Актуальные вопросы антивирусной защиты: ситуация, тенденции, требования, выбор продуктов

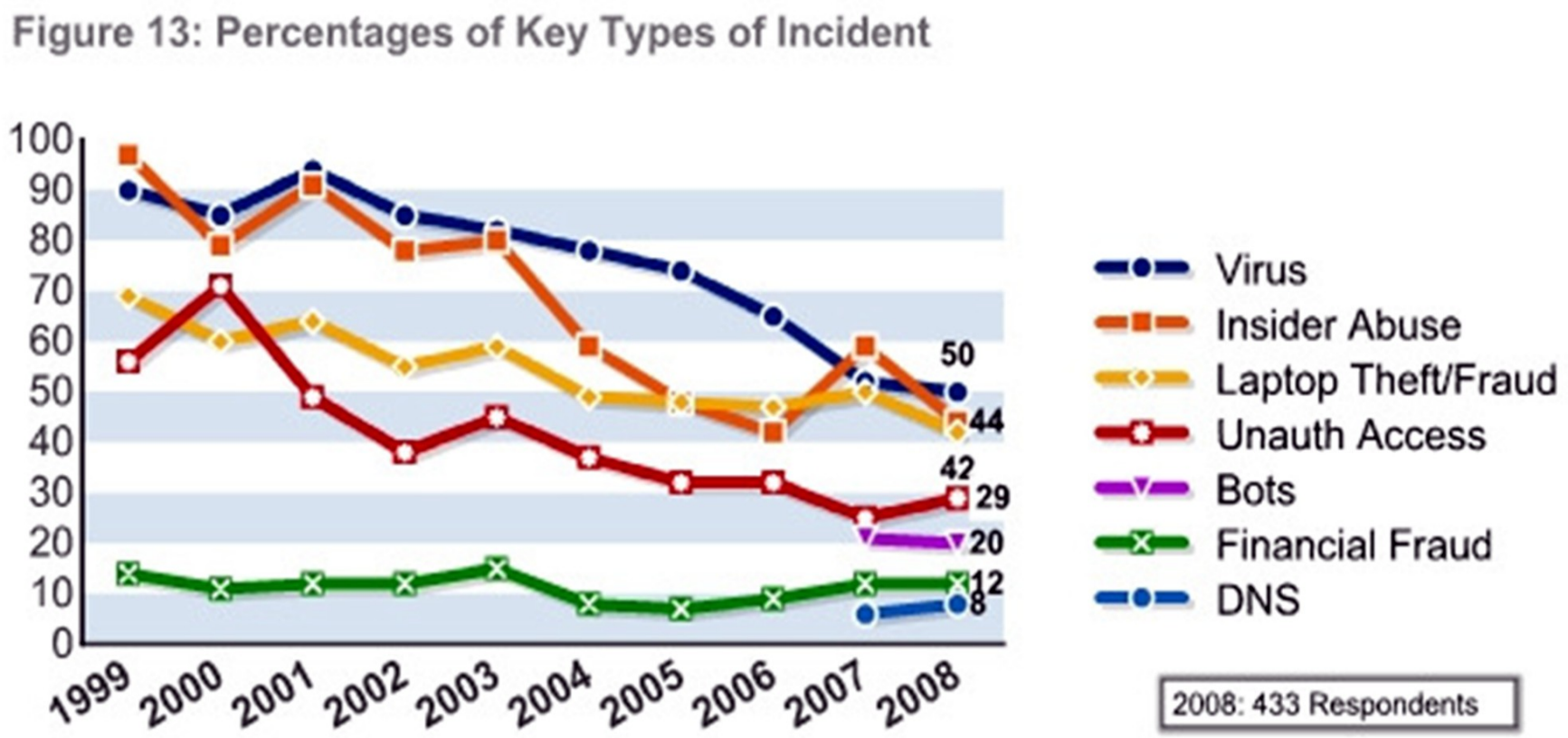
Владмир Тихонов

Руководитель службы консалтинга в Украине, Молдове,Республике Беларусь

Часть 1

Мир, в котором мы живём…

CSI: Подверженность ИТ-угрозам



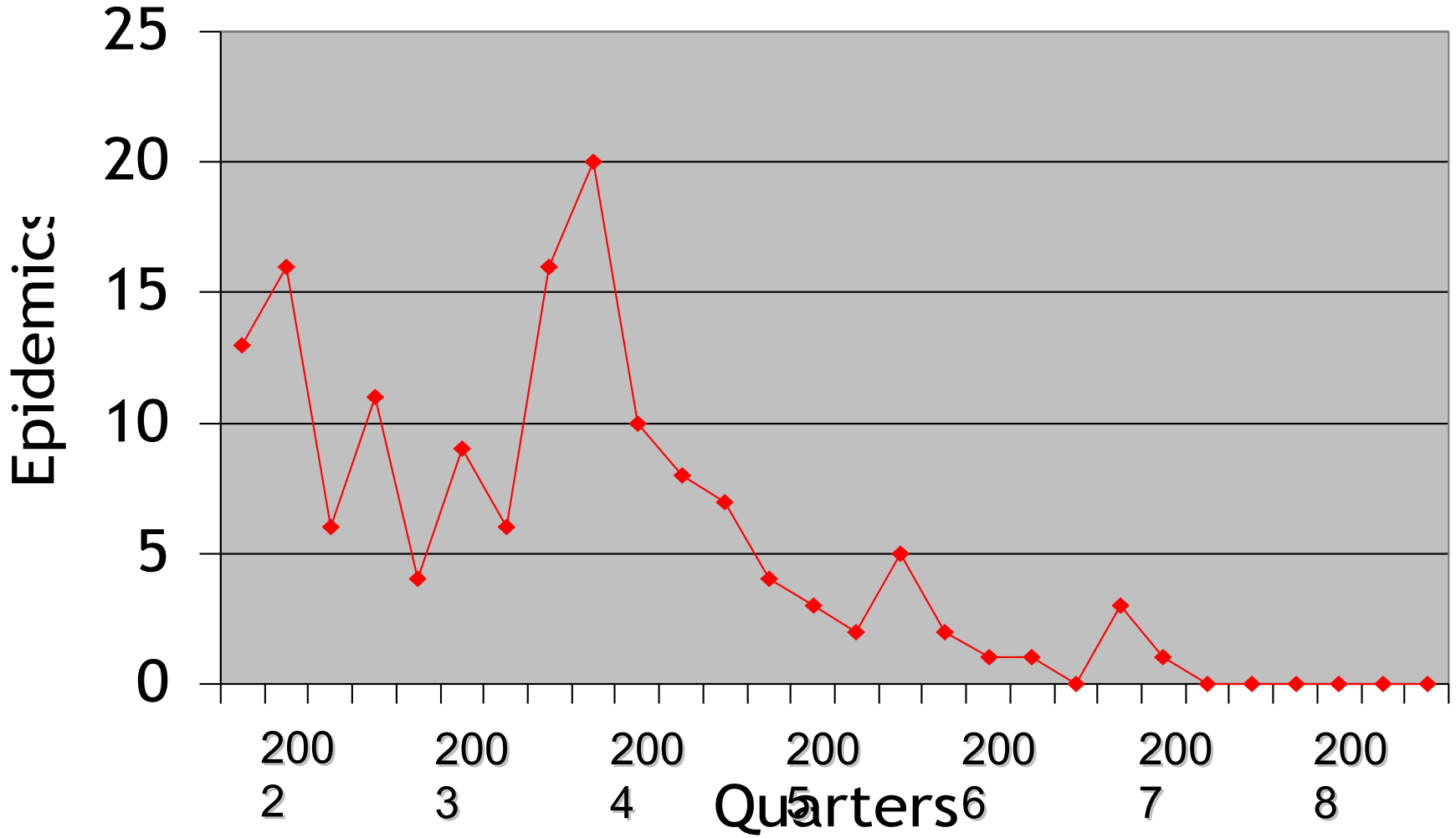
Источник: *2008 CSI Computer Crime and Security Survey*

CSI: Ключевые наблюдения

- Наиболее дорогие угрозы – **финансовое мошенничество**, усреднённая «стоимость» которых составила **$500'000**
  - На втором месте – угрозы, связанные с появлением в корп. сетях **bot-net**'ов, повлёкшие усреднённые потери в размере **$350'000** на респондента
  - Общий **усреднённый уровень потерь** респондентов от угроз – **$300'000**
- Наиболее распространены **вирусные угрозы** – почти половина респондентов (**49%**) имела подобные инциденты
- **27%** респондентов заявили об обнаружении направленных на них атак вредоносных программ
- **Каждая десятая** компания имела **инциденты с DNS** (вследствие уязвимостей реализации)
- Подавляющее большинство респондентов уже имеют (**68%**) или разрабатывают (**18%**) формальную политику безопасности
  - Лишь **1%** респондентов не имеет политики безопасности

Источник: *2008 CSI Computer Crime and Security Survey*

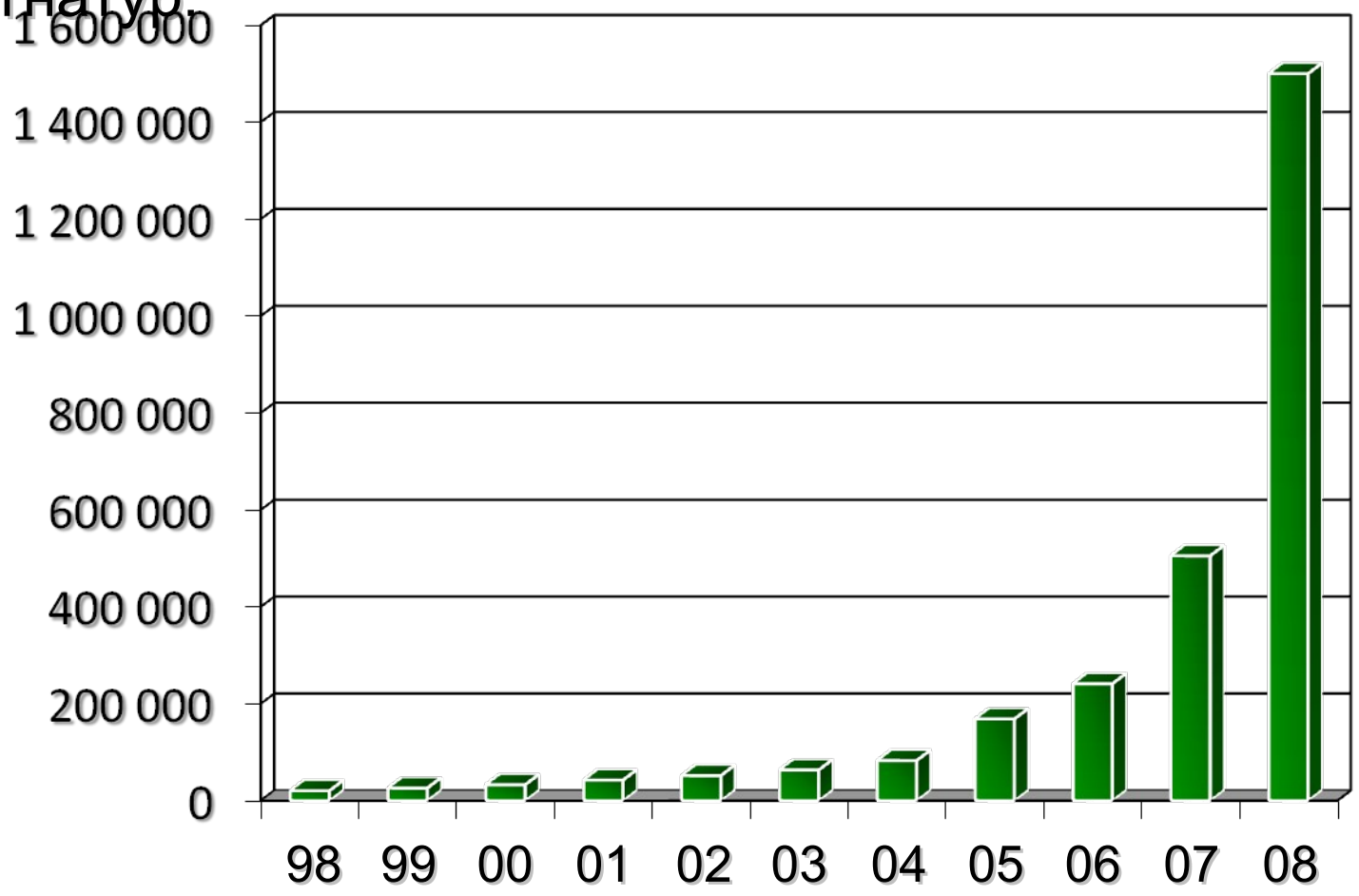
История развития глобальных эпидемий



Источник: *Kaspersky Lab*

Статистика выпуска сигнатур

- 2008 год – более **17’000’000** файлов и более **1’000’000** сигнатур:



