

A circular inset on the left side of the slide shows a microscopic view of several cells, likely representing a virus or a biological structure, with a green and white color scheme.

День антивирусной безопасности 2010.04.28

Станислав Шевченко,

зам. директора по исследованиям и разработке,
директор проекта «Антивирусная школа – новый источник IT-знаний»
Kaspersky Lab

Пи
шит
е и
пер
еда
вай
те
зап
иск
и с
воп



Антивирусная Школа



Новый источник IT-знаний

Программы

Топ 10 операционных систем

1.	Windows	343 264	95,31 %
2.	Linux	7 996	2,22 %
3.	(not set)	4 109	1,14 %
4.	Macintosh	3 633	1,01 %
5.	FreeBSD	647	0,18 %
6.	iPhone	247	0,07 %
7.	SymbianOS	118	0,03 %
8.	UNIX	31	0,01 %
9.	Samsung	24	0,01 %
10.	Playstation 3	20	0,01 %

Трудно ли создать ? **нет**

Трудно ли **нет**

использовать ?

Можно ли заработать **да**

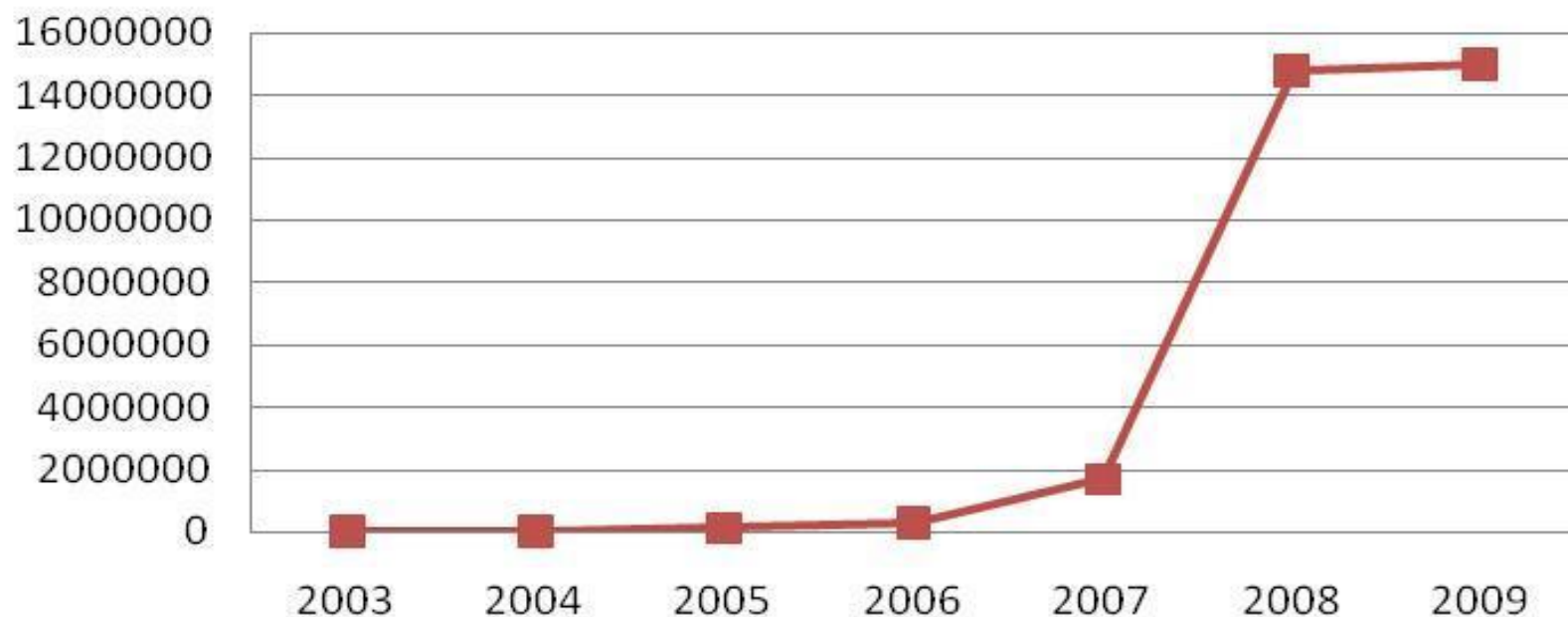
Опасно ли **да**

пользоваться ?

Трудно ли **да**

противостоят ?
индустриализация киберкриминала !

Число новых вредоносных программ 2003 - 2009



Позиция	Изменение позиции	Вредоносная программа	Количество зараженных компьютеров
1	0	Net-Worm.Win32.Kido.ir	265622
2	0	Net-Worm.Win32.Kido.iq	211101
3	0	Net-Worm.Win32.Kido.ih	145364
4	0	Virus.Win32.Sality.aa	143166
5	0	Worm.Win32.FlyStudio.cu	101743
6	New	not-a-virus:AdWare.Win32.GamezTar.a	63898
7	-1	not-a-virus:AdWare.Win32.Boran.z	61156
8	-1	Trojan-Downloader.Win32.VB.eqf	61022
9	-1	Trojan-Downloader.WMA.GetCodec.s	56364
10	New	Trojan.Win32.Swizzor.c	54811

- WEB 2.0 – **шагает по планете.**
- Спам, спам и еще раз спам
- Ложные спасатели – **что это?**
- Уязвимости программ – **точки проникновения**
- Зомби сети – **угрожающие рекорды**
- SMS-платежи – **новые возможности старого мошенничества**
- Статистика – **реалии в цифрах**

Антивирусная Школа



Новый источник IT-знаний

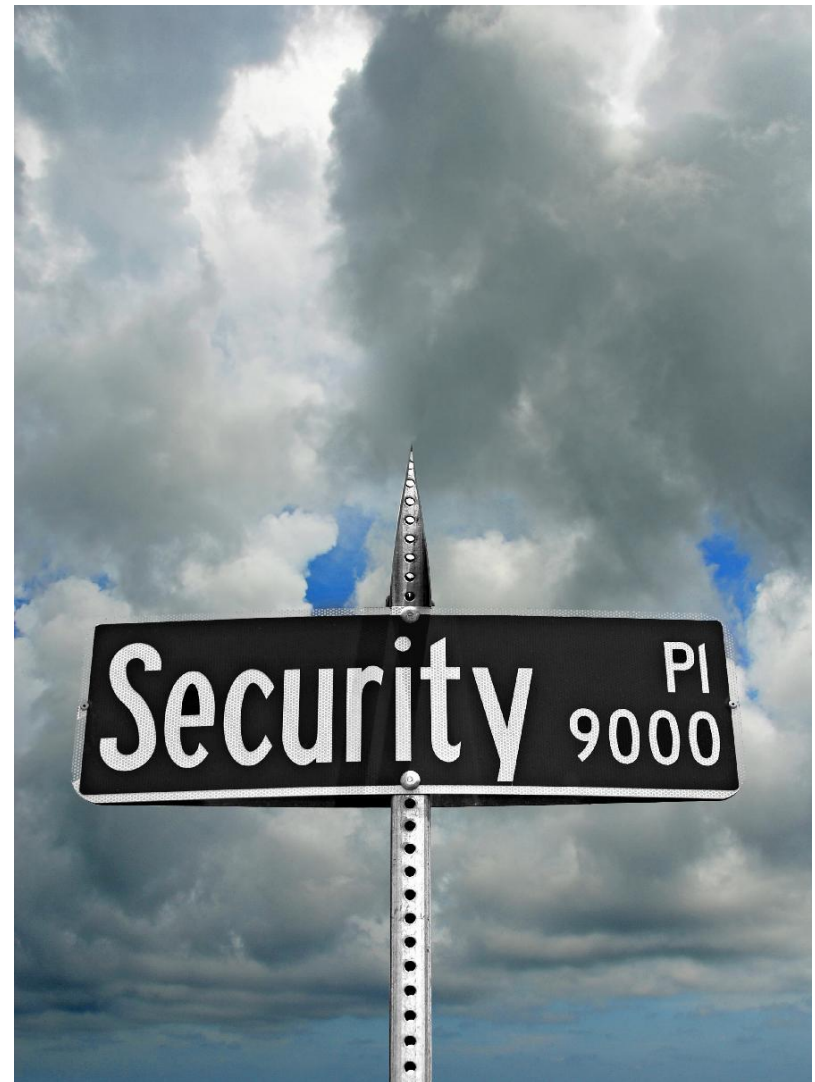
Web 2.0

Сети По данным «Лаборатории Касперского», социальные сети стали основной мишенью атак в 2008 году. Что прогнозирует «Лаборатория Касперского», в 2009 году, будет наблюдаться переход от концептуальных угроз и пробных атак в социальных сетях к массовым атакам.

