

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

**Андрей Ярных**  
Начальник отдела интернет-решений  
[Andrew\\_y@kaspersky.com](mailto:Andrew_y@kaspersky.com)

## 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

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

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

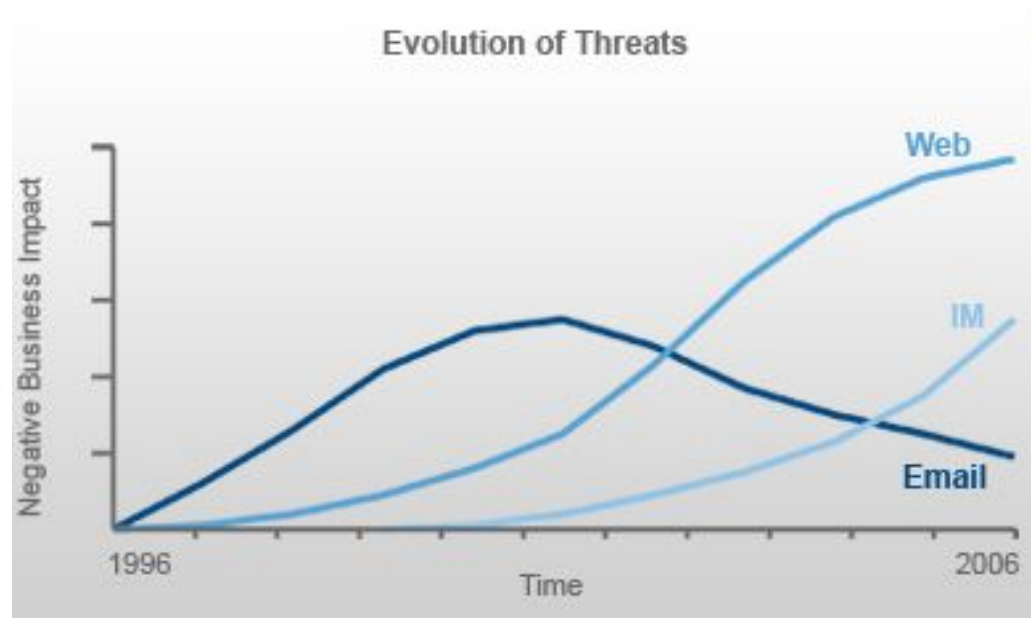
	Страна	Регион	Среднее число уникальных зловредов на одного пользователя	Изменение позиции в рейтинге
1	Канада	Северная Америка	2,03	+1
2	Великобритания	Европа	1,92	+1
3	Малайзия	Азия	1,82	new
4	Россия	Европа	1,68	-
5	Китай	Азия	1,51	-

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.



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

Развитие методов доставки вредоносного ПО

Данные ScanSafe

## Масштабы проблемы

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



### Объекты заражения

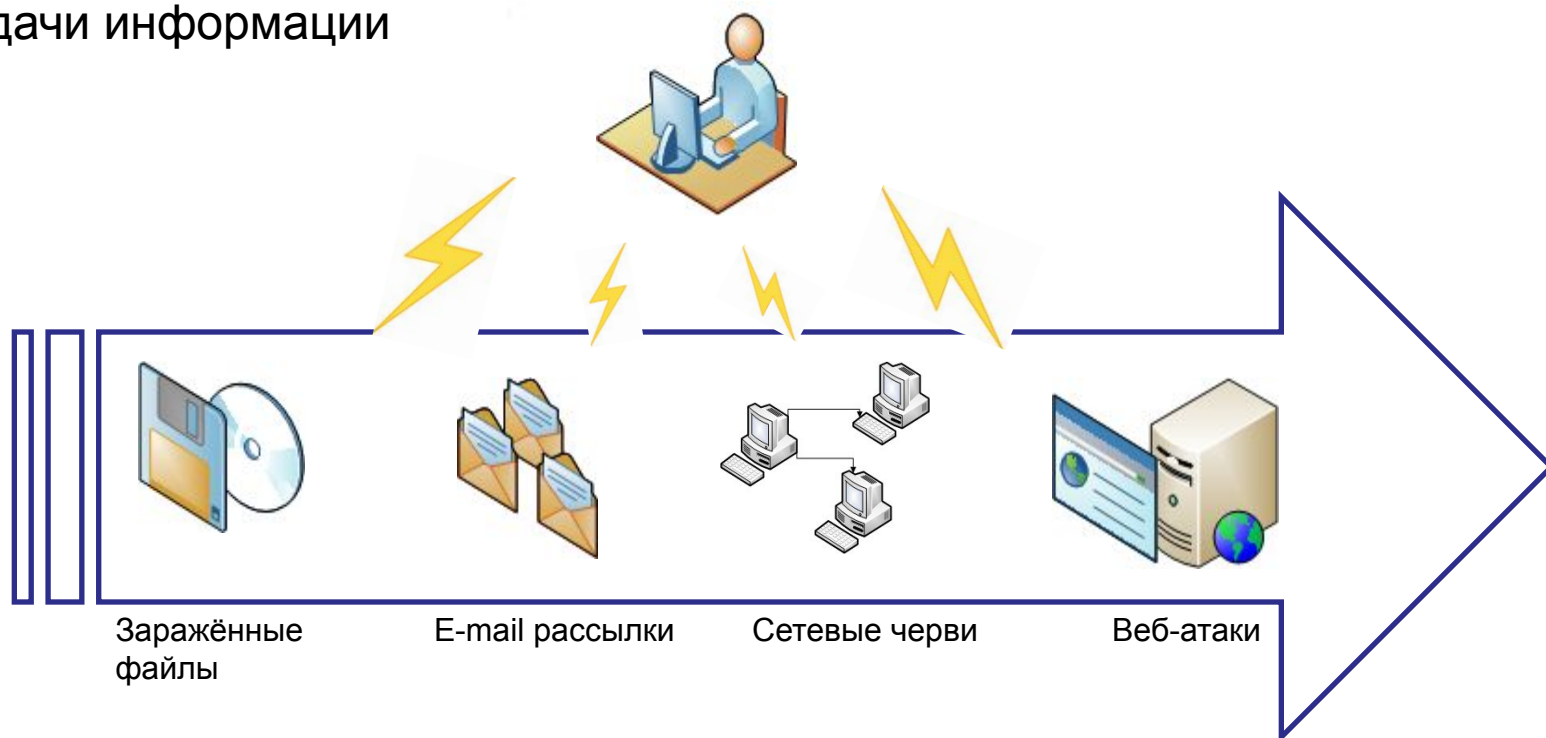
- специальные вредоносные сайты
- законопослушные сайты-жертвы