Источник: *Kaspersky Lab*

Распределение атак в 2008 году (статистика KSN)

- Через электронную почту
  - Вредоносный трафик – от 1,1% до 2,5%
  - Фишинговые атаки – от 0,62% до 0,78%
- Через браузер – 23’680’646 атак
- Сетевые атаки – 30’234’287 атак
- Локальные заражения
  - 6’349’359 инцидентов
  - 189’785 различных вредоносных программ
- Уязвимости – 130’518’320 файлов и приложений
- Динамика появления неизвестных зловредов ~3’400 в день

Источник: *Kaspersky Lab*

Превалирующие источники заражения (Web)

- Web-канал стал основным источником заражения, а электронная почта отошла на второй план
- Подавляющее большинство атак проводится при помощи технологии drive-by-download – незаметно для пользователя во время обычной работы в интернете
  - Взломанные сайты включают скрытые обращения к другим ресурсам, на которых размещён вредоносный код, нацеленный на уязвимости браузеров и плагинов к ним (ActiveX, RealPlayer, Flash Player, …)
  - 10 из 20 наиболее распространённых программ написаны на языке Java-Script в виде HTML-тегов, что говорит о необходимости антивирусной проверки всех исполняемых скриптов
- Время жизни вредоносного URL исчисляется в часах/днях (среднее время жизни – 4 часа)

Источник: *Kaspersky Lab*

Источники атак

- 23’508’073 атаки 2008 года, проводились с интернет-ресурсов, размещённых в 126 странах мира (территориальную принадлежность ещё 172’573 атак определить не удалось)
- Более 99% атак проводились с интернет-ресурсов 20 стран (см. таблицу)
  - По результатам 1-го квартала 2009 Россия переместилась на второе место,
    и во 2-м квартале сохранила позицию ☹
- Более 70% новых вредоносных программ – китайского происхождения

Место	Страна	Количество	Процент
1	CHINA	18568923	78,99%
2	UNITED STATES	1615247	6,87%
3	NETHERLANDS	762506	3,24%
4	GERMANY	446476	1,90%
5	RUSSIAN FEDERATION	420233	1,79%
6	LATVIA	369858	1,57%
7	UNITED KINGDOM	272905	1,16%
8	UKRAINE	232642	0,99%
9	CANADA	141012	0,60%
10	ISRAEL	116130	0,49%
11	LITHUANIA	110380	0,47%
12	SOUTH KOREA	46167	0,20%
13	HONG KONG	44487	0,19%
14	ESTONIA	41623	0,18%
15	SWEDEN	40079	0,17%
16	FRANCE	31257	0,13%
17	ITALY	29253	0,12%
18	BRAZIL	25637	0,11%
19	PHILIPPINES	19920	0,09%
20	JAPAN	16212	0,07%

Источник: *Kaspersky Lab*

Нацеленность атак

- На долю 20 стран пришлось 89% зафиксированных атак
  - Более половины – на Китай
    - Преимущественно троянцы, крадущие учётные записи к он-лайн играм
  - Египет, Турция и Индия в настоящее время переживают «интернет-бум» на фоне крайне низкого уровня квалификации пользователей
    - Создание зомби-сетей (спам, фишинг, распространение новых вредоносных программ)
  - США, Россия, Германия, Великобритания, Франция, Бразилия, Италия и Израиль
    - Учётные записи платёжных систем и персональные данные
  - По результатам 1H09 Россия поднялась на четвёртое место ☹

Место	Страна	Количество	Процент
1	CHINA	12708285	53,67%
2	EGYPT	3615355	15,27%
3	TURKEY	709499	3,00%
4	INDIA	479429	2,03%
5	UNITED STATES	416437	1,76%
6	VIETNAM	346602	1,46%
7	RUSSIAN FEDERATION	335656	1,42%
8	MEXICO	308399	1,30%
9	SAUDI ARABIA	287300	1,21%
10	GERMANY	253097	1,07%
11	MOROCCO	230199	0,97%
12	THAILAND	204417	0,86%
13	INDONESIA	190607	0,81%
14	UNITED KINGDOM	188908	0,80%
15	FRANCE	182975	0,77%
16	SYRIA	134601	0,57%
17	BRAZIL	123736	0,52%
18	TAIWAN	122264	0,52%
19	ITALY	121508	0,51%
20	ISRAEL	118664	0,50%

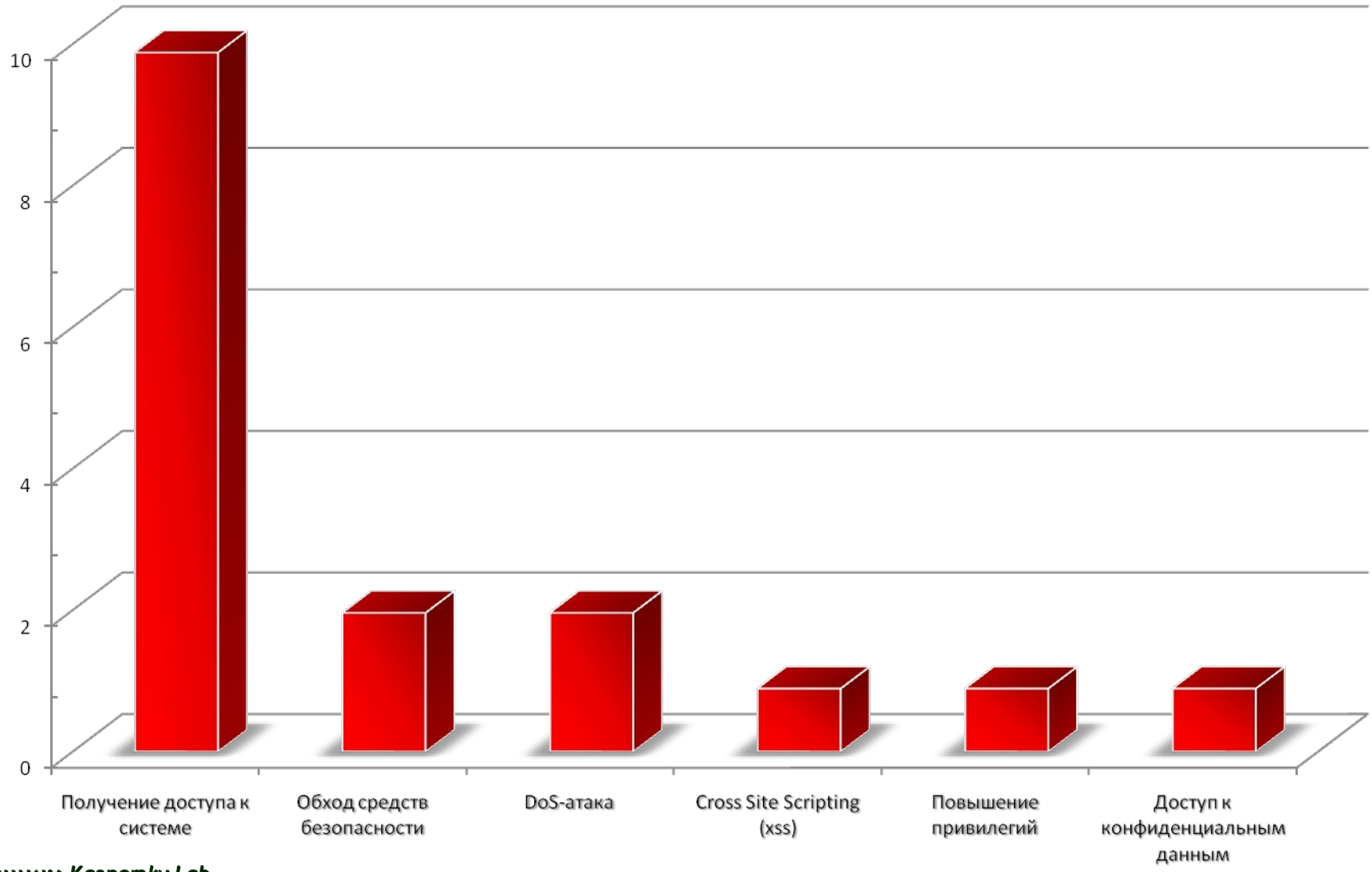
Источник: *Kaspersky Lab*

Лидирующие эксплойты (2Q2009)

- *Intrusion.Win.MSSQL.Worm.Helkern [UDP 1434]* – 61,06%, уязвимость “Buffer Overruns in SQL Server 2000 Resolution Service” (MS02-039)
  - Эпидемия Slammer в январе 2003
- *Intrusion.Win.NETAPI.Buffer-Overflow.Exploit [TCP 445]* – 17,85%, уязвимость в сетевой службе сервера (MS08-067)
  - Сетевой пакет с эксплойтом, одна из самых опасных уязвимостей 2008 года (эксперты узнали о ней лишь путём исследования вредоносных программ, которые её использовали, Kido)
- *Intrusion.Win.DCOM.Exploit [TCP 135]* – 3,73%, уязвимость “Buffer Overruns in RPC Interface” (MS03-026)
  - Эпидемия Lovesan в августе 2003
- Устаревшие, казалось бы, вредоносные программы всё ещё живут и продолжают заражать компьютеры неквалифицированных и неосторожных пользователей

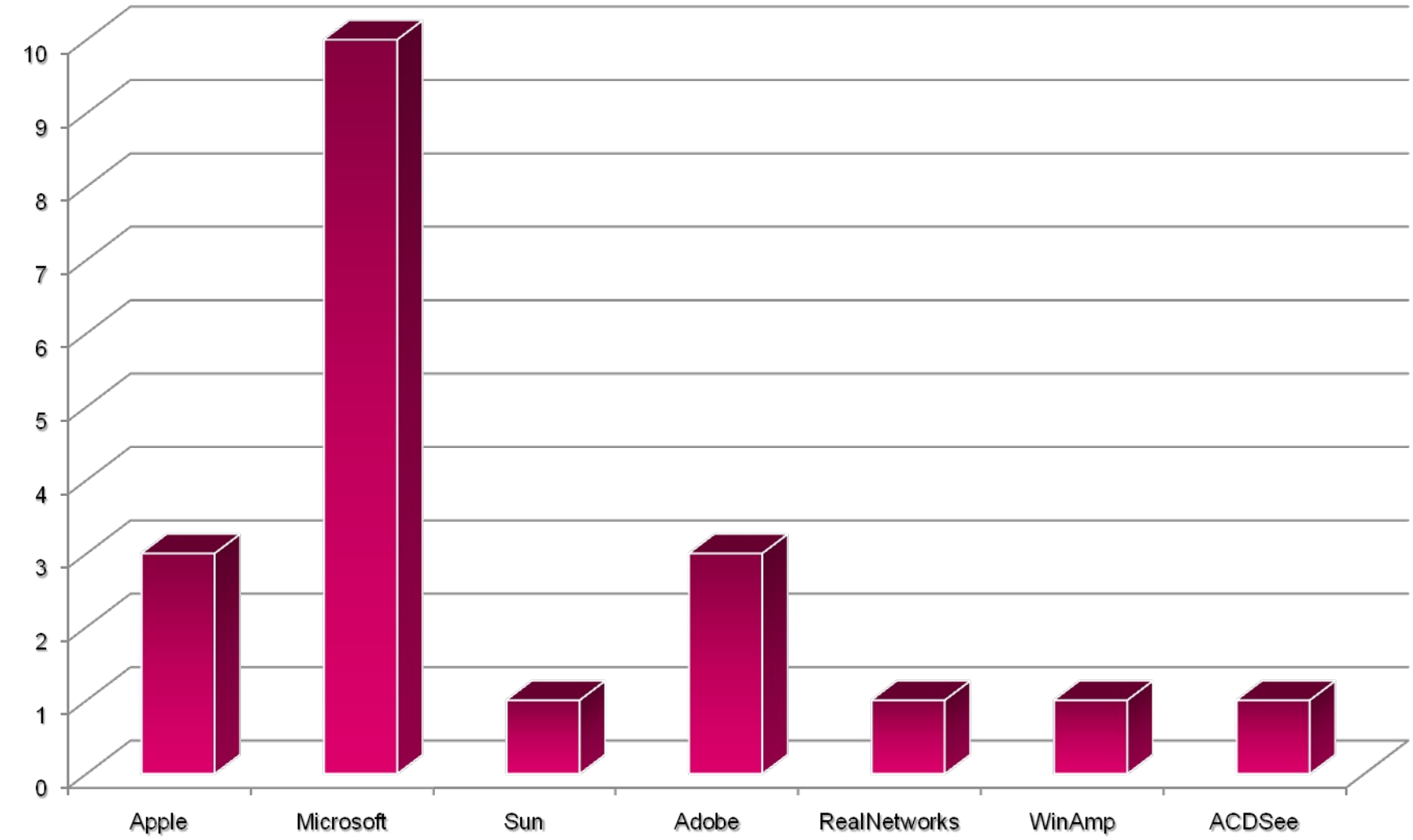
Источник: Kaspersky Lab

Распределение уязвимости по типам



Источник: *Kaspersky Lab*

Top-20 уязвимостей по производителям



Источник: *Kaspersky Lab*

Локальные источники заражения

- 6’394’359 вирусных инцидентов в 2008, не связанных с электронной почтой, интернет-доступом и сетевыми атаками
  - Sality.aa – «угроза года», классический файловый вирус
  - Активное распространение через USB-носители информации и функцию автозапуска ОС Windows
- Наиболее популярный среди вирусописателей способ заражения ПК, обычно комбинируется с функционалом:
  - Заражения файлов
  - Кражи информации
  - Создания ботнетов
- Преимущественно первичное заражение осуществляется через класс Trojan-Downloader – единственный класс, который действительно исполняет роль троянского коня