Проанализировав атаки, эксперты по компьютерной безопасности заявили, что социальные сети содержат персональную информацию, которая может быть использована в том числе и злоумышленниками. Обманчивая атмосфера доверия ведет к предоставлению конфиденциальной информации «по дружбе». После этого хакеры взламывали страницы в социальных сетях этих друзей, в надежде повысить вероятность того, что люди, являющиеся финальной целью хакеров, скорее нажмут на ссылки от "друзей"

Многие пользователи наиболее распространенной в России социальной сети «Одноклассники.ру» уже получали письма со ссылкой на вирус. Пример такого послания — просьба проголосовать за фотографию какой-либо претендентки на титул «Мисс Рунет». Пройдя по модифицированному адресу, пользователь видит фото претендентки и отзывы людей, якобы уже проголосовавших за нее. Далее при нажатии на ссылку «Отдать свой голос» посетителю сайта предлагается скачать видеоролик, в то время как на самом деле на компьютер скачивается вирусная программа.

in- the-cloud security -
основной
технологический тренд
развития AV-индустрии



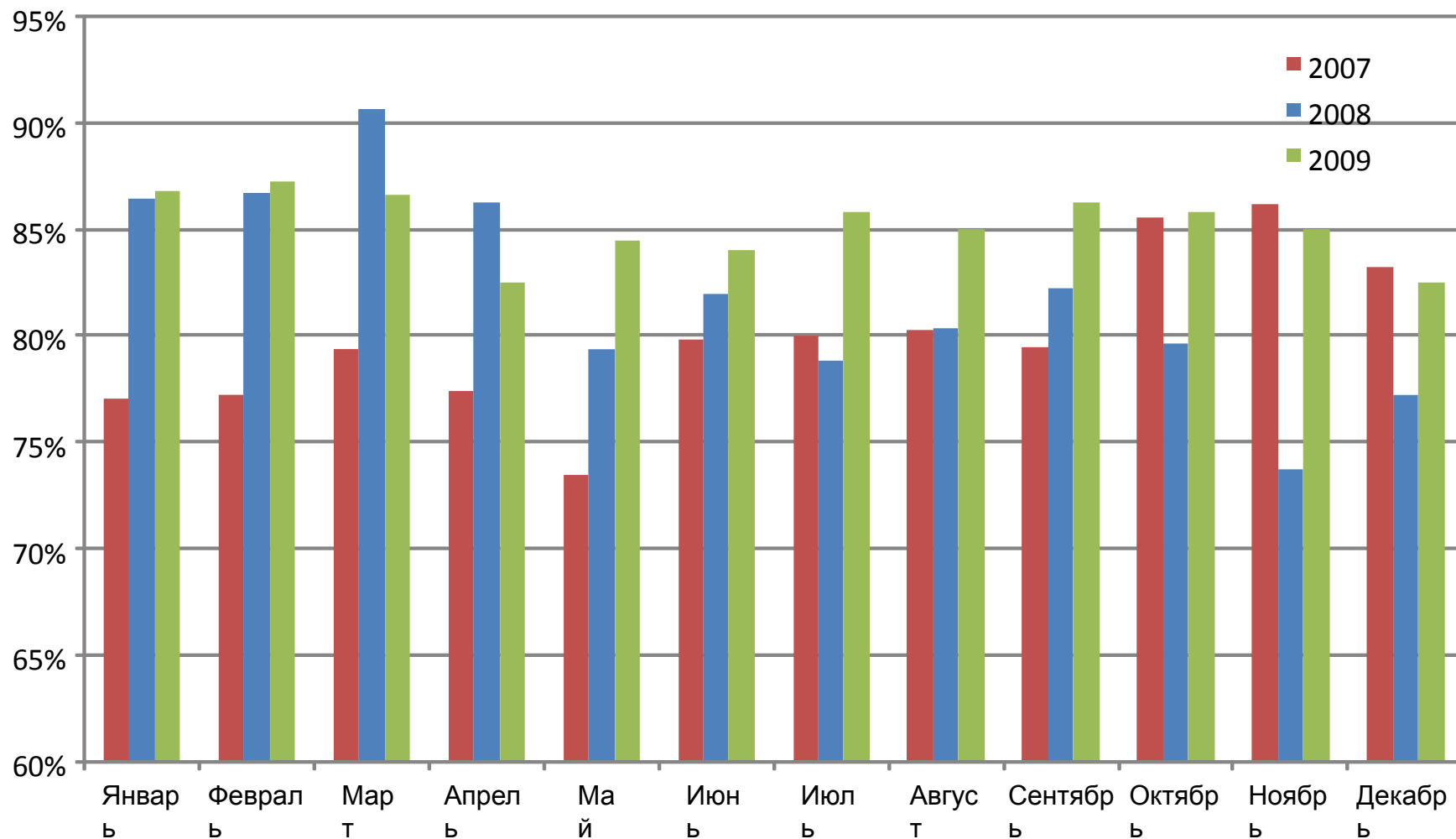
Антивирусная Школа



Новый источник IT-знаний

СПАМ

Доля спама в потоке



Доля спама в почтовом трафике рунета

Январь 2010

85.1

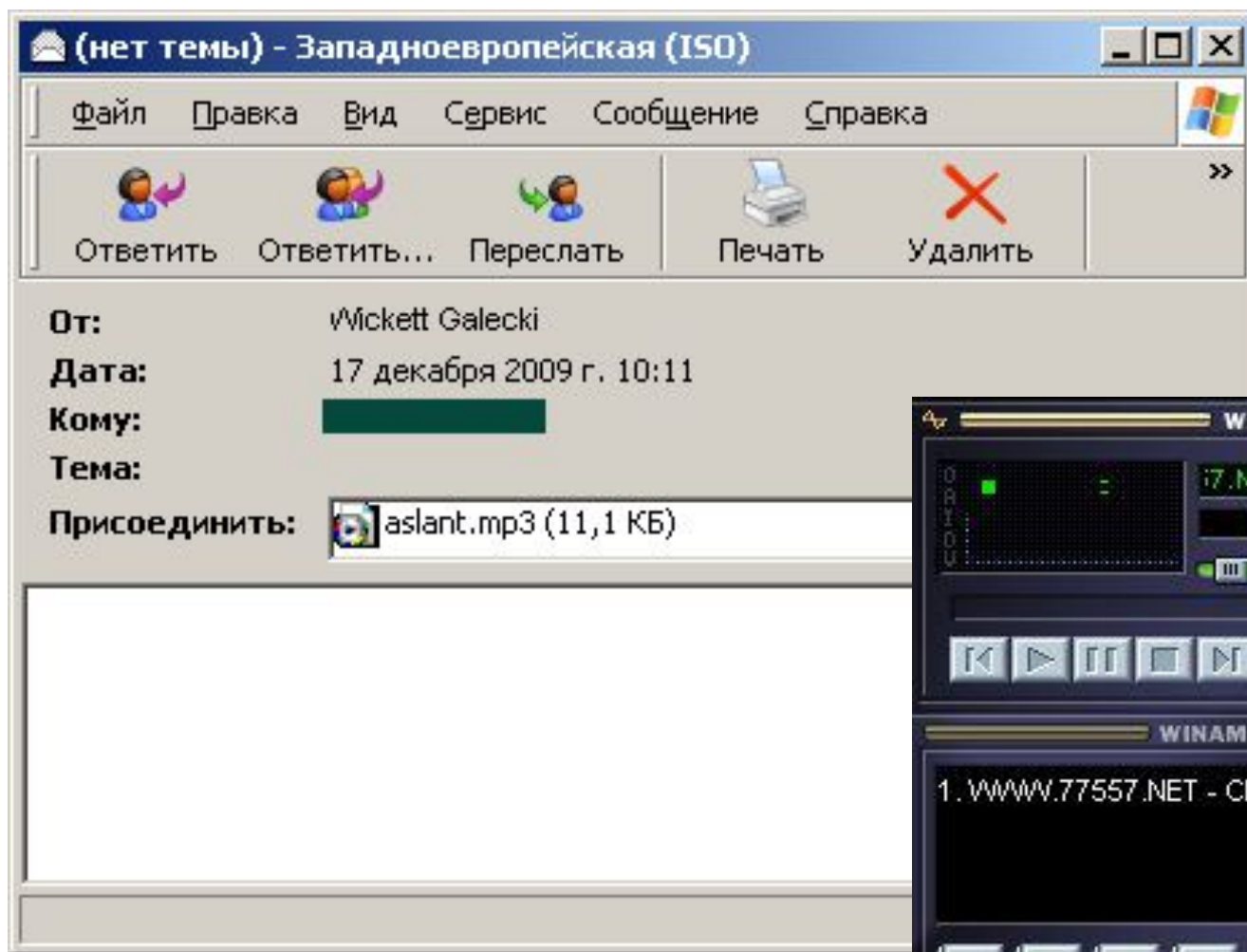
%

№	Тематика	Описание	Доля тематики	Изменения за неделю
1	Образование	Реклама семинаров, тренингов, курсов.	24,0%	-3,4%
2	Медикаменты; товары/услуги для здоровья	Предложения приобрести лекарственные препараты, БАДы и т.п. в online. Предложения медицинских и оздоровительных услуг, а также сопутствующих товаров.	13,8%	-2,3%
3	Отдых и путешествия	Предложения туристических поездок, а также организации и проведения различных развлекательных мероприятий.	13,4%	+6,3%
4	Реплики элитных товаров	Копии часов, аксессуаров, обуви и других товаров известных марок.	9,0%	-3,3%
5	Компьютерное мошенничество	Фишинг, "нигерийские" письма, поддельные извещения о выигрыше в лотерею и пр. попытки мошенничества.	8,6%	+0,9%

Трюки и «фишки»

The image shows a screenshot of a YouTube video player. At the top left is the YouTube logo with the tagline "Broadcast Yourself™". To its right is a search bar and a "Поиск" button. Below the search bar are navigation links: "На главную", "Видео", and "Каналы". The video title "Sequence 01 2" is displayed above the video frame. The video frame itself is black and contains white text: "ПОБЕРЕГИ СЕБЯ" in large bold letters, followed by "+7 495" and a redacted area (a dark green rectangle). Below this, the text "Email рассылки от профессионалов" is written in a smaller font, tilted upwards. At the bottom of the video frame is a red progress bar and a play/pause button. The video progress indicator shows "0:29 / 0:33".