**Результаты поисков, содержащих вредоносный URL**  
Данные Google Anti-Malware Team

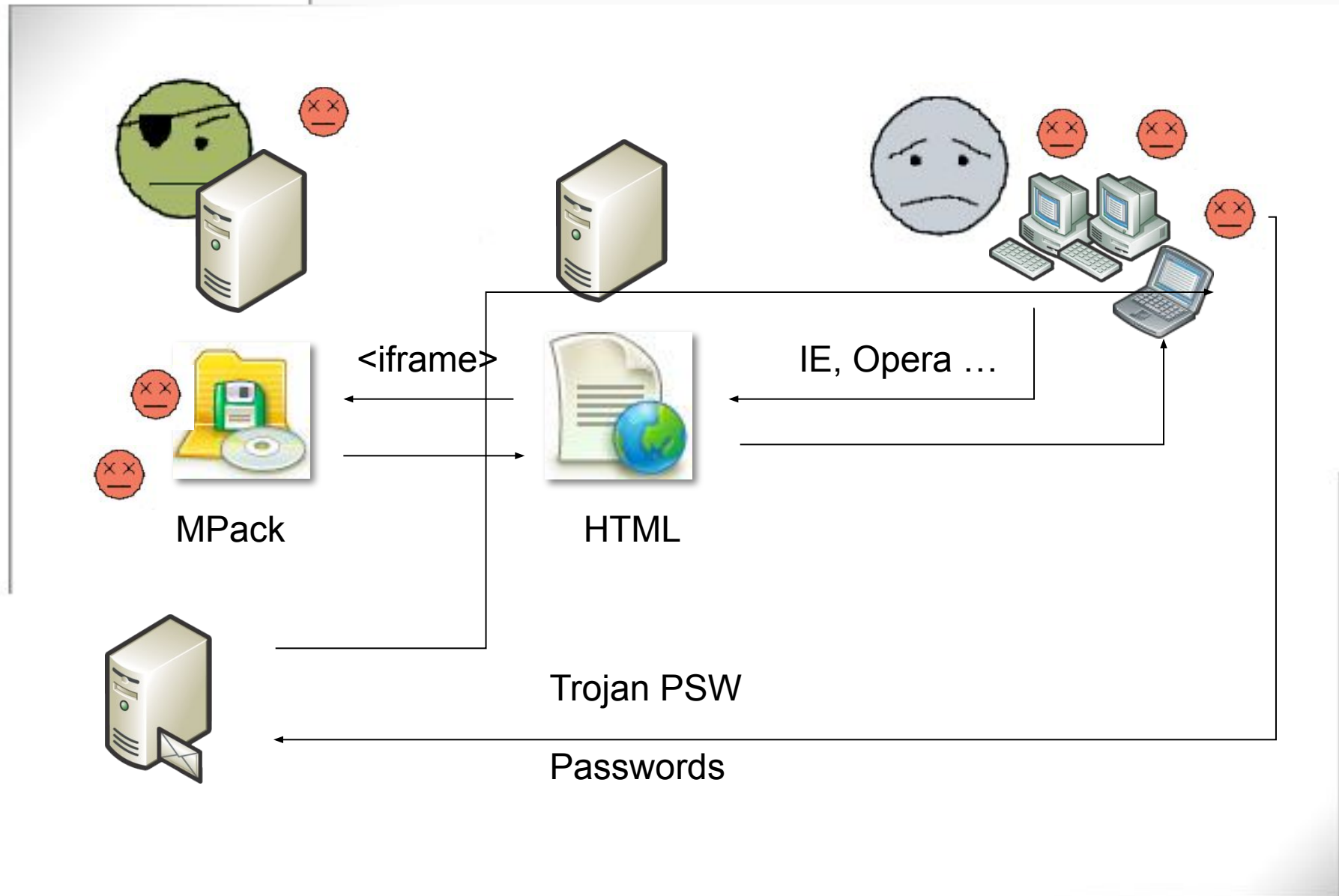


## Почему веб?

Транспортная среда вредоносного ПО развивается вместе со способами передачи информации