Источник: *Kaspersky Lab*

Локальные источники заражения

- Горячая пятёрка’2008
  - *Virus.Win32.Sality.aa* (~30’000 заражений по всему миру)
    - Основной способ распространения – через флэш-карты памяти и ’autorun.inf’
  - *Packed.Win32.Krap.b*
    - Различного рода и назначения троянцы, при создании которых использовался данный упаковщик
  - *Trojan-Downloader.Win32.Small.aacq*
    - «безобидный» троянец-загрузчик
  - *Worm.Win32.Autorun.dui*
    - Распространение – через флэш-карты памяти и “autorun.inf”
  - *Trojan-Downloader.Win32.VB.eql* (~21’000 заражений)
    - «безобидный» троянец-загрузчик

Источник: *Kaspersky Lab*

Иллюстрация: *Virus.Win32.Sality*

- Содержит процедуру самосборки – при запуске выкачивает с Web-ресурсов свои части (якобы в виде картинок), затем собирает новый код и устанавливает в ОС
- Заражает исполняемые файлы, каждый раз заново шифруя своё тело (алгоритм RC4 с изменяемым ключом переменной длины)
- При запуске заражённого файла копирует себя во все запущенные процессы
  - При первом запуске прописывает в реестр собственные драйверы
  - После запуска пытается зарегистрировать DNS-имя *"SOSiTE_AVERI_SOSiTEEE.haha.domainname"* в локальном домене для дальнейшего распространения в корп. сети
- Механизмы распространения в корпоративной сети:
  - Через службу удалённого исполнения команд NetBIOS
  - Подключаясь от имени пользователя к общим и системным папкам других компьютеров (серверов и рабочих станций)
    - Если пользователь – администратор домена, очень быстро будет создан корпоративный ботнет

Источник: *Kaspersky Lab*

- Открывает для спам-ботов порт IPSec в локальном Windows Firewall

Наиболее яркие «достижения» 2008 года

- Китай стал бесспорным лидером
  - Не только активно создаёт собственное вредоносное ПО, но и активно занимается локализацией импортного, и, в первую очередь, российского (эксплойты *IcePack*, *FirePack*, *Mpack*, варианты троянцев *Pinch*, *Zeus* и др.)
  - Обнаружение и первичное использование уязвимости службы сервер (MS08-067) также дело рук китайских вирусописателей
  - Большой китайский «хак» – за апрель-июнь 2008 взломано более 2'000'000 интернет-ресурсов по всему миру (встраивание ссылок на источники заражения)
- Но русские вирусописатели тоже «не лыком шиты» – активная реализация модели MalWare 2.0 (*Rustock.C* и *Sinowal*)
  - Принцип разделения различных вредоносных модулей по функционалу
  - Использование универсальных средств взаимодействия между модулями
  - Защищённые от внешнего воздействия каналы обмена данными

Источник: *Kaspersky Lab*

Backdoor/Trojan-PSW.Win32.Sinowal

- Параметры исследования (Калифорнийский университет, США):
  - Период исследования – **10 дней**
  - Количество компьютеров – **182’800**
  - Объём украденных данных – **70 Гб**
- Состав данных:
  - Учётные записи электронной почты – **54’090**
  - Адреса электронной почты – **1’258’862**
  - Информация, снятая с web-форм – **11’966’532**
  - Учётные записи **http** – **411’039** (google.com, facebook.com, myspace.com…)
  - Учётные записи **ftp** – **12’307**
  - Учётные записи **pop** – **415’206**
  - Учётные записи **smtp** – **100’472**
  - Пароли **Windows** – **1’235’122**

Источник: http://www.cs.ucsb.edu/~sectalkprojects/torpig/torpig.pdf

- Размер потенциального дохода – от **$83’000** до

Камо грядеши?

- Мы констатировали смерть некоммерческого вредоносного ПО в 2007
  - Хулиганские выходки, «пробы пера» и самовозвеличивание остались в прошлом, уступив место коммерческой выгоде
  - 2007-2008 – стремительный рост количества троянских программ, ориентированных на кражу информации
- Мы констатируем смерть эксклюзивного вредоносного ПО в 2008
  - Подавляющее большинство созданного вредоносного ПО идёт на продажу, то есть, увы, стало общедоступным
  - При этом вредоносное ПО обеспечивается технической поддержкой, в том числе и по обходу антивирусных программ
- Старое на новый лад
  - Возвращение к истокам – файловым вирусам
  - Новый технологический уровень – «облачные вычисления»

Что ожидать в 2009 - наш прогноз (1)?

- Глобальные эпидемии – возможно изменение ситуации и появление инцидентов, превосходящих по масштабам эпидемии 2006-2008
  - Передел рынка вследствие конкуренции российских, китайских, бразильских, украинских и турецких злоумышленников
  - Ещё большее увеличение количества киберпреступников вследствие экономического кризиса
- MalWare 2.5
  - Отсутствие стационарного центра управления ботнетом («мигрирующий ботнет»)
  - Использование стойких криптоалгоритмов для взаимодействия
  - Универсализация центров управления разными ботнетами
  - Использование злоумышленниками концепции «Cloud Computing»

Источник: *Kaspersky Lab*

Что ожидать в 2009 - наш прогноз (2)?

- Фишинг/мошенничество – будут «набирать обороты» вследствие экономического кризиса
  - Более нервная и менее продуманная реакция пользователей на любые события, связанные с платёжными и банковскими системами
  - Это более простой, более грубый и более дешёвый способ атак
- Снижение активности игровых троянцев
  - В количественном отношении этот тип преобладает над остальными, «игровой» рынок перенасыщен ими
  - Меняются объективные условия – развитие стран, уровня знаний пользователей и т.п.
- Дифференциация по платформам
  - Будут затронуты абсолютно все платформы
  - Смещение фокуса атак в малоохваченные области (в первую очередь – Mac OC и мобильные платформы)

Источник: Kaspersky Lab

Часть 2

Системы жизнеобеспечения

Главные принципы построения систем защиты

- Эшелонированность
  - Преодолеть несколько линий обороны существенно сложнее, особенно, если они базируются на различных платформах
- Мультивендорность
  - Одновременно обладать глубокими знаниями по нескольких платформам довольно непросто, а воплотить множество механизмов их преодоления в рамках одной атаки многократно сложнее
  - Производители средств защиты используют в своих продуктах различные технологии, а схожие реализуют по-разному – свои «плюсы» и «минусы» есть у каждого продукта
- Комплексность – единство различных средств и мер:
  - Аппаратных
  - Программных
  - Организационно-технических

Необходимо, но недостаточно…

- Системы AV-защиты должны строиться на основе современной архитектуры или, в противном случае, можем получить:
  - наличие незакрытых уязвимостей в используемых ОС и приложениях
  - отсутствие необходимого уровня контроля за действиями пользователей
- Должны существовать выверенные процессы и процедуры эксплуатации систем и средств, их отсутствие приводит к:
  - несвоевременному обновлению средств защиты
  - несоблюдению политик безопасности сотрудниками, вплоть до отключения установленных средств защиты
- Должны быть жёстко регламентированы действия пользователей и установлен постоянный контроль за их средствами защиты
  - Организация карантинных зон для ПК, не удовлетворяющих

Система защиты - единое множество средств

- «Лоскутные технологии» в защите – это ~100%-ная брешь, вызванная отсутствием:
  - Целостности защиты
    - какие-то узлы могут оказаться неучтенными, хотя бы временно
    - конфигурационные настройки «на глаз» не поддаются системному подходу
  - Единых средств мониторинга и управления
    - неконтролируемые действия пользователя
    - сложность эксплуатации и, тем более, оперативной реакции, особенно во время атак и вирусных эпидемий
  - Единого механизма обновления средств защиты (антивирусных баз)
    - несвоевременное обновление оставляет компьютер незащищенным против новейших вирусов, а они часто опаснее предыдущих…
- Концепция Kaspersky OpenSpace Security и продукты ЛК удовлетворяют современным требованиям к построению систем информационной защиты

Задача выбора средств защиты

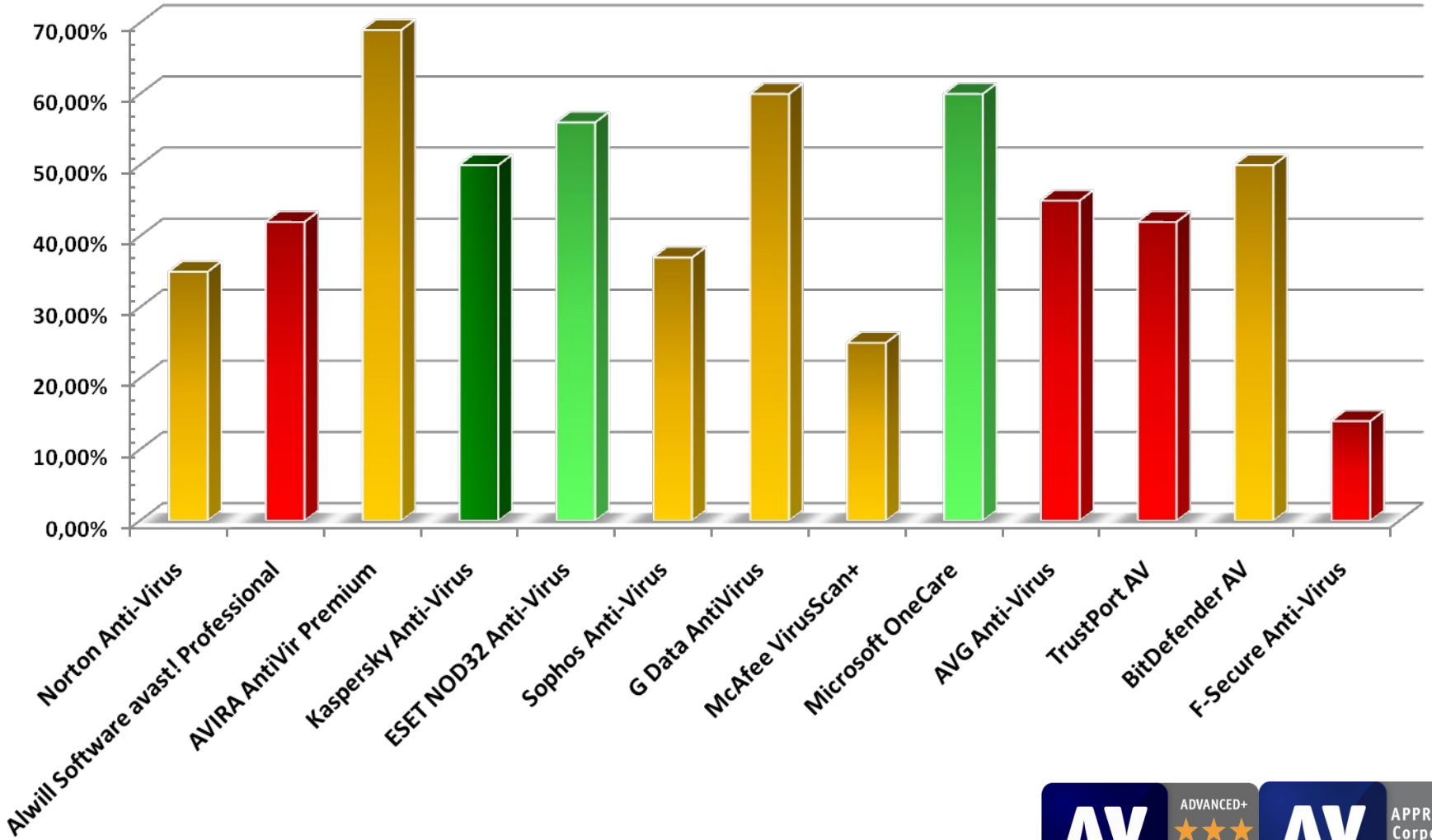
- Абсолютной защиты нет и быть не может, следовательно, верхним порогом затрат является стоимость потерь (задача управления рисками), то есть величина, зависящая от:
  - Стоимостей влияния инцидентов на бизнес организации и
  - Вероятностей возникновения инцидентов нарушения защиты
  - При равных возможностях средств защиты следует опираться на соотношение уровня защиты к затратам на её взлом (самозащиту)
- Выбор средств AV-защиты должен осуществляться на основании следующих критериев:
  - Качество распознавания (детектирования) вредоносного ПО
  - Оперативность (скорость реакции на новые образцы) производителя
  - Функционал, предоставляемый продуктами
  - Сертификация
    - Международных лабораторий
    - Производителей программных и аппаратных платформ