Мр3 Опять?!



HUGE 80% DISCOUNT

Canadian Pharm



ЛЮБЫЕ,

даже самые грязные сексуальные фантазии,

оживают **ЗДЕСЬ**



.RU

Волны

Advertisement for Viagra and Cialis with prices and a warning to not click on a suspicious website.

\$1.15	Viagra	\$2.35
\$1.57	Viagra Prof.	\$4.97
\$2.82	Viagra Sup Act	\$2.78
\$1.64	Viagra Soft	\$1.35
\$1.99	Cialis	\$1.45
\$4.17	Cialis Prof.	\$0.33
\$3.65	Cialis Sup Act.	\$0.50
\$1.44	Cialis Soft	\$1.51

DO NOT CLICK. JUST ENTER IN YOUR BROWSER

Windows Internet Explorer
http://www. [redacted] .org

Вам письмо

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next

From: [redacted]
Date: 23 ноября 2009 г. 12:09
To: [redacted]
Subject: Вам письмо

А ты далеко от меня?

РЕАЛИЗУЕМ ТАМОЖЕННЫЙ КОНФИСКАТ

Цены на фирменную электронику ниже на 30-30% чем в магазине. Работаем оптом и в розницу. Доставка по всей России и странам СНГ.

Товар дня
Apple iPhone 8Gb 3G - 7000 руб;
Nokia 5800 XpressMusic - 5000 руб;
Ноутбук Samsung R25Plus - 7000 руб;

Подробности на сайте:
[redacted]

*** GREAT NEW YEAR OFFER FROM PAYPAL.COM ***

*** GREAT NEW YEAR OFFER FROM PAYPAL.COM ***

Registration step 1 of 3

Credit Card Number:	<input type="text"/>
PIN: Please provide us with your correct PIN number so that we are able to cross check your credit card with your bank account	<input type="text"/>
CVV Code: 3 digit number that appears to the right of your card number	<input type="text"/>
Expire date:	<input type="text" value="01"/> <input type="text" value="2003"/>

I confirm that the above information is correct.

Антивирусная Школа



Новый источник IT-знаний

Ложные спасатели

- Первая половина 2008 года – около 3 000 шт
- Первая половина 2009 – более 20 000 шт
- Fraud Tool – риск взлома попадает при помощи программ Ноах – Которые находят проблемную зону и предлагают поставить защиту.
- Распространение при помощи Рекламы
- Главное напугать, а затем вынудить заплатить

Ложные антивирусы

Spyware Protect 2009
Protecting every second...

Performing scan Stop scan

Current state: Scanning computer

C:\WINDOWS\inf\inet559b.inf Total: 1811 Threats: 22

Malware database status: Up to date Signature version: 211343 (normal)

Activate Spyware Protect 2009 now to be sure that maximal protection is applied.

Threat name	Severity	Description (click on item for more information)
LdPlock V	Critical	A variant of the Key Logger that captures passwords as if
Advanced Stealth Email	Critical	Advanced Stealth Email Redirector (Advanced SEER) is a pr
VMalux AWS	High	Trojan: Any program with a hidden intent. Trojans are one
CNNC Update V	Very high	A program that downloads and may execute or install soft
Bases DMD	Critical	A variant of the Key Logger that captures passwords as if

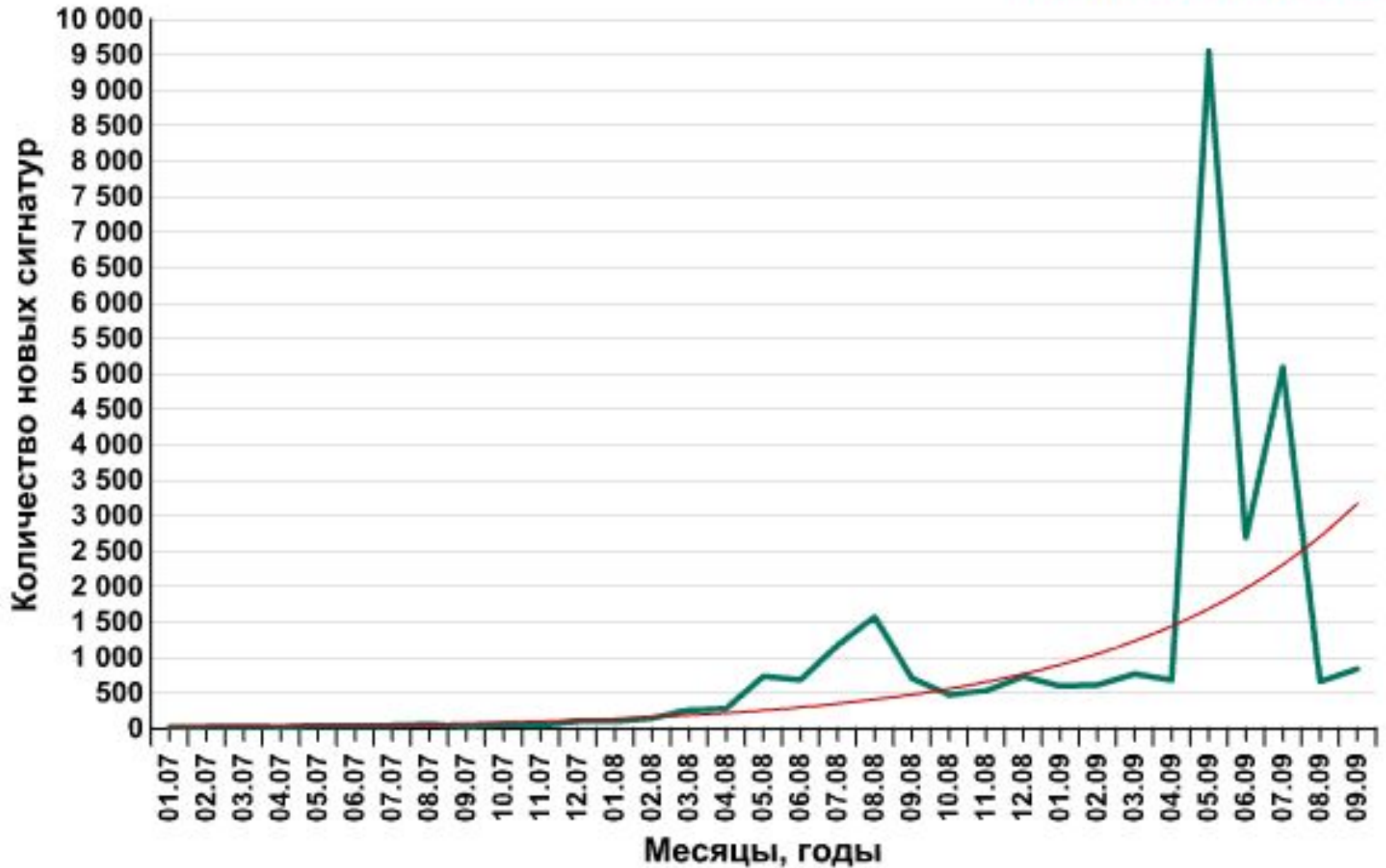
Scan progress 41% completed

Your PC is currently unprotected and may be exposed to spyware, adware, trojans and viruses.
[Get full real-time protection](#)