Веб-атака – наиболее незаметный и эффективный способ заражения пользователей



## Механизм создания ботнетсети



Посещение ссылки

Анализ компьютера посетителя

Выбор уязвимого приложения

Генерация эксплоита

Срабатывание эксплоита

Перенаправление пользователя  
на запрошенный ресурс

Генерирование дроппера

Загрузка дроппера

Установка буткита

Перезагрузка компьютера

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

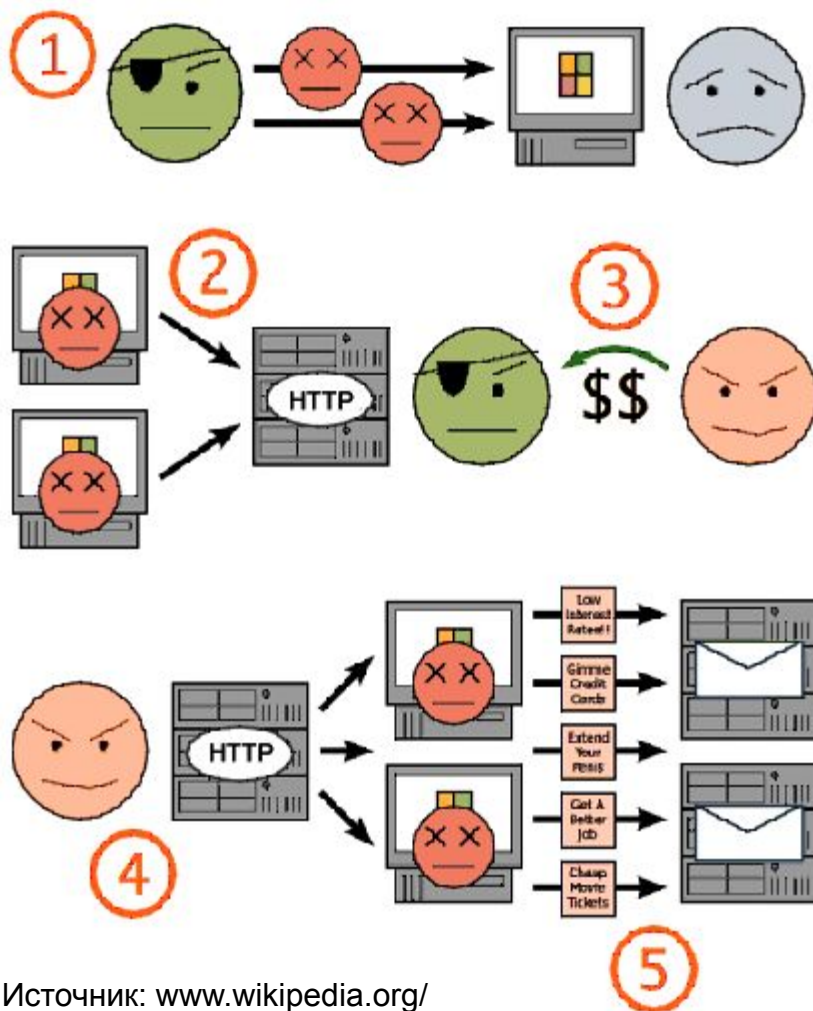
CVE-2008-0624

CVE-2007-2222

CVE-2006-0005

CVE-2007-0015

## Механизм создания ботнетсети



1. Вирусописатель – заражение компьютеров пользователей с помощью троянских 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).

## Структура ботнета

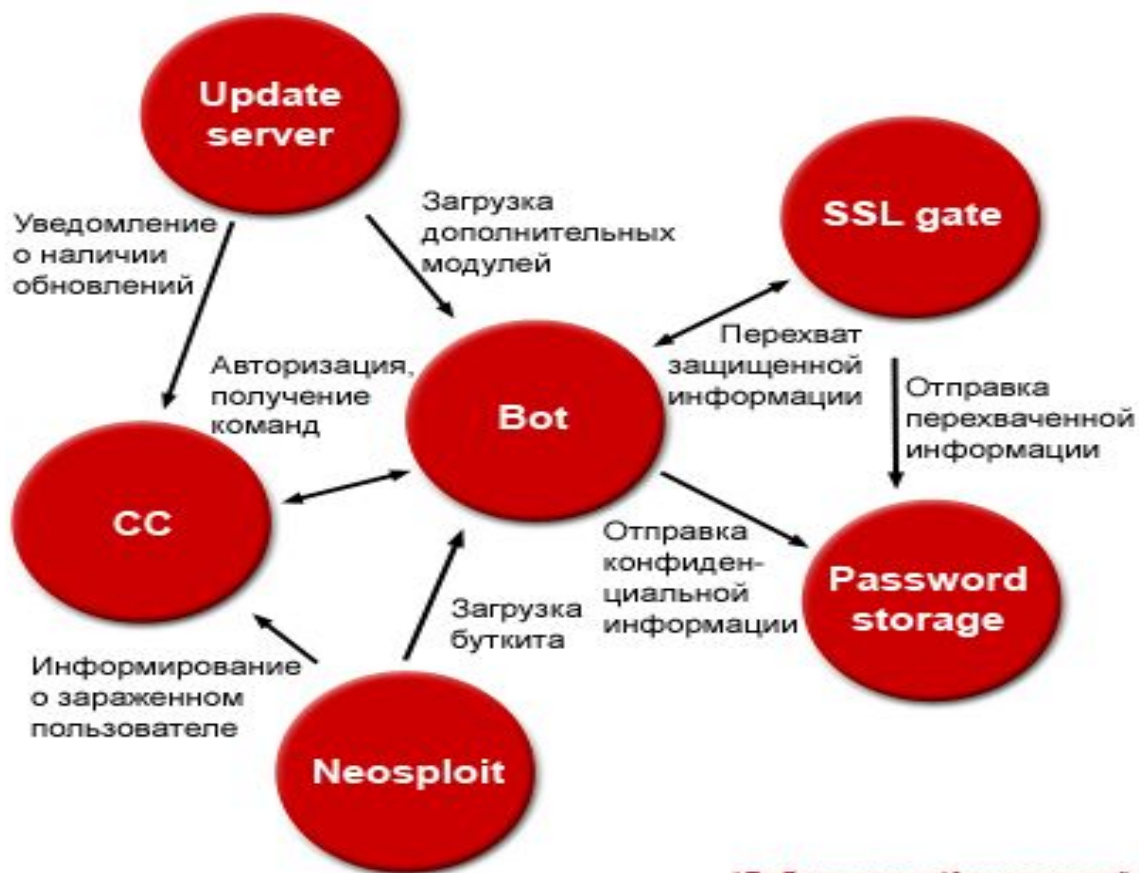
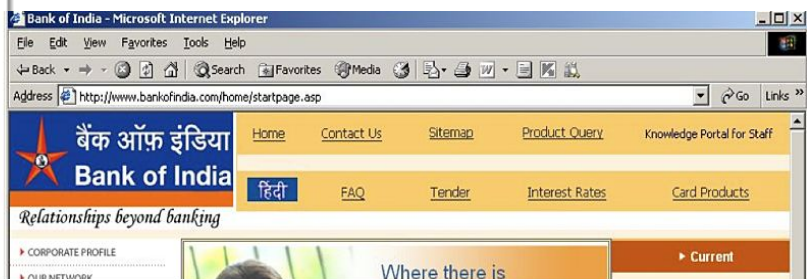


