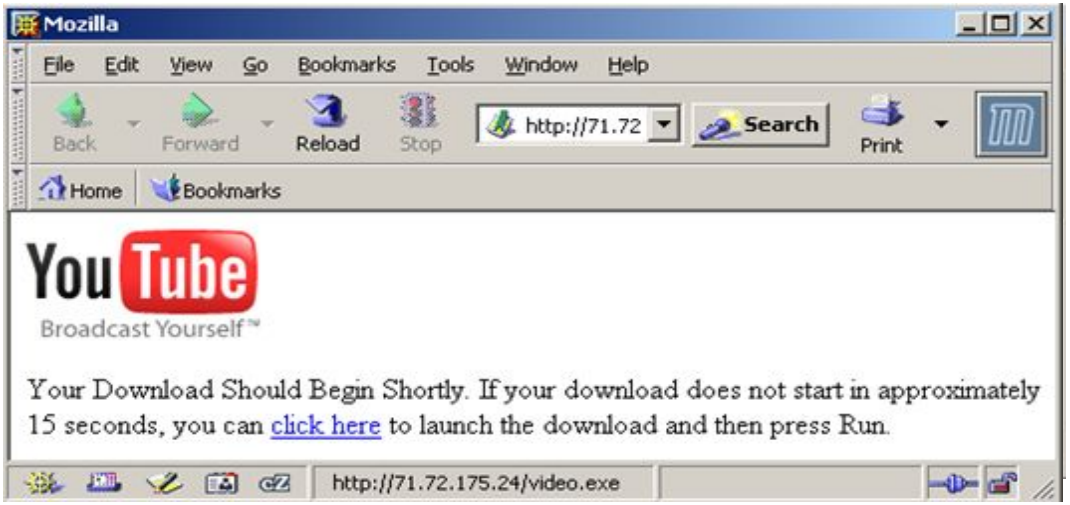




Злоумышленники приобретают набор эксплойтов и размещают его на вредоносном сервере…

# Зараженные интернет сайты

Социальная инженерия.

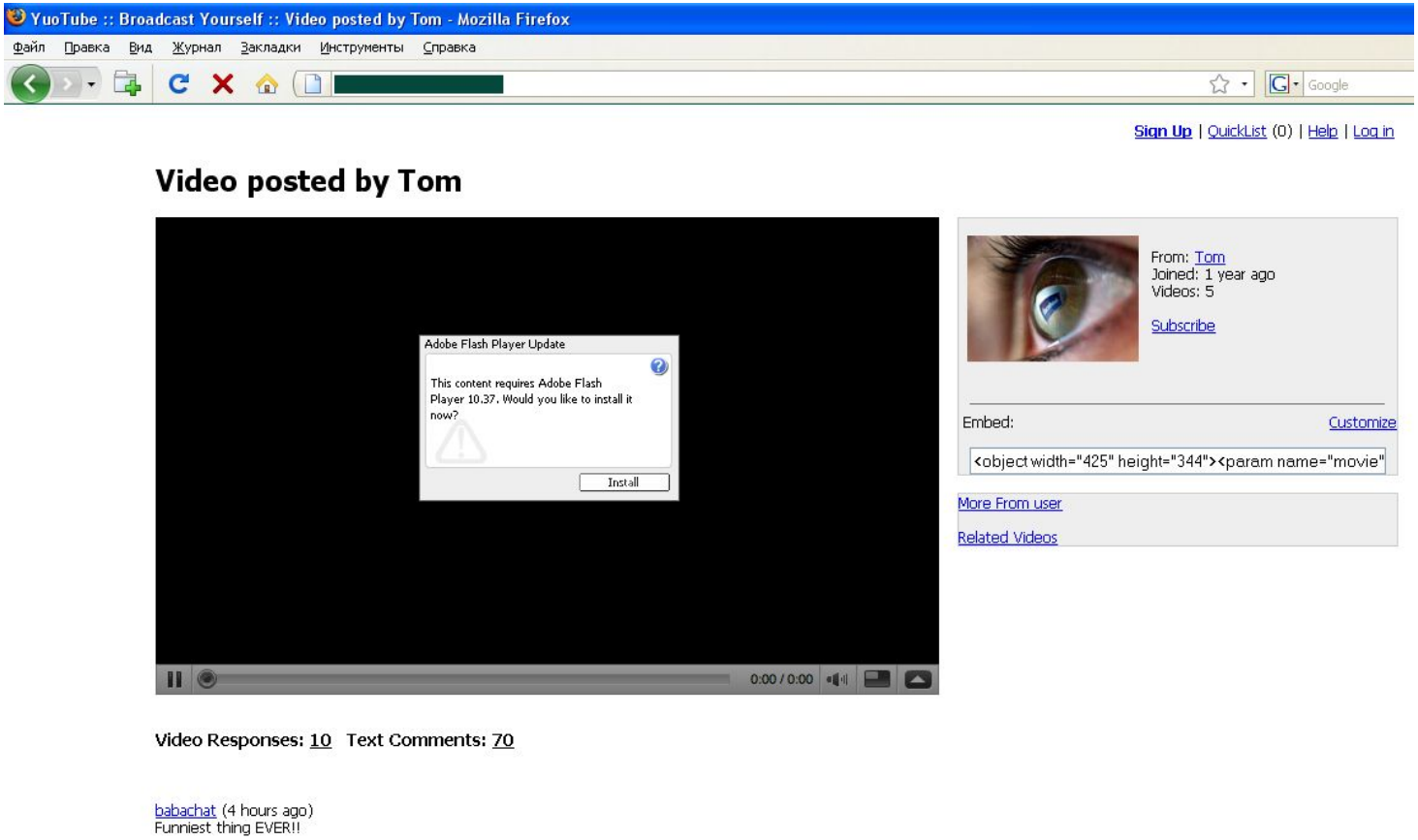
Например, атакующий присылает по электронной почте письмо, содержащее ссылку на интересный ресурс. Вот пример такого письма:




В вышеприведенном письме ссылка на YouTube – просто приманка, которая ведет к странице “video missing” («видео отсутствует»). Однако в HREF ссылке указан IP-адрес другого сайта. Ссылка “click here” указывает на исполняемый файл “video.exe”, вариант червя Zhelatin, также известного под именем Storm.

В результате, то что видит пользователь, когда заходит на указанный сайт

# Экономика ботнетов




**Требование скачать программу для просмотра файла**

# Экономика ботнетов

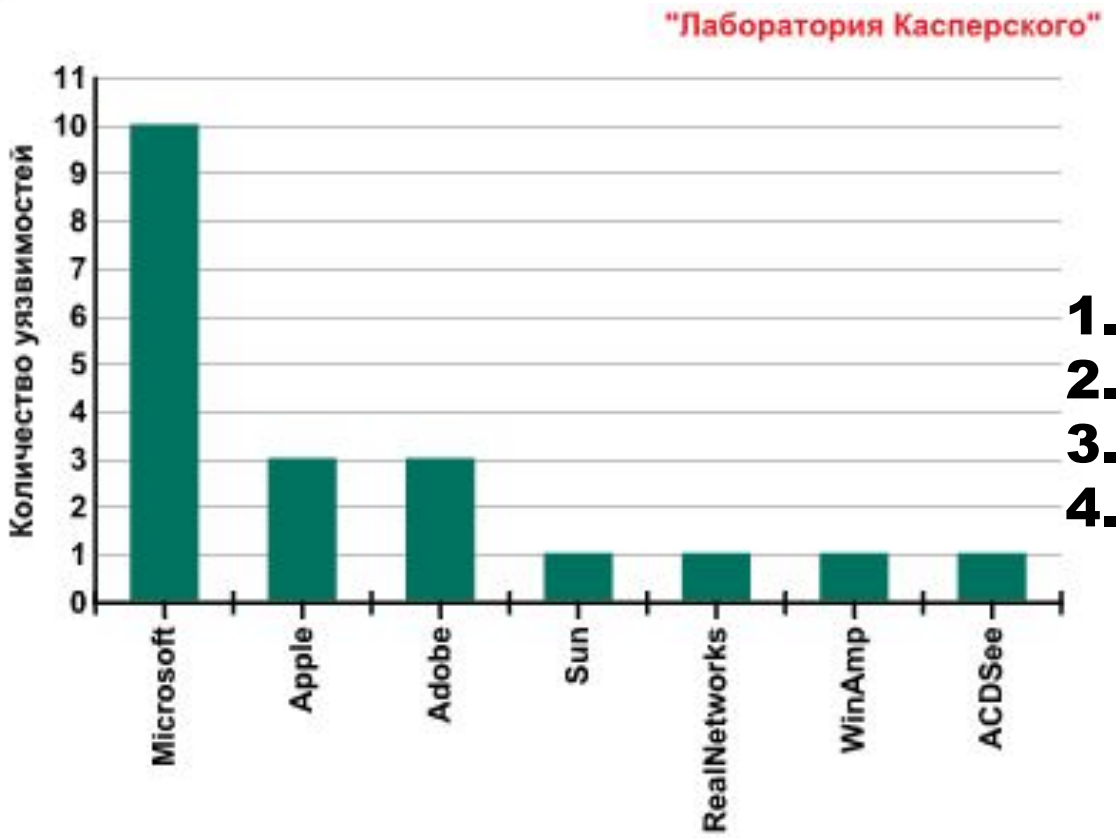

Требование скачать программу для просмотра файла

# Экономика ботнетов

Установка программ на компьютеры пользователей разных стран оплачивается фирмами по-разному. Например, за установку вредоносной программы на тысячу компьютеров в Китае в среднем платят 3 доллара, а в USA — 120 