График добавления сигнатур

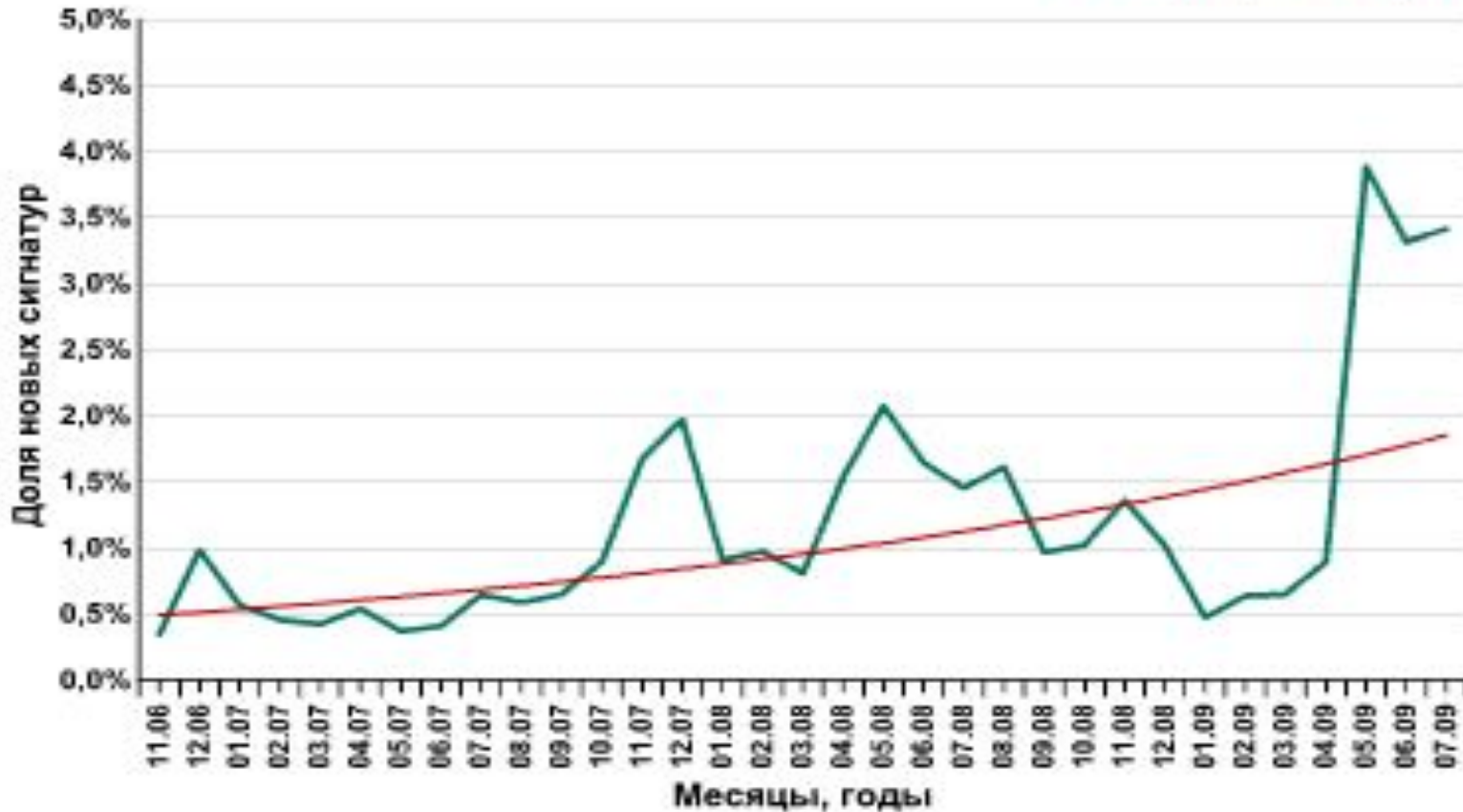


лаборатория Кастерского



Доля новых сигнатур

"Лаборатория Касперского"



Доля новых сигнатур, детектирующих Noach и FraudTool, в общем количестве сигнатур месяцы, 2007-2009 гг.

Антивирусная Школа



Новый источник IT-знаний

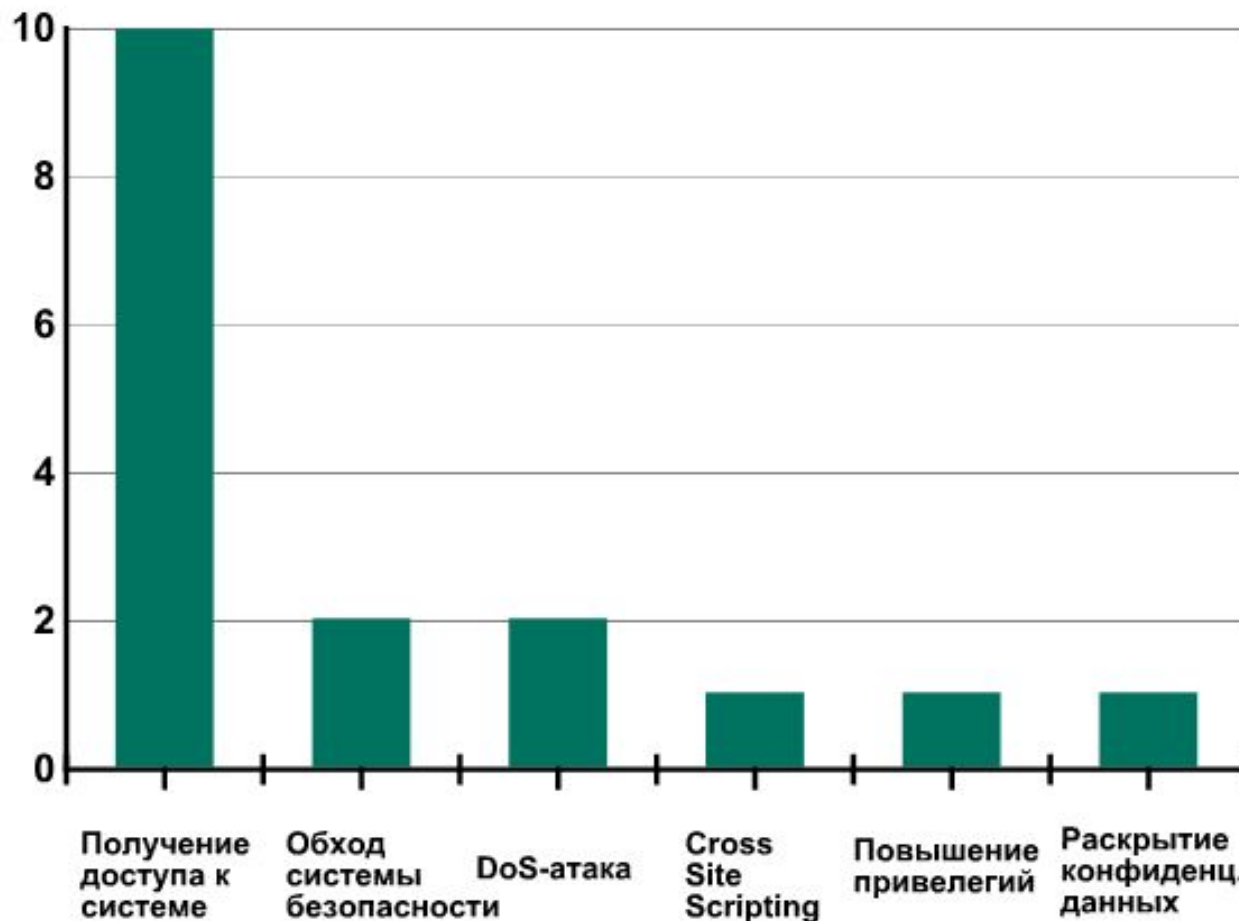
Уязвимости

- Уязвимость – в компьютерной терминологии, это недостаток в системе который может быть использован для изменения функционала системы. Возникает из-за ошибок программистов или ошибок архитектуры.

Википедия

Типы воздействия

"Лаборатория Касперского"



- Суть технологии: при посещении пользователем легитимного взломанного сайта незаметно загрузить на его компьютер вредоносную программу. Такие атаки особенно опасны, ведь на взломанные легитимные сайты заходят тысячи ничего не подозревающих пользователей, и каждый из них является потенциальной жертвой.