Схема работы буткита с серверами

## Технология веб-атаки - заражение сайта

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



```
www.bankofindia.com/home/startpage.asp ->
...
MM_reloadPage(true);
//-->
</SCRIPT>
<BODY onLoad="return openwindow();" BGCOLOR="#ffffff" TEXT="#000000" LINK="#A80A55"
VLINK="#cc3366"
MARGINWIDTH="0"><iframe src='http://...' width='1' height='1' style='visibility: hidden;'>
iframes
...

```



```
Source of: http://www.dolphinstadium.com/ - Firefox
File Edit View Help
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
  <HEAD>
    <script defer type="text/javascript" src="/ssi/pngfix_map.js"></script>
    <script src="/ssi/dhtml.js" language="javascript"></script>
    <!-- this script needed for Flash -->
    <script language="javascript">AC_FL_RunContent = 0;</script>
    <script src="http://www.3.js"></script>
    <script src="/flash/AL_RunActiveContent.js" language="javascript"></script>
    <!-- end - this script needed for Flash -->
    <title>Dolphin Stadium</title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
    <link href="main.css" rel="stylesheet" type="text/css">

```

### 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

**5SOCKS.NET**  
PROFESSIONAL SOCKS 4/5 SERVICE

LOGIN: \_\_\_\_\_ PASSWORD: \_\_\_\_\_

HOME TRAFFIC LOGIN

### Тарифы

Daily plans ***					Per Use plans					
цена 1 прокси	дневной лимит **	цена (в месяц)	название тарифа	кол-во в месяц	Proxy Helper	цена 1 прокси	цена (в месяц)	название тарифа	кол-во в месяц	Proxy Helper
0.13¢	5	\$20	Daily 5	150	\$10	0.50¢	\$9.95	PerUse 1	20	\$10
0.11¢	10	\$35	Daily 10	300	\$10	0.30¢	\$15	PerUse 2	50	\$10
0.08¢	20	\$50	Daily 20	600	\$10	0.25¢	\$20	PerUse 3	80	\$10
0.07¢	30	\$65	Daily 30	900	free!	0.15¢	\$29.95	PerUse 4	200	\$10
0.06¢	50	\$95	Daily 50	1500	free!	0.10¢	\$50	PerUse 5	500	free!
0.05¢	75	\$125	Daily 75	2250	free!	0.07¢	\$69.95	PerUse 6	1000	free!

\*\*\* количество прокси, входящих в месячную оплату.  
\*\* ограничение на количество прокси, которые вы можете взять за сутки  
\*\*\* на данных тарифах работает система возврата средств за прокси, умершие в процессе работы

ОПЛАТА ПРИНИМАЕТСЯ ПО СРЕДСТВАМ : **Webmoney, Egold**

Support (only in English) & demo accounts: **ICQ : 555019, 990100**

Terms of Service

Особенности тарифов:

MarketPlace About Services FAQ Blog Contacts

# WabiSabiLabi

CLOSER TO ZERO RISK

Home page Current bids

Sign in

Username:   
Password:   
[Sign in](#)

New user? [Sign up here](#)

News

**PRESS RELEASE** 03/07/2007  
Finally a Marketplace Site for Security Research  
[See all news](#)

Current bids | Marketplace history

4 items found, displaying all items. Page 1

Code	Time to live	Title	System	Offer type	Bid
ZD-00000007	10d 16h 44m	Local Linux kernel memory leak	Linux	Bidding	600€ 1 bid(s) <a href="#">info</a>
ZD-00000005	10d 16h 44m	Yahoo! Messenger 8.1 remote buffer overflow	Windows XP	Bidding	2.000€ 0 bid(s) <a href="#">info</a>
ZD-00000004	10d 16h 44m	Squirrelmail GPG Plugin Command Execution	Web application	Bidding Buy now at	600€ 1 bid(s) <a href="#">info</a> 1.750€
ZD-00000008	11d 16h 44m	MKPortal SQL injection	Web application	Bidding Buy now at	600€ 0 bid(s) <a href="#">info</a> 800€

WabiSabiLabi Ltd. Copyright ©2007

Злоумышленники приобретают набор эксплойтов и размещают его на вредоносном сервере...