On-demand detection

	Февраль 2004	Август 2004	Февраль 2005	Август 2005	Февраль 2006	Август 2006	Февраль 2007	Август 2007	Февраль 2008	Август 2008	Февраль 2009
AVIRA AntiVir Premium	89,12%	87,99%	91,09%	93,63%	97,71%	99,69%	98,85%	99,45%	99,60%	99,20%	99,70%
G DATA Security G Data AntiVirus					99,89%	99,79%	99,45%	99,31%	99,50%	99,10%	99,80%
Alwill Software avast! Professional	93,09%	92,66%	90,81%	91,06%	93,58%	94,58%	93,86%	95,24%	97,60%	97,30%	98,20%
AVG Technologies AVG Anti-Virus			**86,03%**	87,44%	90,79%	91,55%	96,37%	97,75%	98,10%	94,30%	93,00%
BitDefender BitDefender AV	95,27%	95,72%	94,02%	97,34%	95,65%	96,53%	96,11%	97,51%	96,50%	92,40%	98,00%
Doctor Web Dr.Web	96,09%	94,91%	93,91%	92,42%	92,19%	92,25%	89,27%	89,87%			
F-Secure F-Secure Anti-Virus					99,77%	99,46%	97,91%	97,57%	97,50%	91,10%	93,40%
TrendMicro Internet Security	90,44%	90,66%	91,31%	91,25%							
Kaspersky Lab KAV	99,86%	99,77%	99,65%	99,88%	99,77%	99,45%	97,89%	98,46%	98,30%	95,10%	97,10%
McAfee McAfee VirusScan+	99,26%	99,05%	98,04%	98,19%	98,16%	95,57%	91,63%	93,15%	94,90%	84,40%	99,10%
Microsoft Microsoft OneCare							**82,40%**	90,37%	93,90%	84,60%	87,10%
ESET NOD32 Anti-Virus	95,51%	94,96%	95,50%	98,31%	98,77%	99,07%	96,71%	97,60%	97,70%	93,00%	97,60%
Symantec Norton Anti-Virus	95,15%	95,69%	98,31%	99,41%	98,72%	98,88%	96,83%	98,80%	97,70%	97,90%	98,70%
Panda Software Panda Anti-Virus	99,11%	98,59%			91,05%						
TrustPort TrustPort AV					98,44%	99,06%	99,36%	99,64%	99,80%	97,20%	97,10%
Sophos Sophos Anti-Virus	94,25%	91,98%	90,10%	89,12%					96,60%	90,10%	89,60%

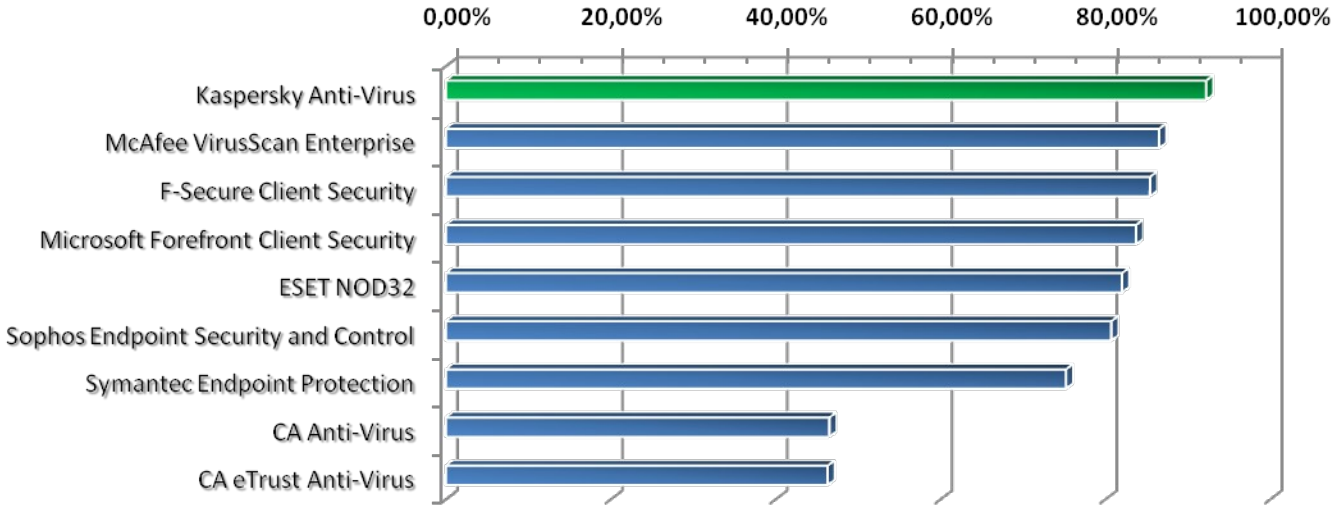
к: *AV-Comparatives, On-Demand Detection Tests from Feb'2004 to Feb'2009*

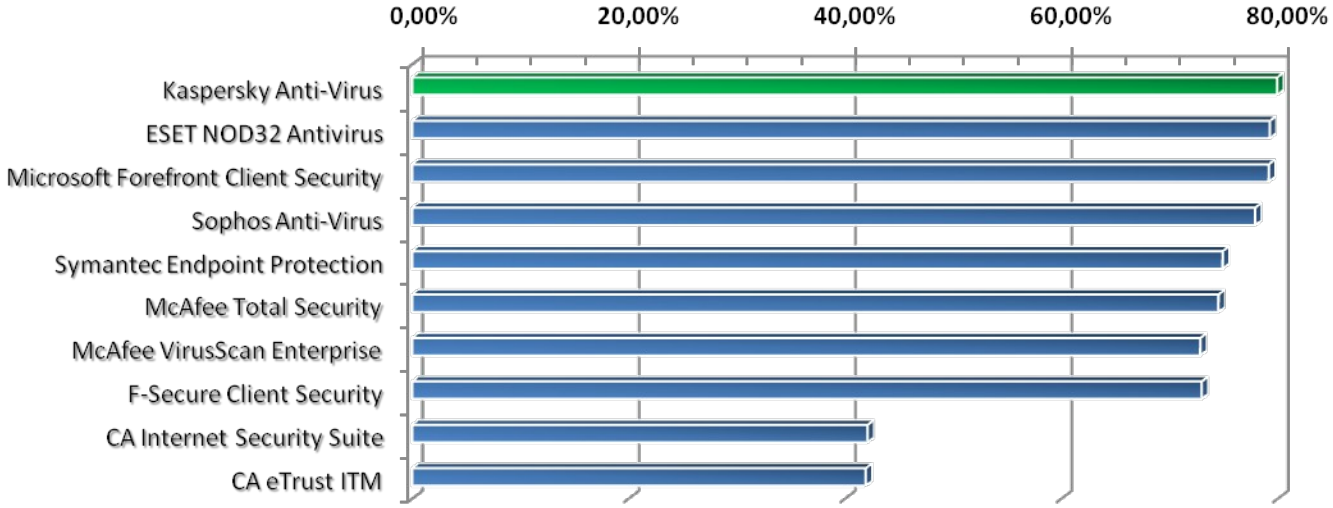
Proactive/retrospective test (May'09)



Источник: *AV-Comparatives, Proactive/retrospective test, May'09*

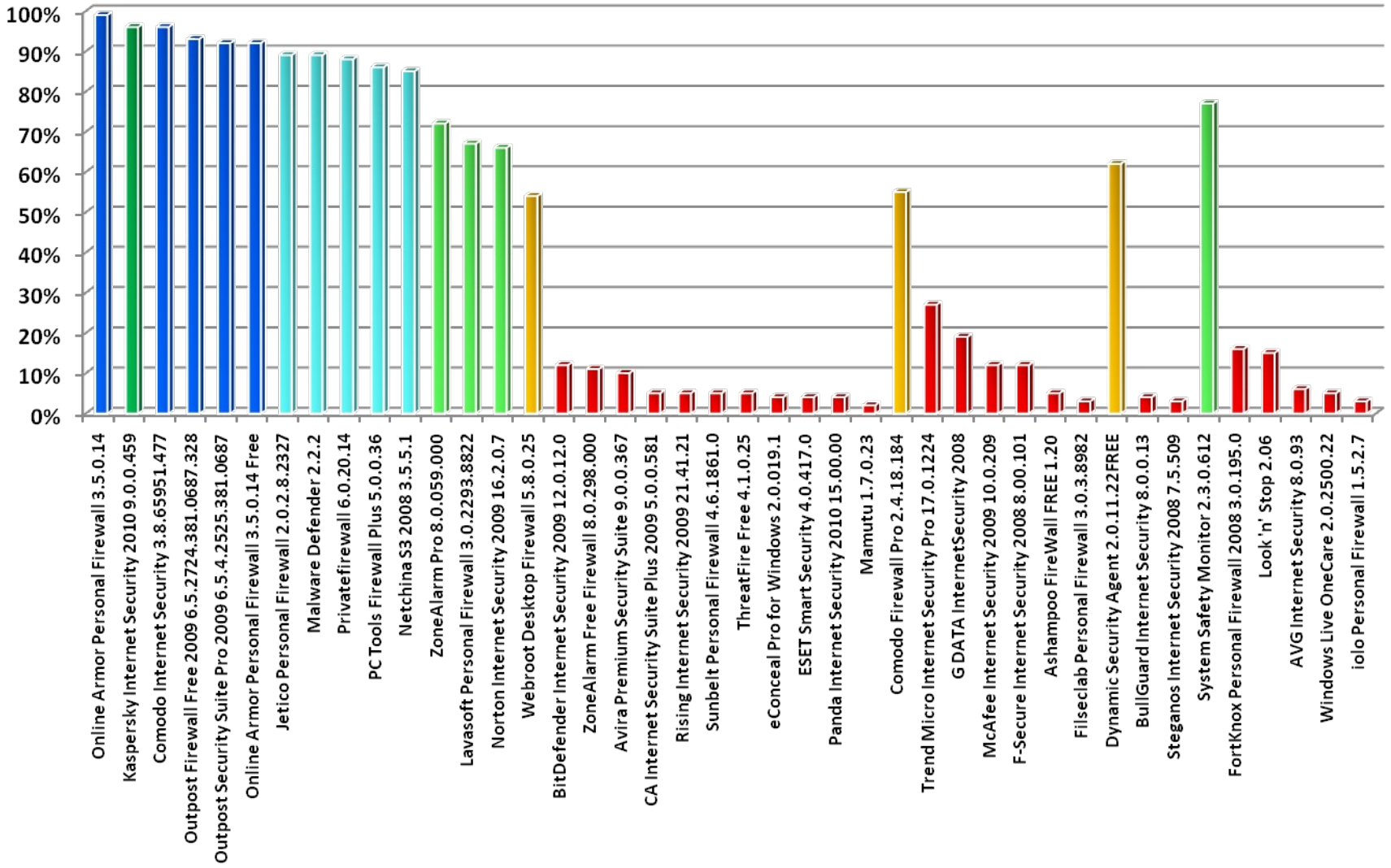
RAP tests (VB100, April'2009, August'2009)