Антивирусная Школа



Новый источник IT-знаний

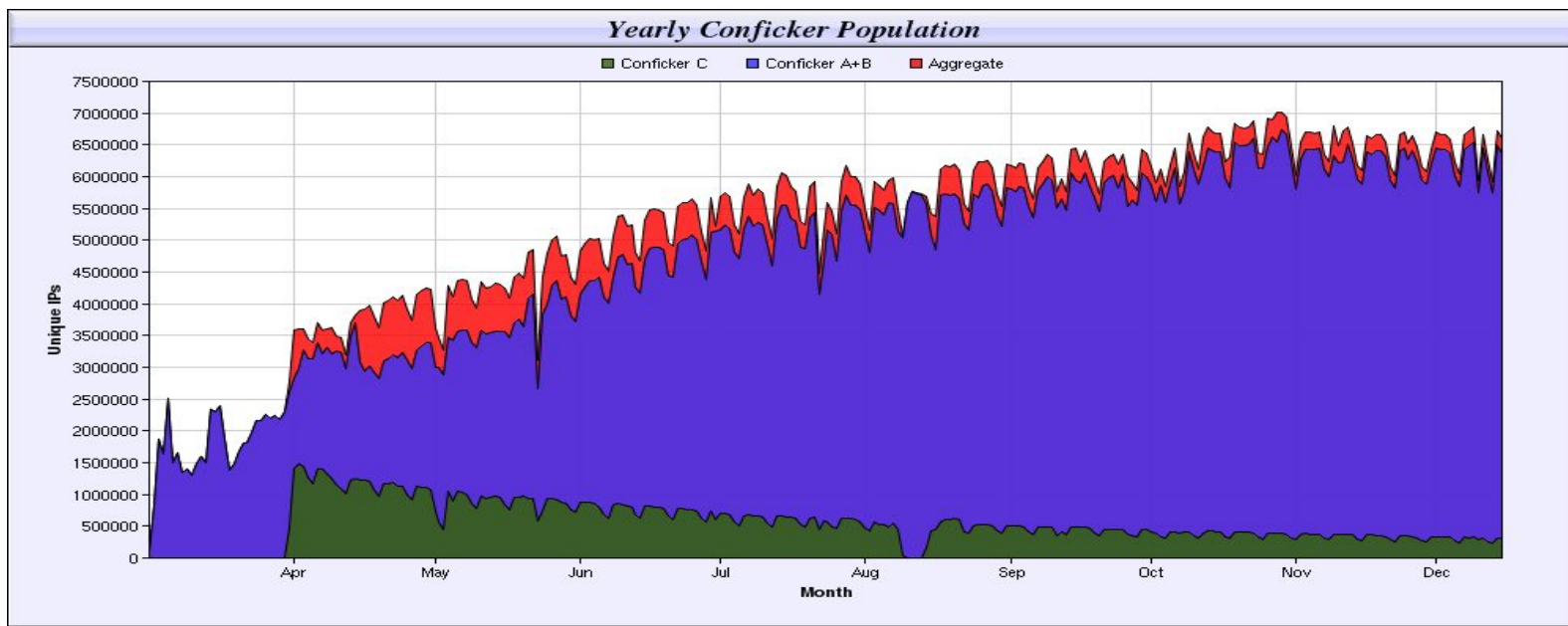
Зомби сети

- Ботами называют вредоносные программы, занимающиеся объединением пораженных компьютеров в ботнеты.

- Самая большая сеть известная на сегодня – сеть созданная Net-Worm.win32.kido
- В каждом письме используется свой уникальный домен (для усложнения детектирования СПАМ рассылки) использованно -40542 домена 3 уровня и 33 домена второго уровня
- За 12 часов работы один только бот отправил 42298 спам письма с

Эпидемия Kido (Conficker) продолжалась на протяжении всего 2009 года. В ноябре количество зараженных систем превысило 7 млн.

Для борьбы с Kido была создана специальная группа Conficker Working Group.



Источник: www.shadowserver.org

- 1 бот iksmas – в сутки отправляет 80000 писем
- Допустим что заражено всего 500000 машин
- Получается что за сутки зомби сеть, только этого бота рассылает 400 000 000 000 (400 миллиардов) писем со спамом

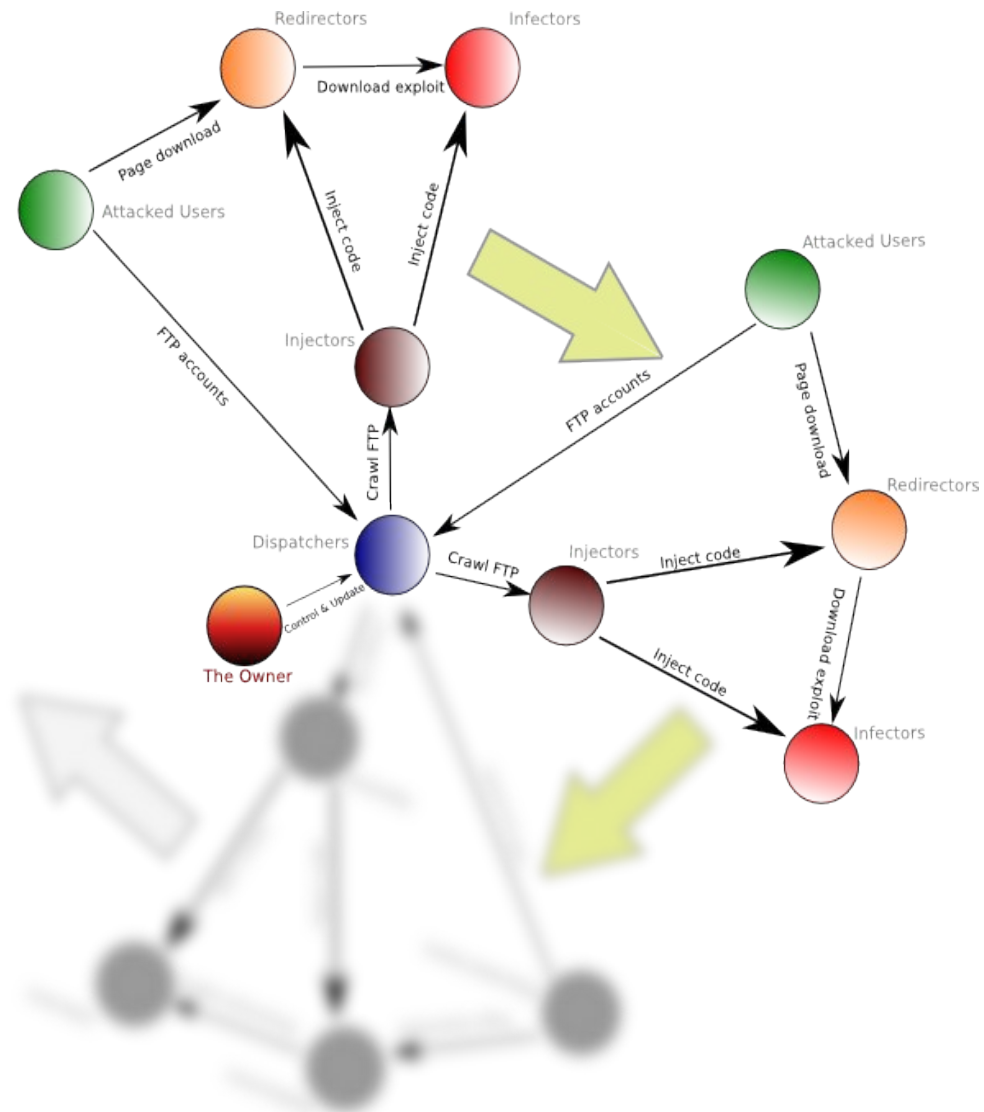
- Помимо спам бота ikstmas кидо на компьютер жертвы устанавливает и уже известный нам поддельный антивирус
- Настойчивость так велика, что скорее всего пользователь установит себе этот ложный антивирус



- Пользователь теряет не только 50 долларов, но и данные кредитных карт и платежные реквизиты
- Кроме аллертов этот ложный антивирус устанавливает еще один компонент а именно троян-загрузчик, trojan-downloader.win32.fraudLoad.ecl – который обеспечивает загрузку новых версий ложного антивируса SpywareProtect2009

Глобальные эпидемии: Gumblar

Система работает по замкнутому циклу





Управление жертвой



Киберпреступность - «сервис»

Attacked hosts (total - uniq)		Traffic (total - uniq)	
IE XP ALL	114721 - 96104	Total traff	159073 - 129089
QuickTime	2175 - 2048	Exploited	44804 - 35574
Win2000	7033 - 6260	Loads count	17408 - 15968
Firefox	12885 - 12514	Loader's response	38.85% - 44.89%
Opera7	1271 - 1264	Efficiency 10.94% - 12.37%	

Browser stats (total)		Modules state	
MSIE	4 0%	Statistic type	MySQL-based
Opera	1 0%	User blocking	ON
		Country blocking	OFF

Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%

- Свое название этот представитель киберфауны получил по причине того, что его первые версии перенаправляли пользователей на домен gumblar.cn
- Этот троянец представляет собой вредоносный зашифрованный сценарий JavaScript, вставленный в тысячи страниц различных взломанных сайтов и перенаправляющий посетителей этих сайтов на вредоносную веб-страницу.
- Компьютеры пользователей, попавших на зараженный сайт, подвергаются атаке с помощью эксплойтов, использующих уязвимости в Adobe Acrobat Reader и Adobe Flash Player.

- Если один из эксплойтов срабатывает, то в систему пользователя незаметно загружается троянская программа. Этот троянец изменяет результаты поиска через Google таким образом, что полученные ссылки могут вести на вредоносные сайты, и заодно собирает с компьютеров ftp-логины и пароли.
- Украденные данные в дальнейшем используются злоумышленниками для доступа к учетной записи на сервере и заражения новых сайтов. Собственно заражением страниц занимался инфектор, написанный на PHP, вставляющий код троянца Gumblar во все веб-документы на сервере после тега <body>.