долларов. Это вполне объяснимо, ведь у пользователей развитых стран можно украсть куда более ценную, точнее более «денежную», информацию.

Стоимость украденных персональных данных напрямую зависит от страны, в которойживет их законный владелец. Например, полные данные жителей США стоят 5-8 долларов. На черном рынке особенно ценятся данные жителей Евросоюза — они стоят в два-три раза дороже данных жителей США и Канады. Это можно объяснить тем, что такими данными преступники могут пользоваться в любой стране, входящей в ЕС. В среднем по миру цена полного пакета данных об одном человеке составляет порядка $7.

# Уязвимости в приложениях




## Рейтинг наиболее уязвимых программ

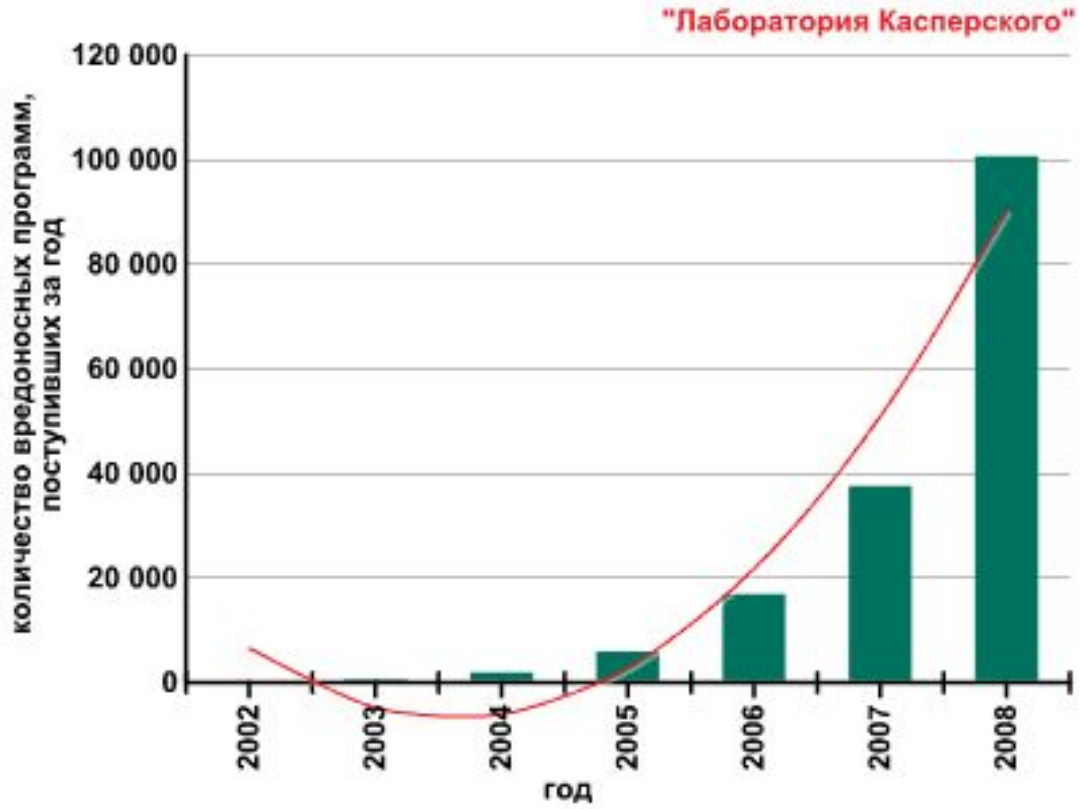
1. Adobe Flash Player
2. Real Player
3. Adobe Acrobat Reader
4. Microsoft Office