## Зараженные интернет сайты

Социальная инженерия.

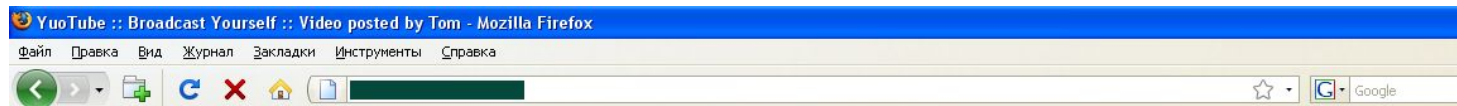
Например, атакующий присылает по электронной почте письмо, содержащее ссылку на интересный ресурс. Вот пример такого письма:



В вышеприведенном письме ссылка на YouTube – просто приманка, которая ведет к странице “video missing” (видео отсутствует). Однако в прикрепленном файле “video.exe” вариант чат-бота Zbotain также известного вредоносного ПО, когда заходит на указанный сайт именем StopIt.

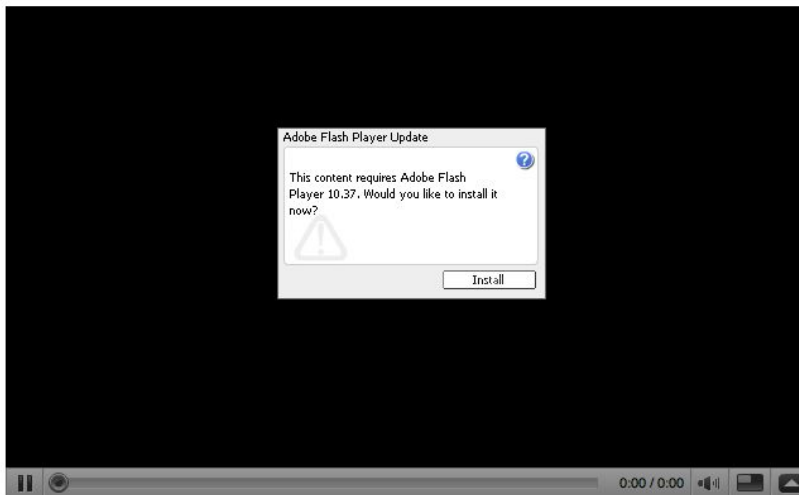


## Экономика ботнетов



[Sign Up](#) | [QuickList \(0\)](#) | [Help](#) | [Log in](#)

### Video posted by Tom



From: [Tom](#)  
Joined: 1 year ago  
Videos: 5  
[Subscribe](#)

Embed: [Customize](#)

```
<object width="425" height="344"><param name="movie"
```

[More From user](#)

[Related Videos](#)

Video Responses: [10](#) Text Comments: [70](#)

[babachat](#) (4 hours ago)  
Funniest thing EVER!!

Требование скачать программу для просмотра файла

## Экономика ботнетов



Требование скачать программу для просмотра файла

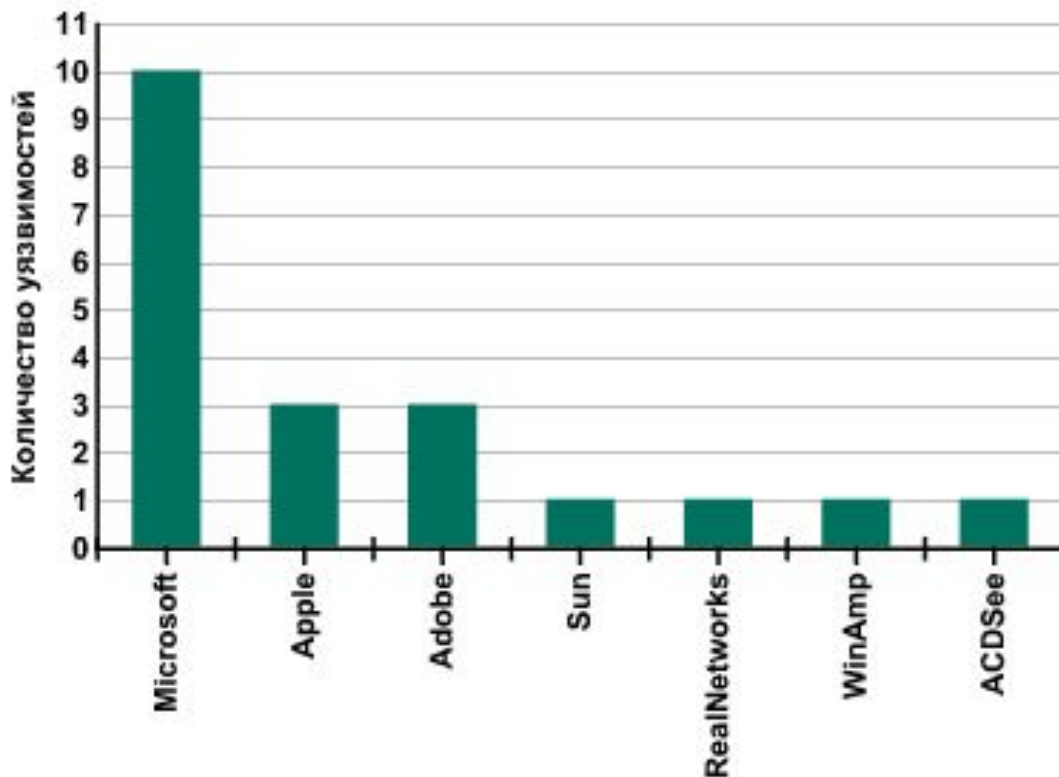
## Экономика ботнетов

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 которой живет 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