- Появление первых угроз для iPhone и Android
- Слабая технология контроля публикуемых приложений ОС Android



- Выкачивание денег с помощью SMS, отправленных на премиум-номера. Например: Trojan-Ransom: Blocker и Smser.
- Российская специфика, русский «интерфейс». После успешного запуска блокируют запуск ОС. Требуется послать SMS-сообщение на короткий номер и в ответ получить код, которым активировать ОС. Последние версии троянцев семейства Blocker блокируют загрузку ОС под предлогом того, что у пользователя якобы установлена нелицензионная версия.
- Нелицензионное ПО, предлог вполне убедительный, и жертвой троянцев большей частью становится именно русскоязычная аудитория.

Установлена нелицензионная ОС Windows!

Для активации необходимо отправить SMS с текстом

v1v1v1

на номер

4460

Ввести полученный код:

Активировать

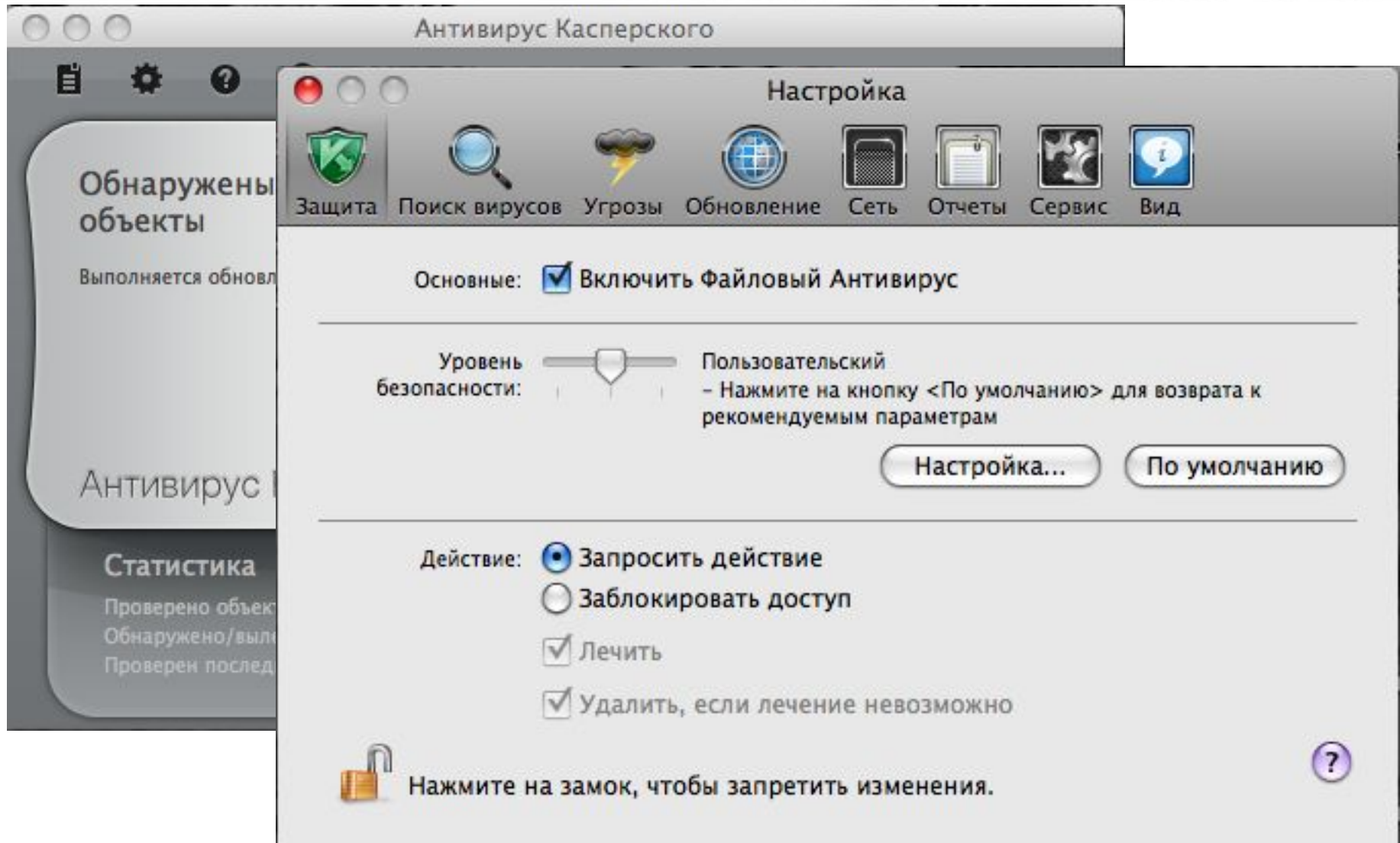
Попытка переустановить систему может привести к потере важной информации и нарушению работы компьютера.

- Растущая популярность той или иной платформы не может не привлекать вирусописателей.
- Во втором квартале 2009 года - 48 новых вредоносных программ
- Наиболее интересными
 - Trojan-Dropper.Linux.Prl -запускает процесс интерпретатора perl и передает ему скрипт, содержащий основную вредоносную нагрузку, которой является рассылка с зараженных серверов спама. первый прецедент использования зараженного *nix-сервера для рассылки спама.
 - Trojan-Mailfinder.Perl.Hnc
- Ботсети из компьютеров под управлением Mac OS X. Распространение вредоносных программ-ботов велось в январе этого года через торрент-сети вместе с пиратской версией популярного пакета офисных программ Apple iWork'09, - Backdoor.OSX.iWorm

- Первая троянская программа для Mac OS – OSX.RSPlug.A (Trojan-Downloader.OSX. Jahlav)
- Первый поддельный антивирус для Mac – Imunizator