**Распределение уязвимостей по компаниям-производителям уязвимых приложений**

# Атаки на социальные сети

- **Почему уязвимы социальные сети**
  - между пользователями социальной сети устанавливаются доверительные отношения
  - социальные сети плохо защищены
- **Схема распространения вредоносных программ**
  - Пользователь получает ссылку от своего доверенного контакта – например, на видеоролик.
  - Для просмотра ролика требуется установить специальную программу
  - После установки эта программа ворует учетную запись и продолжает рассылку вредоносной программы доверенным контактам новой жертвы.

# Атаки на игровые сервисы

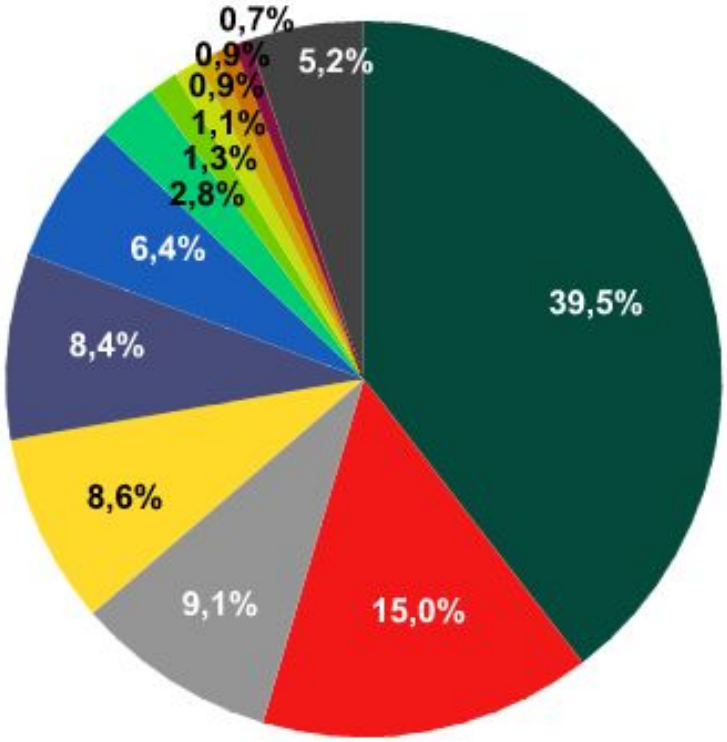



В 2008 году ситуация, к сожалению, ухудшилась: за год нами было обнаружено 100 397 новых игровых троянцев – эта цифра втрое превышает аналогичные показатели 2007 года (32 374).

# Атаки на игровые сервисы

- **В 2009 году для распространения вредоносных программ, ворующих пароли к онлайн-играм, злоумышленники стали активно использовать:**
  - неизвестные уязвимости движков веб-ресурсов для массового заражения сайтов;
  - неизвестные уязвимости клиентского ПО;
  - обновление вредоносного кода чаще регулярных обновлений антивирусных баз на компьютерах пользователей;
  - спам-рассылки писем, содержащих ссылки на зараженные страницы.