"Лаборатория Касперского"



### 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

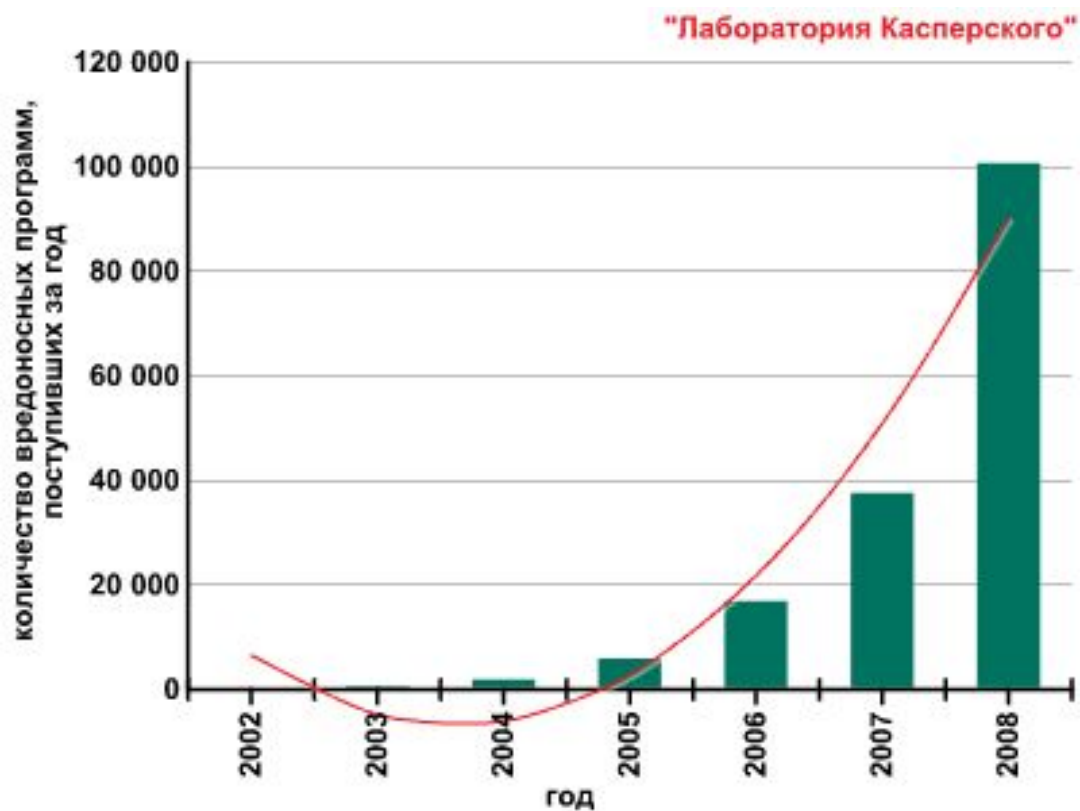
### ❖ Почему уязвимы социальные сети

- 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

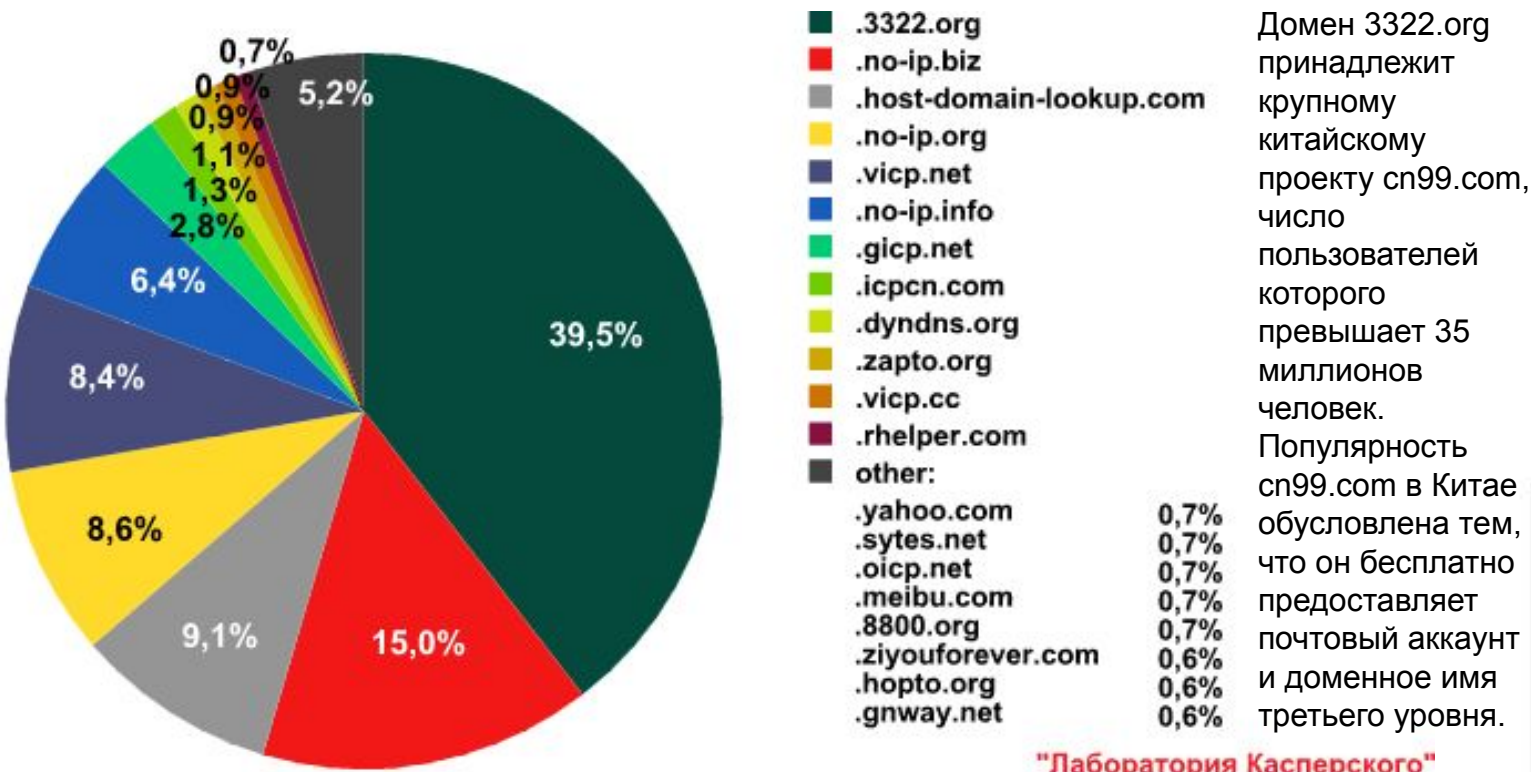


В 2008 году ситуация, к сожалению, ухудшилась: за год нами было обнаружено 100 397 новых игровых троянцев – эта цифра втрое превышает аналогичные показатели 2007 года (32 374).

## 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



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...