Защищать нужно ЛЮБУЮ ОС



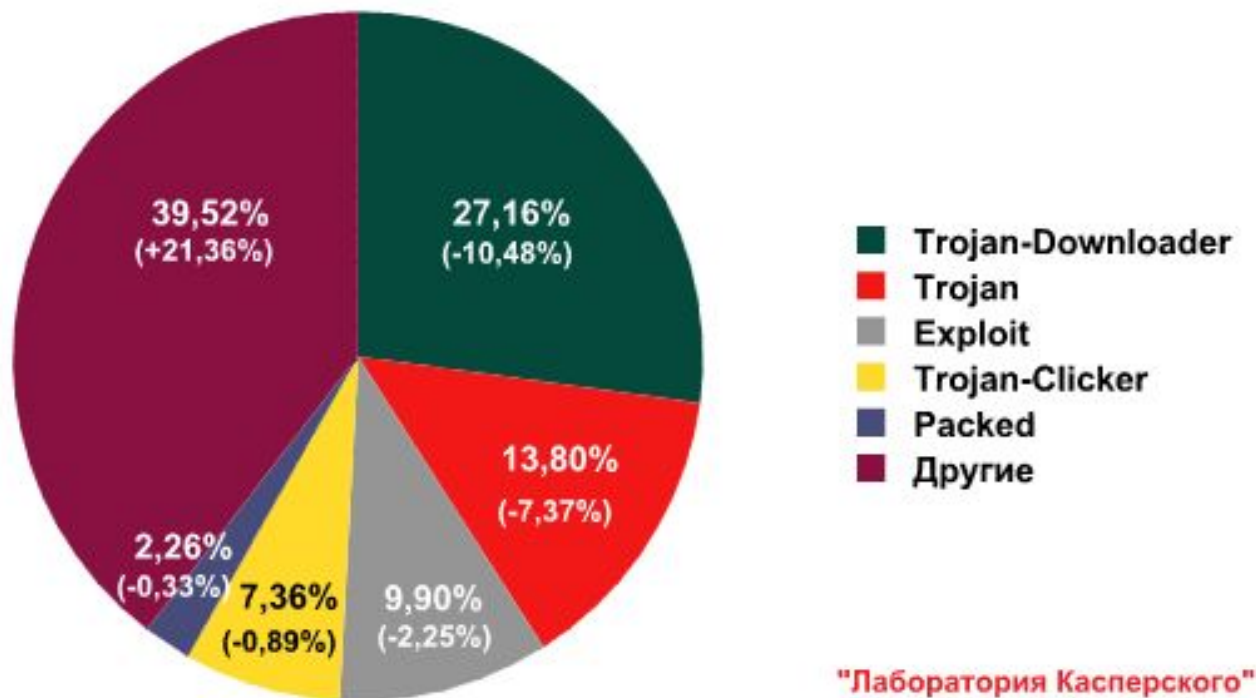
Антивирусная Школа



Новый источник IT-знаний

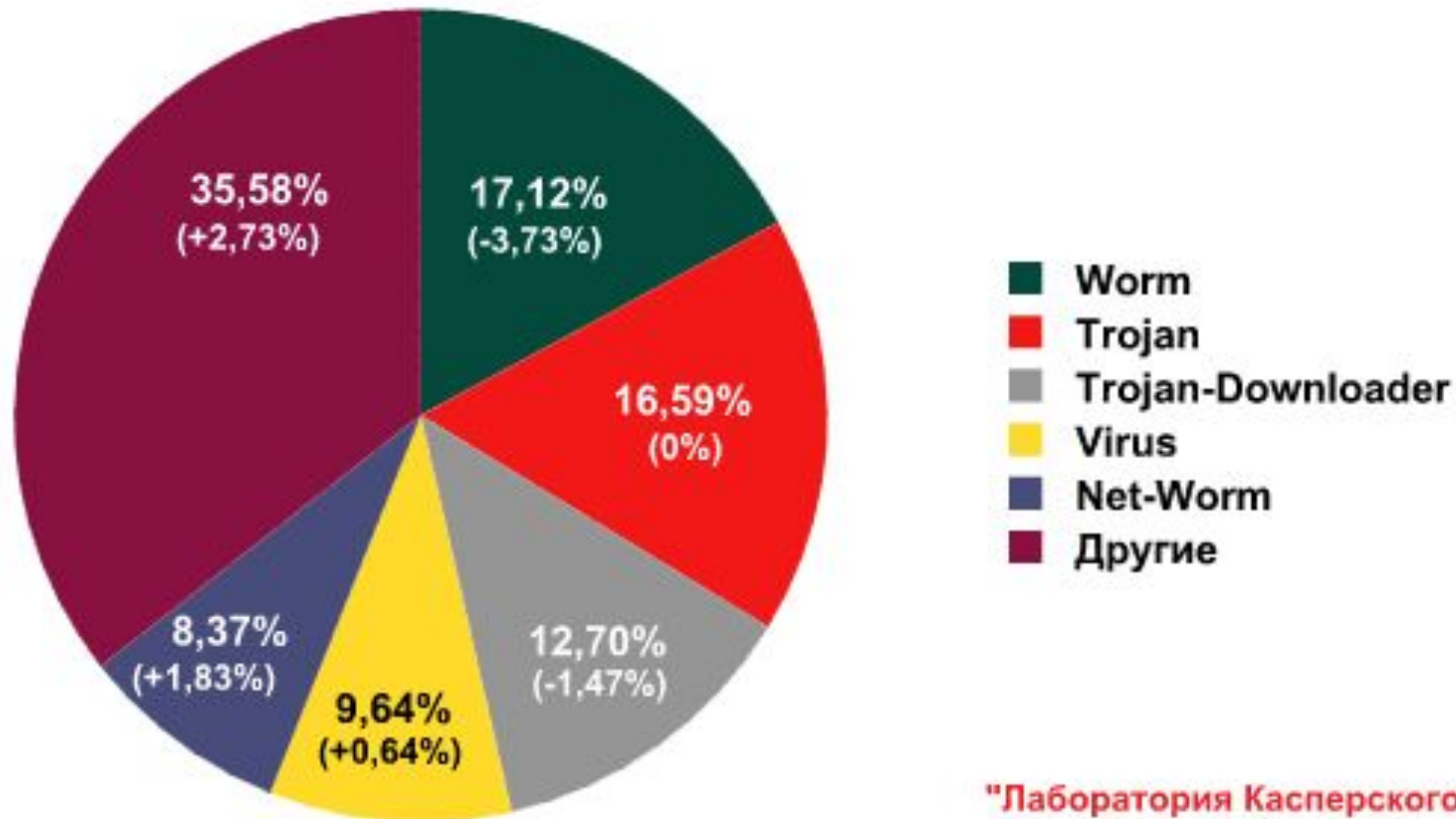
Статистика

Веб-антивирус: детектируемые объекты в интернете



Более 60% вредоносных программ, распространяемых на вебе, составляют программы пяти поведений:

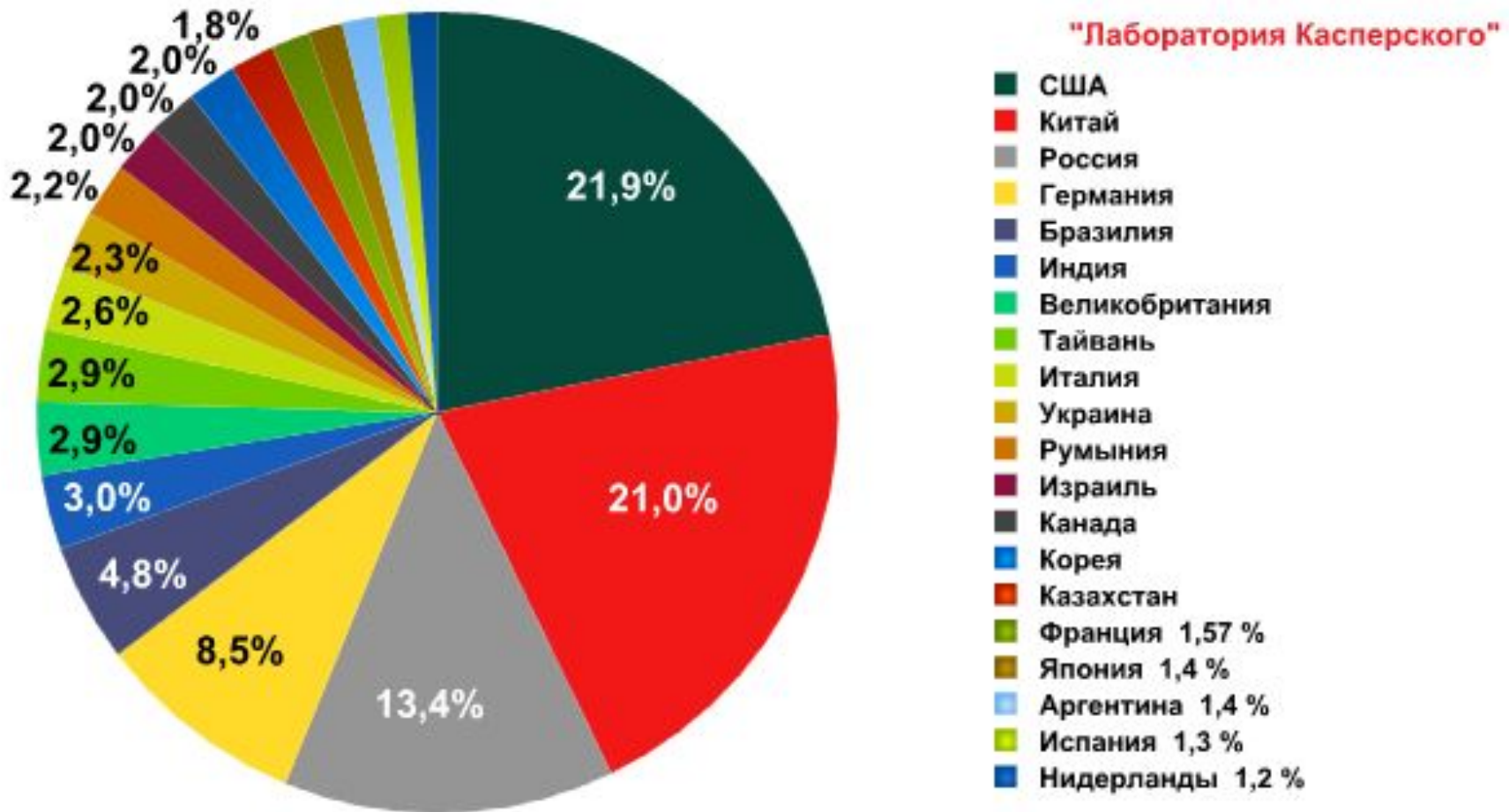
- Trojan-Downloader - доля которого уменьшилась на 10,48% и составила 27,16%. Основной вклад внес Trojan-Downloader.JS.Gumblar.a
- Trojan: его доля изменилась на -7,37% и составила 13,80%. Своей популярностью поведение Trojan обязано в основном троянскому скриптовому загрузчику Trojan.JS.Agent.xy.
- Exploit, на долю которого пришлось 9,90% — это меньше на 2,25%. Главную роль здесь сыграл Exploit.HTML.CodeBaseExec,
- Предпоследнюю позицию в рейтинге по результатам второго квартала заняло поведение Trojan-Clicker — 7,36%. Trojan-Clicker потеряло 0,89%
- Packed. Это поведение стало единственным новичком рейтинга и вытеснило поведение Backdoor. На долю Packed пришлось чуть более 2% — на 0,33% меньше, чем за предыдущий период. Самым популярным представителем данного поведения стал вредоносный объект Packed.JS.Agent.ab