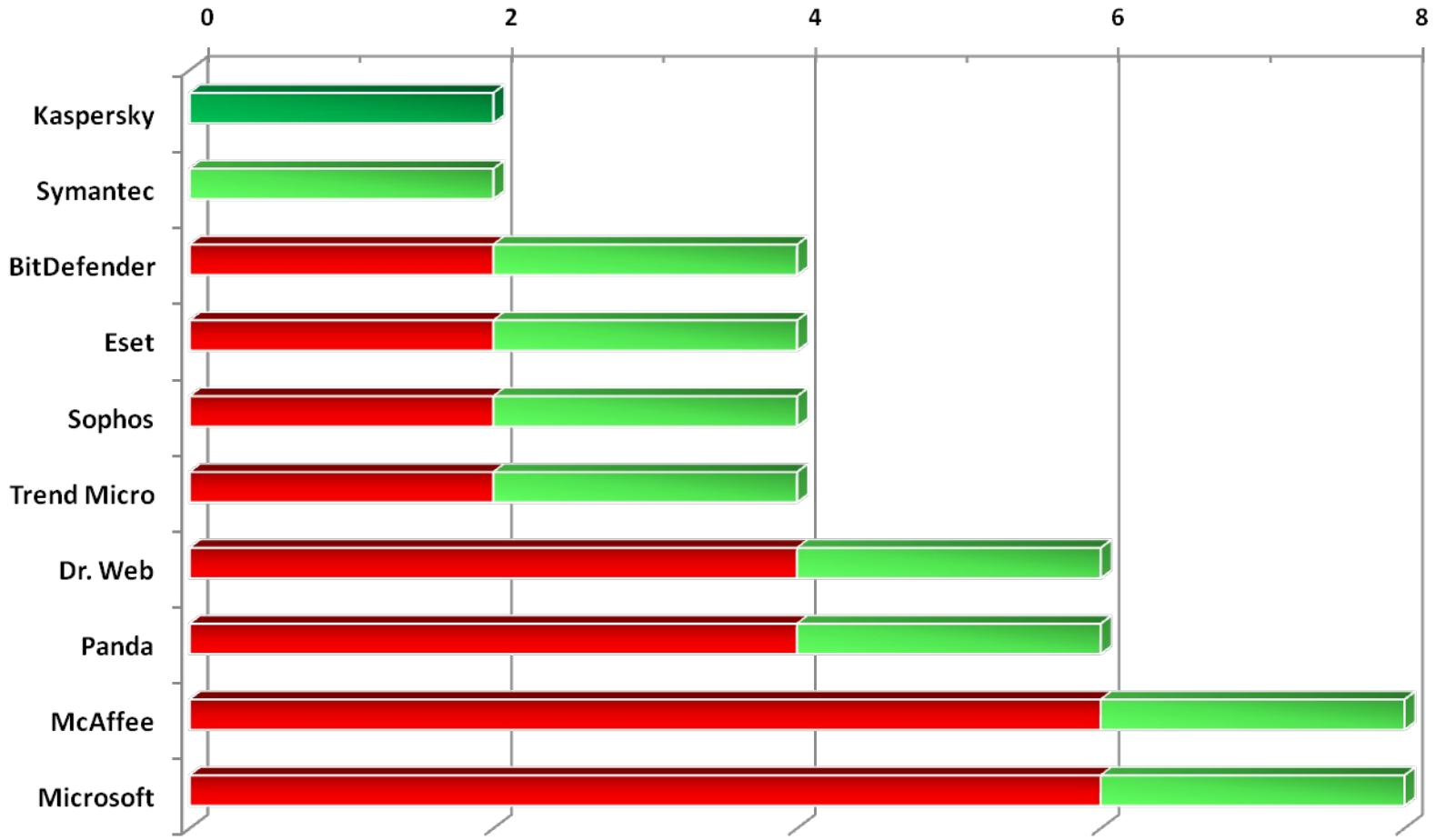
Источник: http://www.virusbtn.com

Matousec Proactive Security Challenge



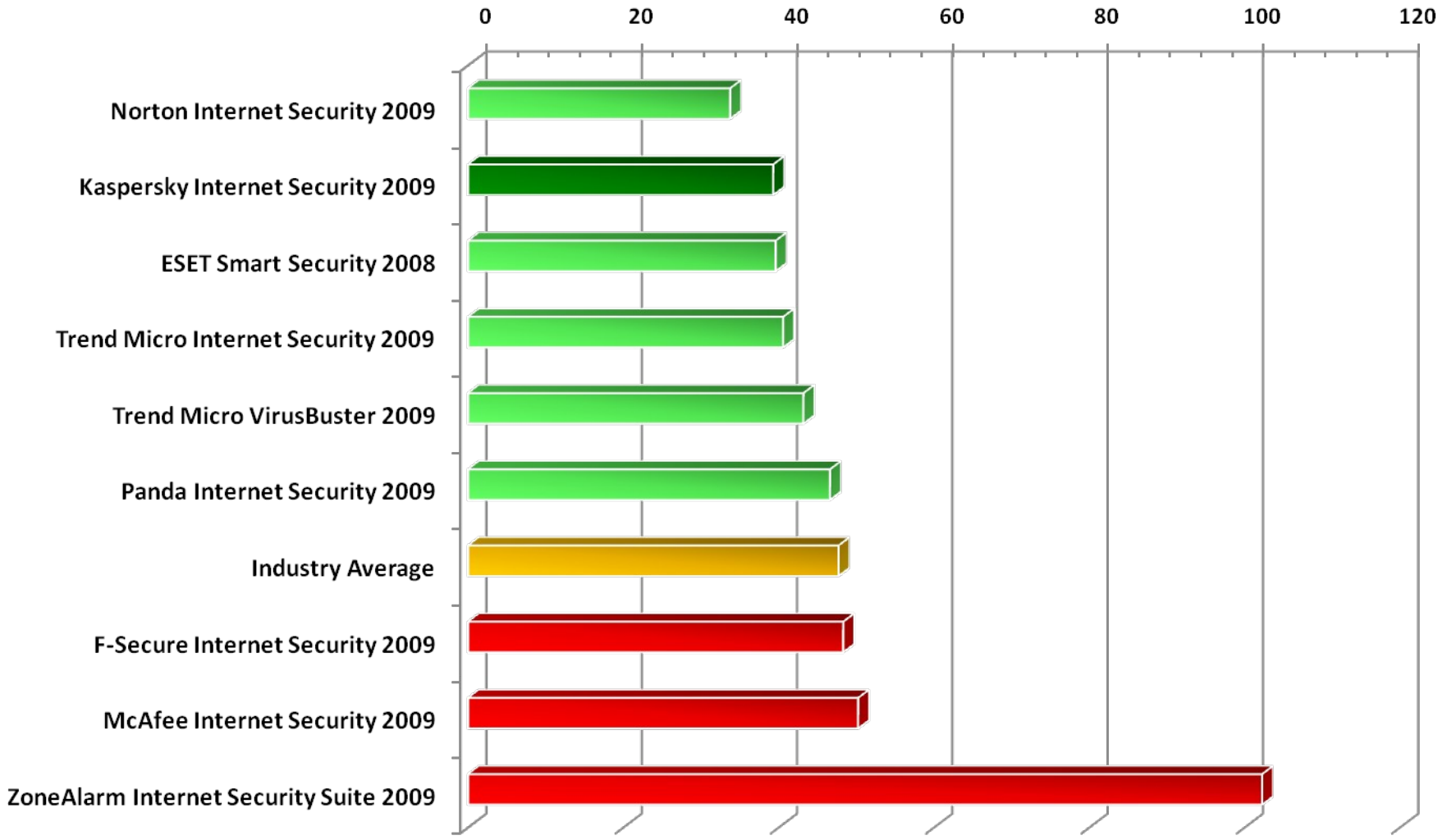
ик: http://www.matousec.com/projects/proactive-security-challenge/results.php

Время реакции на новые угрозы (час.)



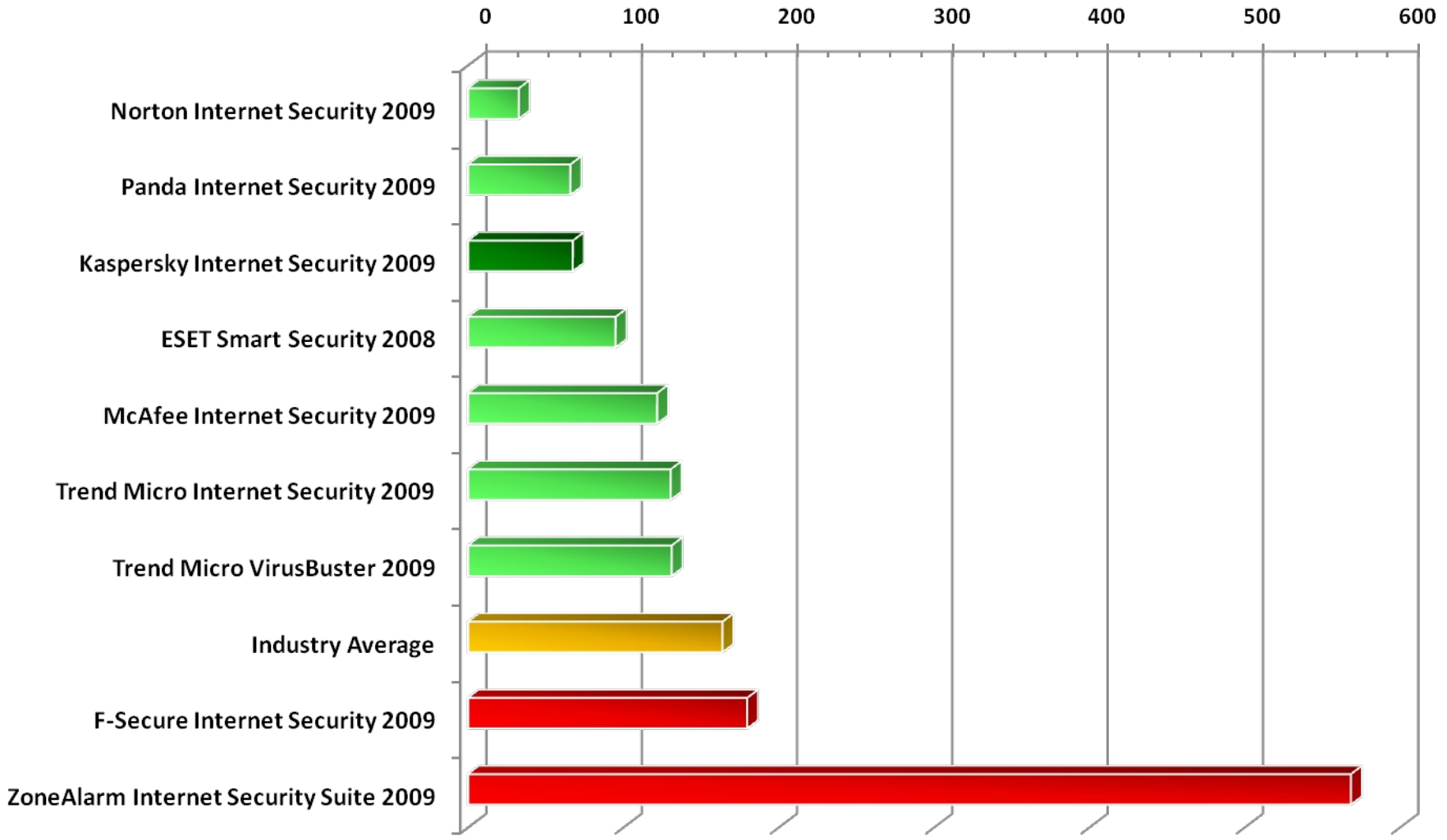
Источник: *AV-Test.org, сентябрь 2008*

Boot Time (sec)



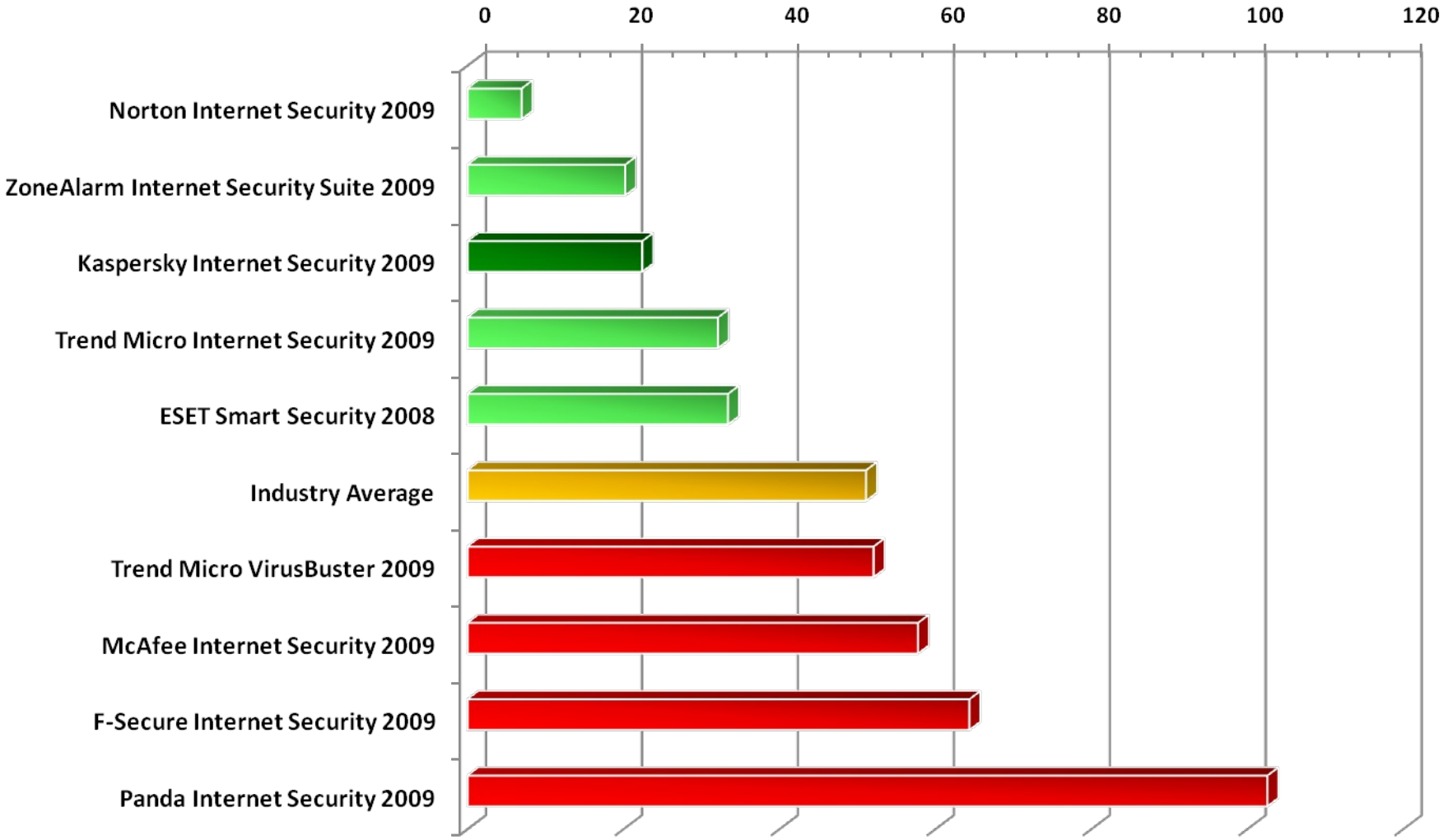
sMark Software, Performance Testing - 2009 Products, Benchmark Report, 16-Mar-09