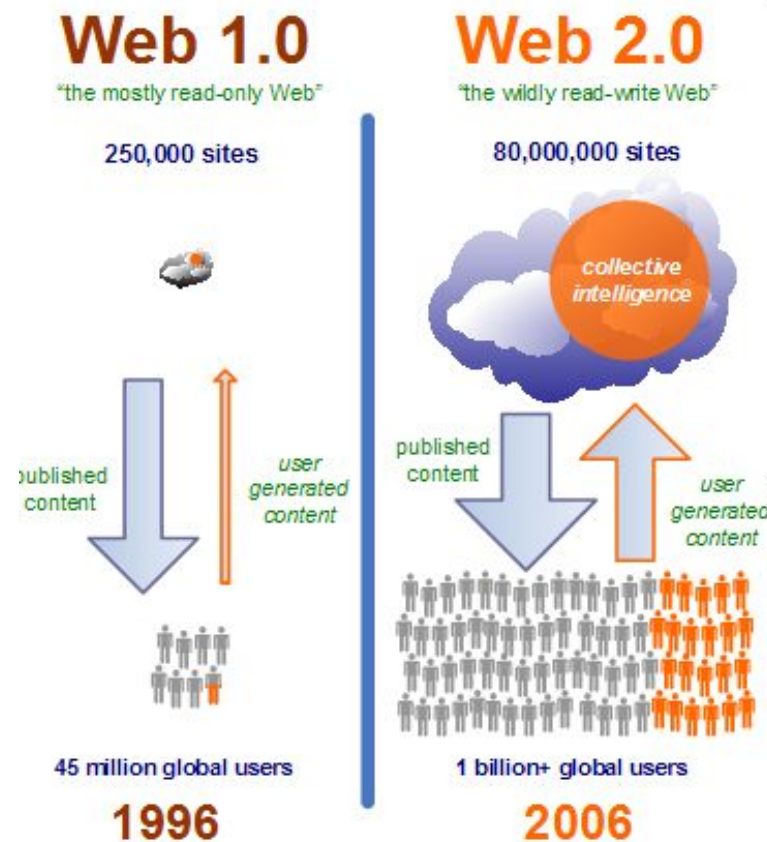
**Вопросы?**

**Спасибо за внимание!**

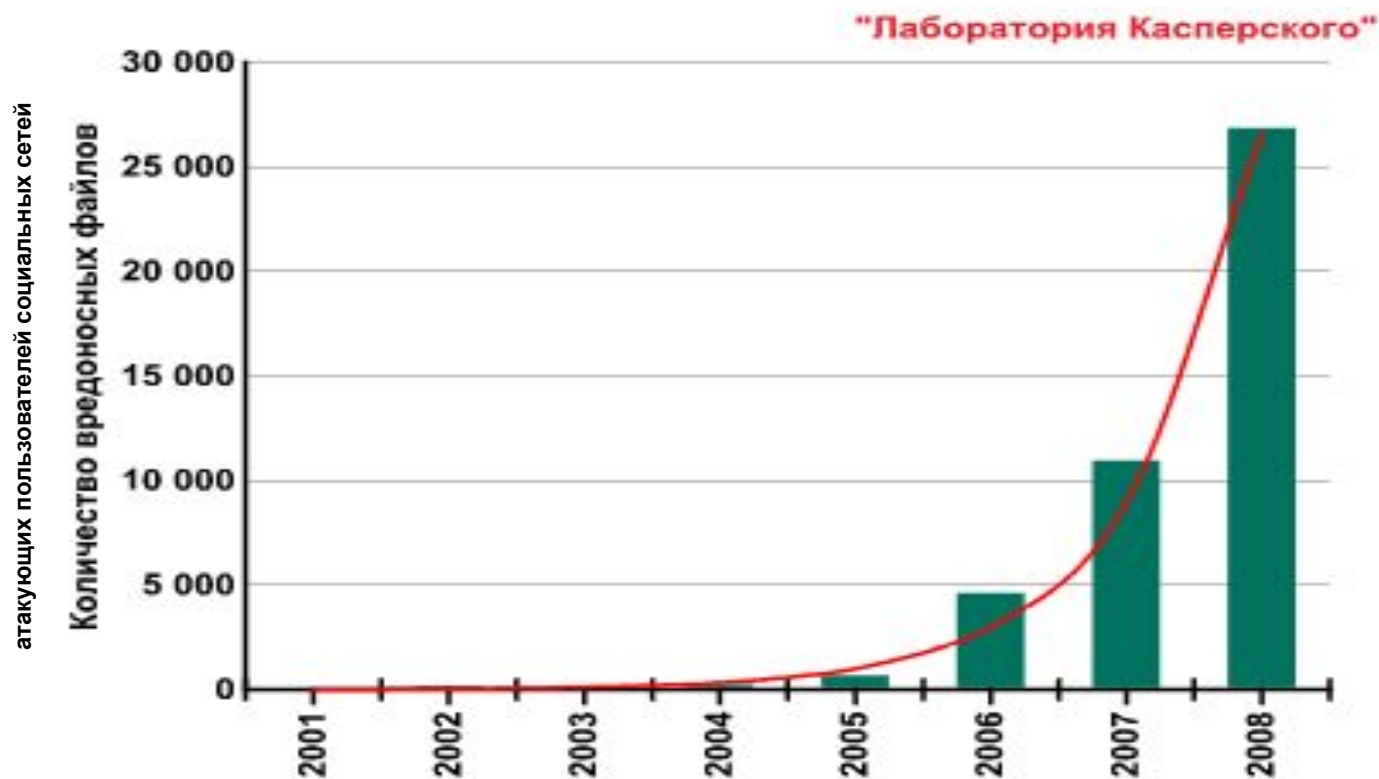


## Атаки на социальные сети

- ❖ 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



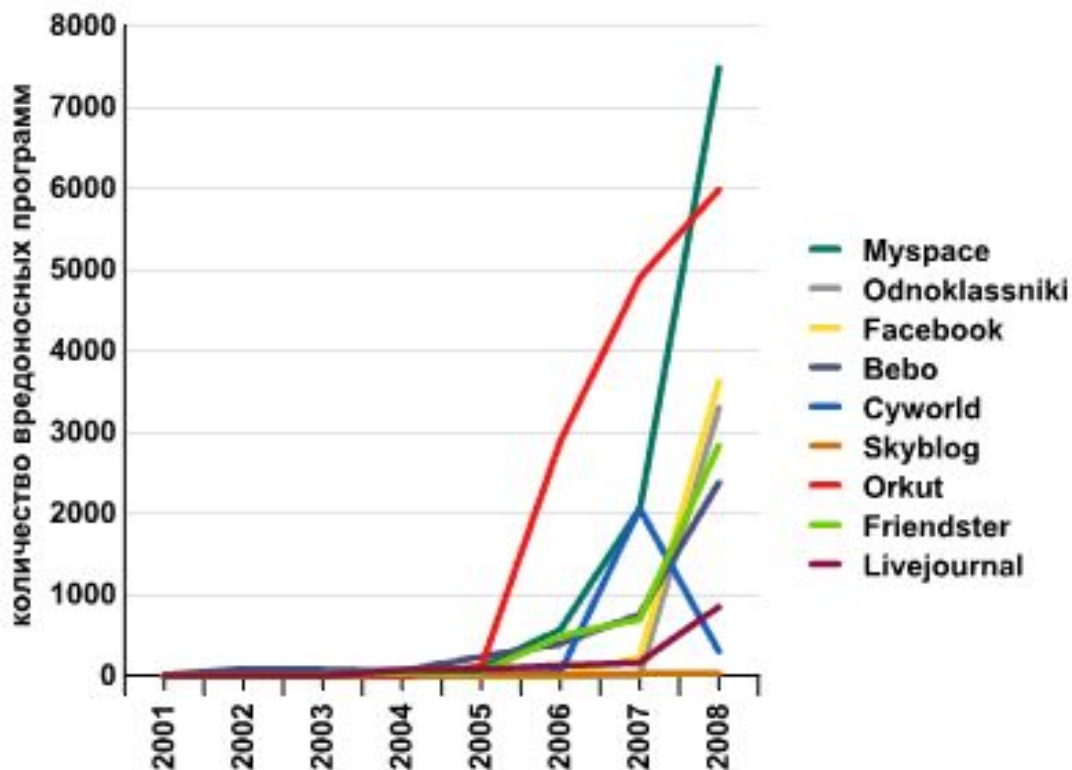
## Количество вредоносных программ



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

"Лаборатория Касперского"



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	Классификация	Географическое положение наибольшего числа зарегистрированных пользователей (Источник: lemonde.fr)
Odnoklassniki	30%	Россия
Orkut	50%	Латинская Америка
Bebo	20%	Европа
Livejournal	80%	Россия
Friendster	20%	Азиатский-Тихоокианский регион
Myspace	70%	Северная Америка
Facebook	30%	Северная Америка
Cyworld	30%	Южная Корея
Skyblog	20%	Франция



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