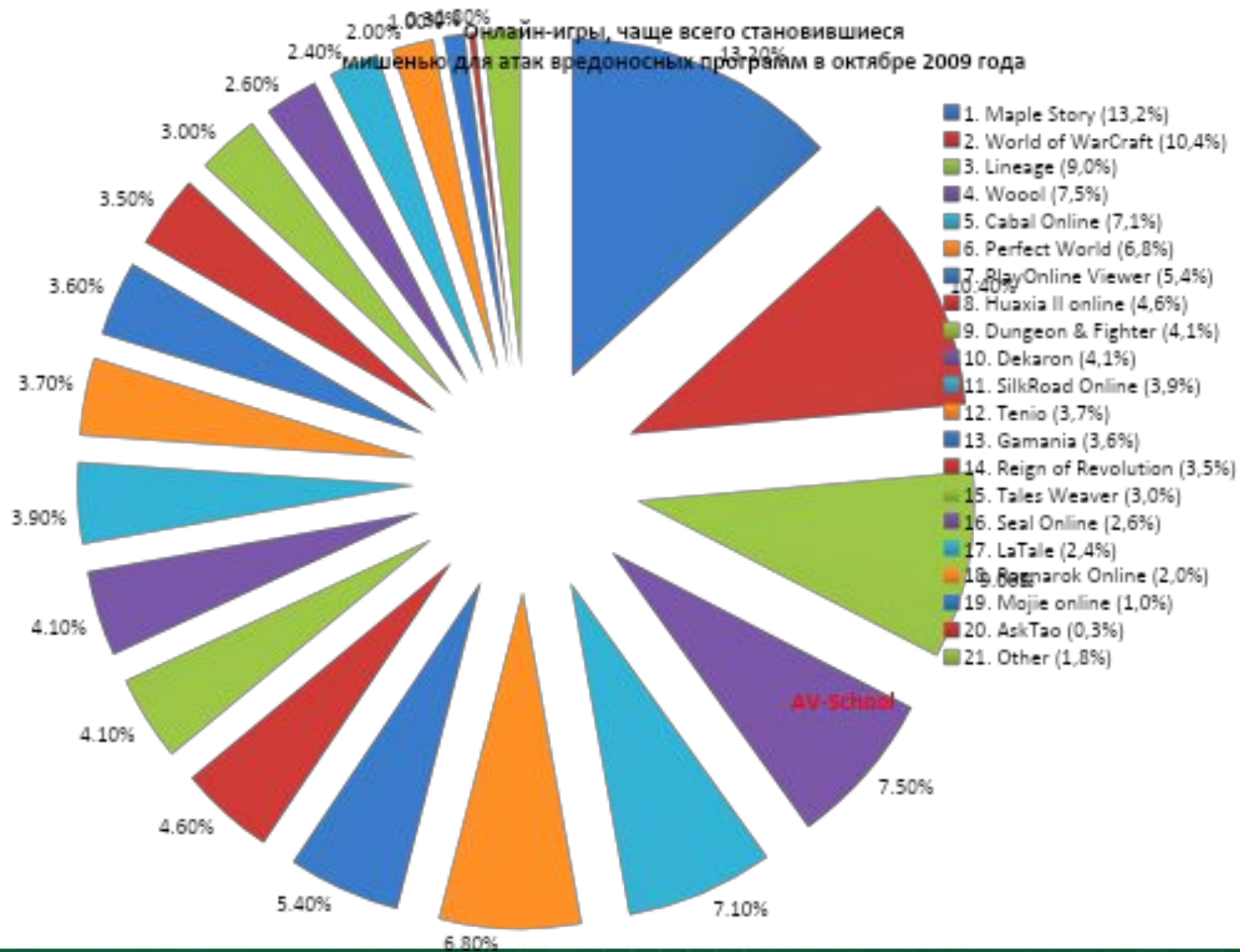
Распределение поведений вредоносных программ по результатам 2009 Q2 (данные on-access сканера).

- Worm (17,12%). Основной вклад в их популярность внесли представители семейства Worm.Win32.AutoRun, которые распространяются на внешних носителях.
- Virus: его доля составила 9,64%, а прирост на 0,64%. Основной вклад в популярность Virus внесли лидеры предыдущих кварталов, сохранившие высокую активность:
 - Virus.Win32.Sality.aa - обычный файловый вирус, вызвавший эпидемию в последнем квартале прошлого года
 - Virus.Win32.Virut.ce. Интересной мишенью атаки в виде web-серверов и многоходовым механизмом заражения
- Net-Worm. На него пришлось 8,37% от всех обнаруженных OAS вредоносных программ, что почти на 2% больше результатов прошлого квартала. Такой популярностью поведение обязано Net-Worm.Win32.Kido.ih.

Распределение вредоносных доменов по странам

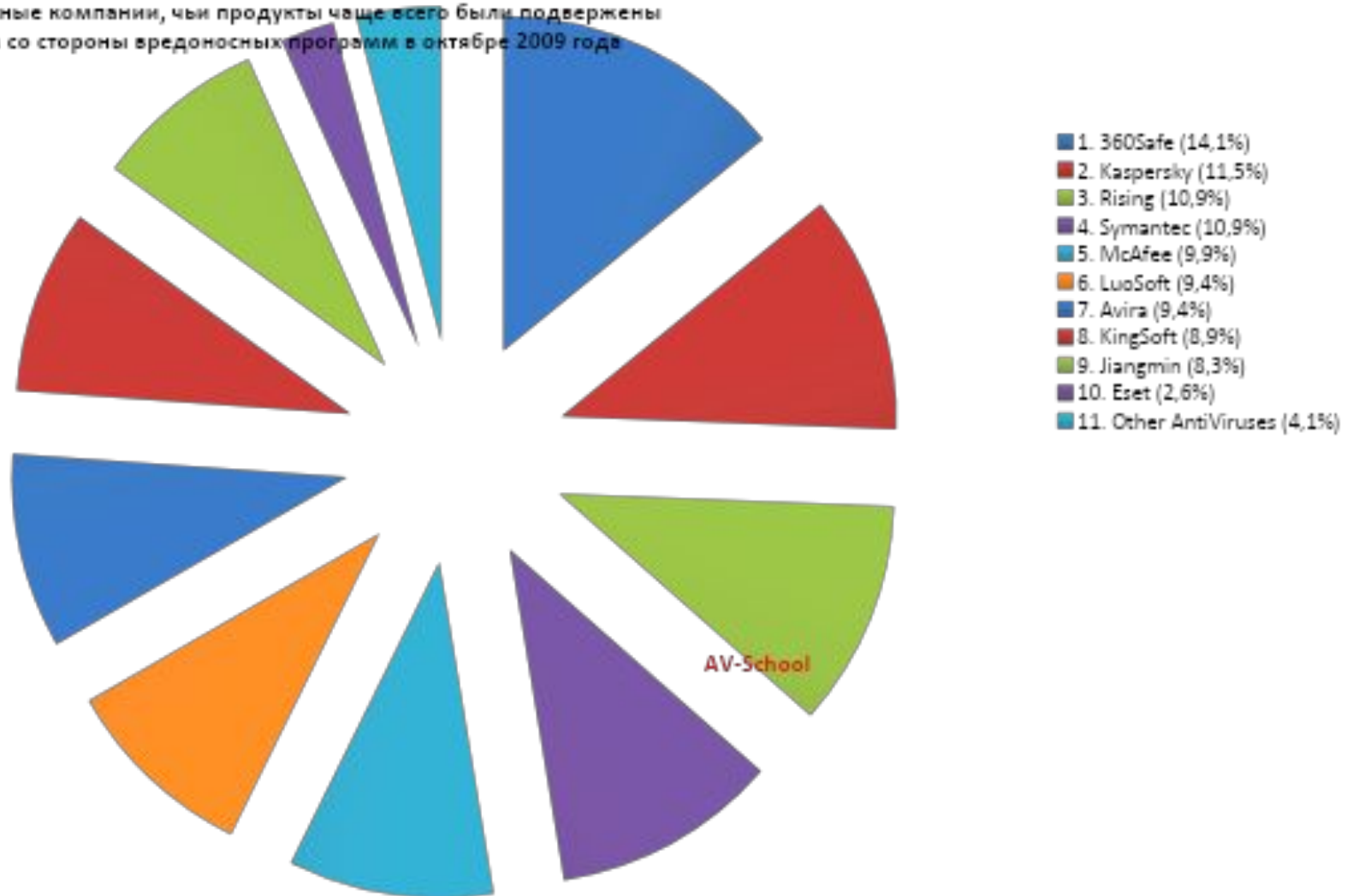


Онлайн-игры, чаще всего становившиеся мишенью для атак вредоносных программ в октябре 2009 года



Атаки на антивирусы

Антивирусные компании, чьи продукты чаще всего были подвержены атакам со стороны вредоносных программ в октябре 2009 года



- Современные вредоносные программы отличаются многообразием способов распространения. В настоящее время, когда среднестатистический пользователь использует большое количество клиентов (почта, веб, интернет-пейджеры, P2P и т.д.), очень важно уделять внимание защите каждого канала передачи данных.
- В каждом трафике - свои зловреды, свои пути проникновения и заражения компьютера.
- Современные антивирусы уже давно перестали быть простыми сканерами: на многообразии вредоносного контента необходимо отвечать многообразием подсистем защиты.
- Неверно думать, что если включена какая-то одна из них, то пользователь будет защищен. Когда речь идет о защите от современных вредоносных программ, лишней защиты не бывает!

- Информация в Интернет:

av-school.ru

[securelist](http://securelist.com)securelist.com

kaspersky.com

Спасибо! Вопросы?

Станислав Шевченко,

зам. директора по исследованиям и разработке,
директор проекта «Антивирусная школа – новый источник IT-знаний»
Kaspersky Lab