Scan Speed (sec)



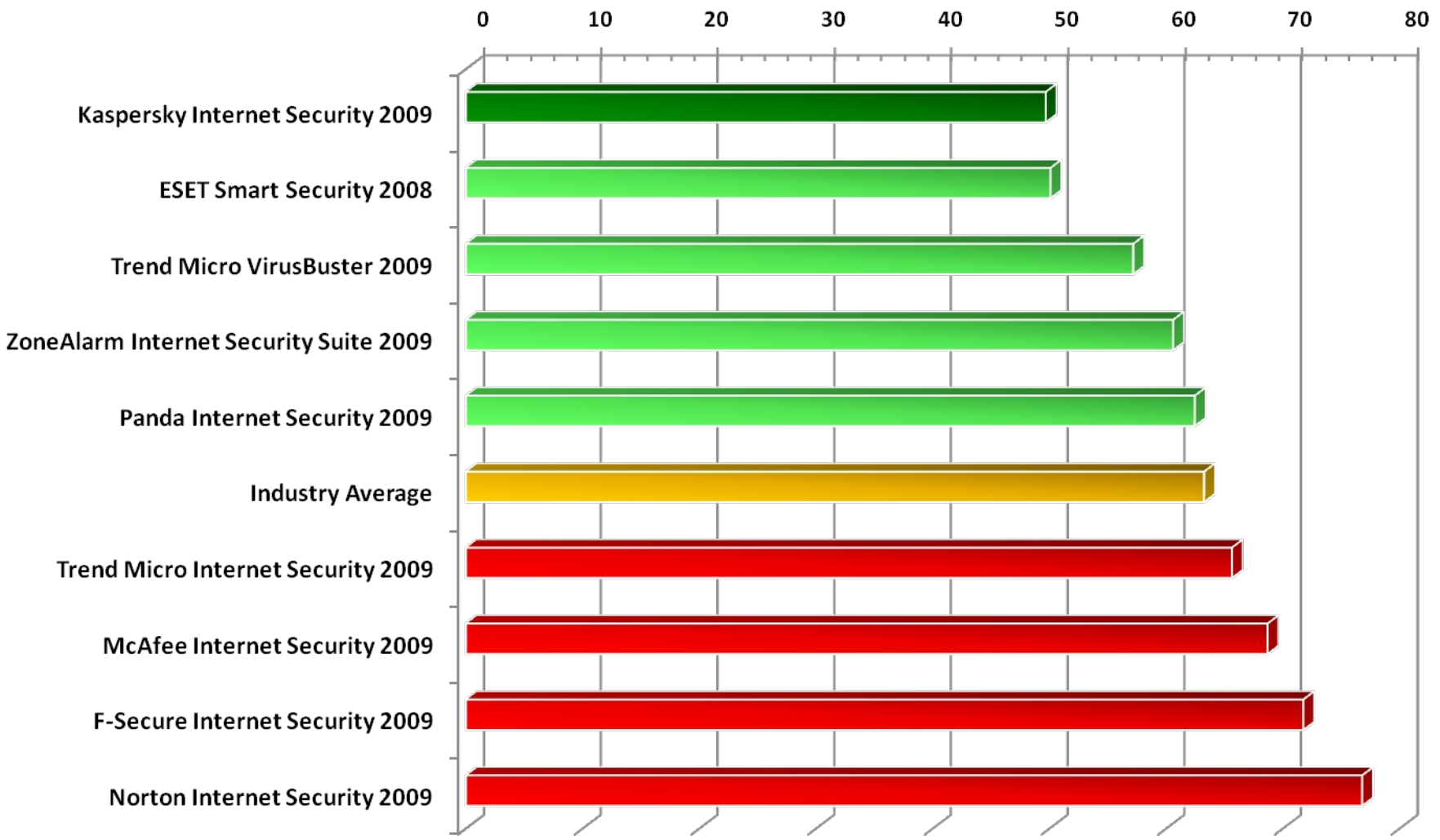
sMark Software, Performance Testing - 2009 Products, Benchmark Report, 16-Mar-09

Memory Utilization (MB)



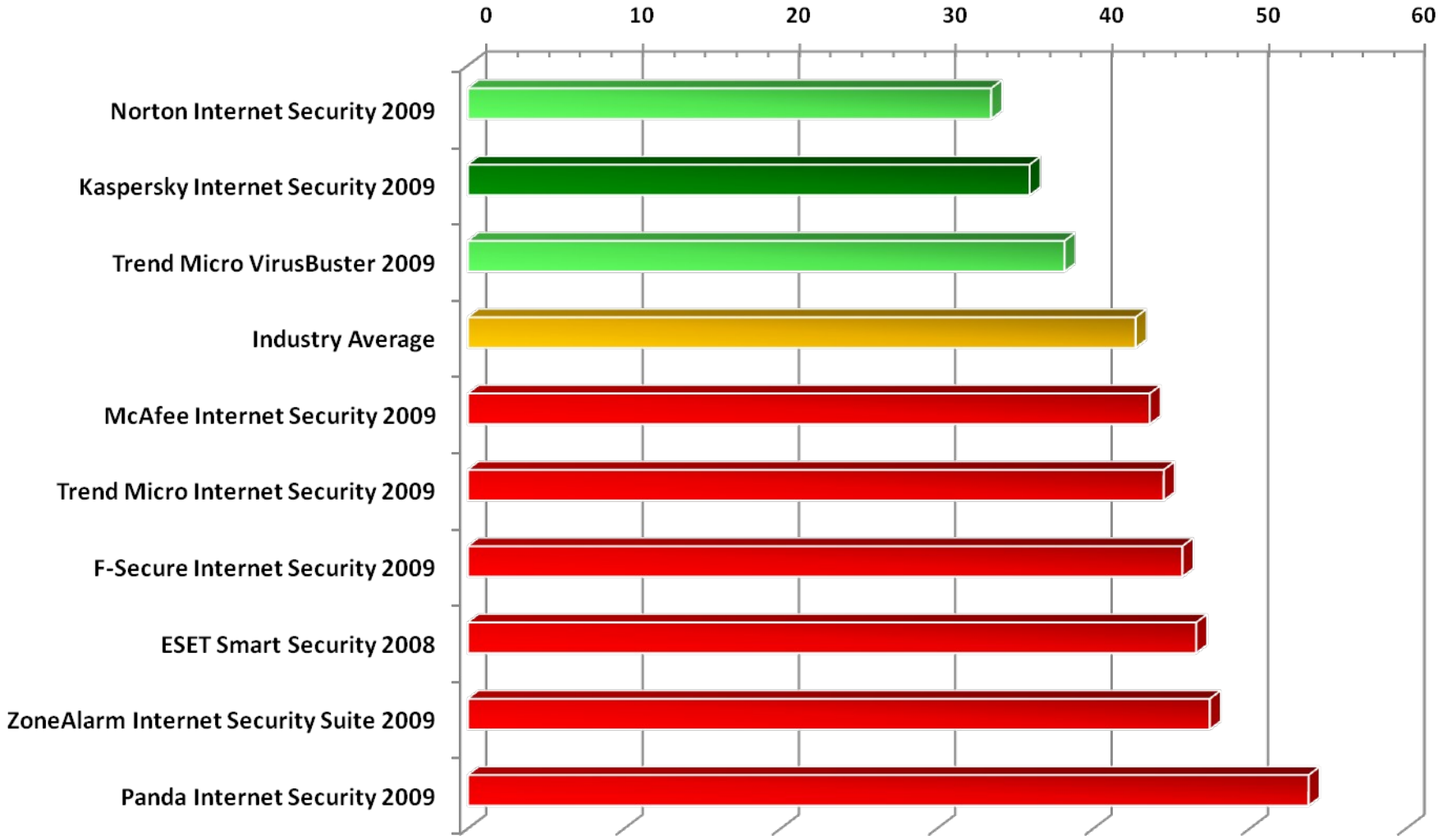
sMark Software, Performance Testing - 2009 Products, Benchmark Report, 16-Mar-09

File Copy, Move and Delete (sec)



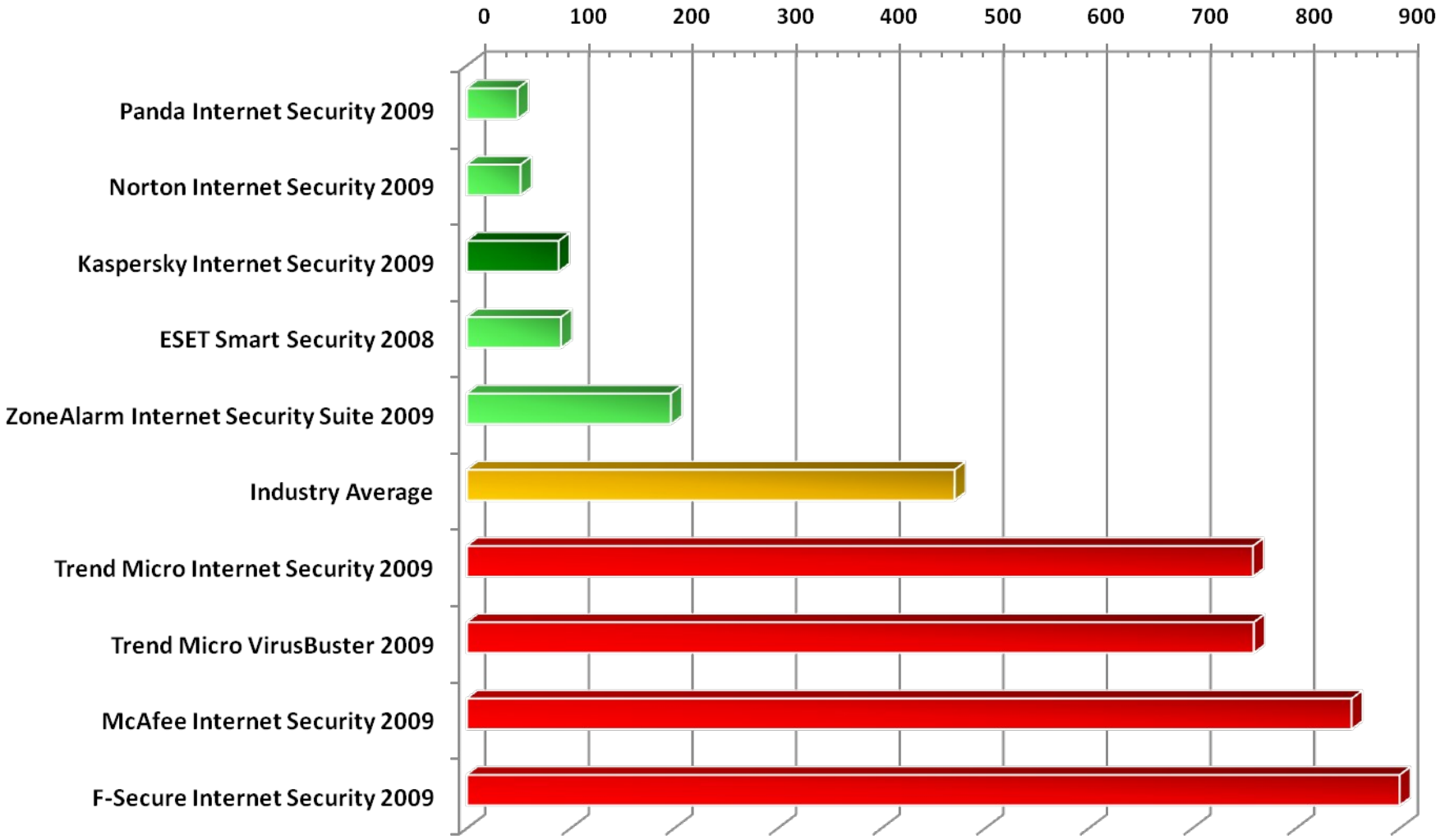
sMark Software, Performance Testing - 2009 Products, Benchmark Report, 16-Mar-09