# Любимые хостинги вирусописателей




| | |
|---|---|
| .3322.org | |
| .no-ip.biz | |
| .host-domain-lookup.com | |
| .no-ip.org | |
| .vicp.net | |
| .no-ip.info | |
| .gicp.net | |
| .icpcn.com | |
| .dyndns.org | |
| .zapto.org | |
| .vicp.cc | |
| .rhelper.com | |
| other: | |
| .yahoo.com | 0,7% |
| .sytes.net | 0,7% |
| .oicp.net | 0,7% |
| .meibu.com | 0,7% |
| .8800.org | 0,7% |
| .ziyouforever.com | 0,6% |
| .hopto.org | 0,6% |
| .gnway.net | 0,6% |

"Лаборатория Касперского"

Домен 3322.org принадлежит крупному китайскому проекту cn99.com, число пользователей которого превышает 35 миллионов человек. Популярность cn99.com в Китае обусловлена тем, что он бесплатно предоставляет почтовый аккаунт и доменное имя третьего уровня.

Просмотрев список наиболее популярных доменов второго уровня, мы довольно быстро обнаружили причину, по которой они попали в TOP 10: все провайдеры, которым принадлежат эти домены, предоставляют услугу, известную как DDNS (Dynamic Domain Name System).
Злоумышленникам такой сервис позволяет быстро и легко регистрировать новое доменное имя, сохраняя анонимность, а также в любое время быстро менять DNS-информацию об используемом сервере.

# Любимые хостинги вирусописателей

**пять самых популярных стран, где на хостингах размещается вредоносное ПО.**
**Источник: «Лаборатория Касперского»**

| | Страна | Регион | Доля вредоносных хостингов | Изменение доли во втором квартале | Изменение позиции в рейтинге |
|---|---|---|---|---|---|
| 1 | Китай | Азия | 19,43% | +0,73% | - |
| 2 | Россия | Европа | 17,35% | +1,62% | - |
| 3 | США | Северная Америка | 13,13% | -1,35% | - |
| 4 | Германия | Европа | 8,06% | +0,47% | - |
| 5 | Бразилия | Южная Америка | 5,45% | +1,65% | +3 |

**Страны, на ресурсах которых размещены вредоносные программы**
На эту пятерку приходится 63,43% всех выявленных вредоносных хостингов.

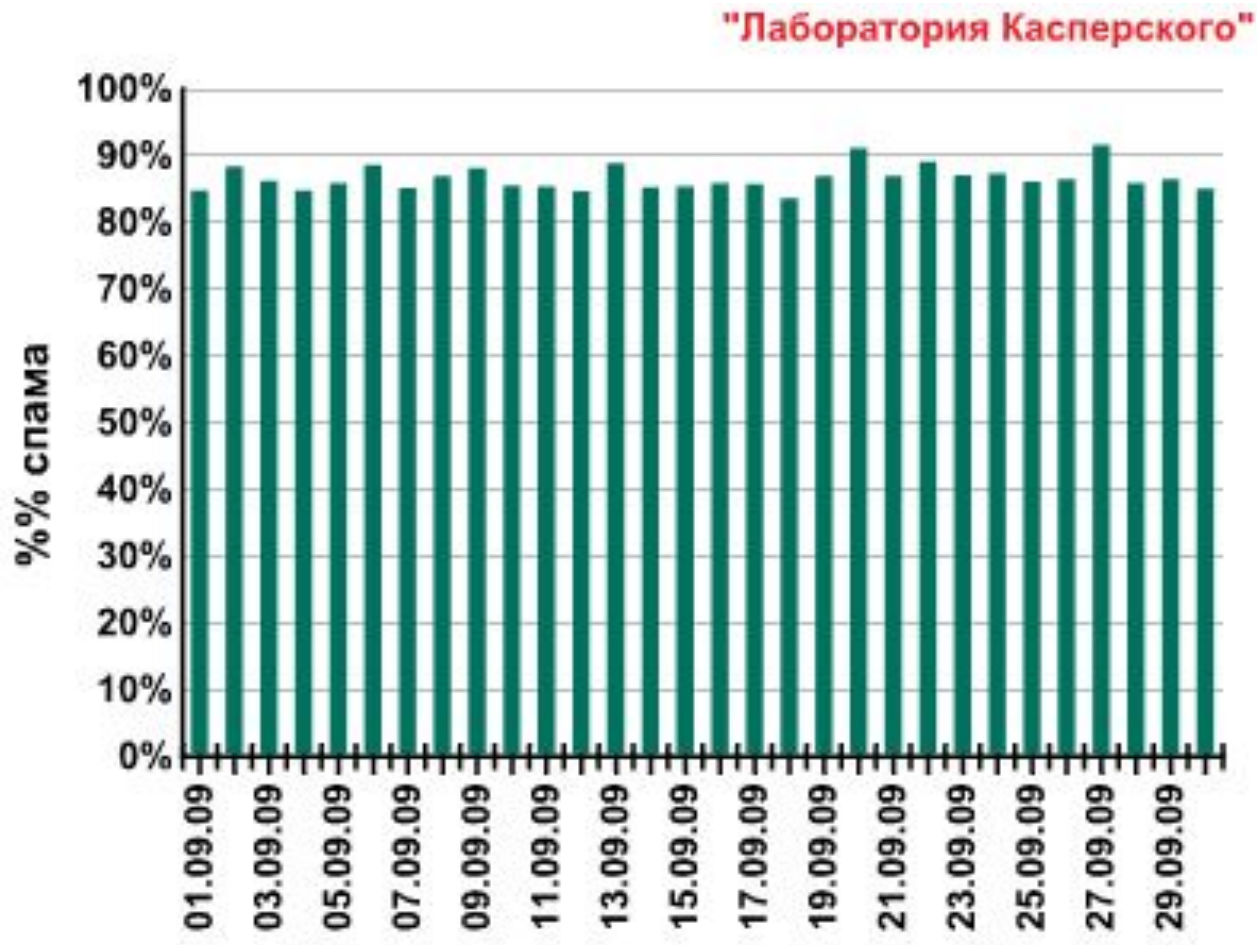
# Мода на альтернативные OS

| Операционные системы | Всего | Backdoors, Hacktools, Exploits & Rootkits | Вирусы и черви | Трояны |
|---|---|---|---|---|
| Linux | 1898 | 942 (50%) | 136 (7%) | 88 (5%) |
| FreeBSD | 43 | 33 (77%) | 10 (23%) | 0 (0%) |
| Sun Solaris | 119 | 99 (83%) | 17 (15%) | 3 (2%) |
| Unix | 212 | 76 (36%) | 118 (56%) | 3 (1%) |
| OSX | 48 | 14 (29%) | 9 (19%) | 11 (23%) |
| Windows | 2247659 | 501515 (22%) | 40188 (2%) | 1232798 (55%) |

Вредоносные программы для Unix-подобных систем имеют совсем другие цели. Они остаются незамеченными и крадут данные о кредитных картах из интернет-магазинов или пароли пользователей. Чаще всего для атаки используются не троянцы, а известные уязвимости серверных сервисов.

# Спам, Особенности месяца

- Доля спама в почтовом трафике по сравнению с августом увеличилась на 1,2% и составила в среднем 86,3%.
- Ссылки на фишинговые сайты находились в 0,84% всех электронных писем, что на 0,25%, меньше чем в августе.
- Вредоносные файлы содержались в 1,22% электронных сообщений, что на 1,17% больше, чем в прошлом месяце.
- Доля саморекламы спамеров продолжает уменьшаться.
- Для обхода антиспам фильтров спамеры вставляли в электронные адреса лишние цифры, которые пользователь должен был самостоятельно из них убрать.




**Доля спама в Рунете в сентябре 2009**

# Тенденции **2009** года

## Malware 2.5

На смену концепции Malware 2.0 приходит новая. Концепция функционирования гигантских распределенных систем-ботнетов, придуманная русскоязычными хакерами и реализованная во вредоносных программах Rustock.C, Sinowal (буткит) и нескольких других, продемонстрировала свою высокую эффективность и надежность.