File Compression and Decompression (sec)



sMark Software, Performance Testing - 2009 Products, Benchmark Report, 16-Mar-09

File Write, Open, Close (sec)



sMark Software, Performance Testing - 2009 Products, Benchmark Report, 16-Mar-09

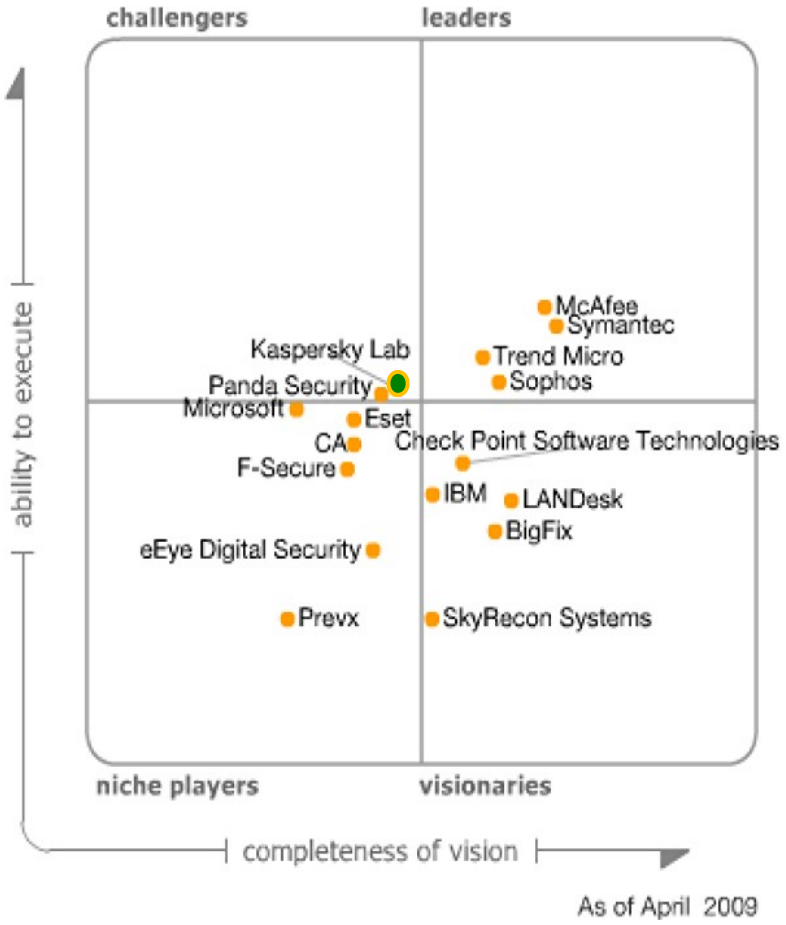
Часть 3

В двух словах о Kaspersky Lab

Лаборатория Касперского сегодня

- Крупнейшая в Европе антивирусная компания, входящая в пятёрку ведущих мировых производителей
  - Возраст компании – **12 лет**
  - Штат сотрудников – **1'500+** высококвалифицированных сотрудников в офисах, расположенных на всех материках (кроме Антарктиды)
  - **250+ млн.** пользователей по всему миру
  - **700+** партнеров первого уровня более чем в **100** странах мира
    - **10'000+** компаний-партнёров по всему миру
    - **3'000+** компаний-партнеров в России
  - Множество технологических партнёров, включая:
    - Microsoft (США), Juniper (США), Aladdin (Израиль), Alcatel-Lucent (Франция), BlueCoat (США), Deerfield (США), Alt-N (США), BorderWare (Канада), Checkpoint (США) и др.

Gartner Magic Quadrant for Endpoint Protection



Источник: *Gartner*

Первое знакомство… (РИФ’2008)

Источник: *Фото пресс-службы Президента России*

Стратегические ИТ-технологии… (ЛК'2009)

Источник: *Фото пресс-службы Президента России*

Обновленные приложения

Приложения **Release 2**:

- Антивирус Касперского для **Windows Workstations** (защита рабочих станций)
- Антивирус Касперского для **Window Servers** (защита серверов)
- Антивирус Касперского **Second Opinion Solution** (совместимый сканер по требованию)

- **Kaspersky Administration Kit 8.0** (средство управления)

Почему Release 2 ?

- Значительное обновление ключевых приложений для защиты рабочих станций и серверов –

  новое антивирусное ядро,
  новые технологии проактивной защиты
- Расширение поддерживаемых платформ –

  Windows 7,
  Windows Server 2008 R2
- Поддержка новой версии системы управления –

  Kaspersky Administration Kit 8.0

= Новый уровень безопасности и возможности управления антивирусной защитой.

Основные преимущества

Улучшенная защита

- Новое антивирусное ядро и проактивные технологии гарантируют эффективную защиту, в том числе от неизвестных угроз
- Контроль доступа к внешним устройствам с возможностью их блокировки
- Сетевой экран поддерживает протокол IPv6

Улучшенная производительность

- Новое ядро работает значительно быстрее и требует меньше ресурсов
- При установке требуется всего одна перезагрузка

Удобство настройки антивирусной защиты

- Улучшен интерфейс средства управления Kaspersky Administration Kit, реализованы гибкие настройки и сценарии использования

Поддержка новых платформ

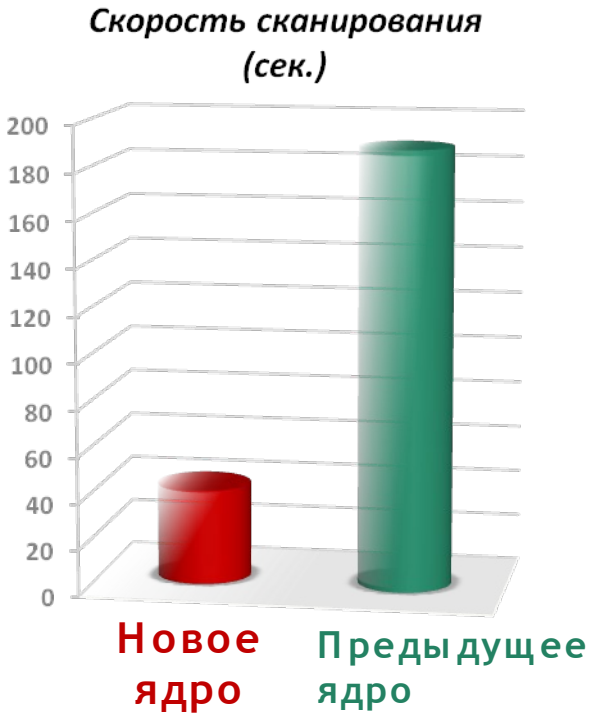
- Microsoft **Windows 7** и **Windows Server 2008 R2**

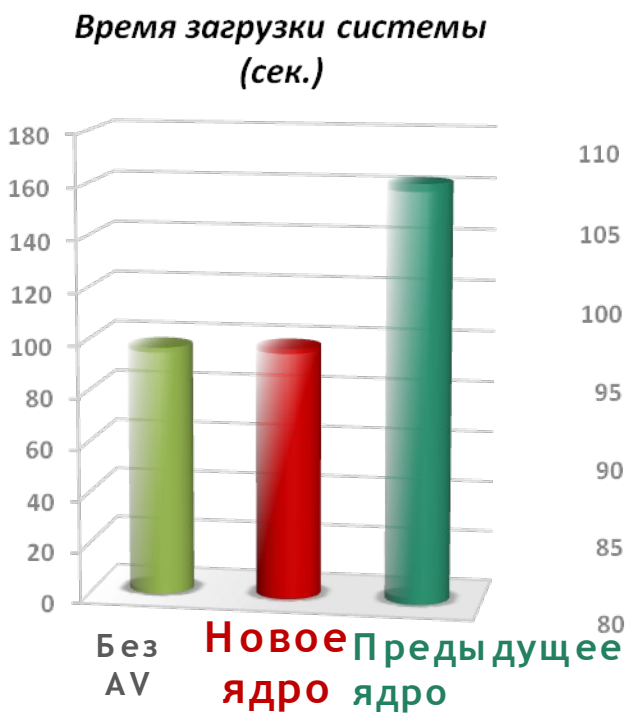
Стратегия развития технологий

лаборатория Касперского

- Фокус на **эффективность и качество** защиты, в том числе от неизвестных угроз
- **Универсальные технологии защиты**, сочетание в продукте различных подходов
- **Улучшение скорости и производительности**, минимальное влияние на работу других приложений

Оценка производительности нового ядра





Что нового? Сравнение версий

Антивирус Касперского для Windows Workstations	6.0	Release 2
Файловый антивирус	✓	✓ Улучшено
Почтовый антивирус	✓	✓ Улучшено
Веб-антивирус	✓	✓ Улучшено
Проактивная защита	✓	✓ Улучшено
Анти-шпион	✓	✓
Сетевой экран	✓	✓ Улучшено
Анти-спам	✓	✓
Контроль устройств	Дополнительные возможности	✓
Поддержка IPv6	Дополнительные возможности	✓
Эвристик с эмулятором	Повышение уровня защиты	✓
Анти-rootkit	Повышение уровня защиты	✓
Проверка ICQ/MSN	Повышение уровня защиты	✓
Поддержка Windows 7	Новая платформа	✓

Что нового? Сравнение версий

Антивирус Касперского для Windows Servers	6.0	Release 2
Файловый антивирус	✓	✓ *Улучшено*
Эвристик с эмулятором		✓
Анти-rootkit		✓
Windows Server 2008		✓
Windows Server 2008 R2		✓

Повышение уровня защиты

Поддержка платформ

Удобство работы администратора

Защита “из коробки”:

- Упрощенная установка и развертывание
- Понятные пошаговые инструкции для настройки и мониторинга антивирусной защиты

+ Расширение функциональности средства управления, сохраняя удобство использования.

Что нового? Сравнение версий

Kaspersky Administration Kit	6.0	8.0
Автоматическое добавление новых компьютеров по группам и установка антивирусного ПО	✓	✓
Иерархия серверов любой вложенности	✓	✓
Поиск по IP-подсетям/Active Directory/Windows Network	✓	✓
Создание логической сети на основе Active Directory	✓	✓
Управление из одной точки	✓	✓
Централизованное обновление из одной точки	✓	✓
Агенты обновлений	✓	✓
Проверка качества обновлений	✓	✓
Политика для мобильных пользователей	✓	✓
Поддержка Wake-on-LAN	✓	✓
Установка из единого дистрибутива (АК + База данных)		✓
Выбор типа установки в зависимости от размера сети		✓
Автоматическое создание инсталляционных пакетов		✓
Автоматическое создание политик		✓
Автоматическое создание задач		✓
Сбор информации об установленных в сети приложениях		✓
Информационные панели (Dashboards)		✓

Простота установки и развертывания

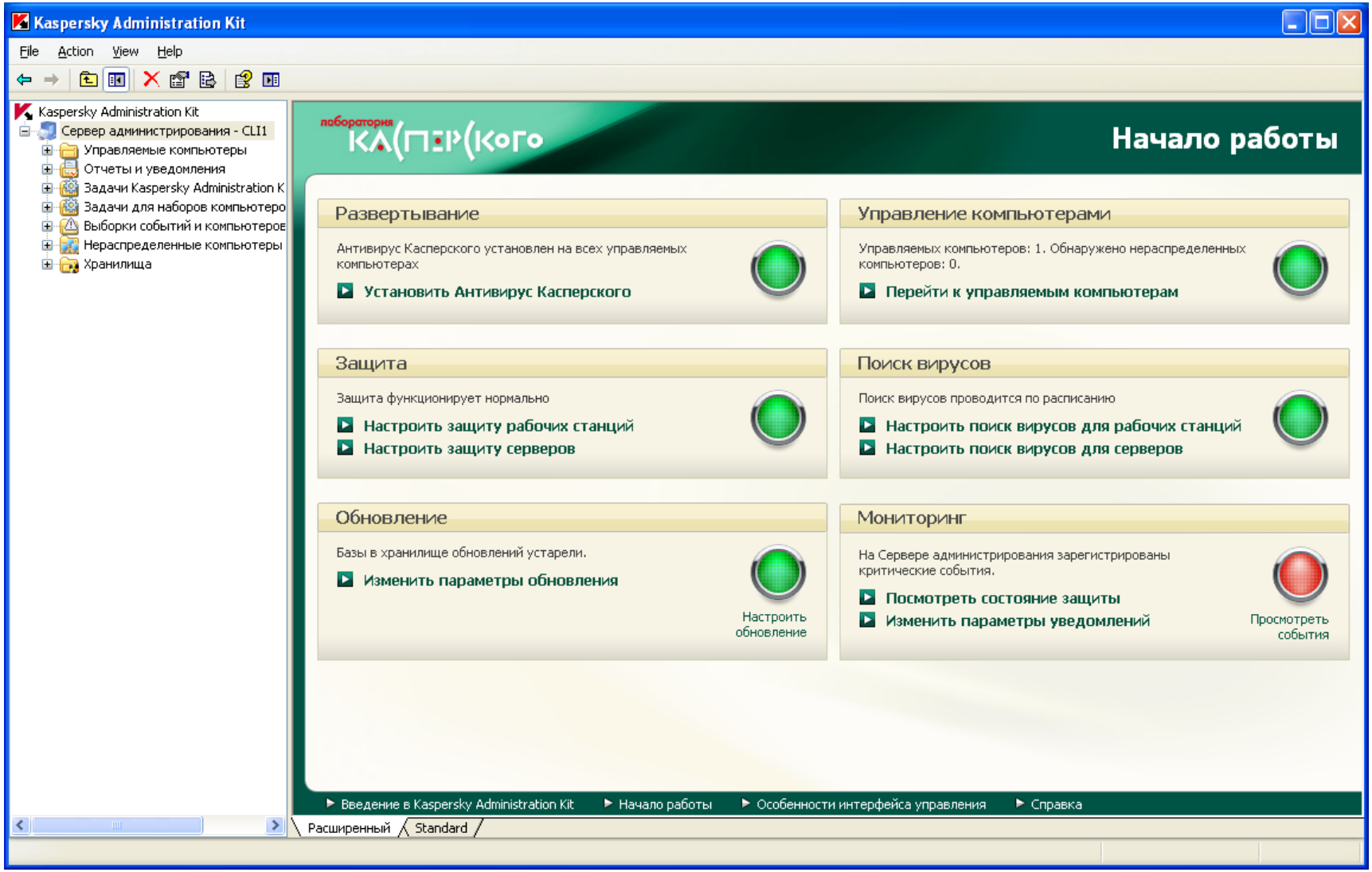
Контроль

Что нового? Сравнение версий

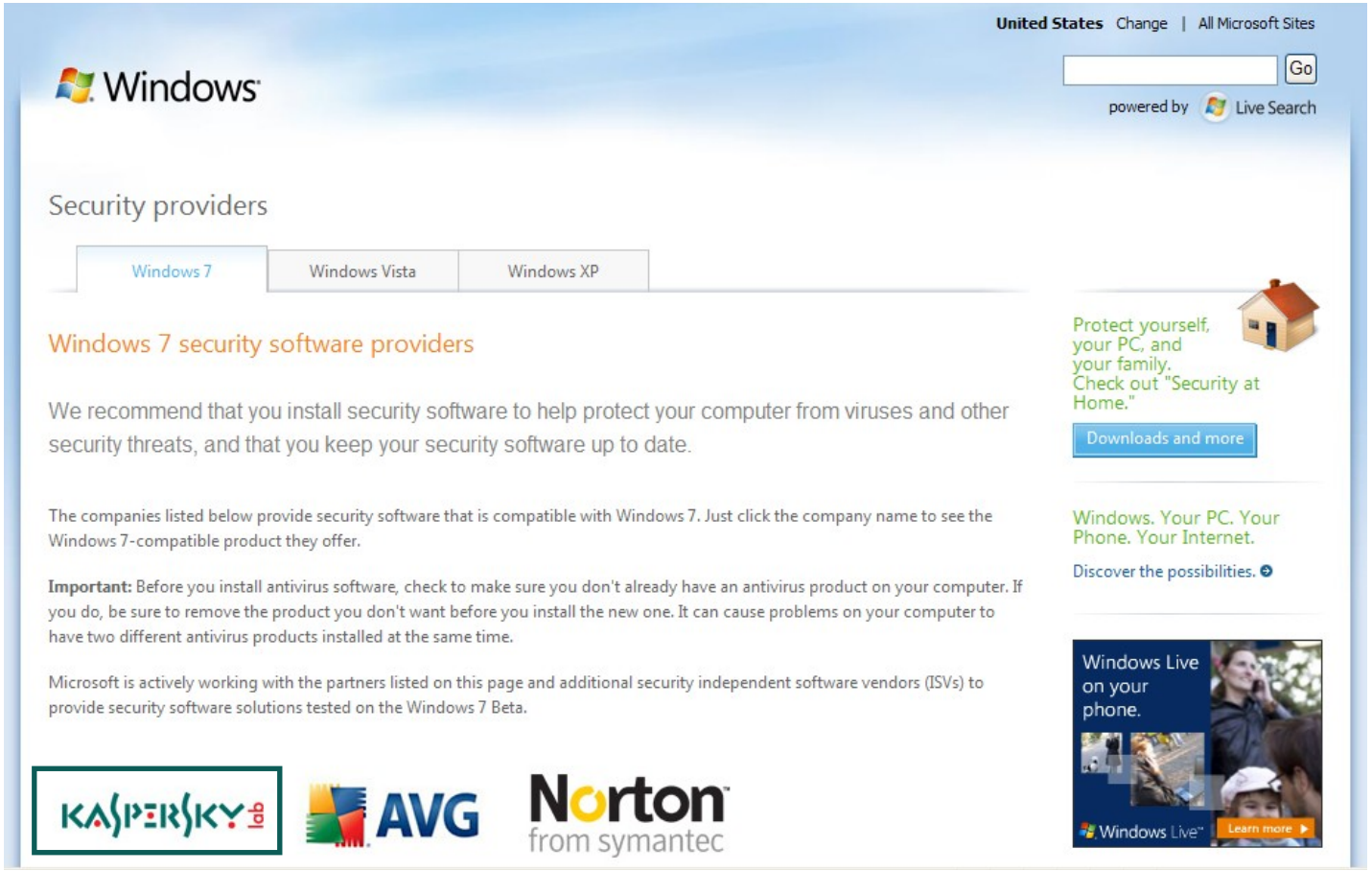
Kaspersky Administration Kit	6.0	8.0
Удаленная установка приложений с помощью RPC/LoginScript/NAgent	✓	✓
Аудит действий администраторов	✓	✓
Разграничение полномочий администраторов	✓	✓
Создание и рассылка отчетов по e-mail	✓	✓
Обнаружение вирусных атак	✓	✓
Экспорт отчетов в HTML/XML/PDF	Только HTML	✓
Утилита удаленной диагностики		✓
Удаленная установка с уже обновленными AV-базами		✓
Количество перезагрузок при удаленной установке	>1	1
Поддержка SNMP		✓
Расширение критериев выборки компьютеров		✓
Копирование объектов из локальных хранилищ на рабочее место администратора		✓
Автоматическое резервное копирование данных сервера администрирования		✓
Интерфейс для утилиты резервного копирования		✓
Поддержка Microsoft NAP		✓

Удобство работы

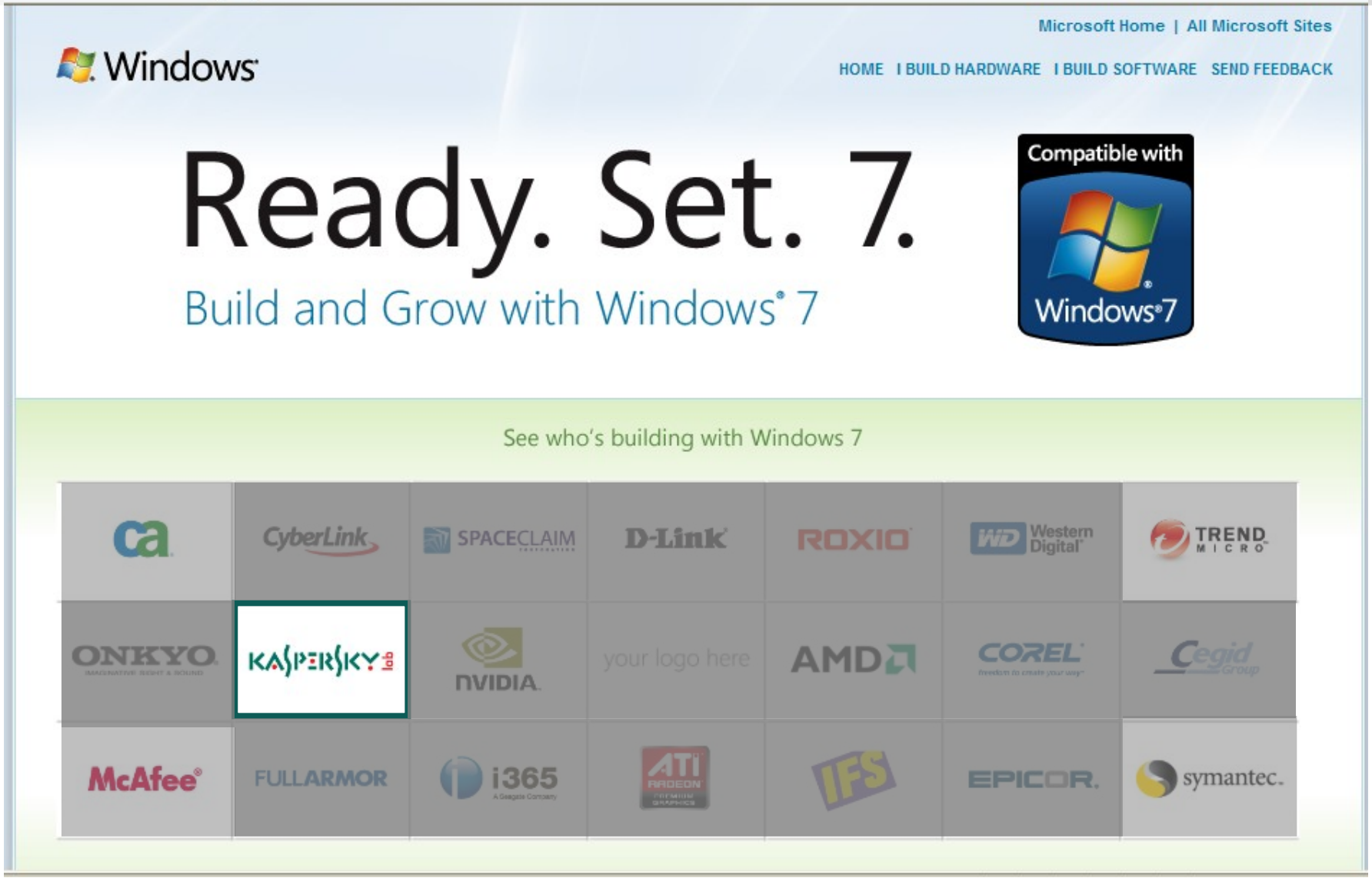
Начало работы



Мы готовы!


United States Change | All Microsoft Sites
Windows
Go
powered by Live Search
Security providers
Windows 7
Windows Vista
Windows XP
Windows 7 security software providers
We recommend that you install security software to help protect your computer from viruses and other security threats, and that you keep your security software up to date.
The companies listed below provide security software that is compatible with Windows 7. Just click the company name to see the Windows 7-compatible product they offer.
Important: Before you install antivirus software, check to make sure you don't already have an antivirus product on your computer. If you do, be sure to remove the product you don't want before you install the new one. It can cause problems on your computer to have two different antivirus products installed at the same time.
Microsoft is actively working with the partners listed on this page and additional security independent software vendors (ISVs) to provide security software solutions tested on the Windows 7 Beta.
KASPERSKY lab
AVG
Norton from symantec
Protect yourself, your PC, and your family. Check out "Security at Home."
Downloads and more
Windows. Your PC. Your Phone. Your Internet.
Discover the possibilities.
Windows Live on your phone.
Windows Live
Learn more

Мы готовы!


Microsoft Home | All Microsoft Sites
Windows
HOME | BUILD HARDWARE | BUILD SOFTWARE | SEND FEEDBACK
Ready. Set. 7.
Build and Grow with Windows® 7
Compatible with
Windows®7
See who's building with Windows 7
CyberLink
SPACECLAIM
D-Link
ROXIO
Western Digital
TREND MICRO
ONKYO
KASPERSKY lab
NVIDIA
your logo here
AMD
COREL
Cegid Group
McAfee
FULLARMOR
i365
ATI RADEON
IFS
EPICOR
symantec.

Благодарю за внимание!
Вопросы?

Владмир Тихонов

Руководитель службы консалтинга в Украине, Молдове,Республике Беларусь

KASPERSKY lab