- Отсутствие стационарного центра управления ботнетом – так называемый «мигрирующий ботнет»
- Использование стойких криптографических алгоритмов при взаимодействии между C&C и машинами в ботнете.
- Использование универсальных центров управления для разных ботнетов. Развитие идеи «универсального кода», реализованной во вредоносной программе Zbot

# Тенденции **2009** года

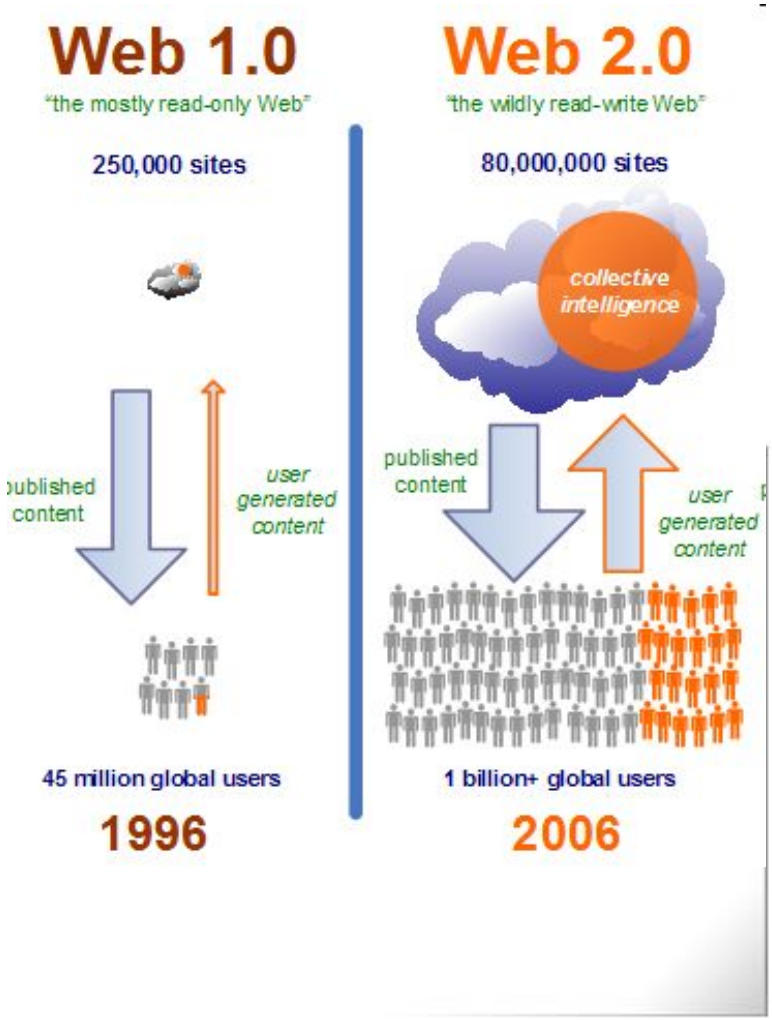
- **Фишинг/мошенничество**
  - Конкуренция среди фишеров растет. Для обмана пользователей простейшей подделки сайта банка будет уже недостаточно – атаки стали более изощренными и интенсивными.
- **Снижение активности игровых троянцев**
  - Доход мал, конкуренция велика, антивирусные компании научились справляться с гигантскими объемами игровых вредоносных программ, пользователи увеличили свой образовательный уровень, игровые компании приняли ряд мер по пресечению незаконных операций с украденными аккаунтами и игровыми ценностями…

# Вопросы?

# Спасибо за внимание!

# Атаки на социальные сети

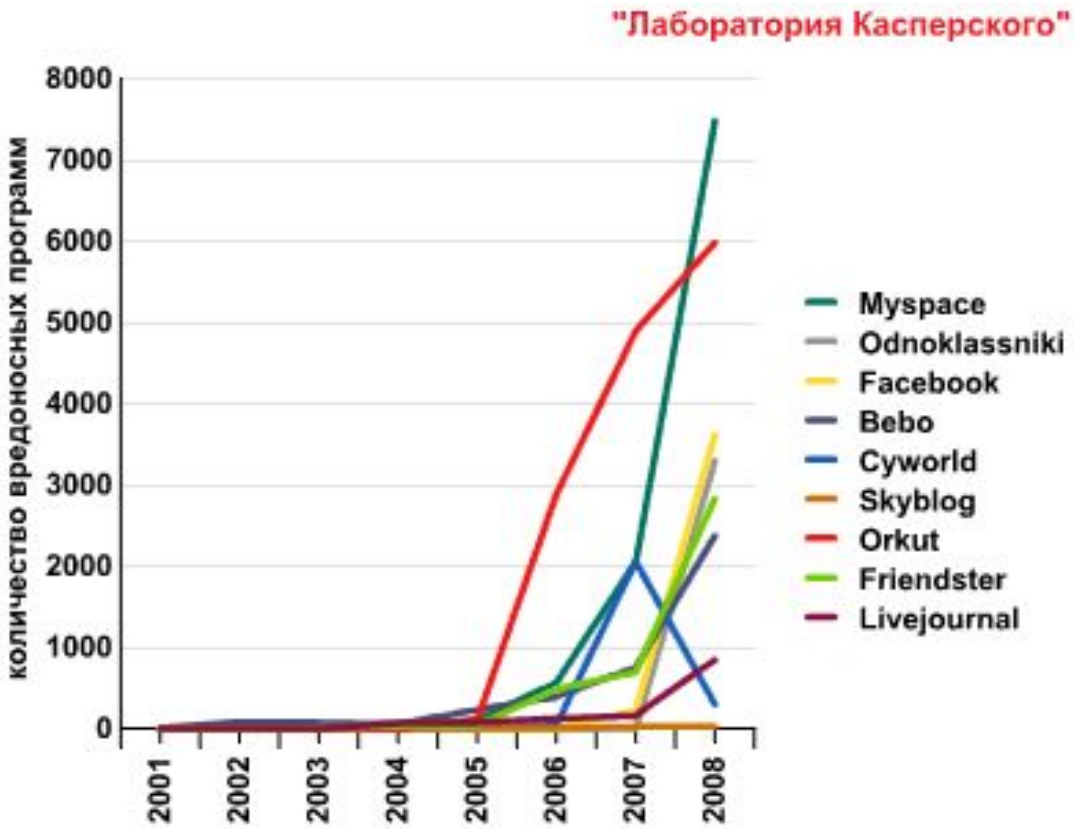
- Миграция пользовательских данных с персонального компьютера в Сеть
- Использование одного аккаунта для нескольких разных сервисов
- Детальная информация о пользователе
- Информация о его связях, контактах и знакомых
- Место для публикации чего угодно
- Доверительные отношения между контактами



# Количество вредоносных программ


В конце 2008 года в коллекции «Лаборатории Касперского» содержалось более 43 000 вредоносных файлов, так или иначе связанных с различными социальными сетями.

# Количество вредоносных программ




Согласно прогнозам компаний RelevantView и eVOC Insights, количество пользователей социальных сетей в 2009 году достигнет 80% от числа всех пользователей интернета и составит более миллиарда человек.

# Опасность в социальной сети

| Социальная сеть | К в п за | Географическое положение наибольшего числа зарегистрированных пользователей (Источник: lemonde.fr) |
|---|---|---|
| Odnoklassniki | 3 | Россия |
| Orkut | 5 | Латинская Америка |
| Bebo | 2 | Европа |
| Livejournal | 8 | Россия |
| Friendster | 2 | Азиаткий-Тихоокианский регион |
| Myspace | 7 | Северная Америка |
| Facebook | 3 | Северная Америка |
| Cyworld | 3 | Южная Корея |
| Skyblog | 2 | Франция |


Пользователи социальных сетей становятся жертвами вредоносных программ различных поведений. Это могут быть Trojan-Spy, Trojan-PSW, Worm, Trojan и многие другие.